



Alcatel-Lucent 5620

SERVICE AWARE MANAGER | RELEASE 9.0 R3
PARAMETER GUIDE

3HE 06496 AAAC TQZZA Edition 01

Alcatel-Lucent assumes no responsibility for the accuracy of the information presented, which is subject to change without notice.

Alcatel, Lucent, Alcatel-Lucent, the Alcatel-Lucent logo, and TiMetra are registered trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners.

Copyright 2011 Alcatel-Lucent.
All rights reserved.

Disclaimers

Alcatel-Lucent products are intended for commercial uses. Without the appropriate network design engineering, they must not be sold, licensed or otherwise distributed for use in any hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life-support machines, or weapons systems, in which the failure of products could lead directly to death, personal injury, or severe physical or environmental damage. The customer hereby agrees that the use, sale, license or other distribution of the products for any such application without the prior written consent of Alcatel-Lucent, shall be at the customer's sole risk. The customer hereby agrees to defend and hold Alcatel-Lucent harmless from any claims for loss, cost, damage, expense or liability that may arise out of or in connection with the use, sale, license or other distribution of the products in such applications.

This document may contain information regarding the use and installation of non-Alcatel-Lucent products. Please note that this information is provided as a courtesy to assist you. While Alcatel-Lucent tries to ensure that this information accurately reflects information provided by the supplier, please refer to the materials provided with any non-Alcatel-Lucent product and contact the supplier for confirmation. Alcatel-Lucent assumes no responsibility or liability for incorrect or incomplete information provided about non-Alcatel-Lucent products.

However, this does not constitute a representation or warranty. The warranties provided for Alcatel-Lucent products, if any, are set forth in contractual documentation entered into by Alcatel-Lucent and its customers.

This document was originally written in English. If there is any conflict or inconsistency between the English version and any other version of a document, the English version shall prevail.

Preface

The Preface provides general information about the 5620 Service Aware Manager documentation suite.



Note — You can use the Search function of Acrobat Reader (File→Search) to find a term in a PDF of this document. To refine your search, use appropriate search options (for example, search for whole words only or enable case-sensitive searching). You can also search for a term in multiple PDFs at once. For more information, see the Help for Acrobat Reader.

5620 SAM documentation suite

The 5620 SAM documentation suite describes the 5620 SAM and the associated network management of its supported devices. Contact your Alcatel-Lucent support representative for information about specific network or facility considerations.

Table 1 lists the documents in the 5620 SAM documentation suite.

Table 1 5620 SAM customer documentation suite

Guide	Description
5620 SAM core documentation	
<i>5620 SAM Planning Guide</i>	The <i>5620 SAM Planning Guide</i> provides information about 5620 SAM scalability and recommended hardware configurations.

(1 of 4)

Guide	Description
<i>5620 SAM 5650 CPAM Installation and Upgrade Guide</i>	<p>The <i>5620 SAM 5650 CPAM Installation and Upgrade Guide</i> provides OS considerations, configuration information, and procedures for the following:</p> <ul style="list-style-type: none"> installing, upgrading, and uninstalling 5620 SAM and 5650 CPAM software in standalone and redundant deployments 5620 SAM system migration to a different system conversion from a standalone to a redundant 5620 SAM system
<i>5620 SAM User Guide</i>	<p>The <i>5620 SAM User Guide</i> provides information about using the 5620 SAM to manage the service-aware IP/MPLS network, including GUI basics, commissioning, service configuration, and policy management.</p> <p>The <i>5620 SAM User Guide</i> uses a task-based format. Each chapter contains:</p> <ul style="list-style-type: none"> a workflow that describes the steps for configuring and using the functionality detailed procedures that list the configurable parameters on the associated forms <p>5620 SAM management information specific to LTE network elements is covered in the <i>5620 SAM LTE ePC User Guide</i> and <i>5620 SAM LTE RAN User Guide</i>.</p> <p>5620 SAM management information specific to 1830 PSS network elements is covered in the <i>5620 SAM Optical User Guide</i>.</p>
<i>5620 SAM Parameter Guide</i>	<p>The <i>5620 SAM Parameter Guide</i> provides:</p> <ul style="list-style-type: none"> parameter descriptions that include value ranges and default values parameter options and option descriptions parameter and option dependencies parameter mappings to the 5620 SAM-O XML equivalent property names <p>There are dynamic links between the procedures in the <i>5620 SAM User Guide</i> and the parameter descriptions in the <i>5620 SAM Parameter Guide</i>. See Procedure 2 for more information.</p> <p>Parameters specific to LTE network elements are covered in the <i>5620 SAM LTE Parameter Reference</i>.</p> <p>Parameters specific to 1830 PSS network elements are covered in the <i>5620 SAM Optical Parameter Reference</i>.</p>
<i>5620 SAM Statistics Management Guide</i>	<p>The <i>5620 SAM Statistics Management Guide</i> provides information about how to configure performance and accounting statistics collection and how to view counters using the 5620 SAM. Network examples are included.</p>
<i>5620 SAM Scripts and Templates Developer Guide</i>	<p>The <i>5620 SAM Scripts and Templates Developer Guide</i> provides information that allows you to develop, manage, and execute CLI-based or XML-based scripts or templates. The guide is intended for developers, skilled administrators, and operators who are expected to be familiar with the following:</p> <ul style="list-style-type: none"> CLI scripting, XML, and the Velocity engine basic scripting or programming 5620 SAM functions
<i>5620 SAM Troubleshooting Guide</i>	<p>The <i>5620 SAM Troubleshooting Guide</i> provides task-based procedures and user documentation to:</p> <ul style="list-style-type: none"> help resolve issues in the managed and management networks identify the root cause and plan corrective action for: <ul style="list-style-type: none"> alarm conditions on a network object or customer service problems on customer services with no associated alarms list problem scenarios, possible solutions, and tools to help check: <ul style="list-style-type: none"> network management LANs network management platforms and operating systems 5620 SAM client GUIs and client OSS applications 5620 SAM servers 5620 SAM databases

(2 of 4)

Guide	Description
<i>5620 SAM Maintenance Guide</i>	The <i>5620 SAM Maintenance Guide</i> provides procedures for: <ul style="list-style-type: none"> generating baseline information for 5620 SAM applications performing daily, weekly, monthly, and as-required maintenance activities for 5620 SAM-managed networks
<i>5620 SAM Integration Guide</i>	The <i>5620 SAM Integration Guide</i> provides procedures to allow the 5620 SAM to integrate with additional components.
<i>5620 SAM System Architecture Guide</i>	The <i>5620 SAM System Architecture Guide</i> is intended for technology officers and network planners to increase their knowledge of the 5620 SAM software structure and components. It describes the system structure, software components, and interfaces of the 5620 SAM. In addition, 5620 SAM fault tolerance, security, and network management capabilities are discussed from an architectural perspective.
<i>5620 SAM Supervision Module User Guide</i>	The <i>5620 SAM Supervision Module User Guide</i> provides information about how to configure and use the web-based 5620 SAM Supervision Module for fault management and at-a-glance network element monitoring.
<i>5620 SAM Network Element Compatibility Guide</i>	The <i>5620 SAM Network Element Compatibility Guide</i> provides release-specific information about the compatibility of managed device features in 5620 SAM releases.
<i>5620 SAM Release Description</i>	The <i>5620 SAM Release Description</i> provides information about the new features associated with a 5620 SAM software release.
<i>5620 SAM Glossary</i>	The <i>5620 SAM Glossary</i> defines terms and acronyms used in all of the 5620 SAM documentation, including 5620 SAM LTE documentation.
<i>5620 SAM XML OSS Interface Developer Guide</i>	The <i>5620 SAM XML OSS Interface Developer Guide</i> provides information that allows you to: <ul style="list-style-type: none"> use the 5620 SAM XML OSS interface to access network management information learn about the information model associated with the managed network develop OSS applications using the packaged methods, classes, data types, and objects necessary to manage 5620 SAM functions
5620 SAM LTE documentation	
<i>5620 SAM LTE ePC User Guide</i>	The <i>5620 SAM LTE ePC User Guide</i> describes how to discover, configure, and manage LTE ePC devices using the 5620 SAM. The guide is intended for LTE ePC network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire <i>5620 SAM LTE ePC User Guide</i> before you attempt to use the 5620 SAM in your LTE network.
<i>5620 SAM LTE RAN User Guide</i>	The <i>5620 SAM LTE RAN User Guide</i> describes how to discover, configure, and manage the Evolved NodeB, or eNodeB, using the 5620 SAM. The guide is intended for LTE RAN network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire <i>5620 SAM LTE RAN User Guide</i> before you attempt to use the 5620 SAM in your LTE network.
<i>5620 SAM LTE Parameter Reference</i>	The <i>5620 SAM LTE Parameter Reference</i> provides a list of all LTE ePC and LTE RAN parameters supported in the 5620 SAM.
<i>5620 SAM LTE Alarm Reference</i>	The <i>5620 SAM LTE Alarm Reference</i> provides a list of LTE ePC and LTE RAN alarms that can be reported in the 5620 SAM GUI.
<i>5620 SAM 3GPP OSS Interface Developer Guide</i>	The <i>5620 SAM 3GPP OSS Interface Developer Guide</i> describes the components and architecture of the 3GPP OSS interface to the 5620 SAM. It includes procedures and samples to assist OSS application developers to use the 3GPP interface to manage LTE devices.
<i>5620 SAM 3GPP OSS Interface Compliance Statements</i>	The <i>5620 SAM 3GPP OSS Interface Compliance Statements</i> document describes the compliance of the 5620 SAM 3GPP OSS interface with the 3GPP standard.
<i>5620 SAM LTE RAN Release Description</i>	The <i>5620 SAM LTE RAN Release Description</i> provides information about the LTE RAN features associated with the release.

(3 of 4)

Guide	Description
5620 SAM optical documentation	
<i>5620 SAM Optical User Guide</i>	The <i>5620 SAM Optical User Guide</i> describes how to discover, configure, and manage optical devices using the 5620 SAM. The guide is intended for optical network planners, administrators, and operators. Alcatel-Lucent recommends that you review the entire <i>5620 SAM Optical User Guide</i> before you attempt to use the 5620 SAM in your network.
<i>5620 SAM Optical Parameter Reference</i>	The <i>5620 SAM Optical Parameter Reference</i> provides a list of all optical device parameters supported in the 5620 SAM.
<i>5620 SAM Optical Alarm Reference</i>	The <i>5620 SAM Optical Alarm Reference</i> provides a list of optical device alarms that can be reported in the 5620 SAM GUI.

(4 of 4)

Procedure 1 To find the 5620 SAM user documentation

The user documentation is available from the following sources:

- the User_Documentation directory on the product DVD-ROM
- Help→5620 SAM User Documentation in the 5620 SAM client GUI main menu



Note — Users of Mozilla browsers may receive an error message when using the User Documentation Index page (index.html) to open the PDF files in the 5620 SAM documentation suite. The offline storage and default cache values used by the browsers are the cause of the error message.

Alcatel-Lucent recommends changing the offline storage (Mozilla Firefox) or cache (Mozilla 1.7) values to 100 Mbytes to eliminate the error message.

Procedure 2 To view parameter descriptions from the 5620 SAM User Guide

You can click on a parameter name in a *5620 SAM User Guide* procedure to open the matching parameter description in the *5620 SAM Parameter Guide*. Ensure the following conditions are true beforehand:

- the *5620 SAM Parameter Guide* and *5620 SAM User Guide* are located in the same directory
 - Adobe Reader Release 5.0 or later is installed
- 1 To view a parameter description when both the *5620 SAM User Guide* and the *5620 SAM Parameter Guide* are open in Adobe Acrobat, click on the parameter name in the *5620 SAM User Guide*.

The parameter description is displayed in the *5620 SAM Parameter Guide*.
 - 2 To view a parameter description when only the *5620 SAM User Guide* is open in Adobe Acrobat:
 - i Click on a parameter name in a procedure in the *5620 SAM User Guide*. The *5620 SAM User Guide* closes and the *5620 SAM Parameter Guide* opens to display the parameter description.
 - ii Double-click on the Previous View button in Adobe Acrobat (or press Alt + ←) to re-open the *5620 SAM User Guide*. The *5620 SAM User Guide* opens and displays the parameter from step i.

Prerequisites

Readers of the 5620 SAM documentation suite are assumed to be familiar with the following:

- 5620 SAM software structure and components
- 5620 SAM GUI operations and tools
- typical 5620 SAM management tasks and procedures
- device and network management concepts

Conventions

Table 2 lists the conventions that are used throughout the documentation.

Table 2 Documentation conventions

Convention	Description	Example
Key name	Press a keyboard key	Delete
Italics	Identifies a variable	<i>hostname</i>

(1 of 2)

Convention	Description	Example
Key+Key	Type the appropriate consecutive keystroke sequence	CTRL+G
Key-Key	Type the appropriate simultaneous keystroke sequence	CTRL-G
*	An asterisk is a wildcard character, which means “any character” in a search argument.	log_file*.txt
↵	Press the Return key	↵
—	An em dash indicates there is no information.	—
→	Indicates that a cascading submenu results from selecting a menu item	Policies→Alarm Policies

(2 of 2)

Procedures with options or substeps

When there are options in a procedure, they are identified by letters. When there are substeps in a procedure, they are identified by Roman numerals.

Example of options in a procedure

At step 1, you can choose option a or b. At step 2, you must do what the step indicates.

- 1 This step offers two options. You must choose one of the following.
 - a This is one option.
 - b This is another option.
- 2 You must perform this step.

Example of substeps in a procedure

At step 1, you must perform a series of substeps within a step. At step 2, you must do what the step indicates.

- 1 This step has a series of substeps that you must perform to complete the step. You must perform the following substeps.
 - i This is the first substep.
 - ii This is the second substep.
 - iii This is the third substep.
- 2 You must perform this step.

Measurement conventions

Measurements in this document are expressed in metric units and follow the *Système international d’unités* (SI) standard for abbreviation of metric units. If imperial measurements are included, they appear in brackets following the metric unit.

Table 3 lists the measurement symbols used in this document.

Table 3 Bits and bytes conventions

Measurement	Symbol
bit	b
byte	byte
kilobits per second	kb/s

Important information

The following conventions are used to indicate important information:



Warning — Warning indicates that the described activity or situation may, or will, cause equipment damage or serious performance problems.



Caution — Caution indicates that the described activity or situation may, or will, cause service interruption.



Note — Notes provide information that is, or may be, of special interest.

Contents

Preface	iii
5620 SAM documentation suite	iii
Procedure 1 To find the 5620 SAM user documentation.....	vi
Procedure 2 To view parameter descriptions from the 5620 SAM	
User Guide.....	vii
Prerequisites.....	vii
Conventions.....	vii
Procedures with options or substeps	viii
Measurement conventions	viii
Important information.....	ix

5620 SAM Parameter Guide overview

1 —	5620 SAM Parameter Guide overview	1-1
1.1	5620 SAM Parameter Guide overview	1-2
	5620 SAM Parameter Guide structure	1-2
	Searching for information.....	1-3
	Procedure 1-1 To view 5620 SAM Parameter Guide parameter	
	descriptions from the 5620 SAM User Guide	1-3
	5620 SAM-O OSS properties	1-4

Application menu parameters

2 —	Task Manager parameters	2-1
2.1	Task Manager parameters.....	2-2
	autoRefreshInterval.....	2-2
	failedTasksPurgeInterval.....	2-2
	maxNumRetainedTasks.....	2-2
	numTasksToPurgeWhenFull.....	2-2
	successfulTasksPurgeInterval.....	2-2
3 —	User Preferences parameters	3-1
3.1	User Preferences parameters.....	3-2
	Access Interface Encap Value (Dot1q only).....	3-2
	Apply User Span of Control.....	3-2
	Debug STM Mode.....	3-2
	Default Client Time Zone.....	3-3
	Default Polling Interval (seconds).....	3-3
	Enable Confirmation for Bulk Change Actions.....	3-3
	Maximum Data Retention Time (seconds).....	3-3
	Overlay Type.....	3-3
	Populate Entire Properties Form on Opening.....	3-3
	Show Alarm Flags.....	3-4
	Show Alarm Flags.....	3-4
	Show Correlated Alarms.....	3-4
	Show Toolbar.....	3-4
	Specify # of Items Per Page.....	3-4
	Suppress Containing Window Warning.....	3-4
	Suppress Template Generation Message.....	3-5
	Turn on Audible Alarms.....	3-5

Create menu parameters

4 —	VPLS parameters	4-1
4.1	VPLS parameters.....	4-2
	AAL5 Encapsulation.....	4-2
	Action.....	4-2
	Activation Timer (seconds).....	4-2
	Administrative State.....	4-3
	Administrative ISID.....	4-3
	Address ID.....	4-3
	Aggregate Rate Limit (Kbps).....	4-3
	Aggregation.....	4-3
	Aging Enabled.....	4-3
	ANCP String.....	4-3
	Application Profile.....	4-3

ARP Host Limit.....	4-3
ARP Reply Agent.....	4-4
ARP Timeout (seconds).....	4-4
ARP Trigger Packet.....	4-5
ATM OAM Alarm Cell Handling.....	4-5
Auto-Assign ID.....	4-5
Automatic Mesh SDP Binding Creation	4-5
Auto Select Tunnels.....	4-5
Backbone STP	4-5
BGP AD Administrative Status	4-5
Block On Mesh Failure	4-6
Boot Timer (seconds)	4-6
Bridge Forward Delay (seconds)	4-6
Bridge Hello Time (seconds).....	4-7
Bridge Max Age (seconds)	4-7
Bridge Max Hops	4-7
Broadcast Address Format	4-8
Calling Station ID	4-8
Circuit ID	4-8
CCM Messages	4-8
Clear Forced Switchover	4-8
Collect Accounting Statistics	4-8
Control Word.....	4-9
Creation MSAP Policy	4-9
Creation MSAP Policy Re-evaluation	4-9
Customer VID	4-9
Default Gateway IP Address	4-9
Default Gateway MAC Address	4-9
Default Mesh VC ID.....	4-10
Default Service Priority	4-10
Description	4-10
Destination Node ID.....	4-10
DHCP Trigger Packet.....	4-10
Direction.....	4-10
Disable Fix Window	4-10
Disable Revert Time (Infinite).....	4-10
Discard Unknown Destinations	4-10
Discard Unknown Source	4-11
Displayed Name	4-11
Dynamic Topology Discovery	4-11
Edge Capability Detection	4-11
Edge Port	4-11
Egress Filter ID.....	4-12
Egress Label	4-12
Egress Mark QinQ Top Bits Only	4-12
Egress Policy ID	4-12
Egress Scheduler Name.....	4-12
Enable.....	4-12
Enable BGP AD.....	4-12
Enable BGP VPLS	4-12
Enable DHCP Relay.....	4-13
Enable IP Interface Binding.....	4-13

Enable Lease Populate	4-13
Enable Multi-homing to.....	4-13
EndPoint ID.....	4-13
Endpoint Type	4-14
Failed Threshold.....	4-14
Fast Leave	4-14
Force L2PT on Managed L2 Access Interface	4-14
Force Switchover	4-15
Force VLAN VC Forwarding	4-15
Formatted VSI ID Prefix	4-15
Fragment Interleave	4-15
FRF-12 End-To-End Fragment Threshold.....	4-15
FRF-12 Mode	4-15
General Query Interval (seconds).....	4-15
Group Address	4-16
High Watermark (%).....	4-16
High Watermark (%).....	4-16
High Watermark (%).....	4-16
Hold Multiplier.....	4-16
ID	4-17
ID	4-17
I/F MAC Address	4-17
IGMP Version	4-17
Ignore Standby Signalling	4-17
Import Policy.....	4-18
Ingress Filter ID.....	4-18
Ingress Label	4-18
Ingress Match Q in Q Dot1P	4-18
Ingress Policy ID	4-18
Ingress Scheduler Name	4-18
Inherit Value	4-18
Inner Encapsulation Value	4-18
Inner Encapsulation Value	4-18
Instance Index	4-18
Interface ID	4-18
IP Address	4-19
IP Address	4-19
Keep Alive (seconds).....	4-19
Last Member Query Interval (tenths of seconds).....	4-19
Learning Enabled	4-19
Limit Mac Move	4-19
Limit Mac Move Level.....	4-20
Link Type	4-20
Local Address	4-20
Local Age Time (seconds)	4-20
Low-priority Defect	4-20
Low Watermark (%)	4-20
Low Watermark (%)	4-21
Low Watermark (%)	4-21
MAC Address	4-21
MAC Flush on fail.....	4-21
MAC Monitoring.....	4-21

MAC Notification Count	4-22
MAC Notification Interval	4-22
MAC Pinning	4-22
MAC Subnet Length	4-22
Mandatory Bandwidth (kbps)	4-22
Max Number of Groups	4-23
Maximum Number of Groups	4-23
Maximum Number of Sources per Group	4-24
Maximum Response Interval (seconds)	4-24
Max VE ID	4-24
Max VLAN ID	4-24
Max. VLAN Tag	4-24
Maximum BPDUs (PDUs/Hello Interval)	4-24
Maximum Entries	4-25
Maximum FIB Entries	4-25
MC Ring Node	4-25
Member Group Name	4-25
Min VLAN ID	4-25
Min. VLAN Tag	4-25
Minimum Authentication Interval (minutes)	4-25
MIP	4-26
MIP MAC Address	4-26
MLD version	4-26
Monitor Access Interface Operational State	4-26
Monitored Group Name	4-26
Move Frequency	4-26
MRP Admin Status	4-26
MRP Attribute-Table-High-Watermark	4-27
MRP Attribute-Table-Low-Watermark	4-27
MRP Flood Time (seconds)	4-27
MRP Join Time (tenths of a second)	4-27
MRP Leave All Time (tenths of a second)	4-27
MRP Leave Time (tenths of a second)	4-27
MRP Max Attributes	4-28
MRP Periodic Enabled	4-28
MRP Periodic Time (tenths of a second)	4-28
MTU	4-28
Multi-homing ID	4-28
Multi-homing Site Name	4-28
Mrouter attached	4-29
Name	4-29
No Egress Aggregate Rate Limit	4-29
Number Of Retries	4-29
OAM Administrative State	4-29
Outer Encapsulation Value	4-29
Outer Encapsulation Value	4-29
Path Cost	4-29
Per Service Hashing for LAG Enabled	4-30
Port	4-30
Port Number	4-30
PPPoE Circuit ID	4-30
PPPoE Trigger Packet	4-30

Prefix Length.....	4-30
Primary Ports Cumulative Factor	4-30
Priority.....	4-31
Priority.....	4-31
Priority.....	4-31
Priority Dscp	4-31
Priority Level for CCM Messages	4-31
Priority Precedence.....	4-31
Priority Type	4-31
Propagate MAC Flush	4-32
Protected Mac Address	4-32
Query Interval (seconds)	4-32
Query source address.....	4-32
Region Name	4-32
Region Revision.....	4-33
Remote Age Time (seconds)	4-33
Remote ID	4-33
Report source address.....	4-33
Residential	4-33
Restrict Protected Source	4-34
Restrict Protected Source Action	4-34
Restrict Unprotected Destination.....	4-34
Retry Timeout	4-34
Return Tunnel Auto-Selection Transport Preference	4-35
Return Tunnel Transport	4-35
Revert Time (seconds).....	4-35
Root Guard	4-35
Robust Count.....	4-35
Route Distinguisher	4-36
Routing Policy Name	4-36
SAP Sub Type.....	4-36
SAP Type.....	4-36
Scheduling Class	4-36
Secondary Ports Cumulative Factor	4-36
Send Flush All But Mine	4-37
Send Flush All From Me.....	4-37
Send Queries	4-37
Service ID.....	4-37
Service Name	4-37
Service Tier	4-37
Service Site Pointer	4-38
Site Activation Timer	4-38
Site ID	4-38
Size (entries).....	4-38
Snooping	4-38
Source Address	4-38
Source MAC Address	4-39
Split Horizon Group	4-39
STP Mode	4-39
Subscriber ID	4-39
Suppress Standby Signalling	4-40
SVC Mgr Service ID	4-40

Table size (entries)	4-40
Tunnel Auto-Selection Transport Preference	4-40
Tunnel Fault Notification	4-40
Tunnel Transport	4-40
Unconstrained Bandwidth (kbps)	4-40
Use Bandwidth-Reserved Paths	4-40
Use Component Package Policy	4-41
Use Node Level Boot Timer	4-41
Use Node Level Site Activation Timer	4-41
Use query source address	4-41
Use SAP Backbone MAC Address	4-42
Use Shared Queue	4-42
VC ID	4-42
VC Type	4-42
VE ID	4-42
VE Name	4-43
VLAN VC Tag	4-43
VPLS ID	4-43
VPLS Mode	4-43
VPLS Tag	4-43

5 — VLL parameters 5-1

5.1	VLL parameters	5-2
	AAL5 Encapsulation	5-2
	AAL5 Frame Aware	5-2
	Active Hold Delay (100s of milliseconds)	5-2
	Admin Concat Limit	5-2
	Administrative State	5-3
	Administrative State	5-3
	Aggregate Rate Limit (Kbps)	5-3
	Aggregation	5-3
	ANCP String	5-3
	Application Profile	5-3
	ATM Connection Type	5-3
	ATM OAM Alarm Cell Handling	5-4
	ATM OAM Terminate	5-4
	Auto-Assign ID	5-4
	Auto-Generate ID	5-4
	Automatic SDP Binding/PBB Tunnel Creation	5-4
	Auto Select Return Transport Tunnel	5-5
	Auto Select Transport Tunnel	5-5
	CCM Messages Enabled	5-5
	CE IP Address	5-5
	Clock Source	5-5
	CLP Change	5-5
	Collect Accounting Statistics	5-6
	Control Word	5-6
	Customer VID	5-6
	Default VC ID	5-6
	Description	5-6
	Destination MAC Address	5-6

Destination Node ID	5-6
Direction	5-6
Disable Fix Window	5-7
EC ID Rx	5-7
EC ID Tx	5-7
Egress Filter ID	5-7
Egress Label	5-7
Egress Policy ID	5-7
Egress Scheduler Name	5-7
Enable AIS	5-7
Enable CE IP Address Discovery	5-7
Enable IPv6	5-8
Enable PW Standby Signaling Master	5-8
Enable PW Standby Signaling Slave	5-9
Encapsulation Value	5-9
Encapsulation Value	5-10
Encapsulation Value	5-10
Fragment Interleave	5-10
FRF-12 End-To-End Fragment Threshold	5-10
FRF-12 Mode	5-10
ID	5-10
Ingress Filter ID	5-10
Ingress Label	5-11
Ingress Match QinQ Dot1P	5-11
Ingress Policy ID	5-11
Ingress Scheduler Name	5-11
Inherit Service ID Value	5-11
Inner Encapsulation Value	5-11
Inner Encapsulation Value (VCI)	5-11
Inner Encapsulation Value (VCI)	5-11
Inner Encapsulation Value	5-11
Inter-Chassis Backup	5-11
Interworking Type	5-12
ISID	5-12
Jitter Buffer (ms)	5-12
Jitter Buffer Depth	5-13
LLF Enabled	5-13
Local ECID	5-13
Low-priority Defect	5-13
MAC Address	5-13
Mac Address	5-13
MAC Refresh Interval	5-14
Max Concat Delay	5-14
MC Ring Node	5-14
Monitor Access Interface Operational State	5-14
MTU	5-14
Name	5-14
Name	5-14
Name	5-15
Name	5-15
No Egress Aggregate Rate Limit	5-15
No Revert	5-15

Outer Encapsulation Value.....	5-15
Outer Encapsulation Value.....	5-16
Outer Encapsulation Value (VPI)	5-16
Outer Encapsulation Value (VPI)	5-16
Payload Size (octets)	5-16
Peer CE IP Address	5-17
Per Service Hashing for LAG Enabled	5-17
Port.....	5-17
Precedence.....	5-17
Priority Level for CCM Messages	5-17
PW Label.....	5-17
Remote ECID	5-17
Remote MAC Address	5-18
Report Alarm.....	5-18
Return Tunnel Auto-Selection Transport Preference	5-18
Return Tunnel Transport	5-18
Revert Time (second).....	5-18
RTP Header.....	5-19
SAP Type.....	5-19
Scheduling Class	5-19
SDP Admin Bandwidth	5-19
Service Class	5-21
Service ID	5-21
Service Name	5-21
Service Priority	5-22
Service Tier	5-22
Signalling VC Type Override	5-22
Site ID	5-22
Specify VLAN Path.....	5-22
Stack Capability Signaling.....	5-22
Subscriber Identification	5-23
SVC Mgr Service ID	5-23
Transport Type	5-23
Tunnel Auto-Selection Transport Preference	5-23
Tunnel Fault Notification	5-23
Tunnel Transport	5-23
Use Bandwidth-Reserved Paths	5-23
Use Broadcast MAC Address	5-23
Use Shared Queue	5-23
VC Type	5-23
VLAN ID	5-24
VLAN VC Tag	5-24
VLL Site Type	5-24

6 —	VP RN parameters	6-1
6.1	VP RN parameters.....	6-2
	AAL5 Encapsulation	6-2
	Action	6-2
	Administrative State	6-2
	Administration Status.....	6-2
	Aggregate Rate Limit (kbps).....	6-2

Aggregation	6-2
Allow Directed Broadcasts	6-2
Allow Send Force Renews	6-3
ANCP String	6-3
Anti-Spoof MAC Address	6-3
Application Profile	6-3
Application Profile String	6-3
ARP Host Limit	6-3
ATM OAM Alarm Cell Handling	6-3
Auto-Assign ID	6-3
Automatic SDP Binding Creation	6-3
Autonomous Address Configuration	6-4
Autonomous System	6-4
Auto Select Return Transport Tunnel	6-4
Auto Select Transport Tunnel	6-4
BFD Enabled	6-4
BGP Enabled	6-4
Broadcast Address Format	6-4
Calling Station ID	6-5
Carrier Carrier VPN	6-5
Collect Accounting Statistics	6-5
Context Value	6-5
Client Applications	6-5
Current Hop Limit	6-5
Days	6-5
Days	6-6
Days	6-6
Days	6-6
Days	6-6
Days	6-6
Days	6-6
Days	6-7
Days	6-7
Default Subscriber Identification String	6-7
Description	6-7
Destination	6-7
Direction	6-7
Disable Fix Window	6-7
Display Name	6-7
Displayed Name	6-7
dot1p	6-8
DSCP	6-8
Dynamic Topology Discovery	6-8
Echo Interval	6-9
Egress Filter ID	6-9
Egress Mark QinQ Top Bits Only	6-9
Egress Policy ID	6-9
Egress Scheduler Name	6-9
Enable DHCP Relay	6-9
Enable GRT Lookup	6-9
Enable Local Proxy	6-9
Enable Local Proxy ARP	6-9
End Address	6-9

Enforce Maximum Number Of Multicast Routes	6-10
Enforce Maximum Number Of Routes	6-10
Export Target AS Value.....	6-10
Export Target AS Value.....	6-10
Export Target AS Value (4Byte)	6-10
Export Target AS Value (4Byte)	6-11
Export Target Community Value	6-11
Export Target Community Value	6-11
Export Target Extended Community Value.....	6-11
Export Target Extended Community Value.....	6-11
Export Target Format.....	6-12
Export Target Format.....	6-12
Export Target IP Address	6-12
Export Target IP Address	6-13
Export Unicast	6-13
FIB Priority	6-13
Forwarding Class	6-13
Fragment Interleave	6-14
Free Addresses Minimum Threshold	6-14
FRF-12 End-To-End Fragment Threshold.....	6-14
FRF-12 Mode	6-14
GSMP Administrative State	6-14
Hold Multiplier.....	6-14
Hours	6-14
Hold-Off Time (seconds)	6-15
Hours	6-15
Hours	6-15
Hours	6-15
Hours	6-15
Hours	6-15
Hours	6-16
Hours	6-16
ID	6-16
IGMP Enabled	6-16
Import Target AS Value.....	6-16
Import Target AS Value.....	6-16
Import Target AS Value (4Byte)	6-16
Import Target AS Value (4Byte)	6-17
Import Target Community Value.....	6-17
Import Target Community Value.....	6-17
Import Target Extended Community Value	6-17
Import Target Extended Community Value	6-17
Import Target Format	6-18
Import Target Format	6-18
Import Target IP Address.....	6-19
Import Target IP Address.....	6-19
Import Unicast	6-19
Ingress Filter ID.....	6-19
Ingress Match QinQ Dot1P.....	6-19
Ingress Policy ID	6-19
Ingress Scheduler Name	6-19
Inner Encapsulation Value	6-19

Inner Encapsulation Value	6-19
Interface ID	6-20
Intermediate Destination ID	6-20
IP Address	6-20
IP Address 1	6-20
IP Address 2	6-20
IP Address 3	6-20
IP Address 4	6-20
IP Address Overlap Avoidance Enabled	6-21
IPv6 Address.....	6-21
IPv6 Delegated Prefix Length.....	6-21
IPv6 Prefix.....	6-21
Keep Alive	6-21
L2 Header	6-21
L2TP Enabled	6-21
Label Mode	6-22
Lease Populate	6-22
Lifetime (seconds)	6-22
Link MTU.....	6-22
LNS	6-22
Local Address	6-22
Log Only	6-23
Log Only	6-23
Log Only	6-23
Log Only	6-23
Loopback Enabled	6-24
Low-priority Defect	6-24
MAC Address	6-24
MAC Monitoring.....	6-24
Managed Address Config	6-24
Mask	6-24
Mask Reply	6-24
Maximum Declined Addresses Stored	6-24
Maximum Number Of Equal Cost Routes.....	6-24
Maximum Number Of IPv6 Routes	6-25
Maximum Number Of Multicast Routes	6-25
Maximum Number Of Routes	6-25
Max Interval (seconds).....	6-25
Max Number of Exported Policies.....	6-25
Metric	6-25
Minimum Authentication Interval (minutes)	6-26
Min Interval (seconds)	6-26
Minutes	6-26
Minutes	6-26
Minutes	6-26
Minutes	6-26
Minutes	6-27
Minutes	6-27
Minutes	6-27
Minutes	6-27
Monitor Access Interface Operational State	6-27

MTU.....	6-28
Multicast Capable Peers.....	6-28
Multiplier	6-28
MVPN VRF Target Type	6-28
Name	6-28
Netbios Node Type.....	6-28
No Expiry	6-29
Number	6-29
Number of Packet Too Big	6-29
Number of Param Problem.....	6-29
Number of Redirects.....	6-29
Number of Time Exceeded.....	6-29
Number of TTL Expired.....	6-30
Number of Unreachables.....	6-30
OAM Administrative State.....	6-30
On-link Determination.....	6-30
Option.....	6-30
OSPFv2 Enabled	6-30
OSPFv3 Enabled	6-31
Other Stateful Config.....	6-31
Outer Encapsulation Value.....	6-31
Outer Encapsulation Value.....	6-31
Packet Too Big.....	6-31
Packet Too Big Time (seconds).....	6-31
Param Problem	6-31
Param Problem Time (seconds)	6-31
Physical Address.....	6-31
PIM Enabled	6-32
Periodic Atm Oam LoopBack	6-32
Policy 1	6-32
Policy 2	6-32
Policy 3	6-32
Policy 4	6-32
Policy 5	6-32
Pool Name.....	6-32
Port.....	6-32
Preference	6-32
Preferred Life Time.....	6-33
Prefix Length.....	6-33
Prefix Delegation.....	6-33
Priority Dscp	6-33
Priority Precedence.....	6-33
Priority Type	6-33
Private Retail Subnet	6-33
Proxy ARP Policy 1	6-33
Proxy ARP Policy 2	6-34
Proxy ARP Policy 3	6-34
Proxy ARP Policy 4	6-34
Proxy ARP Policy 5	6-34
Reachable Time (milliseconds).....	6-34
Reassemble.....	6-34
Rebind Timer	6-34

Receive Interval	6-34
Redirects	6-34
Redirects Time (seconds)	6-34
Remote Proxy ARP	6-34
Renew Timer	6-35
Retransmit Time (milliseconds)	6-35
Return Tunnel Auto-Selection Transport Preference	6-35
Return Tunnel Transport	6-35
RIP Enabled	6-35
Route Distinguisher Type	6-35
Router ID	6-35
Router Lifetime (seconds)	6-36
SAP ARP Host Limit	6-36
Scheduling Class	6-36
Seconds	6-36
Seconds	6-36
Seconds	6-36
Seconds	6-36
Seconds	6-36
Seconds	6-37
Seconds	6-37
Seconds	6-37
Seconds	6-37
Send Advertisement	6-37
Server 1	6-38
Server 2	6-38
Server 3	6-38
Server 4	6-38
Server 5	6-38
Server 6	6-38
Server 7	6-38
Server 8	6-38
Service ID	6-38
Service Name	6-38
Service Priority	6-38
Service Tier	6-38
Session Limit	6-39
Session Limit per SAP	6-39
Single SFM Overload Admin State	6-39
SLA Profile Mapped String	6-40
SNMP Community String	6-40
Source Address Termination	6-40
Source IP Address	6-40
Source IP Application	6-41
Static Route ID	6-41
Start Address	6-41
Subscriber Identification	6-42
Subscriber Mapped Profile String	6-42
Subscriber Identification	6-42
SVC Mgr Service ID	6-42
Tag	6-42
Target AS Value	6-42

Target AS Value	6-42
Target AS Value (4Byte).....	6-43
Target AS Value (4Byte).....	6-43
Target Community Value.....	6-43
Target Community Value.....	6-43
Target Extended Community Value	6-43
Target Extended Community Value	6-43
Target Format	6-44
Target Format	6-44
Target IP Address.....	6-44
Target IP Address.....	6-44
Transmit Interval.....	6-45
Threshold (%)	6-45
Threshold (%)	6-45
Threshold (%)	6-45
Threshold (%)	6-45
Time Exceeded	6-46
Time Exceeded Time (seconds)	6-46
Timeout (seconds)	6-46
Transport	6-46
Trusted.....	6-46
TTL Expired	6-47
TTL Expired Time (seconds)	6-47
Tunnel Auto-Selection Transport Preference	6-47
Tunnel Fault Notification	6-47
Tunnel Transport	6-47
Type	6-47
Type	6-48
Type	6-48
Type 0 Administrative Value	6-48
Type 0 Assigned Value.....	6-48
Type 1 Assigned Value.....	6-49
Type 1 IP Address	6-49
Type 2 Administrative Value	6-49
Type 2 Assigned Value.....	6-49
Unreachables	6-49
Unreachables Time (seconds)	6-49
URPF Check Mode	6-49
URPF Check State	6-50
Use GI Address.....	6-50
Use Pool From Client	6-50
Use Shared Queue.....	6-50
Valid Life Time	6-50
Value	6-50
Version	6-50
VRF Target Type.....	6-51
WAN Host	6-51

7 —	IES parameters	7-1
7.1	IES parameters.....	7-2
	AAL5 Encapsulation	7-2
	Administrative State	7-2
	Administration Status.....	7-2
	Aggregate Rate Limit (Kbps).....	7-2
	Aggregation	7-2
	Allow Directed Broadcasts	7-2
	ANCP String	7-2
	Anti-Spoof Mac Address	7-2
	Application Profile	7-3
	ARP Host Limit.....	7-3
	ATM OAM Alarm Cell Handling.....	7-3
	Auto-Assign ID.....	7-3
	Autonomous Address Configuration	7-3
	Auto Select Transport Tunnel	7-3
	Broadcast Address Format	7-3
	Calling Station ID	7-3
	CCM Messages Enabled	7-3
	Client Applications.....	7-3
	Collect Accounting Statistics	7-3
	Current Hop Limit	7-3
	Default Subscriber Identification String	7-3
	Description	7-4
	Direction.....	7-4
	Echo Interval.....	7-4
	Egress Filter ID.....	7-4
	Egress Mark QinQ Top Bits Only	7-4
	Egress Policy ID	7-4
	Egress Scheduler Name.....	7-4
	Enable DHCP Relay.....	7-4
	Enable DHCPv6 Relay	7-4
	Enable Local Proxy.....	7-4
	Enable Local Proxy ARP	7-4
	Enable Proxy ARP.....	7-4
	Fragment Interleave	7-5
	FRF-12 End-To-End Fragment Threshold.....	7-5
	FRF-12 Mode	7-5
	ID	7-5
	ID	7-5
	Ingress Filter ID.....	7-5
	Ingress Match Q in Q Dot1P	7-5
	Ingress Policy ID	7-5
	Ingress Scheduler Name	7-5
	Inner Encapsulation Value	7-6
	Inner Encapsulation Value	7-6
	Interface ID	7-6
	Interface Id Option.....	7-6
	Interface Id String.....	7-6
	IP Address	7-6
	IPv6 Allowed	7-6
	IPv6 Delegated Prefix Length.....	7-6

IPv6 Prefix.....	7-6
L2 Header	7-6
Lease Populate	7-6
Lifetime (seconds)	7-6
Link MTU.....	7-7
LNS	7-7
Loopback Enabled	7-7
Low-priority Defect	7-7
MAC Address	7-7
MAC Monitoring	7-7
Managed Address Config	7-7
Mask Reply	7-7
Maximum Number of Leases	7-7
Max Interval (seconds).....	7-8
Minimum Authentication Interval (minutes)	7-8
Min Interval (seconds)	7-8
Monitor Access Interface Operational State	7-8
Multiplier	7-8
MTU.....	7-8
Name	7-8
Neighbor Resolution	7-8
No Expiry	7-8
Number of Packet Too Big	7-9
Number of Param Problem.....	7-9
Number of Redirects	7-9
Number of Time Exceeded.....	7-9
Number of TTL Expired.....	7-9
Number of Unreachables	7-9
On-Link Determination	7-9
Other Stateful Config.....	7-9
Outer Encapsulation Value.....	7-9
Outer Encapsulation Value.....	7-9
Packet Too Big.....	7-9
Packet Too Big Time (seconds).....	7-9
Param Problem	7-10
Param Problem Time (seconds)	7-10
Periodic Atm Oam LoopBack	7-10
Physical Address	7-10
Policy 1	7-10
Policy 2	7-10
Policy 3	7-10
Policy 4	7-10
Policy 5	7-10
Port.....	7-10
Preferred Life Time.....	7-10
Prefix Address	7-10
Prefix DUID	7-10
Prefix Delegation.....	7-11
Prefix IAID	7-11
Prefix Length.....	7-11
Prefix Life Time (seconds)	7-11
Prefix Option.....	7-11

Prefix Valid Life Time (seconds)	7-11
Priority Level for CCM Messages	7-11
Proxy Arp Policy 1	7-11
Proxy Arp Policy 2	7-11
Proxy Arp Policy 3	7-11
Proxy Arp Policy 4	7-11
Proxy Arp Policy 5	7-11
Reachable Time (milliseconds)	7-11
Rebind Timer	7-12
Receive Interval	7-12
Redirects	7-12
Redirects Time (seconds)	7-12
Renew Timer	7-12
Retransmit Time	7-12
Return Tunnel Transport	7-12
Router Lifetime (seconds)	7-12
SAP ARP Host Limit	7-12
Scheduling Class	7-12
Send Advertisement	7-12
Server 1	7-12
Server 1	7-13
Server 2	7-13
Server 2	7-13
Server 3	7-13
Server 3	7-13
Server 4	7-13
Server 4	7-13
Server 5	7-13
Server 5	7-13
Server 6	7-13
Server 6	7-13
Server 7	7-13
Server 7	7-14
Server 8	7-14
Server 8	7-14
Service ID	7-14
Service Name	7-14
Service Priority	7-14
Service Tier	7-14
Session Limit	7-14
Session Limit per SAP	7-14
Source IP Address	7-14
Subscriber Identification	7-14
SVC Mgr Service ID	7-15
Time Exceeded	7-15
Time Exceeded Time (seconds)	7-15
Timeout	7-15
Transmit Interval	7-15
Trusted	7-15
TTL Expired	7-15
TTL Expired Time (seconds)	7-15
Tunnel Auto-Selection Transport Preference	7-15

	Tunnel Fault Notification	7-16
	Tunnel Transport	7-16
	Unreachables	7-16
	Unreachables Time (seconds)	7-16
	URPF Check Mode	7-16
	URPF Check State	7-16
	Use Shared Queue	7-16
	Valid Life Time	7-16
	WAN Host	7-16
8 —	VLAN parameters	8-1
8.1	VLAN parameters.....	8-2
	Administrative State	8-2
	Application	8-2
	Auto-Assign ID.....	8-2
	Customer VLAN ID	8-3
	Customer VLAN Tag	8-3
	Description	8-3
	Enable 1x1 STP	8-3
	Enable Authentication.....	8-3
	Enable Flat STP	8-3
	Enable Mobile-Tag	8-3
	Enable STP	8-4
	Ethernet Service Name	8-4
	IP Address	8-4
	Lease Time	8-4
	MAC Address	8-4
	Map Type	8-5
	Mode	8-5
	Multicast Address.....	8-5
	Name	8-5
	Port.....	8-5
	Query Response Time (seconds)	8-5
	Service ID	8-5
	Service Name	8-5
	Service Priority	8-6
	Service Tier	8-6
	Service Access Multi-Point ID	8-6
	Specify VLAN Path.....	8-6
	Subscriber Identification	8-6
	SVC Mgr Service ID	8-6
	Type	8-6
	VLAN ID	8-6
	VLAN Level MAC Address Verification	8-7
	VLAN Level Option-82 Data Insertion	8-7
	VLAN Tagging	8-7

9 —	Mirror parameters	9-1
9.1	Mirror parameters.....	9-2
	Administrative State	9-2
	Auto-Assign ID.....	9-2
	Automatic SDP Binding Creation	9-2
	Auto Select Transport Tunnel	9-2
	Description	9-2
	Destination MAC Address	9-2
	Destination MAC Address	9-2
	Disable Revert Time	9-3
	Egress Aggregate Rate Limit.....	9-3
	Egress Mark QinQ Top Bits Only	9-3
	Enable Egress	9-3
	Enable Ingress	9-3
	Enable Port ID Mirroring.....	9-3
	Encapsulation Type	9-3
	EtherType	9-4
	Forwarding Class	9-4
	Forwarding Classes.....	9-4
	Host IP Address	9-4
	Host MAC Address	9-5
	Ingress Label	9-5
	Intercept ID	9-5
	IP Address	9-5
	Monitor Access Interface Operational State	9-5
	Name	9-6
	Port.....	9-6
	Prefix Length.....	9-6
	Remote ICB.....	9-6
	Remote Site ID.....	9-6
	Remote VC ID	9-6
	Revert Time (seconds).....	9-6
	Routing Instance ID	9-6
	Service ID	9-7
	Service Name	9-7
	Service Priority	9-7
	Service Tier	9-7
	Slice Size	9-7
	Source Administrative State	9-7
	Source MAC Address	9-7
	Source MAC Address	9-8
	Subscriber ID	9-8
	Subscriber Identification String	9-8
	SVC Mgr Service ID	9-8
	Tunnel Auto-Selection Transport Preference	9-8
10 —	Service From Template parameters	10-1
10.1	Service From Template parameters.....	10-2

11 — IPsec VPN parameters	11-1
11.1 IPsec VPN parameters	11-2
Authentication Key.....	11-2
Authentication Key.....	11-2
Authentication Key.....	11-2
Auto-Assign ID.....	11-2
Auto Establish.....	11-2
Delivery Service Interface Address	11-3
Description	11-3
Encryption Key.....	11-3
Encryption Key.....	11-3
Encryption Key.....	11-3
IPsec VPN Name	11-3
ISA-IPSEC Group	11-3
Keying.....	11-4
Keying Type	11-4
Keying Type	11-4
Keying Type	11-4
Link Corporate and Secured Service	11-4
Local Gateway Address.....	11-5
Pre Shared Key	11-5
Remote Gateway Address.....	11-5
Replay Window	11-5
Secure Service Interface Address	11-5
Service Type	11-5
SPI Inbound.....	11-6
SPI Outbound.....	11-6
Static Route Address.....	11-6
Static Route Prefix.....	11-6
Tunnel Type.....	11-6
12 — Topology Group parameters	12-1
12.1 Topology Group parameters	12-2
Background Image.....	12-2
Configuration Name.....	12-2
Description	12-2
Description	12-2
Filter Name	12-2
Group Name.....	12-2
Public	12-3
Span	12-3
13 — Physical Link parameters	13-1
13.1 Physical Link parameters	13-2
Bandwidth (Mbps)	13-2
Bandwidth (%).....	13-2
Booking Factor (%)	13-3
Description	13-3
Endpoint A Type	13-3
Endpoint B Type	13-3

Name	13-4
Name	13-4
Notes	13-4
Unmanaged - Description	13-4
Unmanaged - Management Address	13-5
Unmanaged - Name	13-5
Used Bandwidth (Mbps)	13-5
Used Bandwidth (Mbps)	13-6
Utilization Threshold (%)	13-6
Utilization Threshold (%)	13-6

14 — Common Create menu parameters 14-1

14.1	Common Create menu parameters	14-2
	AAL5 Encapsulation	14-2
	Action	14-2
	Active State	14-3
	Address ID	14-3
	Administrative State	14-3
	Admin Status	14-3
	Aggregated Service Site Operational State	14-4
	Aggregate Rate Limit (kbps)	14-4
	Aggregate Rate Limit (kbps)	14-4
	Aggregate Rate Limit (kbps)	14-4
	Aggregation	14-5
	Allow Directed Broadcasts	14-5
	ANCP String	14-5
	Anti-Spoofing	14-5
	Anti-Spoof MAC Address	14-7
	Application Profile	14-7
	ARP Host Limit	14-7
	ARP Populate	14-7
	ATM OAM Alarm Cell Handling	14-8
	Auto-Assign ID	14-8
	Autonomous Address Configuration	14-8
	Auto Select Return Transport Tunnel	14-9
	Auto-Select Transport Tunnel	14-9
	Auto Select Tunnels	14-9
	BPDU Translation	14-9
	Broadcast Address Format	14-10
	Calling Station ID	14-10
	Circuit ID	14-10
	Class	14-11
	Client Applications	14-12
	Collect Accounting Statistics	14-12
	Composite ID	14-12
	Configured IP MTU (Octets)	14-12
	Current Hop Limit	14-13
	Customer VID	14-13
	Default Mesh VC ID	14-13
	Default Primary DNS Server Address	14-13
	Default Secondary DNS Server Address	14-13

Default Subscriber Id	14-14
Default Subscriber Identification String	14-14
Default Subscriber Identification Type	14-14
Default VC ID.....	14-14
Description	14-14
Displayed Name	14-15
Dynamic Topology Discovery	14-15
Egress Filter ID.....	14-15
Egress Label	14-15
Egress Mark QinQ Top Bits Only	14-15
Egress Policy ID	14-16
Egress Scheduler Name.....	14-16
Emulated Server IP Address	14-16
Enable.....	14-16
Enable DHCP Relay.....	14-16
Enable DHCPv6 Relay	14-17
Enable Egress Forwarding.....	14-17
Enable Ingress Forwarding	14-17
Enable Egress Packets Forwarding.....	14-18
Enable Hash Label.....	14-18
Enable Local Proxy.....	14-19
Enable Local Proxy ARP	14-19
Enable Secure SAPs	14-19
Enable Signal Capability.....	14-19
Enable PW Status Signaling	14-20
Encapsulation Tagging.....	14-21
Ethernet Tunnel Endpoint Control SAP	14-21
Expiry Time	14-21
FlowSpec Validate Enabled	14-21
Forwarding Service ID	14-22
Fragment Interleave	14-22
Frame-Based Accounting.....	14-22
FRF-12 End-To-End Fragment Threshold.....	14-22
FRF-12 Mode	14-22
Gateway IP Address.....	14-23
GSMP Administrative State	14-23
Hold Multiplier.....	14-23
ID	14-23
ID	14-23
ID	14-24
ID	14-24
ID	14-24
ID	14-24
Import Policy.....	14-24
Ingress Counter Mode.....	14-24
Ingress Filter ID.....	14-25
Ingress Label	14-25
Ingress Match QinQ Dot1P.....	14-25
Ingress Policy ID	14-25
Ingress Scheduler Name	14-25
Inherit Service ID Value	14-26
Inherit Service ID Value	14-26

Inner Encapsulation Value	14-26
Inner Encapsulation Value (VCI)	14-26
Inter-Chassis Backup	14-26
Interface ID	14-27
Interface Id Option.....	14-27
Interface Id String.....	14-27
Interface Name	14-27
Interface Type	14-28
Intermediate Destination ID	14-28
Interworking Type.....	14-28
IP Address	14-28
IP address.....	14-29
IP Address	14-29
IP Address	14-29
IP Address	14-29
IP Address	14-29
IP Address	14-30
IPv6 Allowed	14-30
IPv6 Delegated Prefix Length.....	14-30
IPv6 Prefix.....	14-30
Keep-Alive (seconds)	14-30
L2 Header	14-30
L2 Protocol Termination	14-31
L2Uplink	14-31
LAG link selection	14-31
Lease Populate	14-31
Lease Time	14-32
Lease Time RADIUS Override	14-32
Lifetime (seconds)	14-32
Lifetime (seconds)	14-32
Lifetime (seconds)	14-33
Link MTU.....	14-33
LNS	14-33
Local Address	14-33
Loopback Enabled.....	14-33
MAC Address	14-33
MAC Address	14-34
MAC Address	14-34
MAC Address	14-34
MAC Address	14-34
MAC Address	14-34
MAC Monitoring.....	14-34
MAC Name	14-35
MAC Notification Count	14-35
MAC Notification Interval (seconds).....	14-35
Managed Address Config	14-35
Mask Reply	14-35
Match Circuit ID	14-36
Maximum Number of Leases.....	14-36
Max Interval (seconds).....	14-36
Max Number of Groups	14-36
Max Number of Sources per Group	14-36
MC Ring Node	14-36

Min Interval (seconds)	14-37
Minimum Authentication Interval (minutes)	14-37
Monitor Access Interface Operational State	14-37
MTU.....	14-37
MTU.....	14-37
MTU Check	14-37
Name	14-38
Name	14-38
Name	14-39
Neighbor Resolution	14-39
No Egress Aggregate Rate Limit.....	14-40
No Expiry	14-40
No Expiry	14-40
Non-Subscriber Traffic Identification	14-40
Number of Days.....	14-40
Number of Hours	14-41
Number of Minutes.....	14-41
Number of Packet Too Big	14-41
Number of Param Problem.....	14-41
Number of Redirects.....	14-41
Number of Seconds	14-41
Number of Time Exceeded.....	14-42
Number of TTL Expired.....	14-42
Number of Unreachables.....	14-42
OAM Administrative State.....	14-42
OLC State	14-42
On-Link Determination	14-43
Operational State UP While Empty	14-43
Other Stateful Config.....	14-43
Outer Encapsulation Value.....	14-44
Outer Encapsulation Value (VPI)	14-44
Packet Too Big.....	14-44
Packet Too Big Time (seconds).....	14-45
Param Problem	14-45
Param Problem Time (seconds)	14-45
Path ID	14-45
PBB Source Backbone MAC Address.....	14-46
Peer Address	14-46
Periodic ATM OAM Loopback	14-46
Per Service Hashing for LAG Enabled	14-46
Physical Address	14-46
PIM Snooping Enabled	14-46
Policy ID	14-47
Policy 1	14-47
Policy 2	14-47
Policy 3	14-47
Policy 4	14-47
Policy 5	14-47
Port.....	14-47
Precedence.....	14-48
Preferred Life Time.....	14-48
Prefix Address	14-48

Prefix Delegation	14-48
Prefix DUID	14-48
Prefix IAID	14-48
Prefix Length.....	14-49
Prefix Length.....	14-49
Prefix Life Time (seconds)	14-49
Prefix Option.....	14-49
Prefix Valid Life Time (seconds)	14-49
Primary DNS Address.....	14-50
Priority Level for CCM Messages	14-50
Priority Dscp	14-50
Priority Precedence.....	14-50
Priority Type	14-50
Profiled Traffic only	14-50
Profile Name	14-51
Proxy ARP Policy 1	14-51
Proxy ARP Policy 2	14-51
Proxy ARP Policy 3	14-51
Proxy ARP Policy 4	14-51
Proxy ARP Policy 5	14-52
Reachable Time (milliseconds).....	14-52
Rebind Timer	14-52
Receive Interval	14-52
Redirects	14-52
Redirects Time (seconds)	14-52
Relay Plain BOOTP	14-53
Remote ID	14-53
Remote ID String	14-53
Remote Proxy ARP	14-53
Renew Timer.....	14-54
Retransmit Time (milliseconds).....	14-54
Return Tunnel Auto-Selection Transport Preference	14-54
Router Lifetime (seconds)	14-55
SAP Administrative State.....	14-55
SAP ARP Host Limit.....	14-55
SAP Description.....	14-55
SAP Type.....	14-55
Scheduling Class	14-56
Secondary DNS Address.....	14-56
Send Advertisement	14-56
Server 1	14-57
Server 2	14-57
Server 3	14-57
Server 4	14-57
Server 5	14-57
Server 6	14-57
Server 7	14-58
Server 8	14-58
Server Name	14-58
Service ID	14-58
Service Model	14-58
Service Name	14-59

Service Priority	14-59
Service Tier	14-59
Set Default VLAN to VPLS Tag	14-59
SHCV Action	14-59
SHCV Enabled	14-60
SHCV Interval (minutes)	14-60
SHCV Retry Count	14-60
SHCV Retry Timeout (seconds)	14-60
SHCV Source	14-60
SHCV Source IP Address	14-61
SHCV Source MAC Address	14-61
Site ID	14-61
Snooping	14-62
Source IP Address	14-62
Specify VLAN Path	14-62
Subscriber Authentication Policy	14-62
Subscriber Identification	14-63
Subscriber Limit	14-63
SVC Mgr Service ID	14-63
Tag (Inner Encapsulation Value)	14-63
Tag (Outer Encapsulation Value)	14-63
Template Description	14-63
Time Exceeded	14-64
Time Exceeded Time (seconds)	14-64
Timeout (seconds)	14-64
Translation	14-64
Translation ID	14-65
Transmit Interval	14-65
Transport Type	14-65
Trusted	14-66
Trusted	14-66
TTL Expired	14-67
TTL Expired Time (seconds)	14-67
Tunnel Auto-Selection Transport Preference	14-67
Tunnel Fault Notification	14-68
Tunnel Termination Site	14-68
Unnumbered Type	14-68
Unreachables	14-68
Unreachables Time (seconds)	14-69
URPF Check Mode	14-69
URPF Check State	14-69
Use ARP	14-70
Use as source	14-70
Use Bandwidth-Reserved Paths	14-70
Use Multipoint Shared Queue	14-70
Use SAP ID as Subscriber ID	14-71
Use Shared Queue	14-71
Valid Life Time	14-71
VC ID	14-71
VC Type	14-71
VC Type	14-72
Vendor Specific Options	14-72

Vendor String	14-73
VLAN VC Tag	14-73
VPLS Name	14-73
WAN Host	14-73

Manage menu parameters

15 — Templates parameters 15-1

15.1	Templates parameters	15-2
	Auto-Assign ID.....	15-2
	Command Type	15-2
	Description	15-2
	Generate First (Base) Version	15-2
	Generate Velocity Properties	15-2
	Mode	15-2
	Name	15-3
	Script ID	15-3
	Show created object.....	15-3
	State	15-3
	Templated Object Categories	15-3
	Templated Object Class Name	15-3
	Type	15-4

16 — Services parameters 16-1

16.1	Services parameters	16-2
	Administrative State	16-2
	Age (seconds)	16-2
	Inhibit Learning.....	16-2
	Last Member Query Interval (tenths of seconds).....	16-2
	Max Group	16-2
	Max Group Action	16-3
	Multicast Group IP Address	16-3
	Protocol Version	16-3
	Proxying	16-3
	Querier Forwarding	16-4
	Query Interval (seconds)	16-4
	Query Response Interval (tenths of seconds)	16-4
	Querying	16-4
	Robust Count.....	16-5
	Router Timeout (seconds)	16-5
	Source Timeout (seconds)	16-5
	Spoofing	16-5
	Target MAC Address.....	16-6
	Unsolicited Report Interval (seconds).....	16-6
	What type of interface would you like to create?	16-6
	Zapping	16-6

17 —	Mirror Services parameters	17-1
17.1	Mirror Services parameters	17-2
	Allow Binding Of Templates Not Associated With Any Customer	17-2
	Automatic SDP Binding Creation	17-2
	Collect Accounting Statistics	17-2
	Customer ID	17-2
	Description	17-2
	Encapsulation Type	17-3
	Forwarding Class	17-3
	ID	17-4
	Inner Encap Value	17-4
	Name	17-4
	Outer Encap Value	17-4
	Return Tunnel Transport	17-4
	Service Description	17-4
	Service Name	17-4
	Site ID	17-5
	Site Type	17-5
	Slice Size	17-5
	Source Administrative State	17-5
	Template Description.....	17-5
	Transport Type	17-5
	Tunnel Source Site ID.....	17-6
	Tunnel Transport.....	17-6
	Use Bandwidth-Reserved Paths	17-6
18 —	Customers parameters	18-1
18.1	Customers parameters	18-2
	Address	18-2
	Apdex scores below this threshold are unacceptable quality	18-2
	Apdex scores below this threshold are poor quality	18-2
	Apdex scores below this threshold are fair quality	18-2
	Apdex scores below this threshold are good quality.....	18-2
	Auto-Assign ID.....	18-2
	Contact	18-2
	Description	18-2
	Email	18-2
	Equipment Type	18-3
	ID	18-3
	MOS scores below this threshold are bad quality	18-3
	MOS scores below this threshold are poor quality	18-3
	MOS scores below this threshold are fair quality.....	18-3
	MOS scores below this threshold are good quality	18-3
	Name	18-3
	Phone Number	18-3
	Scheduler Name	18-4

19 — LSPs parameters	19-1
19.1 LSPs parameters	19-2
Adjust Down Bandwidth (mbps)	19-2
Adjust Down Threshold (percent)	19-2
Adjust Multiplier	19-2
Adjust Up Bandwidth (mbps)	19-2
Adjust Up Threshold (percent)	19-2
Administrative	19-3
Administrative	19-3
Administrative State	19-3
Administrative State	19-3
Auto Bandwidth	19-3
Auto Select Hop-less Path	19-3
Auto-Assign ID	19-4
Backup Hold Priority	19-4
Backup Setup Priority	19-4
Backup Type	19-4
Collect Accounting Statistics	19-4
Collect Accounting Statistics	19-5
Committed Rate	19-5
Description	19-5
Destination IP Address	19-5
Destination Site ID	19-5
Diff-Serv Backup Class Type	19-5
Diff-Serv Class Type	19-6
Displayed Name	19-6
Dynamic Bypass	19-6
Egress Label	19-6
Egress Label	19-7
Enable Auto-Bind	19-7
Enable CSPF	19-7
Enable SRLG	19-7
Enable TE Metric	19-8
Fast Reroute	19-8
Groups Excluded (bitmap)	19-8
Groups Included	19-8
Groups Included	19-9
Guarded Destination	19-9
Guarding Lsp	19-9
Hold Priority	19-9
Hop Index	19-10
Hop Limit	19-10
Hop Limit	19-10
Hop Limit	19-10
ID	19-10
ID	19-10
Include ADSPEC in RSVP	19-11
IGP Shortcut Enabled	19-11
Ingress Label	19-11
Inherit Value	19-11
Interface Name	19-12
IP Address	19-12

Label Action.....	19-12
LDP over RSVP include.....	19-12
Least-Fill Path Selection	19-13
Main Class Type Retry Limit	19-13
Make before Break	19-13
Maximum Bandwidth (mbps)	19-14
Maximum Transmitted Frame Size	19-14
Metric	19-14
Minimum Bandwidth (mbps)	19-14
Monitor Bandwidth.....	19-14
Name	19-14
Next Hop.....	19-14
Next Hop.....	19-15
Node Protect.....	19-15
Overflow Limit.....	19-15
Overflow Limit Bandwidth (mbps).....	19-15
Overflow Limit Threshold (percent).....	19-15
Overridden Properties	19-15
P2MPId	19-16
Pacing Interval (seconds)	19-16
Path Preference	19-16
Peak Rate.....	19-16
Permit Merge.....	19-16
Persistent.....	19-16
Preference	19-17
Rebuild Timer	19-17
Record Actual Path	19-17
Record Actual Path	19-17
Record Actual Route	19-17
Record Label.....	19-18
Record Label.....	19-18
Reserved Bandwidth	19-18
Reserved Bandwidth (Mbps)	19-18
Resignal.....	19-18
Retry Limit	19-18
Retry Timer (seconds)	19-19
RSVP Reserve Style.....	19-19
Sample Multiplier	19-19
Scheduled Task Description	19-19
Scheduled Task Name	19-20
Sequencing Order	19-20
Sequencing Target	19-20
Setup Priority	19-20
Show created object.....	19-20
Site ID	19-20
Source IP Address	19-21
Source Site ID	19-21
System ID (Loopback IP Address)	19-21
Termination Validation.....	19-21
Type.....	19-21
View the newly created Bypass Only Lsp.....	19-22
View the newly created Dynamic LSP.....	19-22

20 —	MPLS Paths parameters	20-1
20.1	MPLS Paths parameters	20-2
	Administrative	20-2
	Description	20-2
	Hop Type	20-2
	Insert Hop	20-2
	IP Address	20-2
	IP Address	20-2
	IP Address	20-3
	Name	20-3
	Specify Site.....	20-3
	Starting Network Element	20-3
21 —	Service Tunnels parameters	21-1
21.1	Service Tunnels parameters	21-2
	Access Adapt QoS	21-2
	Administrative	21-2
	Administrative MTU	21-2
	Administrative State	21-2
	Advertised MTU Override	21-2
	APS Command.....	21-3
	Auto-Assign ID.....	21-3
	BW (Mbps)	21-3
	CCM Hold Time Down (deciseconds)	21-4
	CCM Hold Time Up (deciseconds)	21-4
	CFM Test.....	21-4
	Class Forwarding Capability	21-4
	Compatible Version	21-4
	Collect Accounting Statistics	21-5
	Configured MAC Address	21-5
	Control Tag (Inner Encapsulation Value)	21-5
	Control Tag (Inner Encapsulation Value)	21-5
	Control Tag (Outer Encapsulation Value).....	21-6
	Control Tag (Outer Encapsulation Value).....	21-6
	Control Tag (Outer Encapsulation Value).....	21-6
	Description	21-6
	Destination Site ID	21-6
	Element ID.....	21-6
	Enable BGP-Tunnel.....	21-7
	Enable LDP	21-7
	Enable Per Forwarding Path Ingress Queue	21-7
	Encap Type.....	21-8
	Enforce Diff-Serv Lsp-Fc Map	21-8
	Ethernet Ring ID	21-8
	Ethernet Tunnel Endpoint Control SAP	21-8
	FRR	21-9
	Group Name.....	21-9
	Guard Time (deciseconds)	21-9
	Guard Time (centiseconds)	21-9
	Hello Message Length.....	21-9
	Hello Request Timeout	21-10

Hello Time.....	21-10
Hold Down Time	21-10
Hold Time Down	21-10
Hold Time Up (deciseconds)	21-10
ID	21-11
ID	21-11
ID	21-11
Interconnected Ethernet Ring Element	21-11
Keep-Alive Enabled	21-11
Max Drop Count.....	21-12
Member Port	21-12
Member Port	21-12
Member Port	21-12
Metric	21-12
Mgr ID	21-12
Mixed Lsp Mode.....	21-13
Name	21-13
Naming Format	21-13
No VLAN VC Ethertype.....	21-14
Operational Path Endpoint Threshold.....	21-14
Order	21-14
Path Endpoint.....	21-14
Path Endpoint.....	21-14
Path Endpoint Type	21-14
Path ID	21-15
Path ID	21-15
Path ID	21-15
PBB Ethernet Type	21-15
Precedence.....	21-15
Precedence.....	21-15
Precedence.....	21-16
Propagate Topology Change	21-16
Protection Type	21-16
R-APS Tag (Inner Encapsulation Value)	21-16
R-APS Tag (Outer Encapsulation Value).....	21-16
Revert Time (seconds).....	21-16
Revert Time (minutes)	21-17
Ring Node ID	21-17
Ring Protection Link Type	21-17
SDP Bandwidth Booking Factor (%)	21-18
Show created object.....	21-18
Signaling	21-18
Site ID	21-19
Source Site ID	21-19
Template Versions	21-19
Transport Destination Address	21-19
Tunnel Creation Pacing Interval (seconds)	21-20
Tunnel Endpoint ID.....	21-20
Tunnel ID	21-20
Tunnel Type.....	21-20
Type	21-20
Underlying Transport	21-21

User Specified Naming Prefix	21-21
Value	21-21
VC Type.....	21-21
View the newly created tunnel	21-22
VLAN VC Ethertype.....	21-22
VLAN VC Tag	21-22
VPLS	21-22

22 — IPsec VPN parameters 22-1

22.1	IPsec VPN parameters	22-2
	Auto-Assign ID.....	22-2
	Authentication Key.....	22-2
	Authentication Key.....	22-2
	Authentication Key.....	22-2
	Authentication Key.....	22-2
	Auto Establish.....	22-3
	Backup Remote Address	22-3
	Description	22-3
	Designated	22-3
	Destination Address.....	22-3
	Destination Address.....	22-3
	Direction.....	22-3
	Direction.....	22-4
	Displayed Name	22-4
	Enabled	22-4
	Encryption Key.....	22-4
	Encryption Key.....	22-4
	Encryption Key.....	22-5
	Encryption Key.....	22-5
	ID	22-5
	IKE Policy	22-5
	IP Address	22-5
	IP Address	22-5
	IP Address	22-6
	Keying.....	22-6
	Link Corporate and Secured Service	22-6
	Local Address Option	22-6
	Local Endpoint Address.....	22-6
	Local Gateway Address.....	22-7
	Name	22-7
	Name	22-7
	Prefix Length.....	22-7
	Prefix Length.....	22-7
	Pre Shared Key	22-7
	Remote Address	22-8
	Remote Address Option	22-8
	Remote Gateway Address.....	22-8
	Replay Window	22-8
	Security Policy ID.....	22-9
	SPI	22-9
	Transform ID 1	22-9

	Transform ID 2	22-9
	Transform ID 3	22-9
	Transform ID 4	22-9
	Tunnel Type	22-9
23 —	VLAN group and path parameters	23-1
23.1	VLAN group and path parameters	23-2
	Description	23-2
	Description	23-2
	Group Name	23-2
	Head Ends	23-2
	Minimum Bandwidth (kbps)	23-2
	Name	23-2
	Node Type	23-2
	Technology	23-3
	Topology	23-3
	VLAN Space Management by SAM	23-3
24 —	Node Redundancy parameters	24-1
24.1	Node Redundancy parameters	24-2
	Administrative State	24-2
	Administrative State	24-2
	Administrative State	24-2
	Administrative State	24-2
	Authentication Key	24-3
	Authentication Key	24-3
	Authentication Key	24-3
	Authentication Key	24-3
	Auto-Assign ID	24-4
	BFD Enabled	24-4
	BFD Enabled	24-4
	BFD Enabled	24-4
	Boot Timer	24-4
	Boot Timer	24-5
	Boot Timer	24-5
	Description	24-5
	Description	24-5
	Description	24-5
	Description	24-5
	Destination IP Address	24-6
	Destination IP Address	24-6
	Destination IP Address	24-6
	Encap Type	24-6
	End VLAN Value	24-6
	Hold On Neighbor Failure	24-6
	Hold On Neighbor Failure	24-7
	Hold On Neighbor Failure	24-7
	IGMP	24-7
	IGMP Snooping	24-7
	Interface Name	24-8

Interval (minutes)	24-8
Keep-Alive Interval (deciseconds)	24-8
Keep-Alive Interval (deciseconds)	24-8
Keep-Alive Interval (deciseconds)	24-8
Keep-Alive Interval (deciseconds)	24-9
LACP Key	24-9
LAG ID.....	24-9
LAG ID.....	24-9
LAG ID.....	24-9
Lost Connection Wait Interval.....	24-9
MAC LSB (hex)	24-10
Maximum Inner Encap Value.....	24-10
Maximum Outer Encap Value	24-10
MC Ring	24-10
Minimum Inner Encap Value	24-10
Minimum Outer Encap Value	24-11
MLD Snooping	24-11
Name	24-11
Passive Mode Enabled	24-11
Passive Mode Enabled	24-11
Passive Mode Enabled	24-12
Peer Address	24-12
Peer Name.....	24-12
Peer Name.....	24-12
Peer Name.....	24-12
Port/LAG Name.....	24-13
Ring Node Name	24-13
SAP Inner Encapsulation Value	24-13
SAP Outer Encapsulation Value	24-13
SAP Service ID.....	24-13
Service ID	24-13
Site ID	24-13
Site ID	24-14
Site Id	24-14
Site Id	24-14
Site ID	24-14
Source Address	24-14
Source Address	24-15
Source Address	24-15
Source Address	24-15
Source IP Address	24-15
Source MAC Address	24-15
SRRP	24-16
Start VLAN Value	24-16
Subscriber Host Tracking.....	24-16
Subscriber Management.....	24-16
Sync Administrative State.....	24-16
Synchronization Tag	24-17
Synchronize IGMP	24-17
Synchronize IGMP-Snooping.....	24-17
Synchronize MC Ring.....	24-17
Synchronize MLD Snooping.....	24-17

Synchronize SRRP	24-18
Synchronize Subscriber Host Tracking	24-18
Synchronize Subscriber Management.....	24-18
Sync Tag Config Level	24-18
Sync Tag Config Level	24-19
Sync Tag Config Level	24-19
System ID	24-19
System Priority	24-19
System Priority	24-20
System Priority	24-20
System Priority	24-20
Use LACP Key	24-20

25 — Routing Instances parameters 25-1

25.1	Routing Instances parameters.....	25-2
	Action	25-2
	Allow Directed Broadcasts	25-2
	Autonomous System.....	25-2
	BGP Enabled	25-2
	Broadcast	25-2
	Broadcast Address Format	25-2
	Cflowd Type.....	25-3
	Circuit ID	25-3
	Class.....	25-3
	Confederation Autonomous System	25-3
	Description	25-3
	Egress Filter ID.....	25-3
	Enable DHCP Relay.....	25-3
	Exclusive.....	25-3
	IGMP Enabled	25-4
	IGP Inhibit	25-4
	Ingress Filter ID.....	25-4
	Interface ID	25-4
	IP Address	25-4
	IS-IS Enabled	25-4
	LDP Enabled.....	25-4
	Loopback Enabled.....	25-5
	MAC Address	25-5
	Mask Reply	25-5
	Maximum Number of Equal Cost Routes	25-5
	Member AS	25-5
	MPLS Enabled	25-6
	Name	25-6
	Network Policy ID	25-6
	Number of Redirects.....	25-6
	Number of TTL Expired.....	25-6
	Number of Unreachables.....	25-6
	OSPFv2 Enabled	25-6
	OSPFv3 Enabled	25-6
	PIM Enabled	25-7
	Physical Address.....	25-7

Prefix Length.....	25-7
Primary	25-7
Redirects	25-7
Redirects Time	25-7
Remote ID	25-8
RIP Enabled	25-8
Router ID	25-8
Server 1	25-8
Server 2	25-8
Server 3	25-8
Server 4	25-8
Server 5	25-8
Server 6	25-8
Server 7	25-9
Server 8	25-9
Shortcut Local TTL Propagate.....	25-9
Shortcut Transit TTL Propagate.....	25-9
Snooping	25-10
Source Address Termination.....	25-10
Source IP Address	25-10
Source IP Application	25-10
Subnet Mask.....	25-11
Timeout.....	25-11
TTL Expired	25-11
TTL Expired Time (seconds)	25-11
Unreachables	25-11
Unreachables Time (seconds)	25-11

26 — VRRP Virtual Routers parameters 26-1

26.1	VRRP Virtual Routers parameters.....	26-2
	Administrative State	26-2
	Backup Address	26-2
	Base Priority	26-2
	Description	26-2
	Destination Address.....	26-2
	Enable BFD Interface	26-2
	Init Delay (seconds).....	26-3
	Key	26-3
	MAC Address	26-3
	Master Inherit Interval.....	26-3
	Message Interval (seconds)	26-4
	Message Interval (milliseconds)	26-4
	Name	26-4
	Owner	26-4
	Ping Reply	26-5
	Preempt Mode	26-5
	SSH Reply	26-5
	Standby Forwarding.....	26-6
	Subnet Mask.....	26-6
	Telnet Reply	26-6
	Traceroute Reply	26-6

	Type	26-6
	Virtual Router ID	26-7
	VRRP Type	26-7
27 —	Virtual Anycast RP parameters	27-1
27.1	Virtual Anycast RP parameters	27-2
	Anycast RP Type	27-2
	Anycast RP Address	27-2
	Auto Created Interface Name	27-2
	Description	27-2
	Name	27-2
	Static Group IP Address	27-3
	Static Group Mask	27-3
28 —	FIB Entries parameters	28-1
28.1	FIB Entries parameters	28-2
	Auto Complete	28-2
	MAC Address	28-2
29 —	Snapshot Instances parameters	29-1
29.1	Snapshot Instances parameters	29-2
	Description	29-2
	Gzip Exported File	29-2
	Include Additional Information Attributes	29-2
	Include Attributes with Read-Only Access	29-2
	Include Components and Attributes with Manufacturer Visibility	29-2
	Include in the snapshot	29-3
	Include States and Statuses	29-3
	Snapshot Name	29-3
30 —	Activation parameters	30-1
30.1	Activation parameters	30-2
	Name	30-2
	Description	30-2
31 —	Gateway configuration parameters	31-1
31.1	Gateway configuration parameters	31-2
	Accounting Interim Interval (s)	31-2
	Accounting Level	31-2
	Administrative State	31-2
	Aggregated Downlink Rate (kbps)	31-2
	Aggregated Uplink Rate (kbps)	31-2
	Allocation Type	31-3
	Application Transaction Timer (s)	31-3
	Auto-Assign ID	31-3
	Bearer Timeout (seconds)	31-3
	Configuration File Limit (Mbps)	31-3

Configuration File Limit (Mbps)	31-3
Description	31-4
Duration before File Closure (hours)	31-4
Duration before File Deletion (days)	31-4
Dynamic PCC	31-4
File Extension	31-4
Home Subscriber Server Assigned	31-4
Ignore All	31-5
Ignore All	31-5
Ignore Home	31-5
Ignore Home	31-6
Ignore Roaming	31-6
Ignore Roaming	31-6
Ignore Visiting	31-7
Ignore Visiting	31-7
Inherit Home Profile From Gateway	31-8
Inherit Roaming Profile From Gateway	31-8
Inherit Visiting Profile From Gateway	31-8
Inclusion of Charging-Group-ID AVP in ACR	31-8
IP Pool Address Hold Timer (minutes)	31-8
IP Pool ID	31-8
IP Pool Name	31-9
IP v4/v6	31-9
IPv4	31-9
IPv4 Primary Address	31-9
IPv4 Primary Address	31-9
IPv4 Primary Address	31-9
IPv4 Secondary Address	31-10
IPv4 Secondary Address	31-10
IPv6	31-10
IPv6 Primary Address	31-10
IPv6 Primary Address	31-10
IPv6 Secondary Address	31-10
Is Exclusive	31-11
Limit for the number of ACRs	31-11
Local Pool	31-11
Mobile Station APN Selection Mode	31-11
Multiple PDNs allowed	31-11
Name	31-11
Network APN Selection Mode	31-12
Node ID	31-12
Operator-string AVP of an ACR Message	31-12
Origin Host	31-12
Origin Realm	31-12
PCRF Selection Dynamic PCC	31-12
Pool Address Block	31-13
Pool Address Type	31-13
Pool IP Address	31-13
Prefix Length	31-13
Primary Compact Flash	31-13
Private Info	31-14
Reject Charging	31-14

	Reject Charging	31-14
	Reject Foreign Subscribers	31-15
	Restriction Type	31-15
	Retry Count	31-15
	Retry Count for ACR Messages (s).....	31-15
	Session Timeout (seconds)	31-15
	Size Limit Before File Closure (Mbps)	31-15
	Span	31-16
	Subscribed APN Selection Mode	31-16
	Transaction Timer (s).....	31-16
	Type	31-16
32 —	Mobile Regions parameters	32-1
32.1	Mobile Regions parameters	32-2
	Auto-Assign ID.....	32-2
	Mobile Country Code.....	32-2
	Mobile Network Code	32-2
	Region ID	32-2
	Region Name	32-2
33 —	LTE User Stats parameters	33-1
33.1	LTE User Stats parameters.....	33-2
	APN Name	33-2
	Bearer Context	33-2
	Bearer ID.....	33-2
	Description	33-2
	IMSI	33-2
	Include All APNs	33-2
	Include All Bearers	33-3
	Include All Directions.....	33-3
	Include All IDs.....	33-3
	Include All Precedences.....	33-3
	PDN Context	33-3
	SDF	33-4
	SDF Direction	33-4
	SDF Filter	33-4
	SDF Filter ID.....	33-4
	SDF Precedence	33-4
34 —	LTE EPS Path Drill Down Hints parameters	34-1
34.1	LTE EPS Paths Drill Down Hints parameters.....	34-2
	Auto-Assign ID.....	34-2
	Connection Type	34-2
	Description	34-2
	Encapsulation Type	34-2
	High Priority.....	34-2
	ID	34-3
	Inner Encapsulation Value	34-3
	Order	34-3

Outer Encapsulation Value.....	34-3
Segment Type.....	34-3
Type.....	34-4

35 — Call Trace parameters 35-1

35.1	Call Trace parameters.....	35-2
	Auto-Assign ID.....	35-2
	Call Trace Session Name	35-2
	Call Trace UDP Port.....	35-2
	Description	35-2
	Disk Usage Alarm Severity	35-2
	Disk Usage Alarm Threshold	35-2
	File Retention Time (hrs)	35-3
	File Rollover Time (min)	35-3
	IRAT Handover Threshold	35-3
	isPCMDEnabled.....	35-3
	isSignBasedCTEnabled	35-3
	RRC Re-establishment Threshold	35-3
	Trace ID.....	35-4
	Trace Interface RRC (Uu)	35-4
	Trace Interface S1-MME	35-4
	Trace Interface X2	35-4
	Traffic Threshold (Connected UE) (%).....	35-4

36 — Common Manage menu parameters 36-1

36.1	Common Manage menu parameters	36-2
	Address ID	36-2
	Administrative State	36-2
	Aggregate Rate Limit (kbps).....	36-2
	Allow Binding Of Templates Not Associated With Any Subscriber	36-2
	Auto-Assign ID.....	36-3
	Configured IP MTU (Octets).....	36-3
	Description	36-3
	Disable Fix Window	36-3
	Frame Base Accounting.....	36-4
	Gateway MAC Address	36-4
	ID	36-4
	Inner Encapsulation Value	36-4
	Interface ID	36-4
	IP Address	36-5
	Keep Alive Interval.....	36-5
	MAC Address	36-5
	Name	36-5
	Next Hop.....	36-5
	Outer Encapsulation Value.....	36-5
	Prefix Length.....	36-6
	Priority.....	36-6
	Remote IP Address	36-6
	SAP Administrative State.....	36-7
	SAP Description.....	36-7

Service Description	36-7
SRRP ID.....	36-7
Subscriber ID	36-7
Trusted.....	36-7
Use Multipoint Shared Queue.....	36-7
Use Shared Queue	36-8
VC ID	36-8
VC Type.....	36-8
VLAN VC Tag	36-8

Policies menu parameters

37 — Access Ingress parameters 37-1

37.1	Access Ingress parameters	37-2
	ATM VCI	37-2
	Auto-Assign ID.....	37-2
	Broadcast Policer ID	37-2
	Broadcast Queue ID	37-2
	Cir	37-2
	Cir Adaptation	37-2
	Committed Burst Size.....	37-2
	Default FC	37-3
	Default FC HSMDA Counter Override	37-3
	Description	37-3
	Destination IP	37-3
	Destination MAC	37-3
	Destination Port	37-3
	Displayed Name	37-3
	Dot1p.....	37-3
	Dot1p.....	37-4
	Dot1p.....	37-4
	DSCP.....	37-4
	Dst Mask	37-4
	Ether Type.....	37-4
	Expedite	37-4
	Forwarding Class	37-4
	Fragment	37-4
	Frame Type	37-5
	High Priority Reserved.....	37-5
	HSMDA Broadcast Queue ID	37-5
	HSMDA Multicast Queue ID	37-5
	HSMDA Queue ID.....	37-5
	ID	37-5
	ID	37-5
	ID	37-6
	In DSCP.....	37-6
	In Precedence.....	37-6
	In Remark.....	37-7

LspExp	37-7
MAC Criteria Type	37-7
Mark DE bit1 as Out of Profile.....	37-7
Mask	37-8
Mask	37-8
Mask	37-8
Mask	37-8
Maximum Burst Size.....	37-8
Mode	37-9
Multipoint	37-9
Multipoint Policer ID	37-9
Multipoint Queue ID.....	37-9
Out DSCP	37-9
Out Precedence	37-9
Out Remark	37-9
Packet Byte Offset (bytes).....	37-10
Packet Byte Offset	37-10
Parent Arbiter	37-10
Pir	37-10
Pir Adaptation	37-10
Policed	37-10
Policer ID	37-10
Precedence.....	37-11
Priority.....	37-11
Priority.....	37-11
Priority.....	37-11
Profile.....	37-11
Protocol.....	37-11
Queue ID	37-12
Scheduler	37-12
SNAP OUI	37-12
SNAP PID	37-12
Source IP.....	37-12
Source MAC.....	37-12
Source Port.....	37-12
Src Mask	37-13
Stats Mode.....	37-13
Unknown Policer ID	37-13
Unknown Queue ID	37-13
Use Policer	37-13
Use Queue Group.....	37-13

38 — 7210 Access Ingress parameters

38-1

38.1	7210 Access Ingress parameters	38-2
	Auto-Assign ID.....	38-2
	Broadcast Meter ID.....	38-2
	CIR (kbps).....	38-2
	CIR Adaptation.....	38-2
	Committed Burst Size (kbps)	38-2
	Default FC	38-2
	Description	38-3

Destination MAC	38-3
Displayed Name	38-3
Dot1p	38-3
DSCP	38-4
Ether Type	38-4
Forwarding Class	38-4
Frame Type	38-4
ID	38-4
Mask	38-4
Mask	38-5
Mask	38-5
Mask	38-5
Maximum Burst Size (kbps)	38-5
Meter ID	38-6
Mode	38-6
MultiPoint	38-6
Multicast Meter ID	38-6
Number of Qos Classifiers	38-7
PIR (kbps)	38-7
PIR Adaptation	38-7
Rate Mode	38-7
Scope	38-7
Source MAC	38-7
Unknown Meter ID	38-8

39 — Access Egress parameters 39-1

39.1	Access Egress parameters	39-2
	Auto-Assign ID	39-2
	CIR (kbps)	39-2
	CIR Level	39-2
	CIR Level	39-2
	CIR Weight	39-2
	CIR Weight	39-2
	CIR Adaptation	39-2
	Committed Burst Size (kb)	39-2
	Description	39-2
	Destination IP	39-2
	Destination Port	39-2
	Displayed Name	39-3
	dot1p	39-3
	DSCP	39-3
	Dst Mask	39-3
	Expedite	39-3
	Force DE value	39-3
	Forwarding Class	39-3
	Fragment	39-3
	High Priority Reserved	39-3
	HSMDA Egress Profiling	39-4
	HSMDA Packet Byte Offset (bytes)	39-4
	HSMDA Queue ID	39-4
	ID	39-4

ID	39-4
ID	39-4
In DSCP.....	39-4
In Precedence.....	39-5
In Profile.....	39-5
Level	39-5
Level	39-5
Low Burst Max Class	39-5
Mark DE bit.....	39-5
Maximum Burst Size (bytes)	39-5
Out DSCP	39-6
Out Profile	39-6
Out Precedence	39-6
Packet Byte Offset	39-6
Packet Byte Offset	39-6
Packet Byte Offset	39-6
Parent Arbiter	39-6
PIR (kbps).....	39-6
PIR Adaptation.....	39-7
Policer ID	39-7
Priority.....	39-7
Port Average Overhead (%)	39-7
Port Parent.....	39-7
Precedence.....	39-7
Profile.....	39-7
Protocol.....	39-7
Queue ID.....	39-7
Scheduler	39-7
Source IP.....	39-7
Source Port.....	39-8
Src Mask	39-8
Stats Mode.....	39-8
Traffic Control.....	39-8
Use As Multiclass MLPPP Policy For 7705 SAR.....	39-8
Use WRED Queue	39-9
Weight	39-9
Weight	39-9

40 — 7210 Access Egress parameters 40-1

40.1	7210 Access Egress parameters	40-2
	Auto-Assign ID.....	40-2
	CIR Adaptation.....	40-2
	CIR (kbps).....	40-2
	Description	40-2
	Displayed Name	40-2
	Forwarding Class	40-2
	ID	40-2
	ID	40-2
	In Profile.....	40-2
	Out Profile	40-3
	PIR (kbps).....	40-3

	PIR Adaptation.....	40-3
	Scope	40-3
41 —	ATM QoS parameters	41-1
41.1	ATM QoS parameters	41-2
	Auto-Assign ID.....	41-2
	CDVT	41-2
	CLP Tagging	41-2
	Description	41-2
	Descriptor Type.....	41-2
	Displayed Name(displayedName)	41-3
	Domain Name	41-3
	MBS (cells).....	41-3
	MIR (kbps)	41-3
	MDCR	41-3
	PCR	41-4
	PIR (kbps).....	41-4
	Shaping	41-4
	SIR (kbps).....	41-4
42 —	MLPPP Ingress QoS Profile parameters	42-1
42.1	MLPPP Ingress QoS Profile parameters.....	42-2
	Auto-Assign ID.....	42-2
	Description	42-2
	Profile ID	42-2
	Reassembly Timeout (msec).....	42-2
43 —	MLPPP Egress QoS Profile parameters	43-1
43.1	MLPPP Egress QoS Profile parameters	43-2
	Auto-Assign ID.....	43-2
	Description	43-2
	Maximum Queue Size (msec)	43-2
	MIR (%)	43-2
	MLPPP Class	43-2
	Profile ID	43-3
	Weight (%).....	43-3
44 —	MCFR Ingress QoS Profile parameters	44-1
44.1	MCFR Ingress QoS Profile parameters.....	44-2
	Auto-Assign ID.....	44-2
	Description	44-2
	Profile ID	44-2
	Reassembly Timeout (msec).....	44-2

45 —	MCFR Egress QoS Profile parameters	45-1
45.1	MCFR Egress QoS Profile parameters.....	45-2
	Auto-Assign ID.....	45-2
	Description	45-2
	Maximum Queue Size (msec)	45-2
	MIR (%)	45-2
	Profile ID	45-2
	Weight (%)	45-2
46 —	Network parameters	46-1
46.1	Network parameters.....	46-2
	Auto-Assign ID.....	46-2
	Default FC	46-2
	Default FC Profile	46-2
	Description	46-2
	Displayed Name	46-2
	Dot1p.....	46-2
	Dot1p In Profile.....	46-2
	Dot1p Out Profile.....	46-3
	DSCP.....	46-3
	DSCP In Profile.....	46-3
	DSCP Out Profile.....	46-4
	Force DE value.....	46-4
	Force DSCP Remark	46-5
	Forwarding Class	46-5
	ID	46-5
	LER Use DSCP	46-5
	LSP Exp	46-5
	LSP Exp In Profile	46-6
	LSP Exp Out Profile	46-6
	Mark DE bit.....	46-6
	Profile.....	46-6
	Queue ID.....	46-6
	Remark.....	46-6
	Use Queue Group.....	46-7
47 —	7210 Network parameters	47-1
47.1	7210 Network parameters	47-2
	Auto-Assign ID.....	47-2
	CIR Adaptation.....	47-2
	CIR (kbps).....	47-2
	Committed Burst Size (kbps)	47-2
	Default FC	47-2
	Default FC Profile	47-2
	Description	47-2
	Displayed Name	47-3
	Dot1p.....	47-3
	Dot1p In Profile.....	47-3
	Dot1p Out Profile.....	47-3
	DSCP.....	47-3

	DSCP In Profile.....	47-3
	DSCP Out Profile.....	47-4
	Forwarding Class	47-4
	ID	47-4
	LSP Exp	47-4
	LSP Exp In Profile	47-4
	LSP Exp Out Profile	47-5
	Maximum Burst Size (kbps)	47-5
	Meter	47-5
	Mode	47-5
	MultiCast-Meter	47-6
	MultiPoint	47-6
	Nw Mgr ID.....	47-6
	PIR Adaptation.....	47-6
	PIR (kbps).....	47-6
	Policy Id	47-6
	Profile.....	47-7
	Remark.....	47-7
	Scope.....	47-7
	Type.....	47-7
48 —	Network Queue parameters	48-1
48.1	Network Queue parameters	48-2
	Burst Limit (bytes)	48-2
	CIR (%)	48-2
	CIR Adaptation.....	48-2
	CIR Level.....	48-2
	CIR Weight.....	48-2
	Committed Burst Size (%)	48-3
	Description	48-3
	Displayed Name	48-3
	Egress HSMDA Queue ID	48-3
	Forwarding Class	48-3
	High Priority Reserved (%)	48-3
	Level	48-4
	Maximum Burst Size (bytes)	48-4
	Maximum Burst Size (%)	48-4
	Multicast.....	48-4
	Multipoint Queue ID.....	48-4
	PIR (%).....	48-5
	Queue ID.....	48-5
	PIR Adaptation.....	48-5
	Port Average Overhead (%)	48-5
	Port Parent.....	48-5
	Weight	48-6
49 —	7210 Network Queue parameters	49-1
49.1	7210 Network Queue parameters.....	49-2
	CIR (%)	49-2
	CIR Adaptation.....	49-2

	Description	49-2
	Displayed Name	49-2
	PIR (%).....	49-2
	PIR Adaptation.....	49-2
50 —	Shared Queue parameters	50-1
50.1	Shared Queue parameters	50-2
	CIR (%)	50-2
	Committed Burst Size (%)	50-2
	Description	50-2
	High Priority Reserved (%)	50-3
	Maximum Burst Size (%)	50-3
	PIR (%).....	50-3
51 —	WRED Slope parameters	51-1
51.1	WRED Slope parameters.....	51-2
	Description	51-2
	Displayed Name	51-2
	High Slope	51-2
	Low Slope.....	51-2
	Max Avg.	51-2
	Max Prob.	51-3
	Start Average	51-3
	Time Average Factor (weight)	51-3
52 —	7210 Slope parameters	52-1
52.1	7210 Slope parameters	52-2
	Administrative State	52-2
	Description	52-2
	Displayed Name	52-2
	Queue1 Drop Rate.....	52-2
	Queue2 Drop Rate.....	52-2
	Queue3 Drop Rate.....	52-3
	Queue4 Drop Rate.....	52-3
	Queue5 Drop Rate.....	52-3
	Queue6 Drop Rate.....	52-3
	Queue7 Drop Rate.....	52-3
	Queue8 Drop Rate.....	52-3
	Start Threshold	52-3
53 —	HSMDA WRED Slope parameters	53-1
53.1	HSMDA WRED Slope parameters	53-2
	Administrative State	53-2
	Description	53-2
	Displayed Name	53-2
	HSMDA High Slope	53-2
	HSMDA Low Slope	53-2
	Max Depth	53-2

	Max Probability	53-3
	Queue MBS (bytes)	53-3
	Start Depth	53-3
54 —	Scheduler parameters	54-1
54.1	Scheduler parameters	54-2
	CIR (kbps)	54-2
	CIR Level	54-2
	CIR Weight	54-2
	Description	54-2
	Displayed Name	54-2
	Frame Based Accounting	54-3
	Level	54-3
	Parent Scheduler	54-3
	PIR (kbps)	54-3
	Port Parent	54-4
	Summed CIR	54-4
	Tier	54-4
	Weight	54-4
55 —	Port Scheduler parameters	55-1
55.1	Port Scheduler parameters	55-2
	CIR (kbps)	55-2
	CIR (kbps)	55-2
	CIR (kbps)	55-2
	CIR (kbps)	55-2
	CIR (kbps)	55-2
	CIR (kbps)	55-2
	CIR (kbps)	55-3
	CIR (kbps)	55-3
	CIR Level	55-3
	CIR Weight	55-3
	Description	55-3
	Displayed Name	55-4
	Level	55-4
	Maximum Rate (kbps)	55-4
	PIR (kbps)	55-4
	PIR (kbps)	55-4
	PIR (kbps)	55-5
	PIR (kbps)	55-5
	PIR (kbps)	55-5
	PIR (kbps)	55-5
	PIR (kbps)	55-5
	PIR (kbps)	55-5
	Weight	55-5
	Weight in group	55-6
	Weight in group	55-6
	Weight in group	55-6
	Weight in group	55-6
	Weight in group	55-6

Weight in group.....	55-6
Weight in group.....	55-6
Weight in group.....	55-7

56 — HSMDA Scheduler parameters 56-1

56.1	HSMDA Scheduler parameters	56-2
	Description	56-2
	Displayed Name	56-2
	Group	56-2
	Group	56-2
	Group	56-2
	Group	56-3
	Group	56-3
	Group	56-3
	Group	56-3
	Group	56-4
	Group	56-4
	Maximum Rate (Mbps)	56-4
	Rate (Mbps)	56-4
	Rate (Mbps)	56-5
	Rate (Mbps)	56-5
	Rate (Mbps)	56-5
	Rate (Mbps)	56-5
	Rate (Mbps)	56-5
	Rate (Mbps)	56-6
	Rate (Mbps)	56-6
	Rate (Mbps)	56-6
	Rate (Mbps)	56-6
	Rate (Mbps)	56-6
	Weight	56-6
	Weight	56-7
	Weight	56-7
	Weight	56-7
	Weight	56-7
	Weight	56-7
	Weight	56-8
	Weight	56-8
	Weight	56-8

57 — HSMDA WRR policy parameters 57-1

57.1	HSMDA WRR Policy parameters	57-2
	Description	57-2
	Displayed Name	57-2
	Class Aggregate Weight	57-2
	Include Queues	57-2
	Packet Byte Offset (bytes).....	57-2
	Schedule Using Class.....	57-2

58 —	7210 Port Scheduler parameters	58-1
58.1	7210 Port Scheduler parameters.....	58-2
	Description	58-2
	Displayed Name	58-2
	Mode	58-2
	Weight	58-2
	Weight	58-2
	Weight	58-3
	Weight	58-3
	Weight	58-3
	Weight	58-3
	Weight	58-3
	Weight	58-3
59 —	Policer Control parameters	59-1
59.1	Policer Control parameters.....	59-2
	Arbiter Name.....	59-2
	Cumulative MBS Contribution	59-2
	Description	59-2
	Displayed Name	59-2
	Fixed MBS contribution.....	59-2
	Frame Based Bandwidth Rate	59-2
	Level	59-2
	Maximum Frame Based Bandwidth	59-2
	Minimum Separation Buffer Space.....	59-3
	Parent Arbiter	59-3
	Priority Level	59-3
	Tier	59-3
	Weight	59-4
60 —	HSMDA Pool parameters	60-1
60.1	HSMDA pool parameters.....	60-2
	Allocation Percent	60-2
	Allocation Percent	60-2
	Allocation Percent	60-2
	Allocation Percent	60-3
	Allocation Percent	60-3
	Allocation Percent	60-3
	Allocation Percent	60-3
	Allocation Percent	60-3
	Allocation Percent	60-4
	Allocation Weight	60-4
	Allocation Weight	60-4
	Allocation Weight	60-5
	Allocation Weight	60-5
	Allocation Weight	60-5
	Allocation Weight	60-5
	Allocation Weight	60-5
	Allocation Weight	60-6
	Allocation Weight	60-6

	Default	60-6
	Description	60-6
	Displayed Name	60-6
	Root Parent	60-6
	Root Parent	60-7
	Root Parent	60-7
	Root Parent	60-7
	Root Parent	60-7
	Root Parent	60-7
	Root Parent	60-7
	Root Parent	60-7
	Root Parent	60-8
	System Reserve (%)	60-8
61 —	Named Buffer Pool parameters	61-1
61.1	Named buffer pool parameters	61-2
	Access Weight.....	61-2
	Default Reserved CBS.....	61-2
	Default Weight.....	61-2
	MDA Weight	61-2
	Network Weight	61-2
	Pool Name	61-2
	Port Weight	61-3
	Reserved CBS (%)	61-3
62 —	Ingress Queue Group Template parameters	62-1
62.1	Ingress Queue Group Template parameters	62-2
	Cir (kbps)	62-2
	Cir Adaptation	62-2
	CIR Level.....	62-2
	CIR Weight.....	62-2
	Committed Burst Size (kb).....	62-2
	Description	62-2
	Displayed Name	62-2
	Expedite	62-2
	High Priority Reserved.....	62-2
	ID	62-2
	Level	62-3
	Maximum Burst Size (bytes)	62-3
	Mode	62-3
	Multicast.....	62-3
	Named Buffer Pool	62-3
	Pir (kbps)	62-3
	Pir Adaptation	62-3
	Policed	62-3
	Scheduler	62-3
	Weight	62-3

63 —	Egress Queue Group Template parameters	63-1
63.1	Egress Queue Group Template parameters	63-2
	CIR	63-2
	CIR (Percentage)	63-2
	CIR Level	63-2
	CIR Weight	63-2
	CIR Adaptation	63-2
	Committed Burst Size	63-2
	Description	63-2
	Displayed Name	63-2
	Expedite	63-2
	Forwarding Class	63-3
	High Priority Reserved	63-3
	ID	63-3
	Level	63-3
	Maximum Burst Size	63-3
	Named Buffer Pool	63-3
	PIR	63-3
	PIR (Percentage)	63-3
	PIR Adaptation	63-3
	Port Parent	63-4
	Queue ID	63-4
	Rate Type	63-4
	Scheduler	63-4
	Use WRED Queue	63-4
	Weight	63-4
64 —	7705 SAR Fabric parameters	64-1
64.1	7705 SAR Fabric parameters	64-2
	Aggregate Rate	64-2
	Auto-Assign ID	64-2
	Description	64-2
	Displayed Name	64-2
	ID	64-2
	Mode	64-2
	MultiPoint Rate	64-2
	Rate To MDA (destRateTo1<card#>)	64-3
65 —	7250 SAS and Telco QoS parameters	65-1
65.1	7250 SAS and Telco QoS parameters	65-2
	Auto-Assign ID	65-2
	Color	65-2
	Description	65-2
	Displayed Name	65-2
	Drop Algorithm	65-2
	DSCP	65-2
	DSCP Value	65-3
	Filter ID	65-3
	Priority	65-3
	Queue Algorithm	65-3

Shaper Rate	65-4
Traffic Class	65-4
Txq 0	65-4
Txq 1	65-5
Txq 2	65-5
Txq 3	65-5
Txq 4	65-5
Txq 5	65-5
Txq 6	65-6
Txq 7	65-6

66 — AOS QoS Policies parameters 66-1

66.1	AOS QoS Policies parameters	66-2
	Action	66-2
	Destination IP	66-2
	Destination IP Port (End)	66-2
	Destination IP Port (Start)	66-2
	Destination LAG	66-3
	Destination MAC	66-3
	Destination Mask	66-3
	Destination Mask	66-3
	Destination Net Mask	66-3
	Destination Port	66-3
	Destination Port	66-4
	Destination Slot	66-4
	Differentiated Services Code Point	66-4
	Displayed Name	66-5
	ICMP Code	66-5
	ICMP Type	66-5
	IP Protocol	66-5
	LAG Number	66-6
	List Type	66-6
	Mask	66-7
	Mask	66-7
	Mask	66-7
	Match Destination IP Port Range	66-7
	Match Destination Port	66-7
	Match Source IP Port Range	66-8
	Match Source Port	66-8
	Maximum Bandwidth (Kbps)	66-8
	Policy Status	66-8
	Port	66-8
	Precedence	66-8
	Priority	66-9
	Priority	66-9
	Share Resources	66-9
	Slot	66-9
	Source IP	66-9
	Source IP Port (End)	66-10
	Source IP Port (Start)	66-10
	Source MAC	66-10

	Source Mask	66-10
	Source Mask	66-10
	Source Net Mask	66-10
	Source Port	66-11
	Source Slot	66-11
	Source VLAN	66-11
	ToS Precedence	66-11
	Type of Service	66-11
	VRF Status	66-11
	VRF Name	66-12
67 —	9500 ATM QoS parameters	67-1
67.1	ATM QoS parameters	67-2
	Auto-Assign ID	67-2
	CDVT (microseconds)	67-2
	Displayed Name(displayedName)	67-2
	Domain Name	67-2
	MDCR	67-2
	PCR (cells/second)	67-2
68 —	ACL MAC Filter parameters	68-1
68.1	ACL MAC Filter parameters	68-2
	Action	68-2
	Administrative State	68-2
	ATM VCI	68-2
	Auto-Assign ID	68-2
	Default Action	68-2
	Description	68-2
	Destination MAC	68-2
	Displayed Name	68-2
	Dot1p	68-3
	Dot1p Mask	68-3
	Dst Mask	68-3
	Entry ID	68-3
	Ether Type	68-3
	Filter ID	68-3
	Frame Type	68-3
	Inner Encap Value	68-4
	MAC Filter Type	68-4
	Outer Encap Value	68-4
	Path ID	68-5
	Port Name	68-5
	SNAP OUI	68-5
	SNAP PID	68-5
	Source MAC	68-5
	Src Mask	68-5
	VC ID	68-5

69 — ACL IP Filter parameters 69-1

69.1	ACL IP Filter parameters	69-2
	Action	69-2
	Administrative State	69-2
	Auto-Assign ID.....	69-2
	Cflowd If Sample	69-2
	Cflowd Sample.....	69-2
	Credit Control Count.....	69-2
	Credit Control Start Entry	69-2
	Description	69-3
	Displayed Name	69-3
	DSCP.....	69-3
	Entry ID	69-3
	Filter ID	69-3
	Forward NH.....	69-3
	Forward NH Interface.....	69-3
	Fragment	69-3
	High WaterMark (%)	69-3
	ICMP Code	69-3
	ICMP Type	69-4
	Inner Encap Value	69-4
	IP Option.....	69-4
	IP Opt Mask.....	69-4
	Is Indirect.....	69-4
	Low WaterMark (%).....	69-4
	Multiple Option	69-4
	Option Present.....	69-4
	Outer Encap Value	69-4
	Path ID	69-5
	Port Name	69-5
	Protocol.....	69-5
	RADIUS Count	69-5
	RADIUS Start Entry	69-5
	Remark Dot1p.....	69-5
	Remark DSCP.....	69-5
	Remark DSCP Mask	69-5
	Source IP.....	69-5
	Source Port.....	69-6
	Src Mask	69-6
	TCP Ack	69-6
	TCP Syn	69-6
	VC ID	69-6

70 — ACL IPv6 Filter parameters 70-1

70.1	ACL IP and ACL IPv6 Filter parameters	70-2
	Action	70-2
	Administrative State	70-2
	Auto-Assign ID.....	70-2
	Credit Control Count.....	70-2
	Credit Control Start Entry	70-2
	Default Action	70-2

	Description	70-2
	Destination IP	70-2
	Dest Port.....	70-2
	Displayed Name	70-2
	DSCP.....	70-2
	Dst Mask	70-3
	Entry ID	70-3
	Filter ID.....	70-3
	High WaterMark (%)	70-3
	ICMP Code	70-3
	ICMP Type	70-3
	Log ID	70-3
	Low WaterMark (%).....	70-3
	Protocol.....	70-3
	RADIUS Count	70-3
	RADIUS Start Entry	70-3
	Source IP.....	70-3
	Source Port.....	70-3
	Src Mask	70-4
	TCP Ack	70-4
	TCP Syn	70-4
71 —	7250 SAS and Telco ACL Standard IP Filter parameters	71-1
71.1	7250 SAS and Telco ACL Standard IP Filter parameters	71-2
	Action	71-2
	Description	71-2
	Displayed Name	71-2
	Filter ID.....	71-2
	Loggable	71-2
	Source IP.....	71-2
	Src Mask	71-3
	VLAN Priority Tag	71-3
72 —	7250 SAS and Telco ACL Extended IP Filter parameters	72-1
72.1	7250 SAS and Telco ACL Extended IP Filter parameters	72-2
	Action	72-2
	Description	72-2
	Dest Mask	72-2
	Destination IP	72-2
	Displayed Name	72-2
	Filter ID.....	72-2
	Loggable	72-3
	Precedence.....	72-3
	Protocol.....	72-3
	Source IP.....	72-4
	Src Mask	72-4
	TOS	72-4
	VLAN Priority Tag	72-5

73 — 7250 SAS and Telco ACL IGMP Filter parameters 73-1

73.1	7250 SAS and Telco ACL IGMP Filter parameters.....	73-2
	Action	73-2
	Auto-Assign ID.....	73-2
	Description	73-2
	Dest Mask	73-2
	Destination IP	73-2
	Displayed Name	73-2
	Filter ID	73-3
	IGMP Option.....	73-3
	Loggable	73-3
	Name	73-3
	Source IP.....	73-3
	Src Mask	73-4

74 — 7250 SAS and Telco ACL MAC Filter parameters 74-1

74.1	7250 SAS and Telco ACL MAC Filter parameters.....	74-2
	Action	74-2
	Description	74-2
	Destination MAC	74-2
	Displayed Name	74-2
	Dst Mask	74-2
	Filter ID	74-2
	Loggable	74-3
	Pattern.....	74-3
	Pattern Mask	74-3
	Source MAC.....	74-3
	Src Mask	74-3

75 — Multicast Package parameters 75-1

75.1	Multicast Package parameters	75-2
	Channel	75-2
	Cost.....	75-2
	Description	75-2
	ID	75-2
	IGMP Option.....	75-2
	Is Root Catalogue.....	75-3
	Loggable	75-3
	Multicast Address.....	75-3
	Name	75-3

76 — Egress Multicast Group parameters 76-1

76.1	Egress Multicast Group parameters	76-2
	Description	76-2
	Destination Chain Limit	76-2
	Displayed Name	76-2
	Dot1 Q Ethertype.....	76-2
	Encapsulation Type	76-2

	QinQ Ethertype	76-2
	QinQ Fixed Tag Value	76-3
77 —	Multicast CAC parameters	77-1
77.1	Multicast CAC parameters	77-2
	Administrative State	77-2
	Bandwidth (kbps)	77-2
	Class	77-2
	Default Action	77-2
	Description	77-2
	End Address	77-3
	Max Bandwidth (kbps)	77-3
	Name	77-3
	Start Address	77-3
	Type	77-3
78 —	Ingress Multicast Path Management parameters	78-1
78.1	Ingress Multicast Path Management parameters	78-2
	Address	78-2
	Admin BW Use Threshold (kbps)	78-2
	Admin State	78-2
	Administrative BW (kbps)	78-2
	Administrative State	78-3
	Ancillary Path Limit (mbps)	78-3
	Black Hole Rate (kbps)	78-3
	Buffer Size	78-3
	BW Decision	78-3
	Channel Type	78-4
	Committed Buffer Space (%)	78-4
	Congestion Priority Threshold	78-4
	Continuity Counter Error	78-4
	Description	78-5
	Description	78-5
	Destination Address	78-5
	Destination UDP Port	78-5
	Displayed Name	78-5
	ECMP Optimization Threshold	78-5
	End Address	78-5
	Explicit Path	78-5
	Falling Delay (seconds)	78-6
	Falling Percent Reset (%)	78-6
	FCC Burst	78-6
	FCC MC Handover Rate	78-7
	FCC Server	78-7
	FCC Server Mode	78-7
	High Bandwidth Alarm	78-7
	High Bandwidth Multicast Traffic Taps Group	78-8
	High Bandwidth Source	78-8
	High Priority Traffic (%)	78-8
	Ingress LER	78-9

Local Server	78-9
Max Delay (Deciseconds)	78-9
Max IGMP Latency	78-9
Max Number of Sessions	78-9
Maximum Buffer Space (%).....	78-9
Min Duration (msec)	78-10
Name	78-10
Name	78-10
Name	78-10
Non Video PID Absent Intv (msec)	78-10
Number of Secondary T2 Paths	78-11
P2MP ID for LDP	78-11
P2MP LSP Name.....	78-11
PAT Repetition Error.....	78-11
PAT Syntax	78-11
Path Limit (mbps)	78-11
PCR Repetition Error.....	78-12
Percentage of Total pool (%)	78-12
PMT Repetition Error	78-12
PMT Syntax Error	78-12
Preference Level	78-12
Primary Interface	78-13
Primary Path Limit (mbps).....	78-13
QoS (msec)	78-13
QoS (msec)	78-13
QoS (msec)	78-13
Re-order Audio Interval (msec)	78-14
Reserved CBS (%)	78-14
RT Payload Type.....	78-14
RT Rate	78-14
(RT) Server	78-14
SCTE35 Error	78-15
Secondary Interface	78-15
Secondary Path Limit (mbps).....	78-15
Source Address	78-15
Source Address	78-15
Start Address.....	78-15
TEI Error	78-15
TNC (msec).....	78-16
TNC (msec).....	78-16
TNC (msec).....	78-16
TOA (msec).....	78-16
TOA (msec).....	78-16
TOA (msec).....	78-16
TS Sync Loss Error	78-17
Unreferenced PID Error	78-17
Video Group ID.....	78-17
Video PID Absent Interval (msec).....	78-17

79 — Time of Day parameters 79-1

79.1	Time of Day parameters	79-2
	End Run Day	79-2
	End Time	79-2
	Frequency	79-2
	Name	79-2
	Ongoing	79-2
	Priority	79-3
	Start Run Day	79-3
	Start Time	79-3

80 — Routing parameters 80-1

80.1	Routing parameters	80-2
	Action	80-2
	All Instances	80-2
	BGP AS Path Name	80-3
	Begin Length	80-3
	BGP AS Path Action	80-3
	BGP AS Prepend number	80-3
	BGP Local Preference	80-4
	Check Dependencies	80-4
	Community Action 1	80-4
	Community Action 2	80-5
	Community List Name	80-5
	Community Member	80-5
	Community Member	80-6
	Community Name	80-6
	Community Name 1	80-7
	Community Name 2	80-7
	Damping Name	80-7
	Damping Profile Name	80-7
	Default Action	80-7
	Description	80-8
	Displayed Name	80-8
	Entry ID	80-8
	Half Life	80-9
	IGMP Host Prefix List Name	80-9
	Instance ID	80-9
	Interface	80-9
	Interface Name	80-10
	IS-IS External Route	80-10
	Level	80-10
	Local Preference Set	80-10
	Mask	80-11
	Max Suppression	80-11
	Metric Action	80-11
	Metric Value	80-12
	Multicast Group Prefix List Name	80-12
	Multicast Source IP Address	80-12
	Neighbor IP Address	80-12
	Neighbor Prefix List Name	80-12

Next Hop.....	80-12
Next Hop Self	80-13
Next Hop Type.....	80-13
No Route Tag.....	80-13
Origin.....	80-13
OSPF Area	80-14
OSPF Area Set.....	80-14
OSPF, RIP, or ISIS Tag (Hex)	80-14
OSPF Route Type	80-15
Path Name.....	80-15
Policy Statement Name	80-15
Prefix.....	80-16
Prefix List 1	80-16
Prefix List 2	80-16
Prefix List 3	80-16
Prefix List 4	80-16
Prefix List 5	80-16
Prefix List Name.....	80-16
Prefix List Flag.....	80-16
Prepend Count.....	80-17
Protocol.....	80-17
Regular Expression	80-17
Reuse	80-18
Route Origin.....	80-19
Route Preference	80-19
Static Route Tag.....	80-19
Suppress	80-19
Through Length.....	80-20
Triggered Re-evaluation of Route Policies	80-20
Type.....	80-20
Use Next Hop	80-21
Value	80-21
View the newly created Policy Statement	80-21

81 — VRRP parameters

81-1

81.1	VRRP parameters.....	81-2
	Displayed Name	81-2
	Delta in Use Limit	81-2
	Description	81-2
	Hold Clear (seconds).....	81-2
	Hold Set (seconds)	81-2
	Hop Address.....	81-2
	ID	81-3
	Interface Name	81-3
	Interval for Echo Request (seconds).....	81-3
	IP Address	81-3
	LAG ID.....	81-3
	Less Specific	81-3
	Limit of Echo Request Failures.....	81-4
	Mask	81-4
	Number of Ports Down	81-4

	Priority	81-4
	Priority Type	81-4
	Protocol	81-5
	Timeout for Echo Request (seconds)	81-5
82 —	MPLS parameters	82-1
82.1	MPLS parameters	82-2
	Backup Type	82-2
	Description	82-2
	Displayed Name	82-2
	Enable CSPF	82-2
	Enable TE Metric	82-2
	Fast Reroute	82-3
	Hop Limit	82-3
	Make before Break	82-3
	Record Actual Path	82-4
	Record Label	82-4
	Reserved Bandwidth	82-4
	Retry Limit	82-4
	Retry Timer (seconds)	82-4
	Value	82-4
83 —	Auto Tunnels parameters	83-1
83.1	Auto Tunnels parameters	83-2
	Administrative	83-2
	Auto-Rule Execution	83-2
	Class Forwarding Capability	83-2
	Description	83-2
	Enable LDP-over-RSVP	83-2
	Group Name	83-2
	Name	83-3
	Naming Format	83-3
	Order	83-3
	Template Versions	83-3
	Tunnel Creation Pacing Interval (seconds)	83-3
	Tunnel Type	83-3
	Underlying Transport	83-4
	User Specified Naming Prefix	83-4
	View the newly created tunnel	83-4
84 —	RADIUS Based Accounting parameters	84-1
84.1	RADIUS Based Accounting parameters	84-2
	Access Algorithm	84-2
	Calling Station ID Type	84-2
	Enable	84-2
	Host Accounting Message	84-2
	Port	84-3
	Port Binary Specification	84-3
	Port Prefix String	84-3

	Port Prefix Type	84-3
	Port Suffix Type	84-4
	Port Type	84-4
	Port Type Value	84-4
	RADIUS Attributes	84-4
	Retry Attempts	84-5
	Router Instance.....	84-5
	Secret Name	84-6
	Server IP Address.....	84-6
	Session ID Format	84-6
	Source Address	84-6
	Timeout (seconds)	84-6
	Use Standard Accounting Attribute.....	84-7
	Value (minutes).....	84-7
85 —	ISA-IPsec Transform parameters	85-1
85.1	ISA_IPsec Transform parameters	85-2
	Authentication Algorithm	85-2
	Auto-Assign ID.....	85-2
	Description	85-2
	Encryption Algorithm	85-2
	Policy ID	85-3
86 —	IPsec Static Security Association parameters	86-1
86.1	IPsec Static Security Association parameters.....	86-2
	Authentication Algorithm	86-2
	Authentication Key.....	86-2
	Authentication Key Type	86-2
	Auto-Assign ID.....	86-2
	Direction.....	86-3
	Protocol.....	86-3
	Security Parameter Index	86-3
	Static SA Description	86-3
	Static SA Name	86-3
87 —	ISA-IPsec Tunnel Template parameters	87-1
87.1	ISA-IPsec Tunnel Template parameters.....	87-2
	Auto-Assign ID.....	87-2
	Description	87-2
	Policy ID	87-2
	Replay Window	87-2
	Reverse Route	87-2
88 —	IKE Policy parameters	88-1
88.1	IKE Policy parameters	88-2
	Authentication Algorithm	88-2
	Authorization Method.....	88-2
	Auto-Assign ID.....	88-2

	Dead Peer Detection (DPD)	88-2
	Description	88-3
	Diffie-Hellman (DH) Group.....	88-3
	Encryption Algorithm	88-3
	Force Keep Alive	88-4
	ID	88-4
	Internet Security Association and Key Management Life Time (seconds)	88-4
	Interval	88-4
	IPsec Life Time (seconds)	88-4
	Keep Alive Interval.....	88-4
	Max Retries.....	88-5
	Mode	88-5
	NAT Traversal.....	88-5
	Perfect Forward Secrecy (PFS).....	88-5
	PFS DH Group	88-6
	Version	88-6
89 —	NAT Policy parameters	89-1
89.1	NAT Policy parameters	89-2
	ALG Protocols	89-2
	Description	89-2
	Displayed Name	89-2
	Filtering.....	89-2
	High Watermark	89-2
	ICMP Query (sec)	89-3
	Low Watermark.....	89-3
	Port Reservation Count.....	89-3
	Priority Session Forwarding Class Set	89-3
	Reservation Count.....	89-3
	Session High Watermark.....	89-4
	Session Limit	89-4
	Session Low Watermark	89-4
	SIP (sec)	89-4
	TCP Established (sec).....	89-4
	TCP Syn (sec)	89-4
	TCP Time Wait (sec)	89-5
	TCP Transitory (sec)	89-5
	UDP (sec)	89-5
	UDP DNS (sec).....	89-5
	UDP Inbound Refresh	89-5
	UDP Initial (sec)	89-5
90 —	Application Assurance parameters	90-1
90.1	Application Assurance parameters	90-2
	Action	90-2
	Address	90-2
	Address	90-2
	Address	90-2
	Address Length	90-2

Address Length	90-3
Address Operator	90-3
Address Operator	90-3
Administrative State	90-3
Application Flag	90-3
Application Group Operator	90-4
Application Operator	90-4
ASO Characteristic	90-4
ASO Characteristic Default Value	90-4
ASO Characteristic Operator	90-4
ASO Characteristic Value	90-5
ASO Characteristic Value	90-5
Auto-Assign ID	90-5
Bit Rate High Watermark	90-5
Bit Rate Low Watermark	90-5
Capacity Cost	90-5
CBS (KB)	90-6
CIR (Kbps)	90-6
CIR	90-6
Collect Accounting Statistics	90-7
Custom Protocol Expression Direction	90-7
Custom Protocol Expression Offset	90-7
Description	90-7
DHCP	90-7
Displayed Name	90-8
Displayed Name	90-8
Displayed Name	90-8
Displayed Name	90-8
Displayed Name	90-8
Displayed Name	90-8
Divert	90-9
Drop	90-9
DSCP	90-9
DSCP Operator	90-10
Entry ID	90-10
ESM Subscriber	90-10
Forwarding Class	90-10
Flow Count (flows)	90-10
Flow Full High Watermark	90-11
Flow Full Low Watermark	90-11
Flow Setup High Watermark	90-11
Flow Setup Low Watermark	90-11
Flow Set-up Direction	90-11
Frustrated (milliseconds)	90-12
Frustrated (milliseconds)	90-12
Frustrated (milliseconds)	90-12
Frustrated (%)	90-12
Granularity	90-12
Group ID	90-13
Index	90-13
IP Protocol Number	90-13
IP Protocol Operator	90-14

ISA-AA Group ID.....	90-14
ISA-AA Partition ID	90-14
MBS (KB)	90-15
MBS (flows).....	90-15
Mean Total Delay Tolerated (milliseconds)	90-15
Mirror Source All Inclusive	90-15
Operator	90-15
Operator	90-15
Packet Loss Tolerated (%).....	90-16
Packet Rate High Watermark.....	90-16
Packet Rate Low Watermark	90-16
Partition ID	90-16
PIR (Kbps)	90-16
PIR	90-16
Policy ID	90-17
Port ID	90-17
Port High Value	90-17
Port High Value	90-17
Port Operator	90-17
Port Operator	90-18
Port Value/Low Value	90-18
Port Value/Low Value	90-18
Port Value Type	90-18
Port Value Type	90-18
Priority.....	90-18
Protocol Administrative State	90-19
Protocol Operator	90-19
Protocol Type	90-19
RADIUS	90-19
Remark DSCP In Profile.....	90-20
Remark DSCP Out Profile.....	90-20
Round Trip Time Tolerated (milliseconds)	90-21
SAP Subscriber	90-21
Server Address	90-21
Server Address Mask	90-22
Server Address Operator	90-22
Server Port First Packet Policy.....	90-22
Server Port High Value	90-22
Server Port Operator	90-23
Server Port Value Type.....	90-23
Server Port/Low Value	90-23
Service ID	90-23
Spoke Subscriber	90-24
String	90-24
String	90-24
Subscriber name.....	90-24
Subscriber Operator	90-24
SubscriberType	90-24
Threshold Administrative State	90-25
Total Delay Standard Deviation Tolerated (milliseconds)	90-25
Traffic Direction.....	90-25
Transit Subscriber	90-25

	Tunnel ID	90-25
	Type	90-26
	Type	90-26
91 —	802_1x parameters	91-1
91.1	802_1x parameters	91-2
	Accounting Port	91-2
	Administrative Status	91-2
	Authorization Port	91-2
	Description	91-2
	Displayed Name	91-2
	IP Address	91-2
	Password	91-2
	Request Timeout	91-3
	Retry Attempts	91-3
	Server Index	91-3
	Server Type	91-3
	Source Address	91-3
92 —	PBB MRP parameters	92-1
92.1	PBB MRP parameters	92-2
	Action	92-2
	Auto-Assign ID	92-2
	Default Action	92-2
	Description	92-2
	Entry ID	92-3
	High ISID	92-3
	Low ISID	92-3
	Name	92-3
	Scope	92-4
93 —	AOS Ethernet Service parameters	93-1
93.1	AOS Ethernet Service parameters	93-2
	802.1AB	93-2
	802.1x	93-2
	802.3ad	93-2
	AMAP	93-3
	Bandwidth Sharing	93-3
	CDP	93-4
	CVLAN Treatment	93-4
	Description	93-4
	Displayed Name	93-4
	DTP	93-4
	GVRP	93-5
	Ingress Bandwidth (Mb)	93-5
	LACPMARKER	93-5
	OAM	93-6
	MVRP	93-6
	PAGP	93-7

	Priority	93-7
	Priority Mapping	93-7
	PVST	93-7
	STP	93-8
	Tunnel MAC.....	93-8
	UDLD	93-8
	UPLINK	93-9
	VLAN.....	93-9
	VTP	93-10
94 —	Connection profile parameters	94-1
94.1	Connection profile policy parameters	94-2
	Connection Profile ID	94-2
	Description	94-2
	VCI	94-2
	VPI	94-2
95 —	Service PW Template parameters	95-1
95.1	Service PW Template parameters	95-2
	Auto-Assign ID.....	95-2
	Collect Stats	95-2
	Description	95-2
	Discard Unknown Source	95-2
	Egress Filter Type	95-2
	Enable Control Word.....	95-2
	IGMP Fast Leave	95-3
	IGMP General Query Interval (seconds).....	95-3
	IGMP Import Policy.....	95-3
	IGMP Last Member Interval (deciseconds).....	95-3
	IGMP Max Number Groups.....	95-3
	IGMP Max Number Sources Per Group.....	95-4
	IGMP Query Response Interval (seconds)	95-4
	IGMP Robust Count.....	95-4
	IGMP Send Queries	95-4
	IGMP Version	95-4
	Import Route Target	95-5
	Ingress Filter Type	95-5
	Limit MAC Move.....	95-5
	MAC Address Limit	95-5
	MAC Aging	95-5
	MAC Learning	95-5
	MAC Pinning	95-6
	Policy ID	95-6
	Restrict Protected Source	95-6
	Restrict Unprotected Destination.....	95-6
	Split Horizon Group Name	95-6
	Use Provisioned SDP	95-7
	VC Type.....	95-7
	VLAN VC Tag	95-7

96 —	Residential Subscriber parameters	96-1
96.1	Residential Subscriber parameters	96-2
	Action	96-2
	Accounting Enabled	96-2
	Active	96-2
	Activity Threshold (kbps)	96-2
	Administrative State	96-2
	Administrative State	96-2
	Administrative Version	96-3
	Administrative State	96-3
	Aggregate Rate Limit (kbps)	96-3
	ANCP String	96-3
	Application	96-3
	Application Profile	96-4
	Application Profile String	96-4
	Authentication Key	96-4
	Assign Aggregate Rate Limit	96-4
	Average Frame Size	96-4
	BGP Keychain	96-4
	Circuit ID	96-5
	Circuit ID Format	96-5
	Cluster ID	96-5
	Connection Timer (seconds)	96-5
	Credit Control Server	96-5
	Credit Exhaust Threshold (%)	96-5
	Credit Type	96-5
	Credit Type Override	96-6
	Custom Option Number	96-6
	Days	96-6
	Default Application Profile	96-6
	Default Credit Time (seconds)	96-7
	Default Credit Type	96-7
	Default Credit Volume	96-7
	Default Credit Volume Unit	96-7
	Default Intermediate Destination Id Type	96-7
	Default Intermediate Destination Id	96-8
	Default SLA Profile	96-8
	Default Subscriber ID	96-8
	Default Subscriber Identification Policy	96-8
	Default Subscriber Identification Type	96-8
	Default Subscriber Profile	96-9
	Description	96-9
	Destination Host	96-9
	Destination IP	96-9
	Destination Name	96-9
	Destination Realm	96-9
	DHCP String	96-9
	Disable AC Cookies	96-10
	Disable SHCV	96-10
	Disable SHCV Hold Time (seconds)	96-10
	Disable SHCV Notification	96-10
	Displayed Name	96-10

Domain Name	96-11
DSCP	96-11
Dst Mask	96-11
Egress Aggregate Rate Limit (kbps)	96-11
Egress Aggregate Rate Limit (kbps)	96-11
Enable Reply On PADT	96-11
Encapsulation Offset	96-11
Encapsulation Offset Mode	96-12
Entry ID	96-12
Error Handling Action	96-12
Failover Support	96-13
Failure Handling	96-13
Fast Leave	96-13
Filter Direction	96-13
Fragment	96-13
Frame Base Accounting	96-13
Group Name	96-14
Host Limit	96-14
Host MAC	96-14
Host Name	96-14
Hours	96-14
Include RADIUS User	96-14
Ingress Aggregate Rate Limit (kbps)	96-14
Inner Encapsulation Value	96-15
Intermediate Destination	96-15
Intermediate Destination ID	96-15
IP Address	96-15
IP Address 1	96-15
IP Address 2	96-15
IP Address 3	96-16
IP Address 4	96-16
IP Address	96-16
IP Address Pool Name	96-16
IP Address Prefix Length	96-16
IP Option	96-16
IP Opt Mask	96-16
IPCP Subnet Negotiation	96-16
IPv6 Address	96-17
IPv6 Prefix	96-17
IPv6 Prefix Length	96-17
Last Active State Change	96-17
LCP Keep-Alive Hold Up Multiplier	96-17
LCP Keep-Alive Interval (seconds)	96-17
Local Address	96-18
MAC Address	96-18
MAC Address	96-18
Mandatory Bandwidth (kbps)	96-18
Match Type	96-18
Match Type	96-19
Match Type DHCP 1	96-19
Match Type DHCP 2	96-19
Match Type DHCP 3	96-20

Match Type DHCP 4	96-20
Match Type PPPoE 1	96-20
Match Type PPPoE 2	96-21
Match Type PPPoE 3	96-21
Maximum Cumulative Buffer Space	96-21
Maximum Frame Based Bandwidth	96-21
Maximum Host Lost Connectivity Rate (traps per second).....	96-21
Maximum Number of Groups	96-21
Maximum Sessions Per MAC	96-21
MD5 Authentication	96-22
MED Source	96-22
Minimum Separation Buffer Space.....	96-22
Minutes	96-22
Monitoring Period	96-22
MSAP Group Interface Name.....	96-22
MSAP Policy Name.....	96-22
MSAP Service ID.....	96-23
Multiple Option	96-23
Netbios Node Type.....	96-23
New Subscriber Identification.....	96-23
No Constraint	96-24
Non-Subscriber Traffic Application Profile	96-24
Non-Subscriber Traffic SLA Profile	96-24
Non-Subscriber Traffic Identification	96-24
Non-Subscriber Traffic Subscriber Profile	96-24
Number	96-24
Option.....	96-25
Option 60	96-25
Option Number	96-25
Option Present.....	96-25
Option Protocol.....	96-26
Option Type	96-26
Option Value	96-26
Origin Subscription ID.....	96-26
Out Of Credit Action	96-26
Outer Encapsulation Value.....	96-27
Packet Byte Offset (bytes).....	96-27
PADO Delay (100's of milliseconds)	96-27
Password Type.....	96-27
Password.....	96-27
PIR (kbps).....	96-28
Policy 1	96-28
Policy 2	96-28
Policy 3	96-28
Policy 4	96-28
Policy 5	96-28
Policy 1	96-28
Policy 2	96-29
Policy 3	96-29
Policy 4	96-29
Policy 5	96-29
Polling Interval	96-29

Port Number	96-29
PPP MTU	96-29
PPPoE Session ID.....	96-30
Preference	96-30
Prefix Length.....	96-30
Prefix String.....	96-30
Primary Script Administrative State.....	96-30
Primary Script URL	96-31
Profiled Traffic Only	96-31
Protocol.....	96-31
Protocol.....	96-31
RADIUS Called-Station-ID.....	96-31
Rate Adjustment	96-31
Rate Adjustment	96-31
Rate Exceeded Raises Alarm	96-32
Rate Modification	96-32
Rate Modification	96-32
Rate Modification Scheduler.....	96-32
Rate Modification Scheduler.....	96-32
Rate Modification Scheduler.....	96-33
Rate Monitor (kbps).....	96-33
Rate Monitor (kbps).....	96-33
Rate Monitor Notification	96-33
Rate Monitor Notification	96-33
Rate Reduction (kbps).....	96-33
Rate Reduction (kbps).....	96-34
Rating Group	96-34
Redirection Policy.....	96-34
Remote ID	96-34
Remote ID Format.....	96-34
Remove oldest Subscriber Host	96-34
Residential Subscriber Creation.....	96-35
Retail Service ID	96-35
Retention Time (hours).....	96-35
SAP ID	96-35
SAP ID	96-36
SAP ID	96-36
Scheduler Type	96-36
Secondary Script Administrative State.....	96-36
Secondary Script URL	96-36
Seconds	96-37
Server Address.....	96-37
Service Context ID	96-37
Service ID.....	96-37
Service ID.....	96-37
Service Name	96-37
SLA Profile String.....	96-38
SLA Profile String.....	96-38
Source IP.....	96-38
Src Mask	96-38
Static Multicast Group.....	96-38
Static Source	96-38

Strings From Option.....	96-38
Subscriber ID Alias	96-38
Subscriber ID	96-39
Subscriber Identification	96-39
Subscriber Identification	96-39
Subscriber Limit	96-39
Subscriber Mapped Profile String	96-39
Subscriber Mapped SLA Profile String	96-39
Subscriber Profile String	96-40
Subscriber Profile String	96-40
Subscription ID Type	96-40
Suffix Length	96-40
Suffix String	96-40
System ID	96-41
Tertiary Script Administrative State	96-41
Tertiary Script URL.....	96-41
Transaction Timer (seconds)	96-41
Trap Dropped Raises Alarm	96-41
Tx Timer (seconds).....	96-41
Type	96-42
Unconstrained Bandwidth (kbps)	96-42
Units.....	96-42
Use Client Pool	96-42
Use Direct Map as Default	96-42
Use Egress QoS Marking From SAP	96-43
Use GI Address.....	96-43
Use Multipoint Shared Queue.....	96-43
Use Shared Queue	96-43
User Name.....	96-44
User Name Format	96-44
Virtual Router Type	96-44
VLAN for all Services (Bridged)	96-44
VLAN for all Services (Routed)	96-44
VLAN per ISP per Service (Bridged).....	96-44
VLAN per ISP per Service (Routed)	96-45
VLAN per Service (Bridged)	96-45
VLAN per Service (Routed).....	96-45
VLAN per Subscriber (Bridged)	96-45
VLAN per Subscriber (Routed).....	96-45
Watchdog Timer (seconds).....	96-45

97 — Network and Service Audits policy parameters 97-1

97.1	Network and Service Audits policy parameters	97-2
	Auto-Assign ID.....	97-2
	Administrative State	97-2
	Description	97-2
	Enabled	97-2
	ID	97-2
	Remove Empty Service	97-2

98 —	Diameter Peer Profile parameters	98-1
98.1	Diameter Peer Profile parameters	98-2
	Application Type	98-2
	Auto-Assign ID.....	98-2
	Description	98-2
	Destination Realm.....	98-2
	Displayed Name	98-2
	Load Balance Enabled	98-2
	Peer Administrative State	98-2
	Peer ID	98-3
	Peer IP Address	98-3
	Peer Port	98-3
	Transport Protocol	98-3
99 —	Diameter Profile parameters	99-1
99.1	Diameter Profile parameters	99-2
	Connection Timer (s)	99-2
	Description	99-2
	Displayed Name	99-2
	DPR Timeout (s)	99-2
	IP DSCP.....	99-2
	IP TTL (s)	99-2
	Refresh Time (s).....	99-2
	Retry Count	99-3
	Retry Time (min)	99-3
	Transaction Timer (s).....	99-3
	Watch Dog Timer (s)	99-3
100 —	GTP Prime Server Group Profile parameters	100-1
100.1	GTP Prime Server Group Profile parameters	100-2
	Administrative State	100-2
	Administrative State	100-2
	Description	100-2
	Displayed Name	100-2
	Configuration File Limit (Mbytes).....	100-2
	Configuration File Limit (Mbytes).....	100-2
	Dead Time (seconds)	100-3
	Echo Interval (seconds)	100-3
	File Closure Lifetime (hours)	100-3
	File Closure Max Records.....	100-3
	File Closure Size (Mbytes).....	100-3
	File Extension	100-3
	File Obsolete Time (days).....	100-3
	File Private Info	100-4
	Inactive Time (minutes).....	100-4
	Maximum CDRs per PDU	100-4
	Maximum Requests.....	100-4
	Primary Compact Flash.....	100-4
	Primary Server Address.....	100-4
	Queue Size	100-5

	Retries	100-5
	Server Port	100-5
	Server Priority	100-5
	Time Out (seconds)	100-5
101	— GTP Profile parameters	101-1
101.1	GTP Profile parameters	101-2
	Description	101-2
	Displayed Name	101-2
	IP DSCP.....	101-2
	IP TTL	101-2
	Keep-Alive Retry Count	101-2
	Keep-Alive T3 Response Time (s)	101-2
	Keep-Alive Timeout (s).....	101-2
	Message Retransmit Retry Count	101-3
	Message Retransmit Timeout (s)	101-3
102	— PGW Charging Profile parameters	102-1
102.1	PGW Charging Profile parameters	102-2
	Charging Profile ID	102-2
	Description	102-2
	Offline Charging	102-2
	Time Limit (s).....	102-2
	Volume Limit.....	102-2
103	— PLMN List Group parameters	103-1
103.1	PLMN List Group parameters	103-2
	Displayed Name	103-2
	Description	103-2
	Mobile Country Code.....	103-2
	Mobile Network Code	103-2
104	— QCI Policy parameters	104-1
104.1	QCI Policy parameters.....	104-2
	Description	104-2
	Displayed Name	104-2
	DSCP for In Profile Packets	104-2
	DSCP for Out Profile Packets	104-2
	DSCP Preserve	104-3
	Forwarding Class Name.....	104-3
	Profile.....	104-3
105	— SGW Charging Profile parameters	105-1
105.1	SGW Charging Profile parameters	105-2
	Charging Profile ID	105-2
	Description	105-2
	Maximum Number of Changes.....	105-2

	MS Time Zone Changes	105-2
	Offline Charging	105-2
	QoS Change.....	105-2
	Time Limit (s).....	105-2
	User Location Change	105-2
	Volume Limit (Kbytes).....	105-2
106	— ANR Profile parameters	106-1
106.1	ANR Profile parameters	106-2
	Active Phase Measurement Report Hysteresis	106-2
	Active Phase Measurement Report Threshold	106-2
	Dormant Phase Timer For ECGI Discovery	106-2
	DRX Cycle For Report CGI.....	106-2
	Second Threshold EUTRAN RSRP	106-2
	Second Threshold EUTRAN RSRQ.....	106-3
	Threshold EUTRAN RSRP	106-3
	Threshold EUTRAN RSRQ	106-3
	UE Contribution In Wake Up Phase	106-3
107	— eNodeB IPsec Profile parameters	107-1
107.1	eNodeB IPsec Profile parameters	107-2
	Auto-Assign ID.....	107-2
	Description	107-2
	Displayed Name	107-2
	IKE Authentication Method	107-2
	IKE SA Life Duration (s).....	107-2
	IPsec Anti-Replay Windows Size	107-2
	IPsec Keep Alive Period	107-2
	IPsec Perfect Forward Secrecy.....	107-2
	IPsec Policy.....	107-3
	IPsec SA Life Duration (Kbytes/s).....	107-3
	IPsec SA Life Duration (s)	107-3
	IPsec Tunnel Address (IPv4)	107-3
	IPsec Tunnel Subnet Mask (IPv4).....	107-3
	Pre-Shared Secret	107-3
	SEG Address (IPv4)	107-4
108	— CPE Test-Head Profile parameters	108-1
108.1	CPE Test-Head Profile parameters	108-2
	Description	108-2
	Destination Endpoint	108-2
	Destination IP	108-2
	Destination MAC	108-2
	Destination Port	108-2
	Direction.....	108-2
	Drop Enable	108-2
	Ether Type.....	108-3
	Frame Size (bytes)	108-3
	Frame Type	108-3

	Name	108-3
	Pattern.....	108-3
	Priority.....	108-3
	Protocol.....	108-3
	Role	108-4
	Source Endpoint	108-4
	Source IP.....	108-4
	Source MAC.....	108-4
	Source Port.....	108-4
	TOS	108-4
	TTL	108-5
	Tx Rate (kbps)	108-5
	VLAN-Tag	108-5
109	— Remote Network Monitoring (RMON) parameters	109-1
109.1	Remote Network Monitoring (RMON) parameters	109-2
	Auto-Assign ID.....	109-2
	Community	109-2
	Description	109-2
	Displayed Name	109-2
	Falling Threshold	109-2
	ID	109-2
	Interval (seconds)	109-3
	Monitored Object OID	109-3
	Owner	109-3
	Rising Threshold	109-3
	Sample Type	109-4
	Start Up Alarm.....	109-4
	Type.....	109-4
110	— Size Constraint parameters	110-1
110.1	Size Constraint parameters	110-2
	Apply Threshold To	110-2
	Auto-Assign ID.....	110-2
	Description	110-2
	Objects To Be Deleted When Threshold Exceeded (# of objects)	110-2
	Policy Id	110-2
	Threshold (# of objects)	110-3
111	— Format and Range Policies parameters	111-1
111.1	Format and Range Policies parameters.....	111-2
	Administrative State	111-2
	Auto-Assign ID.....	111-2
	Auto Assign By Default	111-2
	Auto Assignment Enabled	111-2
	Copy Text From Position	111-2
	Default Value	111-2
	Displayed Text.....	111-2
	Mask	111-3

Maximum	111-3
Max. Length	111-3
Minimum	111-3
Min. Length.....	111-4
Name	111-4
Object Type	111-4
Policy ID	111-4
Priority	111-4
Property Name.....	111-4
Read Only.....	111-5
Source Object Name	111-5
Source Property Name.....	111-5
Tooltip Text	111-5
Through To Position.....	111-5
Unlimited	111-5

112 – Common Policies menu parameters 112-1

112.1	Common Policies menu parameters	112-2
	Action	112-2
	Administrative State	112-2
	Administrative State	112-2
	Administrative State	112-3
	Administrative State	112-3
	Application	112-3
	Auto-Assign ID.....	112-3
	Burst Limit (bytes)	112-3
	Burst Limit (kb).....	112-4
	Charging Profile ID	112-4
	CIR (kbps).....	112-4
	CIR (%)	112-5
	CIR Adaptation.....	112-5
	CIR Level.....	112-5
	CIR Level.....	112-5
	CIR Level.....	112-6
	CIR Percent (%)	112-6
	CIR Weight.....	112-7
	CIR Weight.....	112-7
	CIR Weight.....	112-7
	Committed Burst Size (kbps)	112-7
	Committed Burst Size (kb).....	112-7
	Configuration Mode	112-8
	Credit Control Count.....	112-8
	Credit Control Start Entry	112-8
	Default	112-8
	Default Action	112-9
	Default FC	112-9
	Description	112-9
	Destination IP	112-10
	Destination Port	112-10
	Dest Port.....	112-10
	Displayed Name	112-11

Distribution Mode	112-11
Dot1p	112-12
Dot1p In Profile	112-12
Dot1P-LSP-EXP-Shared In Profile	112-12
Dot1P-LSP-EXP-Shared Out Profile	112-12
Dot1p Out Profile	112-13
DSAP	112-13
DSAP Mask	112-13
DSCP	112-13
Dst Mask	112-14
Egress Remark	112-14
Entry ID	112-15
Ether Type	112-15
Expedite	112-15
Filter ID	112-16
Forwarding Class	112-16
Fragment	112-17
High Priority Reserved	112-17
High WaterMark (%)	112-17
HSMDA Counter Override	112-17
HSMDA Egress Profiling	112-17
HSMDA Packet Byte Offset	112-18
HSMDA Packet Byte Offset (bytes)	112-18
HSMDA Packet Byte Offset (bytes)	112-18
ICMP Code	112-18
ICMP Type	112-19
ID	112-19
In Profile	112-19
Ingress Meter	112-19
Ingress Meter Burst	112-20
Ingress Meter Rate (kbps)	112-20
Inner Encap Value	112-20
Inner Tag Value	112-20
Inner Tag VID Mask	112-20
IP Address	112-20
IP Option	112-21
IP Opt Mask	112-22
Level	112-22
Level	112-22
Level	112-22
Location	112-23
Loggable	112-23
Log ID	112-24
Low WaterMark (%)	112-24
MAC Monitoring	112-24
Max Average	112-24
Max Average	112-24
Max Average	112-24
Max Probability	112-25
Max Probability	112-25
Max Probability	112-25
Maximum Burst Size (kbps)	112-25

Maximum Burst Size (kb)	112-25
Maximum Burst Size (bytes)	112-25
Maximum Number of Changes	112-26
Maximum Queue Size (msec)	112-26
MIR (%)	112-26
MS Time Zone Change	112-26
Mode	112-27
Multipoint	112-27
Multiple Option	112-27
MultiPoint	112-28
Name	112-28
Named Buffer Pool	112-28
NE DoS Protection	112-29
New Entry ID	112-29
Offline Charging	112-29
Option Present	112-29
Out Profile	112-29
Outer Encap Value	112-30
Outer Tag Value	112-30
Outer Tag VID Mask	112-30
Override CIR	112-30
Override CIR Adaptation	112-31
Override Committed Burst Size	112-31
Override High Priority Reserved	112-31
Override Maximum Burst Size	112-31
Override Packet Offset	112-32
Override PIR	112-32
Override PIR Adaptation	112-32
Override Port Average Overhead	112-33
Override Queue CIR Weight	112-33
Override Queue Weight	112-33
Override Summed CIR	112-33
Packet Byte Offset	112-34
Parent Arbiter	112-34
Path ID	112-34
Peer IP Address	112-34
PIR (%)	112-34
PIR (kbps)	112-35
PIR Adaptation	112-35
PIR Percent (%)	112-35
Policed	112-36
Policer ID	112-36
Policing	112-36
Port Average Overhead (%)	112-37
Port Name	112-37
Port Parent	112-37
Precedence	112-37
Priority	112-37
Profile	112-38
Profile ID	112-38
Protocol	112-38
QoS Change	112-40

Queue CIR Weight	112-40
Queue ID	112-40
Queue Weight	112-40
RADIUS Count	112-41
RADIUS Start Entry	112-41
Rate Type	112-41
Reassembly Timeout (msec)	112-41
Redirect URL	112-42
Remarking	112-42
Scheduler button	112-42
Scope	112-42
Service Category	112-42
SGW Change	112-44
Source IP	112-44
Source Port	112-44
Src Mask	112-45
SSAP	112-45
SSAP Mask	112-45
Start Average	112-45
Start Average	112-46
Start Average	112-46
Stats Mode	112-46
Summed CIR	112-47
TCP Ack	112-47
TCP Syn	112-48
Termination of SDF	112-48
Time Average Factor	112-48
Time Limit per Rating Group (s)	112-49
Time Limit (s)	112-49
Type	112-49
Use WRED Queue	112-49
User Location Change	112-49
VC ID	112-50
VLAN Priority Tag	112-50
Volume Limit (Kbytes)	112-50
Volume Limit per Rating Group (kocetets)	112-50
Weight	112-51
Weight	112-51
Weight	112-51
Weight (%)	112-51
WRR Weight	112-52

113 – LTE LI delivery function peer parameters

113-1

113.1	LTE LI delivery function peer parameters	113-2
	Description	113-2
	Address	113-2
	Address	113-2
	ID	113-2
	Port	113-2
	Port	113-2

114	— LTE LI interception target parameters	114-1
114.1	LTE LI interception target parameters	114-2
	Content Type	114-2
	Description	114-2
	Target ID.....	114-2
	Target Type	114-2
	Content Type	114-2
115	— Trusted Peer List parameters	115-1
115.1	Trusted Peer List parameters	115-2
	Administrative State	115-2
	Displayed Name	115-2
	Description	115-2
	GTP Echo	115-2
	Mobile Country Code.....	115-2
	Mobile Network Code	115-2
	Node Type	115-3
	Peer IP Address	115-3
	Prefix.....	115-3
	Radio Access Technology.....	115-3

Tools menu parameters

116	— Service Test Manager parameters	116-1
116.1	Service Test Manager parameters	116-2
	Accounting Files	116-2
	Administrative State	116-2
	Age (seconds)	116-2
	Alarm Threshold (%)	116-2
	Alarm Clearing Threshold (%).....	116-2
	ANCP String	116-2
	ATM Interface ID.....	116-3
	Auto-Assign ID.....	116-3
	Bypass Routing.....	116-3
	Clear Alarm on Falling Threshold	116-3
	Continuously Executed	116-3
	Control MEP	116-4
	Control Plane	116-4
	Count.....	116-4
	Count.....	116-4
	Count.....	116-4
	Customer ID	116-5
	Data Pattern	116-5
	Data Size.....	116-5
	Data Size (octets)	116-5
	Description	116-5

Destination Address.....	116-5
Destination IP Address.....	116-5
Destination Path Address	116-6
Destination Type	116-6
DiffServ Field	116-6
DMR Frames Transmitted	116-6
DNS Name	116-6
DNS Server Address	116-7
DNS Server Type	116-7
Do Not Fragment	116-7
Duration (minutes).....	116-7
Egress Interface Index.....	116-7
Enable Test.....	116-8
Entity Type	116-8
EPS Path ID	116-8
First Run Execution Sequence	116-8
Flood	116-9
Force OAM.....	116-9
Forwarding Class	116-9
Forwarding Profile	116-10
From Access Gateway	116-10
From IP Address	116-10
Generate Alarm on Rising Threshold	116-10
Generator Frame Size (bytes)	116-11
Generator Tx Rate	116-11
ID	116-11
ID	116-11
ID	116-12
Ignore Probe Results	116-12
Include Falling Threshold	116-12
Increase Tx Rate Every Iteration.....	116-12
Inhibit Learning.....	116-12
Initial Time to Live.....	116-12
Interface Type	116-13
Interval (seconds)	116-13
Interval (seconds)	116-13
Interval	116-13
IP Address	116-13
IP Address	116-13
Last Run Execution Sequence	116-14
LDP Prefix	116-14
LDP Prefix Length	116-14
LDP Prefix Length	116-14
Lightweight Execution.....	116-15
Loopback Location (hex)	116-15
Maximum Concurrent Pings.....	116-15
Maximum Concurrent Traces	116-15
Maximum Failures.....	116-15
Maximum Hop.....	116-16
Maximum Number of Hops	116-16
Maximum Number of Results to Keep	116-16
Maximum Time to Live	116-16

MTU End Size (octets)	116-16
MTU Start Size (octets).....	116-17
MTU Step Size (octets)	116-17
Multicast Group.....	116-17
Multicast Source	116-17
Name	116-17
Name	116-18
Name	116-18
Name	116-18
NE Persistent.....	116-18
NE Schedulable	116-18
Next Hop Address	116-19
Next Hop Interface Address	116-19
Next Hop Interface Name	116-19
Number of Loopback Sent	116-19
Number of Test Iterations	116-19
Number of Test Probes	116-20
Packet Size (octets).....	116-20
Path ID	116-20
Port ID	116-21
Positional Data Pattern.....	116-21
Priority.....	116-21
Priority.....	116-21
Priority.....	116-21
Probe Failure Threshold.....	116-21
Probe History Size (rows)	116-22
Probe Interval (seconds)	116-22
Probe Timeout (seconds).....	116-22
Rapid	116-22
Reply Control	116-23
Reply Type	116-23
Reply Via Control Plane	116-23
Response Address	116-23
Retry Counter	116-23
Return LSP.....	116-24
Return Tunnel	116-24
Select All S2L Paths	116-24
Send Via Control Plane	116-24
Service Name	116-24
Site ID	116-24
Size (octets).....	116-25
Source Address	116-25
Source IP Address	116-26
Source MAC Address	116-26
Source Site ID	116-26
Strategy.....	116-26
Subscriber Ident String	116-26
System ID (Loopback Ip Address)	116-27
Target IP Address.....	116-27
Target MAC	116-27
Target MAC Address.....	116-27
Target Type	116-27

Target Type	116-27
Target Type	116-28
Test Failure Threshold	116-28
Test Iteration Duration	116-28
Threshold Reporting State	116-29
Threshold Value	116-29
Time To Live	116-29
Time To Wait (milliseconds)	116-29
Timeout	116-30
Timeout (seconds)	116-30
Timeout	116-30
Timeout (seconds)	116-30
Timeout (seconds)	116-30
Trap Generation	116-31
TTL	116-31
Type	116-31
Unlimited Concurrent Pings	116-31
Unlimited Concurrent Traces	116-32
Update Test Result Status	116-32
Use Local Tunnel	116-32
Use Remote Tunnel	116-33
Using EPS Path	116-33
Validation Test Suite	116-33
VC's Label Time Live	116-33
Virtual Router ID	116-33
VC Type	116-34
VLAN ID	116-34
VLAN Priority	116-34
VLAN VC Tag	116-34

117 – Ethernet CFM parameters 117-1

117.1	Ethernet CFM parameters	117-2
	AIS Enabled	117-2
	AIS Interval (seconds)	117-2
	AIS Meg Level	117-2
	AIS Priority	117-2
	Auto-Assign ID	117-2
	Auto MEG Site Creation	117-3
	CCM interval	117-3
	CCM Messages Enabled	117-3
	CFM Hold Down Timer (centiseconds)	117-3
	Data Size (octets)	117-3
	Description	117-4
	Direction	117-4
	Direction	117-4
	Direction	117-4
	Eth Test Enabled	117-5
	Eth Test Pattern	117-5
	Eth Test Threshold (number of bit errors)	117-5
	Facility Fault Notify	117-5
	Facility VLAN ID	117-6

Fault Alarm Time (centiseconds)	117-6
Fault Propagation	117-6
Fault Reset Time (centiseconds).....	117-6
ID	117-7
Id-Permission.....	117-7
Initial CCM Interval	117-7
Initial CFM Hold Down Timer (centiseconds).....	117-7
Initial MHF-Creation	117-8
Interface Type	117-8
Interval (seconds)	117-8
Level	117-8
Low-priority Defect	117-8
Mac Address	117-9
MC-LAG Prop Hold Time	117-9
MC-LAG Standby Inactive	117-9
MD Mgr Object ID.....	117-9
MEP ID.....	117-10
MEP Mac Address	117-10
MEP(s) Creation on Access Interfaces	117-10
MEP(s) Creation on SDP Bindings.....	117-10
MHF-Creation	117-10
MIP(s) Creation on Access Interfaces.....	117-11
MIP(s) Creation on SDP Bindings	117-11
Name	117-11
Name	117-11
Name Format	117-11
Name Type	117-12
Object ID	117-12
One-way-delay Test Threshold (seconds)	117-12
Originating MEP.....	117-12
Priority.....	117-13
Priority Level for CCM Messages	117-13
Run Continuity Check Protocol.....	117-13
Send Count (packets)	117-13
Service ID.....	117-13
Set Control MEP property on created MEPs	117-13
Timeout (seconds)	117-14
Type.....	117-14
Virtual MEP(s) Creation on B-Sites.....	117-14
VLAN ID	117-14

118 — Scripts parameters

118-1

118.1	Scripts parameters	118-2
	Answer	118-2
	Auto-Assign ID.....	118-2
	Comment	118-2
	Content Type	118-2
	Continue On Command Failure.....	118-2
	Default Value	118-2
	Description	118-3
	Label	118-3

Mode	118-3
Name	118-3
Network Element Version Information	118-3
Question	118-3
Reserve Targets	118-4
Script ID	118-4
State	118-4
Type	118-4
Use Latest Version	118-4
Version Number	118-4

119 – Auto-Provision Profiles parameters 119-1

119.1	Auto-Provision Profiles parameters	119-2
	Adjacent NE Managed	119-2
	Adjacent Site ID	119-2
	Auto-Assign ID	119-2
	Description	119-2
	Name	119-2
	Name	119-2
	Network Element Type	119-3
	Network Element Version Information	119-3
	Script ID	119-3
	Type	119-3
	View the newly created Auto-Provisioning	119-3

120 – Bulk Operations parameters 120-1

120.1	Bulk Operations parameters	120-2
	Admin State	120-2
	Auto-Assign ID	120-2
	Batch ID	120-2
	Batch Size	120-2
	Batch Status	120-2
	Batch Status Summary	120-3
	Changed	120-3
	Continue on Failure	120-3
	Creator	120-3
	Description	120-3
	Duration	120-4
	Execution Status	120-4
	Failures	120-4
	Last Total Changed	120-4
	Name	120-4
	Not Changed	120-4
	Not Found	120-5
	Not in Span	120-5
	Object Type	120-5
	Operation ID	120-5
	Range	120-5
	Time Last Started	120-5
	Time Last Finished	120-5

121	Card Migration Event Manager parameters	121-1
121.1	Card Migration Event Manager parameters.....	121-2
	Additional Information	121-2
	Auto-Assign ID.....	121-2
	Auto Reboot	121-2
	Description	121-2
	ID	121-2
	New Type	121-2
122	MIB Policies parameters	122-1
122.1	MIB Policies parameters.....	122-2
	Administrative State	122-2
	Auto-Assign ID.....	122-2
	Displayed Name	122-2
	Number of Varbind per PDU	122-2
	Policy ID	122-2
	Polling Admin State	122-2
	Polling Interval	122-3
	Polling Synchronization Time.....	122-3
123	Server Performance Statistics parameters	123-1
123.1	Server Performance Statistics parameters	123-2
	Accounting Stats Failure Periodic Threshold.....	123-2
	Accounting Stats Pending Periodic Threshold.....	123-2
	Accounting Stats Processed Periodic Threshold	123-2
	Accounting Stats Total Periodic Threshold	123-2
	Administrative State	123-2
	Alarm Total Periodic Threshold	123-2
	Cleared Periodic Threshold	123-3
	Collection Interval	123-3
	Condition Periodic Threshold.....	123-3
	Critical Periodic Threshold	123-3
	Dropped Backpressure Periodic Threshold	123-3
	Dropped Duplicate Periodic Threshold.....	123-3
	Dropped Full Resync Periodic Threshold.....	123-3
	Dropped Not Managed Periodic Threshold	123-4
	Dropped Out Of Sequence Periodic Threshold.....	123-4
	Incoming Periodic Threshold	123-4
	Indeterminate Periodic Threshold.....	123-4
	Info Periodic Threshold.....	123-4
	Major Periodic Threshold	123-4
	Minor Periodic Threshold.....	123-4
	Polling Synchronization Time.....	123-4
	Retention Time (hours).....	123-5
	Scheduled Polling Stats Pending Periodic Threshold	123-5
	Scheduled Polling Stats Processed Periodic Threshold	123-5
	Scheduled Polling Stats Total Periodic Threshold.....	123-5
	Scheduled Resync Failure Periodic Threshold	123-5
	Scheduled Resync Processed Periodic Threshold.....	123-5
	Scheduled Resync Received Periodic Threshold.....	123-5

Scheduled Stats Failure Periodic Threshold	123-6
Threshold Reporting State	123-6
Unscheduled Resync Failure Periodic Threshold	123-6
Unscheduled Resync Processed Periodic Threshold	123-6
Unscheduled Resync Received Periodic Threshold	123-6
Used Heap Memory Periodic Threshold	123-6
Used Non Heap Memory Periodic Threshold	123-6
Unscheduled Polling Stats Pending Periodic Threshold	123-7
Unscheduled Polling Stats Processed Periodic Threshold	123-7
Unscheduled Polling Stats Total Periodic Threshold	123-7
Unscheduled Stats Failure Periodic Threshold	123-7
Warning Periodic Threshold	123-7

124 – Accounting Policies parameters 124-1

124.1	Accounting Policies parameters	124-2
	All Overrides	124-2
	All Queues	124-2
	Application Assurance Counters	124-2
	Auto-Assign ID	124-2
	Administrative	124-2
	Collection Interval (m)	124-3
	Counters	124-3
	Counters	124-3
	Counters	124-4
	Counters	124-4
	Default	124-4
	Description	124-4
	Displayed Name	124-4
	Egress Counters	124-4
	Egress Counters	124-5
	File ID	124-5
	From Subscriber Counters	124-5
	ID	124-6
	ID	124-6
	Ingress Counters	124-6
	Ingress Counters	124-7
	Name	124-7
	Significant Change Delta	124-7
	To Subscriber Counters	124-8
	Type	124-8
	Use Default Interval	124-9

125 – File Policies parameters 125-1

125.1	File Policies parameters	125-2
	Auto-Assign ID	125-2
	Description	125-2
	Displayed Name	125-2
	Drive	125-2
	ID	125-2
	Retention (hours)	125-2

	Rollover (minutes)	125-2
	Storage Drive - Backup	125-3
126	— Statistics Browser parameters	126-1
126.1	Statistics Browser parameters	126-2
	Administrative State	126-2
	Statistics Type	126-2
	Retention Time (hours).....	126-2
	Threshold Reporting State	126-2
127	— TCA Policies parameters	127-1
127.1	TCA Policies parameters	127-2
	Alarm Severity	127-2
	Auto-Assign ID.....	127-2
	Displayed Name	127-2
	Flow Direction	127-2
	Policy ID	127-2
	Rule ID	127-2
	Threshold (%)	127-3
	Threshold Direction	127-3
128	— RAN Performance Management Policies parameters	128-1
128.1	RAN Performance Management Policies parameters	128-2
	Administrative State	128-2
	Collection Interval (min)	128-2
129	— Schedules parameters	129-1
129.1	Schedules parameters	129-2
	Administrative State	129-2
	Change Current User To.....	129-2
	Delay Time (seconds)	129-2
	Description	129-2
	Enable.....	129-2
	Frequency	129-2
	Name	129-3
	Current Client End Time	129-3
	Current Client Start Time.....	129-3
	Ongoing	129-4
	Run Every	129-4
	Run Every	129-4
	Run Every	129-5
	Run Every	129-5
	Run Every Day.....	129-6
	Run Every Days	129-6
	Run Every Hour	129-6
	Run Every Hours	129-6
	Run Every Minute.....	129-6
	Run Every Minutes.....	129-7

	Run Every Month.....	129-7
	Run Every Months	129-7
	Run Every Second	129-7
	Run Every Seconds	129-7
	Run Every Week	129-7
	Run Every Weeks	129-8
	Scheduled Task Description	129-8
	Scheduled Task Name	129-8
	Time Alignment Setting	129-8
130	— Policies Audit parameters	130-1
130.1	Policies Audit parameters	130-2
	Include Non Applicable Attributes.....	130-2
	Set to “Local Edit Only” upon finding of differences.....	130-2
	Set to “Sync with Global” upon finding of no differences	130-2
131	— Time Range Entry Assignment parameters	131-1
131.1	Time Range Entry Assignment parameters	131-2
	End Date	131-2
	Search by Time Of Day Entry Type	131-2
	Start Date	131-2
	Time Of Day Entry Policy Type.....	131-2
	Time Range Entry Container Type.....	131-2
132	— Copy/Move SAPs parameters	132-1
132.1	Copy/Move SAPs parameters	132-2
	Action Type	132-2
	Continue on individual Failure	132-2
	Current Mode	132-2
	Inner Encap Value End.....	132-2
	Inner Encap Value Offset.....	132-2
	Inner Encap Value Start	132-3
	Outer Encap Value End.....	132-3
	Outer Encap Value Offset.....	132-3
	Outer Encap Value Start	132-3
	Service Type	132-3
133	— NE Sessions parameters	133-1
133.1	NE Sessions parameters	133-2
	Append to file	133-2
	Background color	133-2
	Bold.....	133-2
	Font Name.....	133-2
	Font Size.....	133-3
	Foreground color	133-3
	Italic.....	133-3
	Log File Location	133-3

Minimum number of scrolling lines	133-4
Send Console To a File	133-4

134 – Common Tools menu parameters 134-1

134.1	Common Tools menu parameters.....	134-2
	Administrative State	134-2
	Auto-Assign ID.....	134-2
	Description	134-2
	Displayed Name	134-2
	Forwarding Class	134-2
	ID	134-3
	Name	134-3
	Polling Synchronization Time.....	134-3
	Retention Time (hours).....	134-4

Administration menu parameters

135 – 5620 SAM User Security parameters 135-1

135.1	5620 SAM User Security parameters.....	135-2
	Account Expiry.....	135-2
	Account Expiry (days)	135-2
	Administrative State	135-2
	Advance Password Expiry Notification (days).....	135-2
	Apply Local Authentication Only.....	135-2
	Attempts before e-mail	135-3
	Attempts before lockout	135-3
	Client Timeout (minutes)	135-3
	Confirm Password	135-3
	Created In	135-3
	Description	135-4
	E-mail Address	135-4
	E-mail Subject	135-4
	E-mail Subject	135-4
	E-mail text	135-4
	E-mail text	135-4
	E-mail User Name	135-5
	E-mail User Password	135-5
	Enable IP Address validation	135-5
	Enable.....	135-5
	Enabled	135-5
	LI Filter Lock	135-5
	Maximum GUI Sessions Allowed	135-6
	Maximum OSS Sessions Allowed	135-6
	Maximum Sessions Allowed	135-6
	Maximum User Sessions Allowed	135-6
	Minimum User Name Length Allowed	135-7
	Name	135-7

Override Global Timeout	135-7
Password Change Required	135-8
Password Expiry	135-8
Password Expiry (days)	135-8
Password History Duration (days)	135-8
Password Reuse Cycle	135-8
Priority	135-8
Profile ID	135-9
Profile Name	135-9
Profile Name	135-9
Remote User	135-9
Reserve Administrator Login	135-9
Reserve Administrator Login	135-9
Retention Time (hours)	135-10
Role ID	135-10
Role Name	135-10
Server	135-10
Span ID	135-10
Span Name	135-10
Span Rule ID	135-11
Statement	135-11
Test Message	135-11
Threshold Reporting State	135-11
User Group	135-11
User Group	135-12
User Group State	135-12
User Name	135-12
User Password	135-12
User State	135-13
Valid Client IP address	135-13
136 — Change Password parameters	136-1
136.1 Change Password parameters	136-2
Confirm Password	136-2
New Password	136-2
Old Password	136-2
137 — TCP Key Chains parameters	137-1
137.1 TCP Key Chains parameters	137-2
Admin State	137-2
Auto-Assign ID	137-2
Begin Time	137-2
Displayed Name	137-2
Description	137-2
End Time	137-2
Key	137-3
Key Direction	137-3
Key ID	137-3
Receive Option	137-3
Secret Key Algorithm	137-4

Send Option	137-4
Tolerance (seconds)	137-4

138 — 5620 SAM RADIUS/TACACS+ User Authentication

parameters 138-1

138.1	5620 SAM RADIUS/TACACS+ User Authentication parameters	138-2
	Address	138-2
	Administrative State	138-2
	Authentication Order 1	138-2
	Authentication Order 2	138-2
	Authentication Order 3	138-2
	Description	138-3
	Displayed Name	138-3
	Exit On Reject	138-3
	Port	138-3
	Retry Attempts	138-3
	Secret	138-3
	Single Connection	138-3
	Timeout (seconds)	138-3

139 — NE Management Access Filters parameters 139-1

139.1	NE Management Access Filters parameters	139-2
	Action	139-2
	Administrative Status	139-2
	Auto-Assign ID	139-2
	Configuration Mode	139-2
	Default Filter Action	139-2
	Description	139-3
	Destination Port	139-3
	Destination Port Mask	139-3
	Displayed Name	139-3
	ID	139-3
	Protocol	139-3
	Source IP	139-4
	Source IP Mask	139-4
	Source Port ID	139-4
	Source Port Type	139-4

140 — NE CPM Filter parameters 140-1

140.1	NE CPM Filter parameters	140-2
	Action	140-2
	Administrative Status	140-2
	Auto-Assign ID	140-2
	CIR (kb/s)	140-2
	Committed Burst Size (KB)	140-2
	Configuration Mode	140-3
	CFM Opcode	140-3
	CFM Val 1	140-3
	CFM Val 2	140-3

Default Filter Action	140-3
Description	140-4
Destination IP	140-4
Destination MAC	140-4
Destination Mask	140-4
Destination Mask	140-4
Destination Mask	140-5
Destination Port	140-5
Displayed Name	140-5
Dot1p	140-5
Dot1p Mask	140-5
DSCP	140-6
DSAP	140-6
DSAP Mask	140-6
Dst Mask	140-7
Entry ID	140-7
Ether Type.....	140-7
Flow Label.....	140-7
Fragment	140-7
Frame Type	140-8
ICMP Code	140-8
ICMP Type	140-8
ID	140-8
IP Option.....	140-8
IP Option Mask	140-9
IPv6 Administrative Status	140-10
MAX.....	140-10
Maximum Burst Size (KB).....	140-10
Multiple Option	140-10
Next Header.....	140-11
Option Present.....	140-11
PIR (kb/s).....	140-11
Protocol.....	140-11
Queue ID	140-11
Routing Instance.....	140-11
Service Id	140-12
SNAP OUI	140-12
SNAP PID	140-12
Source IP.....	140-12
Source IP Mask	140-12
Source MAC.....	140-13
Source Mask	140-13
Source Mask	140-13
Source Mask	140-13
Source Port.....	140-13
Src Mask	140-13
SSAP	140-14
SSAP Mask	140-14
TCP Ack	140-14
TCP Syn	140-14

141 — NE DoS Protection parameters	141-1
141.1 NE DoS Protection parameters	141-2
Auto-Assign ID	141-2
Description	141-2
Level Set	141-2
Overall Rate Limit (pps)	141-2
Out Profile Rate (pps)	141-2
Packet Rate Limit (pps)	141-2
Policy ID	141-3
Receive Notification	141-3
142 — NE User Profiles parameters	142-1
142.1 NE User Profiles parameters	142-2
Action	142-2
Auto-Assign ID	142-2
Configuration Mode	142-2
Default Profile Action	142-2
Description	142-3
Displayed Name	142-3
ID	142-3
LI Profile	142-3
Match String	142-3
143 — NE User Configuration parameters	143-1
143.1 NE User Configuration parameters	143-2
Access	143-2
Additional ID	143-2
Authentication Protocol	143-2
Configuration Mode	143-3
Confirm New Auth Password	143-3
Confirm New Privacy Password	143-3
Confirm Password	143-3
Console Cannot Change Password	143-3
Console Login Exec File	143-4
Console New Password At Login	143-4
Description	143-4
Home Directory	143-4
New Authentication Password	143-4
New Privacy Password	143-4
Password	143-5
Privacy Protocol	143-5
Restrict to Home	143-5
User Name	143-5
144 — NE Password Policy parameters	144-1
144.1 NE Password Policy parameters	144-2
Admin Password	144-2
Authentication Order 1	144-2
Authentication Order 2	144-2

Authentication Order 3.....	144-3
Auto-Assign ID.....	144-3
Complexity	144-3
Configuration Mode	144-3
Confirm Password	144-3
Days Before Expiration	144-3
Description	144-3
Exit on Reject.....	144-4
Health Check.....	144-4
Health Check Interval	144-4
ID	144-4
Lockout Time (minutes).....	144-4
Maximum Attempts	144-4
Maximum Attempts Time (minutes).....	144-4
Minimum Length.....	144-5
Name	144-5
Password Never Expires	144-5

145 — NE RADIUS Authentication parameters 145-1

145.1	NE RADIUS Authentication parameters	145-2
	Address	145-2
	Administrative State	145-2
	Configuration Mode	145-2
	Description	145-2
	Displayed Name	145-2
	Enable Accounting	145-2
	Enable Authorization	145-2
	ID	145-2
	Port.....	145-2
	RADIUS Authorization Algorithm	145-2
	Retry Attempts	145-3
	Secret	145-3
	Source Address	145-3
	Timeout (seconds)	145-3

146 — NE TACACS+ Authentication parameters 146-1

146.1	NE TACACS+ Authentication parameters	146-2
	Accounting Type.....	146-2
	Address	146-2
	Administrative State	146-2
	Configuration Mode	146-2
	Description	146-2
	Displayed Name	146-2
	Enable Accounting	146-2
	Enable Authorization	146-3
	ID	146-3
	Secret	146-3
	Single Connection	146-3
	Source Address	146-3
	Timeout (seconds)	146-3

147 — NE AOS Security Authentication parameters	147-1
147.1 NE AOS Security Authentication parameters.....	147-2
Account Port	147-2
Authentication Port	147-2
Port.....	147-2
Retries	147-2
Secret	147-2
Secret	147-2
148 — NE System Security parameters	148-1
148.1 NE System Security parameters.....	148-2
Access	148-2
Console Login Exec File	148-2
CPM Per-Peer-Queuing	148-2
Home Directory	148-2
Link Rate Limit (pps)	148-2
Port Overall Rate Limit (pps).....	148-3
Protection Administrative State	148-3
Restricted to Home Directory	148-3
Servers Enabled	148-3
SSH	148-3
149 — Subscriber Authentication Policy Manager parameters	149-1
149.1 Subscriber Authentication Policy Manager parameters	149-2
Accept CoA	149-2
Access Algorithm	149-2
Append To User Name	149-2
Auto-Assign ID.....	149-2
Authentication Hold Down Time	149-2
Calling Station ID Type	149-3
Description	149-3
Domain Name	149-3
Displayed Name	149-3
Fallback Action	149-3
ID	149-3
Password.....	149-4
Port.....	149-4
Port Prefix String.....	149-4
Port Prefix Type	149-4
Port Suffix Type	149-4
Port Type	149-4
Port Type Value	149-5
PPPoE Access Method.....	149-5
RADIUS Attributes	149-5
Re-Authenticate When DHCP Lease Expires.....	149-6
Retry Attempts	149-6
Router Instance.....	149-6
Secret Key	149-7
Server IP Address.....	149-7
Source Address	149-7

Timeout (seconds)	149-7
User Name Format	149-7
User Name Operation.....	149-8

150 – NE Maintenance parameters 150-1

150.1	NE Maintenance parameters.....	150-2
	ATCA Image Root Path.....	150-2
	Auto-Activate After Successful File Transfer	150-2
	Auto-Assign ID.....	150-2
	Auto Backup Scheme	150-2
	Auto Backup Threshold (operations)	150-3
	Auto-Purge Scheme	150-3
	Auto-Reboot After Successful Upgrade	150-3
	Auto-Reboot After Successful Activation	150-4
	Auto Save Scheme.....	150-5
	Auto Save Threshold	150-5
	Boot Option File Mode	150-6
	CFlash Backup Root Path.....	150-6
	CFlash Image Root Path	150-6
	CLI Config File Mode	150-6
	CLI Config Save Details	150-6
	CLI Debug Save Config File Mode	150-7
	Deployment Mode	150-7
	Enable Backup	150-7
	File Compression	150-7
	Forced Download	150-8
	FTP Password	150-8
	FTP Server IP.....	150-8
	FTP Server Port.....	150-8
	FTP User ID.....	150-8
	Image Root Path.....	150-9
	In Service Software Upgrade	150-9
	Maximum Backup Age (days)	150-9
	Name	150-9
	Number of Backups	150-9
	Policy ID	150-9
	Policy Type.....	150-10
	Retry Interval	150-10
	Retry Scheme	150-10
	Retry Threshold	150-11
	Root Directory	150-11
	Save Certified Directory.....	150-11
	Save Details	150-11
	Save Network Directory	150-12
	Scheduled Backup Interval.....	150-12
	Scheduled Backup Scheme.....	150-12
	Scheduled Backup Sync Time.....	150-13
	Scheduled Backup Threshold (operations)	150-13
	Scheduled Save Interval.....	150-13
	Scheduled Save Scheme	150-14
	SFTP Password	150-14

	SFTP User ID.....	150-14
	Timer To Wait For Fallback To Previous IP Version	150-14
	Timer To Wait For Fallback To Previous Software Version	150-14
	Transfer Protocol.....	150-15
	Upgrade File Type.....	150-15
151	— Database parameters	151-1
151.1	Database parameters	151-2
	Accounting Statistic Data Retention Period (Days)	151-2
	Auto-Assign ID.....	151-2
	Backup Interval	151-2
	Backup Type	151-2
	Description	151-2
	Enable Backup File Compression.....	151-2
	Interval Unit	151-3
	Manual Backup Directory.....	151-3
	Max (Collective) Log Size	151-3
	Number of Archives	151-4
	Number to Keep	151-4
	Policy ID	151-4
	Purge Mode.....	151-4
	Scheduled Backup Directory.....	151-5
	Schedule Enabled	151-5
	Start Time	151-5
152	— System Information parameters	152-1
152.1	System Information parameters	152-2
	Maximum UI Sessions	152-2
153	— System Preferences parameters	153-1
153.1	System Preferences parameters	153-2
	Auto Discover Composite Services.....	153-2
	Default Service Priority.....	153-2
	Maximum number of sites that can be moved.....	153-2
	Remove Empty Service	153-2
	Suppress VPRN SNMP Community String Warning	153-3
154	— Alarm Settings parameters	154-1
154.1	Alarm Settings parameters	154-2
	Administrative State	154-2
	Alarm deletion.....	154-2
	Attribute Name	154-2
	auto	154-2
	Automatically Assigned Urgency	154-2
	automatic deletion of correlated alarms.....	154-3
	automatic severity alterations	154-3
	clearing (if self-clearing alarm).....	154-3
	De-escalation	154-4

De-escalation	154-4
de-escalation (defined by specific policy)	154-4
Description	154-4
Detailed Text	154-4
Domain	154-4
Escalation	154-5
Escalation	154-5
escalation (defined by specific policy)	154-5
Frequency	154-5
Group Tag	154-6
History Enabled	154-6
implicit severity demotion	154-6
implicit severity promotion	154-6
Initial Severity Assignment	154-6
Interval	154-7
Log On Change	154-7
Log On Deletion	154-7
manual	154-8
manual severity alterations	154-8
Max 24hr Partition Log Size (records)	154-8
Object Type	154-8
Order	154-9
Overwrite existing	154-9
Reason for change	154-9
Severity	154-9
Severity Alterable	154-10
severity demotion	154-10
severity promotion	154-10
Squelch	154-11

155 – Discovery Manager parameters

155-1

155.1	Discovery Manager parameters	155-2
	Administrative State	155-2
	Auto-Assign ID	155-2
	Description	155-2
	Displayed Name	155-2
	Element Manager System Name	155-2
	Group Name	155-2
	Host Name	155-2
	ID	155-2
	Ignore Timestamps	155-3
	IP Address	155-3
	Last Active Management IP	155-3
	Management Protocol	155-3
	Mask Bits	155-3
	OLC State	155-3
	Password	155-4
	Read Policy ID	155-4
	Server IP Address	155-4
	Server Port Number	155-5
	Server Type	155-5

Usage	155-5
Use Original Management IP	155-5
User Name	155-6
Write Policy ID	155-6

156 – Generic NE Manager parameters 156-1

156.1	Generic NE Manager parameters.....	156-2
	Additional Text	156-2
	Administrative State	156-3
	Alarm Name	156-3
	Answer	156-4
	Auto-Assign ID.....	156-4
	Catalogue Name	156-4
	Catalogue Name	156-4
	Catalogue Name	156-4
	Chassis MAC Object ID	156-4
	CLI Supported	156-4
	Command Prompt	156-5
	Description	156-5
	Default Element Manager URL	156-5
	Default External EMS	156-5
	Default Out Value	156-6
	Disable Paging Command	156-6
	Enable Confirm Prompt	156-6
	Enable Login Command	156-6
	Enable Login Prompt.....	156-6
	Enable Second Login	156-7
	Error Indicator	156-7
	Execution Command Timeout (seconds)	156-7
	External EMS	156-7
	FDN Extension	156-7
	Full Node Resync on Max Trap Gap.....	156-8
	Generic NE Type.....	156-8
	Generic NE Category.....	156-9
	ID	156-9
	Idle Session Warning Message	156-9
	In Value	156-9
	In Value Type	156-9
	Login Prompt Optional	156-9
	Login Timeout (seconds)	156-10
	Max Number Of Sessions	156-10
	Minimum Time Interval Between Full Node Resyncs (seconds)	156-10
	Maximum Trap Gap	156-10
	Out Value	156-10
	Out Value Type	156-10
	Pre Login Prompt.....	156-11
	Probable Cause	156-11
	Prompt	156-11
	Read Login Prompt.....	156-11
	Read Password Prompt	156-11
	Reset Command	156-12

Script ID	156-12
Script ID	156-12
Severity	156-12
Specify Default Out Value	156-12
Specify Transform Function	156-13
Specify Transform Function	156-13
Specify Transform Function	156-13
Supports Trap Restoration Logs	156-13
Supports Trap Sequence Number	156-13
Sys Object ID	156-14
Telnet Port	156-14
Transform Function Name	156-14
Trap Name	156-14
Trap OID	156-14
Use Default Additional Text	156-15
Varbind Position	156-15
Varbind Position	156-15
Varbind Position	156-15
Varbind Transform Function	156-15
Varbind Transform Function	156-15
Varbind Transform Function	156-16
Version	156-16
Write Login Prompt	156-16
Write Password Prompt	156-16

157 – Mediation parameters

157-1

157.1	Mediation parameters	157-2
	Administrative State	157-2
	Auto-Assign ID	157-2
	Communication Protocol	157-2
	Community String	157-2
	Connect Timeout (sec)	157-2
	Description	157-2
	Discovery Rule Scan Interval	157-2
	Displayed Name	157-3
	File Transfer Type	157-3
	Network Element Type	157-4
	Number of Varbind per PDU	157-4
	Ping Command Timeout (seconds)	157-5
	Ping Interval (minutes)	157-5
	Ping Interval (seconds)	157-5
	Policy ID	157-5
	Polling Admin State	157-5
	Polling Interval	157-5
	Polling Synchronization Time	157-6
	Port	157-6
	Read Timeout (sec)	157-6
	Retry	157-6
	Schedule Enabled	157-7
	Security Model	157-7
	SSH2 Server Port	157-7

	Timeout (milliseconds)	157-8
	User Name	157-8
	User Password	157-8
158	NE Self Config Policy Manager parameters	158-1
158.1	NE Self Config Policy Manager parameters	158-2
	Checkpoints Before	158-2
	Name	158-2
	Process Flow	158-2
159	RAN License Manager parameters	159-1
159.1	RAN License Manager parameters	159-2
	Email Recipient Address	159-2
	First Expiration Threshold (days)	159-2
	First Usage Threshold (%)	159-2
	Report File Format	159-2
	Second Usage Threshold (%)	159-2
	Second Expiration Threshold (days)	159-2
160	Pre-Provisioned NE Manager parameters	160-1
160.1	Pre-Provisioned NE Manager parameters	160-2
	Active Management IP	160-2
	Chassis Type	160-2
	Hardware Identifier	160-2
	Network Element ID	160-2
	Network Element Version	160-2
161	Common Administration menu parameters	161-1
161.1	Common Administration menu parameters	161-2
	Accounting Port	161-2
	Address	161-2
	Administrative State	161-2
	Authentication Port	161-2
	Auto-Assign ID	161-2
	CoA Only	161-3
	Configuration Mode	161-3
	Confirm Password	161-3
	Description	161-3
	Displayed Name	161-4
	Distribution Mode	161-4
	Enable Accounting	161-4
	Enable Authorization	161-5
	Enable User Template	161-5
	Exit On Reject	161-5
	ID	161-5
	IP Address	161-6
	IP Address 2	161-6
	Password	161-6

Polling Synchronization Time.....	161-6
Port.....	161-6
Protocol.....	161-6
Protocol Name.....	161-8
Retry Attempts.....	161-8
Secret Name.....	161-8
Single Connection.....	161-8
Source Address.....	161-9
Source IP.....	161-9
Source IP Mask.....	161-9
Time Out.....	161-9
Timeout (seconds).....	161-9

Equipment navigation tree parameters

162 – Device parameters 162-1

162.1	Device parameters.....	162-2
	Active Management IP.....	162-2
	Active Time-out (minutes).....	162-2
	Administrative State.....	162-2
	Administrative Status.....	162-2
	Admission Control.....	162-3
	Aggregation Type.....	162-3
	ATM OAM Loopback Location ID.....	162-3
	ATM OAM Loopback Period.....	162-4
	Autonomous System.....	162-4
	Auto Revert to Preferred.....	162-4
	Bridge Type.....	162-5
	Cache Size.....	162-5
	CFLOWD State.....	162-5
	Description.....	162-6
	DNS Domain.....	162-6
	Egress.....	162-6
	Enable L3 Management Interface.....	162-6
	Fast Transmission Interval (Seconds).....	162-6
	Group Name.....	162-6
	Hold Down Time.....	162-7
	Hold Up Time.....	162-7
	Host Address.....	162-7
	Ignore Timestamps.....	162-7
	In-Active Time-out (seconds).....	162-7
	Ingress.....	162-7
	IP Address.....	162-8
	IP Address.....	162-8
	IP Address.....	162-8
	Interface Ip Address.....	162-8
	L3 Management Interface.....	162-8
	L4 Load Balancing.....	162-8

LACP System Priority	162-9
Latitude (degrees)	162-9
LI Local Save Allowed.....	162-9
Location	162-9
Longitude (degrees)	162-9
Management IP Address	162-9
Management IP Selection	162-10
Mask	162-10
Mask	162-11
Mask	162-11
Maximum Consecutive Transmissions	162-11
MEP Id.....	162-11
Next Hop.....	162-11
Notification Interval (Seconds).....	162-11
Number of Tries for Down State	162-12
Number of Tries for Up State.....	162-12
Over Flow (percent)	162-12
PDUs in Fast Transmission	162-12
Persistent SNMP Indices	162-12
Physical Impedance	162-13
Port Number	162-13
Primary DNS	162-13
Primary Route Preference	162-13
QoS Classification	162-13
Redundant Synchronization Mode	162-14
Re-Init Delay (Seconds).....	162-14
Resource Group ID	162-14
Route Destination	162-14
Router ID	162-15
Sample Rate.....	162-15
Scheduled Polling	162-15
Secondary DNS.....	162-15
Secondary Route Preference	162-15
Separate LI Administration	162-16
Slot	162-16
SSH Session	162-17
System ID (Loopback Ip Address)	162-17
System IP Address	162-17
Telnet Session	162-18
Template Re-transmit (seconds).....	162-18
Template Type	162-18
Template Type	162-18
Tertiary DNS	162-18
Transmission Delay (Seconds)	162-18
Transmission Interval (Seconds)	162-19
Transmission Multiplier.....	162-19
Uplink	162-19
Vendor-Specific ICMP Extensions	162-19
Version	162-19
View Shelf	162-19
VLAN ID	162-20

VLAN ID	162-20
VPLS Mode	162-20

163 – CCAG parameters 163-1

163.1	CCAG parameters	163-2
	Access Adapt QoS	163-2
	Administrative State	163-2
	CCAG ID	163-2
	CCA Rate (kbps)	163-2
	CCA Rate Enabled	163-2
	CC ID	163-3
	Description	163-3
	Egress Reserved CBS (%)	163-3
	Ingress Reserved CBS (%)	163-3
	MTU (octets)	163-3
	Path Rate (Kb/s)	163-3
	Path Rate Enabled	163-3
	Path Rate Option	163-3
	Path Weight (%)	163-4

164 – TWAMP parameters 164-1

164.1	TWAMP parameters	164-2
	Administrative State	164-2
	Administrative Status	164-2
	Conn Idle Time Periodic Threshold (seconds)	164-2
	Conn Session Count Periodic Threshold	164-2
	Conn Test Packets Rx Periodic Threshold	164-2
	Conn Test Packets Tx Periodic Threshold	164-3
	Conn Test Sess Completed Periodic Threshold	164-3
	Conn Test Sess Rejected Periodic Threshold	164-3
	Description	164-3
	Inactivity Timeout (Seconds)	164-3
	Maximum Connections	164-3
	Maximum Sessions	164-3
	Maximum # Connections	164-4
	Maximum # Sessions	164-4
	Prefix Address	164-4
	Prefix Length	164-4
	Retention Time (hours)	164-4
	Srv Pfx Conn Count Periodic Threshold	164-5
	Srv Pfx Conns Rejected Periodic Threshold	164-5
	Srv Pfx Session Count Periodic Threshold	164-5
	Srv Pfx Test Packets Rx Periodic Threshold	164-5
	Srv Pfx Test Packets Tx Periodic Threshold	164-5
	Srv Pfx Test Sess Abort Periodic Threshold	164-5
	Srv Pfx Test Sess Completed Periodic Threshold	164-6
	Srv Pfx Test Sess Rejected Periodic Threshold	164-6
	Threshold Reporting State	164-6

165 — IGH parameters 165-1

165.1	IGH parameters.....	165-2
	Administrative State	165-2
	CLI Name	165-2
	IGH ID	165-2
	Minimum Active Link Threshold.....	165-2

166 — ISA-AA Group parameters 166-1

166.1	ISA-AA Group parameters	166-2
	AA Stats Type	166-2
	AA Subscriber Name	166-2
	AA Subscriber Type	166-2
	Administrative State	166-2
	Buffer Utilization High Water Mark.....	166-2
	Buffer Utilization High Water Mark.....	166-3
	Buffer Utilization Low Water Mark	166-3
	Buffer Utilization Low Water Mark	166-3
	Capacity Cost High Threshold	166-3
	Capacity Cost Low Threshold.....	166-4
	Collector Port.....	166-4
	Description	166-4
	Reserved CBS (%)	166-4
	Reserved CBS (%)	166-4
	Forwarding Class Name.....	166-4
	Group Number	166-5
	Host Address	166-5
	ISA-AA MDA Role	166-5
	Operation Upon Failure	166-5
	Overload Cut-Through	166-5
	Override ASO Characteristic Name	166-6
	Override ASO Characteristic Value	166-6
	Partition ID	166-6
	Partitions	166-6
	Performance Administrative State	166-6
	Performance Administrative State	166-6
	Sample Flow Rate	166-7
	Sample Flow Rate	166-7
	Sampling Rate	166-7
	Subscriber Scale	166-7
	Template Re-transmit	166-8
	Transit Subscriber Name	166-8
	Version	166-8
	Volume Administrative State	166-8

167 — ISA-IPsec Group parameters 167-1

167.1	ISA-IPsec Group parameters	167-2
	Administrative State	167-2
	Description	167-2
	Group Number	167-2

168 — ISA-LNS Group parameters 168-1

168.1	ISA-LNS Group parameters	168-2
	Administrative State	168-2
	Description	168-2
	Group Number	168-2

169 — ISA-NAT Group parameters 169-1

169.1	ISA-NAT Group parameters	169-2
	Active MDA Limit	169-2
	Administrative State	169-2
	Description	169-2
	Group Number	169-2
	Reservation Count.....	169-2
	Session Watermark High.....	169-2
	Session Watermark Low	169-2

170 — ISA-Video Group parameters 170-1

170.1	ISA-Video Group parameters	170-2
	Address Type.....	170-2
	Ad Insert Server	170-2
	Administrative State	170-2
	ADI Administrative Status	170-2
	ADI Zone Multicast Address	170-2
	ADI Zone Unicast Source Address	170-3
	Analyzer	170-3
	Associated Multicast Service ID	170-3
	Description	170-3
	Fast Channel Change Server	170-3
	Gateway Address	170-3
	Group Number	170-4
	IP Address	170-4
	Local Retransmission Server	170-4
	Multicast Channel IP Address	170-4
	Name	170-4
	Prefix Length.....	170-4
	Reserve Retransmission Bandwidth (Mbps).....	170-5
	RT Client Address	170-5
	SCTE 30 Control Address	170-5
	SCTE 30 Data Address.....	170-5
	SCTE 35 Action.....	170-5
	Server Address	170-6
	Stream Selection	170-6
	Unicast Source IP Address.....	170-6

171 — LAG parameters 171-1

171.1	LAG parameters	171-2
	Active Sub-Group Selection Criteria.....	171-2
	Actor Administration Key	171-2
	Actor Administration Key	171-2

Actor Administration Key	171-3
Actor System ID.....	171-3
Actor System Priority	171-3
Administrative State	171-3
Admin Key	171-3
Admin Key	171-3
Admin Port	171-3
Admin Port Priority	171-3
Admin State	171-4
Admin State	171-4
Admin System Id.....	171-5
Admin System Priority.....	171-5
Auto-Assign ID.....	171-5
Auto-Generate	171-6
Automatic VLAN Binding	171-6
Class.....	171-6
Configured Address	171-7
Description	171-7
Dynamic Cost	171-7
Enable Per Forwarding Path Ingress Queue	171-8
Encap Type.....	171-9
Hold Time (100s of milliseconds)	171-9
L2Uplink	171-9
LACP Mode	171-9
LACP System ID	171-9
LACP System Priority	171-9
LACP System Priority	171-10
LACP Transmit Interval.....	171-10
LACP Transmit Standby.....	171-10
LAG ID.....	171-10
Mode	171-11
Name	171-11
Partner Administration Key.....	171-11
Partner System ID	171-11
Partner System Priority	171-11
Port Threshold.....	171-11
Port Threshold Action	171-12
Port Type	171-12
Priority.....	171-12
QoS Adaptation	171-13
Show Only Compatible Ports	171-13
Size	171-14
Slave to Partner	171-14
Standby Signalling.....	171-14
Sub-Group ID	171-15
System Id	171-15
System Priority	171-15
Type.....	171-15
View the newly created interface	171-15

172 – Shelf parameters	172-1
172.1 Shelf parameters	172-2
Activation	172-2
Active Timeout	172-2
Administrative Mode	172-2
Administrative State	172-3
Administrative State	172-4
Administrative State	172-4
Administrative State	172-4
Administrative State	172-5
Administrative State	172-5
Administrative State	172-5
Administrative State	172-5
Alarm Clear Message	172-5
Alarm Severity	172-5
Alarm Trigger Message	172-6
Analog Threshold (mV)	172-6
Announce Interval	172-6
Announce Receive Timeout	172-6
Clock ID	172-6
Clock MDA	172-6
Clock Priority 1	172-7
Clock Priority 2	172-7
Clock Slave Only	172-7
Clock Type	172-7
Command to Apply	172-7
Control Status	172-8
Control Type	172-9
Connected To	172-9
CPU Threshold (%)	172-9
Delayed Activation Timer	172-9
Description	172-9
Domain	172-9
Dynamic Peers	172-10
First Timing Reference Input	172-10
First Timing Reference Interface Type	172-10
First Timing Reference PTP Clock	172-10
Force Mode	172-10
Fourth Timing Reference Input	172-11
ID	172-11
Impedance Type	172-11
Input 1	172-11
Input 2	172-11
Input 3	172-11
Input 4	172-12
Input 5	172-12
Input 6	172-12
Input 7	172-12
Input 8	172-12
Input Administrative State	172-12
Input Type	172-12

Interface Name	172-13
Interface Type	172-13
Log Event	172-13
Master 1 Address	172-13
Master 2 Address	172-13
Memory Threshold (%)	172-13
Mixed Mode State on Chassis Enabled	172-14
Monitored Status	172-14
Name	172-14
Network Type	172-15
Operation	172-15
Output Administrative State	172-15
Output Line Length	172-15
Output Type	172-15
Peer ID	172-16
Peer IP Address	172-16
Peer Priority	172-16
Polarity	172-16
Port or Channel Name	172-17
Primary Multicast Bandwidth (mbps)	172-17
Primary Multicast Bandwidth for Dual-SFM Mode (mbps)	172-17
Primary Reference Type	172-17
PTP Profile	172-17
Quality Level Override	172-18
Quality Level Reference	172-18
Reference Input Mode	172-18
Reference Input Mode (revertive)	172-19
Reference Input Mode (revertive)	172-19
Role	172-19
Rx Threshold (%)	172-19
Sampling Interval (seconds)	172-20
Second Timing Reference Input	172-20
Second Timing Reference Interface Type	172-20
Second Timing Reference PTP Clock	172-20
Secondary Multicast Bandwidth (mbps)	172-20
Secondary Multicast Bandwidth for Dual-SFM Mode (mbps)	172-21
Secondary Reference Type	172-21
Severity	172-21
Status	172-21
SSM	172-22
Sync Interval	172-22
Sync In Port	172-22
Sync Out Port	172-22
System Quality Level	172-22
Temperature Threshold	172-23
Temperature Threshold Unit	172-23
Third Timing Reference Input	172-23
Trigger Rule	172-24
TxRx Threshold (%)	172-24
Type	172-24
Type	172-24
Update Chassis Relays	172-24

Wait to Restore Time (Min):	172-25
Wait to Restore Time (Secs):	172-25

173 – APS Groups parameters 173-1

173.1	APS Groups parameters	173-2
	Administrative State	173-2
	Advertise Interval (100s of milliseconds)	173-2
	Auto-Assign ID.....	173-2
	Channel Role	173-2
	Command Switch	173-2
	Description	173-3
	Direction.....	173-3
	Group Number	173-3
	Hold Time (100s of milliseconds)	173-4
	Hold Time for Line Signal Degradation (100s of milliseconds)	173-4
	Hold Time for Line Signal Failure (100s of milliseconds).....	173-4
	Network Interface.....	173-4
	Network Interface.....	173-4
	Network Interface.....	173-5
	RDI Alarm Generation	173-5
	Reversion Mode	173-5
	Wait To Restore (seconds)	173-5

174 – Card Slot parameters 174-1

174.1	Card Slot parameters	174-2
	Administrative	174-2
	Administrative State	174-2
	Assigned Card Type	174-2
	Capability.....	174-4
	Combo Port.....	174-4
	Command Action	174-4
	Commands.....	174-5
	Enable Power Capacitor Detection	174-5
	Enable Priority Disconnect.....	174-5
	Maximum Power (Watts)	174-5
	Operational	174-5
	Pool Mode	174-5
	Port Maximum Power (MilliWatts)	174-6
	Power State	174-6
	Protection Type	174-6
	Reserved CBS Max (%)	174-7
	Reserved CBS Min (%)	174-7
	Restoration Criteria.....	174-7
	Saved Slot NI Number.....	174-7
	Shutdown IOM for Memory Parity Errors	174-7
	Slot Priority	174-7
	Stacking Action	174-8
	Temperature Threshold (Celsius)	174-8
	Type	174-8

175 — Daughter Card and Daughter Card Slot parameters 175-1

175.1	Daughter Card and Daughter Card Slot parameters	175-2
	Administrative State	175-2
	Administrative State	175-2
	Assigned Daughter Card Type	175-2
	Assigned MCM Card Type	175-2
	Buffer Allocation Max (%)	175-2
	Buffer Allocation Min (%)	175-3
	Channel ID	175-3
	Clock Mode	175-3
	Clock Mode	175-4
	Companding Law	175-4
	Differential Timestamp Frequency	175-4
	Gateway IP Address	175-4
	In MDA Carrier Module Slot	175-4
	IP Address	175-5
	Mask	175-5
	Mode	175-5
	Packet Byte Offset	175-5
	Reserved CBS %	175-5
	Signalling Type	175-5
	Synchronous Ethernet	175-5
	Threshold High Burst Increase	175-6
	Threshold Low Burst Multiplier	175-6
	Use WRED Queue	175-6

176 — Bundles parameters 176-1

176.1	Bundles parameters	176-2
	Ack Timer	176-2
	Administrative State	176-2
	ATM Interface Cell Format	176-2
	ATM Minimum VPI Value	176-2
	Auto-Assign ID	176-2
	Bundle ID	176-2
	Bundle MRRU (bytes)	176-3
	Bundle Number	176-3
	Bundle Type	176-4
	Class Count	176-4
	Clock Source	176-4
	Configured MAC	176-4
	Daughter Card CLI Name	176-4
	Description	176-4
	DDM Event Suppression	176-5
	Encap Type	176-5
	End Point Class ID	176-5
	End Point ID	176-5
	Error Threshold	176-5
	Error Threshold	176-5
	First Network Element	176-5
	Fragment Threshold (bytes)	176-5
	Full Enquiry Interval	176-6

Hello Retry Count	176-6
Hello Timer.....	176-6
IMA Version.....	176-6
Link Activation Timer.....	176-6
Link Deactivation Timer.....	176-6
Link Fragmentation and Interleaving.....	176-7
LMI Mode.....	176-7
LMI Type	176-7
Magic Number	176-7
Maximum Links	176-7
MCFR Egress Qos Profile.....	176-8
MCFR Ingress Qos Profile	176-8
Minimum Links	176-8
Monitored Events.....	176-8
Monitored Events.....	176-8
MTU.....	176-8
Polling Interval (seconds)	176-8
Polling Interval (seconds)	176-9
Protection Type	176-9
Red Diff Delay (milliseconds).....	176-9
Red Diff Delay Action.....	176-9
Second Network Element	176-10
Short Sequence	176-10
Show Only Compatible Channels.....	176-10
Test Member	176-10
Test Pattern.....	176-10
Time Slots	176-10
Yellow Diff Delay (milliseconds)	176-10

177 – Port parameters

177-1

177.1	Port parameters	177-2
	Accounting Enabled.....	177-2
	Activation	177-2
	Administrative State	177-2
	Administrative State	177-2
	Administrative Status.....	177-3
	Advertised Capability.....	177-3
	Aggregate Rate Limit (kbps).....	177-3
	ALS Signal Type	177-4
	Applicant Mode	177-4
	Async Mapping	177-4
	Authenticate	177-4
	Auto-Assign ID.....	177-5
	Automatic VLAN Binding	177-5
	Auto-negotiate.....	177-5
	Backpressure	177-6
	BER Signal Degradation Threshold.....	177-6
	BER Signal Failure Threshold	177-6
	Bind Type	177-6
	Broadcast Limit (kbps)	177-7
	Broadcast Limit (Pkts/s)	177-7

Cable Length	177-7
CFM LoopBack Mode	177-8
Channel	177-8
Channel Number	177-10
Clock Source	177-10
Collect Accounting Statistics	177-11
Commands.....	177-11
Configured Alarms	177-11
Configured Data Rate (Gb/s)	177-13
Configured MAC.....	177-13
Control Mode.....	177-13
Controlled Port Control	177-13
Critical Event Notify	177-13
Db Loss.....	177-14
DDM Event Suppression.....	177-14
Default 802.1p.....	177-14
Default Classification	177-14
Default DSCP	177-15
Default VLAN Enable.....	177-15
Default VLAN Restore.....	177-15
Description	177-15
Destination MAC Address	177-15
Destination String	177-15
Detect Remote Faults	177-16
Detection	177-16
Dispersion	177-16
Dot1 Q Acceptable Frames	177-16
Dot1 Q Ethertype.....	177-16
Down When Looped	177-17
Duplex.....	177-17
Dying Gasp Notify	177-17
Egress Max-Burst	177-18
Egress Percentage of Rate (%).....	177-18
Egress Percentage of Rate (%).....	177-18
Egress Rate (Kbps)	177-18
Egress Scheduler Mode	177-19
Enable Multicast Limit Mode	177-19
Enable Port Mobility	177-19
Encap Type.....	177-19
Errored Frame Window (dsec).....	177-19
Errored Frame Period Window (frames)	177-20
Errored Frame Seconds Summary Window (dsec)	177-20
Ethernet Down Reason	177-20
Expected Payload Type (hex)	177-20
Expected Rx Bytes	177-20
Expected Rx Mode.....	177-21
Expected Rx String.....	177-21
First Network Element	177-21
FEC Mode	177-22
Flow	177-22
Forbid IGMP Snooping.....	177-22
Forward All Multicast Traffic	177-22

Frame-Based Accounting	177-23
Frames Delay (ms)	177-23
Framing	177-23
Hold Time (s)	177-23
Hold Time Down	177-23
Hold Time Down (100s of ms)	177-23
Hold Time Down (seconds).....	177-24
Hold Time Up	177-24
Hold Time Up (100s of ms).....	177-24
Hold Time Up (seconds)	177-24
Host String.....	177-25
Ignore BPDU	177-25
Ingress Filtering	177-25
Ingress Percentage of Rate (%).....	177-25
Ingress Percentage of Rate (%).....	177-26
Ingress Rate (Mbps)	177-26
Initialize	177-26
Inter-Frame Gap (bytes)	177-26
IP Source Filtering	177-26
J0 Byte	177-27
J0 String	177-27
Join Timer	177-27
Keep Alive Interval (Sec).....	177-27
L2Uplink	177-27
Leave All Timer.....	177-27
Leave Timer.....	177-28
Line Buildout.....	177-28
Line Code	177-28
Line Impedance.....	177-28
Line Length.....	177-29
Line Length.....	177-29
LLDP TLVs	177-30
Load Balance Algorithm	177-30
Loopback	177-30
Loopback	177-30
Loopback	177-31
MAC Address	177-31
Max Egress BW (kbps).....	177-31
Max Ingress BW (kbps).....	177-31
Max Req.....	177-32
Maximum Power (milliwatt)	177-32
Maximum Rate (Mbps)	177-32
Mode	177-32
Mode	177-32
Mode	177-33
MTU (bytes)	177-33
Multiplier (Intervals).....	177-33
Name	177-33
Notifications	177-34
Notify	177-34
Number of Frames	177-34
ODU-TIM reaction	177-34

Optical Transport Channel Unit	177-34
OPU-PLM reaction	177-34
OPU-TIM reaction	177-35
OTU-TIM reaction	177-35
Payload Type (hex)	177-35
Period Notify	177-35
Period Threshold (frames)	177-35
Periodic Timer	177-36
Periodic Transmission Status	177-36
Port Framing	177-36
Port Type	177-36
Port Usage	177-37
Power Priority	177-37
Power State	177-37
Protection Type	177-38
Q in Q Ethertype	177-38
Queue 1 through Queue 8	177-38
Q0	177-39
Q0	177-39
Q0	177-39
Q1	177-39
Q1	177-39
Q1	177-40
Q2	177-40
Q2	177-40
Q2	177-40
Q3	177-40
Q3	177-40
Q3	177-40
Q4	177-40
Q4	177-41
Q4	177-41
Q5	177-41
Q5	177-41
Q5	177-41
Q6	177-41
Q6	177-41
Q6	177-41
Q7	177-42
Q7	177-42
Q7	177-42
QoS Status	177-42
Quiet Period	177-42
Rate (Mbps)	177-42
Rate (Mbps)	177-43
Rate (Mbps)	177-43
Rate (Mbps)	177-43
Rate (Mbps)	177-44
Rate (Mbps)	177-44
Rate (Mbps)	177-44
Rate (Mbps)	177-44
Rate (Mbps)	177-45

Rate (Mbps)	177-45
Rate (Mbps)	177-45
Rate (kbps)	177-45
Reauth Enabled	177-45
Reauth Period	177-46
Reauthenticate Control	177-46
Received Remote Loopback Requests	177-46
Receiver	177-46
Registration Mode	177-47
Report Alarms	177-47
Reserved CBS%	177-48
Restoration Criteria	177-48
Restrict-Static-VLAN-Registration	177-48
Restrict-Advertisement	177-48
Restrict-Registration	177-49
Retry Timeout (Sec)	177-49
Rx Decision Threshold Voltage Adjustment	177-49
SAP Id	177-49
SD Threshold (10E-n bits received)	177-49
Seconds Summary Notify	177-49
Seconds Summary Threshold (framesec)	177-50
Second Network Element	177-50
Server Timeout	177-50
Servicing Mode	177-50
Set Local Loopback	177-51
Set Remote Loopback	177-51
SF Threshold (10E-n bits received)	177-52
SF-SD Method	177-52
Signal Mode	177-52
Single Fiber	177-52
Start L1-Ping	177-53
Status	177-53
SONET Section Trace Mode	177-53
Source MAC Address	177-53
Speed	177-53
SSM Code-Type	177-54
Status	177-54
Supplicant Timeout	177-54
Swap MAC Address	177-54
Synchronous status messages	177-54
Target Power	177-55
Test Name	177-55
Threshold (frames)	177-55
Time (seconds)	177-55
Timeout Period (Days)	177-55
Timeout Period (Hrs)	177-55
Timeout Period (Mins)	177-56
Traffic Type	177-56
Transmit Interval	177-56
Transmit Management Address	177-56
Transmitter Bytes	177-57
Transmitter Mode	177-57

Transmitter String.....	177-57
Trust Mode	177-58
Trusted.....	177-58
Tunneling	177-58
Tx DUS/DNU	177-59
Tx Period	177-59
Type	177-59
Type	177-59
Type	177-60
Type	177-60
Type	177-60
VLAN.....	177-60
Wave Key1.....	177-60
Wave Key2.....	177-63
Wave Tracker Encode.....	177-63
Wave Tracker Power Control	177-64
Weight in Group	177-64
Weight in Group	177-64
Weight in Group	177-64
Weight in Group	177-65
Weight in Group	177-65
Weight in Group	177-65
Weight in Group	177-65
Weight in Group	177-65
Weight in Group	177-66
XGig Mode	177-66

178 — HSMDA Egress Secondary Shaper parameters

178-1

178.1	HSMDA Egress Secondary Shaper parameters	178-2
	Class Burst Threshold (bytes).....	178-2
	Class 1 Burst Threshold (bytes)	178-2
	Class 2 Burst Threshold (bytes)	178-2
	Class 3 Burst Threshold (bytes)	178-2
	Class 4 Burst Threshold (bytes)	178-3
	Class 5 Burst Threshold (bytes)	178-3
	Class 6 Burst Threshold (bytes)	178-3
	Class 7 Burst Threshold (bytes)	178-3
	Class 8 Burst Threshold (bytes)	178-3
	Class Monitor Threshold (Kbytes)	178-3
	Class 1 Monitor Threshold (Kbytes).....	178-4
	Class 2 Monitor Threshold (Kbytes).....	178-4
	Class 3 Monitor Threshold (Kbytes).....	178-4
	Class 4 Monitor Threshold (Kbytes).....	178-4
	Class 5 Monitor Threshold (Kbytes).....	178-4
	Class 6 Monitor Threshold (Kbytes).....	178-5
	Class 7 Monitor Threshold (Kbytes).....	178-5
	Class 8 Monitor Threshold (Kbytes).....	178-5
	Class Rate (kbps)	178-5
	Class 1 Rate (kbps).....	178-6
	Class 2 Rate (kbps).....	178-6
	Class 3 Rate (kbps).....	178-6

Class 4 Rate (kbps)	178-6
Class 5 Rate (kbps)	178-6
Class 6 Rate (kbps)	178-6
Class 7 Rate (kbps)	178-7
Class 8 Rate (kbps)	178-7
High Burst Increase	178-7
Low Burst Limit	178-7
Low Burst Max Class	178-7
Monitor Threshold (Kbytes)	178-7
Name	178-8
Rate (Mbps)	178-8

179 – Channel parameters 179-1

179.1	Channel parameters	179-2
	Accounting Enabled	179-2
	Administrative State	179-2
	Administrative Status	179-2
	ATM Interface Cell Format	179-2
	ATM Minimum VPI Value	179-2
	BER SF Link Down	179-2
	Bit Error Insertion Rate	179-2
	C2 Byte (hex)	179-3
	Channel Framing	179-3
	Channelized	179-3
	Channel Type	179-4
	Clock Source	179-4
	Collect Accounting Statistics	179-4
	Compression	179-4
	Configured MAC	179-5
	CRC	179-5
	CRC Precision	179-5
	Description	179-5
	Destination ECID	179-5
	Destination IP Address	179-6
	Destination MAC Address	179-6
	Destination Port	179-6
	Down Count	179-6
	Drop Count	179-6
	Ds3 Channel Payload Type	179-6
	Duration (seconds)	179-7
	Edit ATM button	179-7
	Edit ILMI Link button	179-7
	Edit PPP button	179-7
	Egress Traffic Descriptor	179-7
	Encap Type	179-7
	Equipment ID Code	179-7
	Error Threshold	179-7
	Error Threshold	179-7
	Facility ID Code	179-8
	Fragment Threshold	179-8
	Frame ID Code	179-8

Full Enquiry Interval	179-8
Generator Number String	179-8
Idle Cycle Flags	179-8
ILMI Link VCI	179-9
ILMI Link VPI	179-9
IME Type	179-9
Ingress Traffic Descriptor	179-9
Interface ID	179-9
Interface Mapping	179-9
J1 String	179-10
Keep Alive (seconds)	179-10
Keep-Alive Polling Count	179-10
Keep-Alive Polling Frequency (seconds)	179-10
Keep-Alive Test Frequency (seconds)	179-10
Link Identifier	179-11
LMI Mode	179-11
LMI Type	179-11
Load Balance Algorithm	179-11
Local Channel ID	179-11
Local ECID	179-11
Local Port	179-12
Location ID Code	179-12
Loop Respond	179-12
Loopback	179-12
Max Jitter Expected (ms)	179-13
MCFR Egress QoS Profile	179-13
MDL Message Type	179-13
Mode	179-14
Mode	179-14
Monitored Events	179-14
Monitored Events	179-14
MTU (bytes)	179-14
Network Queue Policy Name	179-14
Pattern	179-15
Payload Scrambling Enabled	179-15
Payload Type	179-15
Period	179-16
Polling Interval (seconds)	179-16
Polling Interval (seconds)	179-16
Port Number String	179-16
Priority	179-16
Protocol	179-16
Protocol Version	179-17
Report Alarms	179-17
Reserved CBS%	179-18
Restore Keep-Alive Defaults	179-18
Respond to Remote Loop Signal	179-18
Samples Aggregation	179-19
Scramble	179-19
Signal Mode	179-19
Speed	179-19
STs1 Channel Payload Type	179-19

	Subrate CSU Mode	179-19
	Subrate Range	179-20
	Time Slots	179-20
	Time Slots per DS0 Channel Group	179-20
	Unit ID Code.....	179-20
	Up Count.....	179-20
	Vt15 Channel Payload Type.....	179-21
180	— Gateway parameters	180-1
180.1	Gateway parameters	180-2
	Administrative State	180-2
	Dynamic PCC	180-2
	EPC ID	180-2
	Group ID	180-2
	Node ID	180-2
181	— ISA-MG Group parameters	181-1
181.1	ISA-MG Group parameters	181-2
	Group ID	181-2
	Redundancy Type	181-2
182	— Common equipment navigation tree parameters	182-1
182.1	Common equipment navigation tree parameters	182-2
	Access Weight.....	182-2
	Access Weight.....	182-2
	Access Weight.....	182-2
	Accounting Enabled	182-2
	Administrative State	182-3
	Administrative Status.....	182-3
	ATM Interface Cell Format.....	182-3
	Auto-Assign ID.....	182-3
	Commands.....	182-3
	Commands.....	182-5
	Commands.....	182-5
	Configured MAC.....	182-5
	Default VLAN.....	182-6
	Description	182-6
	DDM Event Suppression.....	182-6
	Encap Type	182-6
	Error Threshold	182-8
	Error Threshold	182-9
	Error Threshold	182-9
	Full Enquiry Interval	182-9
	LMI Mode.....	182-9
	LMI Type	182-9
	Load Balance Algorithm	182-10
	Log-history	182-10
	MCFR Egress QoS Profile	182-10
	Mode	182-11

Monitored Events.....	182-11
Monitored Events.....	182-11
Monitored Events.....	182-12
MTU (bytes)	182-12
Multiple PDU Count	182-13
Network Weight	182-14
Network Weight	182-14
Network Weight	182-14
OLC State	182-14
Polling Interval	182-15
Polling Interval (seconds)	182-15
Polling Interval (seconds)	182-15
Reserved CBS%.....	182-15
Restoration Criteria.....	182-16
Restoration Criteria.....	182-16
Restoration Criteria.....	182-16
Speed.....	182-16
Telnet Session button	182-17
Statistics.....	182-17
Time Slots	182-17

OSPF navigation tree parameters

183 — OSPF navigation tree parameters	183-1
183.1 OSPF navigation tree parameters.....	183-2

IS-IS navigation tree parameters

184 — IS-IS navigation tree parameters	184-1
184.1 IS-IS navigation tree parameters.....	184-2

Routing navigation tree parameters

185 — NE parameters	185-1
185.1 NE parameters.....	185-2

186	— Routing Instance parameters	186-1
186.1	Routing Instance parameters	186-2
	Action	186-2
	Action	186-2
	Action	186-2
	Address	186-2
	Administrative State	186-2
	Administrative State	186-3
	Administrative State	186-3
	Admin Link Local Address	186-3
	Admin Link Local Address Preferred	186-3
	AFTR Address	186-3
	Aggregator.....	186-4
	Aggregator AS	186-4
	Aggregator IP Address	186-4
	Allow Directed Broadcasts	186-4
	Allow Send Force Renews	186-4
	As Set	186-4
	Auto-Assign.....	186-5
	Autonomous Address Configuration	186-5
	Autonomous System.....	186-5
	B4 Address.....	186-5
	Binding Database Mode.....	186-5
	Binding Persistency	186-6
	BGP Enabled	186-6
	Broadcast	186-6
	Broadcast Address Format	186-6
	Bypass Option-82 Check.....	186-6
	Cflowd Type.....	186-6
	Circuit ID	186-7
	Class.....	186-7
	Confederation Autonomous System	186-7
	Configured Primary Status	186-7
	Copy To Option 43	186-7
	Current Hop Limit	186-7
	Days	186-8
	Days	186-8
	Days	186-8
	Days	186-8
	Days	186-8
	Days	186-9
	Days	186-9
	Days	186-9
	Description	186-9
	DHCP Snooping Mode	186-9
	Displayed Name	186-10
	Dot1p.....	186-10
	DSCP.....	186-10
	DS Lite	186-11
	Egress Filter ID.....	186-11
	Enable DHCP Relay.....	186-11
	Enable Forwarding	186-11

Encap Type	186-11
Enforce Maximum Number Of Multicast Routes	186-11
End Address	186-12
EUI-64	186-12
Exclusive	186-12
Exported Address Prefix	186-12
Forwarding Address	186-12
Forwarding Class	186-13
Forwarding Delay (seconds)	186-13
Forwarding Option	186-13
Free Addresses Minimum Threshold	186-14
High Watermark	186-14
Hold Time (seconds)	186-14
Hours	186-14
Hours	186-15
Hours	186-15
Hours	186-15
Hours	186-15
Hours	186-15
Hours	186-15
Hours	186-16
Hours	186-16
IGMP Enabled	186-16
IGP Inhibit	186-16
Infinite	186-16
Ingress Filter ID	186-16
Inside IP Address	186-16
Inside Port	186-17
Interface ID	186-17
IP Address	186-17
IP Address 1	186-17
IP Address 2	186-17
IP Address 3	186-17
IP Address 4	186-17
IP Address Preferred	186-18
IP Address Prefix	186-18
IPv6 Address	186-18
IPv6 Prefix	186-18
IS-IS Enabled	186-18
L2TP Enabled	186-19
LDP Enabled	186-19
LDP Shortcut Enabled	186-19
LDP Synchronization Timer	186-19
Lifetime (seconds)	186-20
Lifetime (seconds)	186-20
Lifetime (seconds)	186-20
Loopback Enabled	186-20
Low Watermark	186-20
Lsp Name	186-21
MAC Address	186-21
MAC Address Verification	186-21
Managed Address Config	186-21
Max Interval (seconds)	186-21

Mask	186-22
Mask Reply	186-22
Maximum Declined Addresses Stored	186-22
Maximum Hops.....	186-22
Maximum Number of Equal Cost Routes	186-22
Member AS	186-22
Min Interval (seconds)	186-23
Minutes	186-23
Minutes	186-23
Minutes	186-23
Minutes	186-23
Minutes	186-24
Minutes	186-24
Minutes	186-24
Minutes	186-24
Minutes	186-24
MLD Enabled	186-25
Monitored Address Prefix	186-25
MPLS Enabled	186-25
MSDP Enabled	186-25
MTU.....	186-25
Name	186-25
NAT Pool Type	186-26
Netbios Node Type.....	186-26
Network Policy ID	186-26
Number	186-26
Number of Redirects.....	186-26
Number of TTL Expired.....	186-26
Number of Unreachables.....	186-27
On-Link Determination	186-27
Option.....	186-27
Option-82 Data Insertion	186-27
Option-82 Format Type.....	186-28
Option-82 User String.....	186-28
OSPFv2 Enabled	186-29
OSPFv3 Enabled	186-29
Other Stateful Config.....	186-29
Outside IP Address	186-29
Outside Port.....	186-29
P2MP ID	186-30
Peer Address	186-30
PIM Enabled	186-30
Physical Address.....	186-30
Port Forward Range End	186-30
Port Mode	186-30
Pool Name.....	186-31
Port Reservation Type.....	186-31
Port Reservation Value	186-31
Prefix Length.....	186-31
Primary	186-31
Protocol.....	186-31
PXE Support	186-32

Range End	186-32
Range Start.....	186-32
Reachable Time (milliseconds).....	186-32
Redirects	186-32
Redirects Time	186-32
Relay Agent Information Mode	186-32
Relay Agent Information Policy	186-33
Relay Service Description	186-33
Relay Service Port.....	186-34
Remote ID	186-34
Remote ID String	186-34
Retransmit Time (milliseconds)	186-34
RIP Enabled	186-34
Root Node	186-34
Router ID	186-34
Seconds	186-34
Seconds	186-35
Seconds	186-35
Seconds	186-35
Seconds	186-35
Seconds	186-35
Seconds	186-35
Seconds	186-35
Seconds	186-36
Send Advertisement	186-36
Sender Address	186-36
Server Name	186-36
Source Address Termination.....	186-37
Source IP Address	186-37
Source IP Application	186-37
Start Address.....	186-38
Steering Route Address Prefix.....	186-38
Strip Label.....	186-39
Subnet Mask	186-39
Subscriber Limit	186-39
Subscriber Prefix Length	186-39
Summary Only	186-39
Synchronization Timeout (seconds)	186-40
Timeout.....	186-40
TTL Expired	186-40
TTL Expired Time (seconds)	186-40
Tunnel; MTU (bytes)	186-40
Type	186-40
Type	186-40
Type	186-41
UDP Relay Service	186-41
Unreachables	186-41
Unreachables Time (seconds)	186-41
Use GI Address.....	186-41
Use Pool From Client	186-42
Use Virtual MAC Address	186-42

Value	186-42
VRF Name	186-42

187 – Bridge Instance parameters 187-1

187.1	Bridge Instance parameters	187-2
	Admin Edge.....	187-2
	Administrative State	187-2
	Auto Edge.....	187-2
	Auto VLAN Containment.....	187-2
	Bridge Max Hops	187-3
	CLI Name	187-3
	Connection Type	187-3
	Default Bridged Disposition.....	187-3
	Default IGMP Disposition	187-4
	Default Routed Disposition	187-4
	Default Servicing Mode.....	187-5
	Description	187-5
	Displayed Name	187-5
	Ethertype	187-5
	Hello Time (seconds)	187-5
	High MAC Range	187-6
	IGMP Snooping	187-6
	Instance BPDU Switching.....	187-6
	Instance Index	187-6
	Instance Name	187-7
	Jumbo Frame	187-7
	Last-Member Interval (seconds).....	187-7
	Learning Time Window (minutes).....	187-7
	Low MAC Range.....	187-8
	MAC Address	187-8
	MAC Address	187-8
	Max Age (seconds)	187-8
	Max. Filtered MACs to Learn.....	187-8
	Max. MAC Addresses to Learn	187-8
	Max VLAN	187-9
	Mode	187-9
	Mode	187-9
	Mode	187-9
	MVR Admin Status	187-10
	MVR Source Interface.....	187-10
	Path Cost	187-10
	Path Cost	187-10
	Path Cost	187-10
	Port Action	187-11
	Port Max Group.....	187-11
	Priority.....	187-11
	Priority.....	187-12
	Priority.....	187-12
	Priority.....	187-12
	Protocol.....	187-12
	Q0.....	187-13

Q1.....	187-13
Q2.....	187-13
Q3.....	187-13
Q4.....	187-13
Q5.....	187-13
Q6.....	187-13
Q7.....	187-14
QoS Status.....	187-14
Query Interval (seconds)	187-14
Query Source IP Zero	187-15
Query Time (seconds)	187-15
Region Name	187-15
Region Revision	187-15
Response Time (seconds)	187-15
Restricted Role	187-16
Restricted TCN.....	187-16
Robustness (packets)	187-16
Status	187-17
Status	187-17
STP Mode	187-17
Super VLAN Uplink Interface	187-17
TLS Admin Status.....	187-18
TLS Mode	187-18
TLS Uplink Interface	187-18
Transparent Switching Status	187-18
Trap Threshold	187-19
Trust Ports	187-19
TX Hold Count	187-19
Upper Ring Adjacency	187-19
Violation	187-19
VLAN ID	187-20
VLAN Registration Protocol Type	187-20

188 – Interface parameters

188-1

188.1	Interface parameters	188-2
	Administrative State	188-2
	Administration Status.....	188-2
	Allow Directed Broadcasts	188-2
	Broadcast	188-2
	Broadcast Address Format	188-2
	Cflowd Type.....	188-2
	Class.....	188-2
	Description	188-2
	Echo Interval.....	188-2
	Egress Filter ID.....	188-3
	Enable Local Proxy.....	188-3
	Enable Local Proxy ARP	188-3
	IGP Inhibit	188-3
	Ingress Filter ID.....	188-3
	Interface ID	188-3
	IP Address	188-3

Lifetime (seconds)	188-3
Lifetime (seconds)	188-4
MAC Address	188-4
Mask Reply	188-4
Multiplier	188-4
Name	188-4
Network Policy ID	188-4
No Expiry	188-4
No Expiry	188-5
Number of Redirects	188-5
Number of TTL Expired	188-5
Number of Unreachables	188-5
Physical Address	188-5
Policy 1	188-5
Policy 2	188-5
Policy 3	188-5
Policy 4	188-5
Policy 5	188-5
Port	188-5
Primary	188-6
Proxy Arp Policy 1	188-6
Proxy Arp Policy 2	188-6
Proxy Arp Policy 3	188-6
Proxy Arp Policy 4	188-6
Proxy Arp Policy 5	188-6
Receive Interval	188-6
Redirects	188-7
Redirects Time (seconds)	188-7
Remote Proxy ARP	188-7
Router ID	188-7
Routing Instance ID	188-7
Subnet Mask	188-7
Transmit Interval	188-7
Timeout	188-7
Trusted	188-8
TTL Expired	188-8
TTL Expired Time (seconds)	188-8
Unnumbered Reference	188-8
Unnumbered Type	188-8
Unreachables	188-9
Unreachables Time (seconds)	188-9
View the newly created Network Interface	188-9
What type of interface would you like to create?	188-9

189 – BGP parameters

189-1

189.1	BGP parameters	189-2
	Address Family	189-2
	Address Family	189-2
	Administrative State	189-2
	Advertise Inactive Routes	189-2
	Advertise Label	189-3

Advertise LDP Prefix	189-3
Aggregator ID Zero	189-3
Apply Export Route Policies	189-4
Apply Import Route Policies	189-4
AS Override.....	189-5
AS Path Ignore	189-5
AS Path Ignore Family	189-5
Cluster ID	189-6
Connect Retry Time (seconds)	189-6
Damping	189-6
Description	189-7
Disable 4Byte ASN	189-7
Disable Client Reflect	189-7
Disable Extended Communities	189-7
Disable Fast External Failover.....	189-8
Disable Standard Communities	189-8
Disallow IGP.....	189-9
Dynamic Peer	189-9
EIBGP LoadBalance.....	189-9
Enable Inter AS VPRN	189-9
Enable Peer Tracking	189-10
Enable Rapid Withdrawal	189-10
Graceful Restart.....	189-10
Hold Time (seconds)	189-10
Hold Time Strict	189-11
IBGP MultiPath.....	189-11
Inherit Value	189-11
Keep Alive (seconds).....	189-11
Key	189-11
Limited.....	189-12
Local Address	189-12
Local AS.....	189-12
Local Preference	189-12
Loop Detect	189-13
MED Compare	189-13
MED Source.....	189-13
MED Value	189-14
Min AS Origination (seconds)	189-14
Min. Route Advertisement	189-14
Minimum TTL Value	189-14
Multi Hop	189-14
Multi Path	189-15
Name	189-15
Next Hop Self	189-15
Passive	189-15
Peer Address	189-16
Peer AS.....	189-16
Peer Type.....	189-16
Policy 1	189-16
Policy 2	189-17
Policy 3	189-17
Policy 4	189-17

	Policy 5	189-17
	Preference	189-17
	Prefix Limit.....	189-17
	Prefix Limit Log Only	189-17
	Prefix Limit Threshold.....	189-18
	Private	189-18
	Purge Time (minutes)	189-18
	Remove Private AS	189-18
	Router ID	189-19
	Stale Routes Time (seconds)	189-19
	Type.....	189-19
190	— IGMP parameters	190-1
190.1	IGMP parameters	190-2
	Administrative State	190-2
	Administrative Version	190-2
	Configured Source.....	190-2
	Configured Source Type.....	190-2
	Constraint Admin State.....	190-2
	Description	190-2
	End Mcast Address	190-3
	End Mcast Address Type.....	190-3
	Import Policy.....	190-3
	Last Member Query Interval (seconds).....	190-3
	Last Member Query Interval (tenths of seconds).....	190-3
	Lsp Name	190-3
	Mandatory Bandwidth (kbps)	190-4
	Max Group	190-4
	Max Group Action	190-4
	Maximum Number of Groups	190-4
	Protocol Version	190-4
	Proxying	190-5
	Querier Forwarding	190-5
	Query Interval (seconds)	190-5
	Query Response Interval (seconds)	190-5
	Query Response Interval (tenths of seconds)	190-6
	Querying	190-6
	Robust Count.....	190-6
	Robust Count.....	190-6
	Router Timeout (seconds)	190-7
	Source Timeout (seconds)	190-7
	Spoofing	190-7
	Start Mcast Address	190-7
	Start Mcast Address Type	190-7
	Static Multicast Group.....	190-7
	Static Source	190-8
	Subnet Check	190-8
	Unconstrained Bandwidth (kbps)	190-8
	Unsolicited Report Interval (seconds).....	190-8
	Zapping	190-8

191 – L2TP parameters 191-1

191.1	L2TP parameters	191-2
	Administrative State	191-2
	Authentication Protocol	191-2
	Auto Established	191-2
	AVP Hiding	191-2
	Calling Number Format	191-3
	Challenge	191-3
	Description	191-3
	Destruct Timeout (seconds)	191-3
	Excluded AVPs	191-4
	Group Name	191-4
	Hello Interval (seconds)	191-4
	Idle Timeout (seconds)	191-4
	IPCP Subnet Negotiation	191-5
	Keep-Alive Interval (seconds)	191-5
	Keep-Alive Multiplier	191-6
	LNS Group ID	191-6
	Local IP Address	191-6
	Local Name	191-7
	Max Retries Established	191-7
	Max Retries Not Established	191-7
	MTU (bytes)	191-7
	Password	191-8
	Peer Address Change Policy	191-8
	Peer IP Address	191-8
	Preference	191-8
	Proxy Authentication	191-9
	Proxy LCP	191-9
	Receive Window Size	191-9
	Remote Name	191-9
	Session Assign Method	191-10
	Session Limit	191-10
	Tunnel Name	191-10
	Type	191-11

192 – LDP parameters 192-1

192.1	LDP parameters	192-2
	Address Type	192-2
	Administrative State	192-2
	Administrative State	192-2
	Administrative State	192-2
	Administrative State	192-3
	Advertised Label	192-3
	Aggregate Prefix Match Enabled	192-3
	Description	192-3
	Discovery Interval (Minutes)	192-3
	Discovery Timeout (Seconds)	192-3
	DoD Label Distribution	192-4
	Enforce Graceful Restart	192-4
	FEC Prefix	192-4

Forward State Holding Time (seconds)	192-4
Forwarding Class	192-4
Hello Factor	192-4
Hello Timeout (seconds)	192-5
IP Prefix.....	192-5
Keep-Alive Factor	192-5
Keep-Alive Timeout (seconds)	192-5
Key	192-6
LDP Prefix	192-6
LDP Prefix Length	192-6
Local LSR ID	192-6
Maximum Failures	192-6
Maximum Paths	192-6
Maximum Recovery Time (seconds)	192-6
Maximum Time to Live	192-7
Maximum TTL	192-7
Minimum TTL Value	192-7
Multicast Forwarding	192-7
Multi Path Make Before Break Time (seconds).....	192-7
Name	192-7
Neighbor Liveness Time (seconds).....	192-8
NE Persistent.....	192-8
Next Hop.....	192-8
Next Hop Type.....	192-8
Number of Test Probes	192-8
Probe History Size.....	192-8
Probe Interval (seconds)	192-9
Peer Address	192-9
Policy 1	192-9
Policy 2	192-9
Policy 3	192-9
Policy 4	192-9
Policy 5	192-9
Prefer Tunnel-in-Tunnel	192-9
Prefix Length.....	192-9
Probe Interval (Minutes)	192-10
Probe Timeout (seconds).....	192-10
Probe Timeout (Minutes).....	192-10
Profile.....	192-10
Reconnect Time (seconds).....	192-10
Remote Peer	192-10
Retry Count	192-10
Retry Count	192-10
Retry Counter	192-11
Swap Label	192-11
Targeted Sessions Allowed.....	192-11
Timeout (seconds)	192-11
Trap Generation.....	192-11
Tree Trace	192-12
Tunnel Down Damp Time (seconds)	192-12
Tunneling Enabled	192-12
Type.....	192-12

193 — MLD parameters	193-1
193.1 MLD parameters	193-2
Configured Source	193-2
End Multicast Address	193-2
End Multicast Address	193-2
Group Address	193-2
Group Source Address	193-2
Import Policy	193-2
Last Member Query Interval (seconds)	193-3
Maximum Number of Groups	193-3
Maximum Response Time between Group Messages (seconds)	193-3
Maximum Response Time For MLDv2 (seconds)	193-3
Query Interval (seconds)	193-3
Query Interval (seconds)	193-4
Query Response Interval (seconds)	193-4
Robust Count	193-4
Start Multicast Address	193-4
Start Multicast Address	193-4
194 — MPLS parameters	194-1
194.1 MPLS parameters	194-2
Adjust Multiplier	194-2
Administrative State	194-2
Administrative State	194-2
Collect Accounting Statistics	194-2
CSPF On Loose Hop	194-2
Description	194-2
Enable	194-3
Enable	194-3
Enable SRLG for FRR	194-3
Exponential Backoff Retry	194-4
Fast Reroute	194-4
Groups Included	194-4
Hold Timer (seconds)	194-4
Include Groups Assigned	194-4
Include Groups Unassigned	194-4
Inter Area CSPF To First Loose Hop	194-5
Least Minimum Threshold	194-5
Least Reoptimization Threshold	194-5
LSP Name	194-5
Propagate Admin Group	194-6
Resignal Timer (min)	194-6
Sample Multiplier	194-6
Sender Address	194-6
Static LSPs Fast Retry Timer (seconds)	194-6
Strict	194-7
View the newly created MPLS path	194-7

195 — MSDP parameters 195-1

195.1	MSDP parameters.....	195-2
	Administrative State	195-2
	Data Encapsulation.....	195-2
	Default Peer.....	195-2
	IP Prefix.....	195-2
	Key	195-2
	Local IP Address	195-2
	Mask	195-3
	Mode	195-3
	Name	195-3
	Peer Address	195-3
	Receive Message Interval (seconds)	195-3
	Receive Message Rate	195-3
	Receive Message Threshold	195-4
	RPF Lookup Sequence	195-4
	SA Cache Lifetime (seconds)	195-4
	SA Limit	195-4
	Type	195-4

196 — PIM parameters 196-1

196.1	PIM parameters.....	196-2
	Administrative State	196-2
	Administrative State IPv4	196-2
	Apply To	196-2
	Assert Period.....	196-2
	Auto-Discovery.....	196-2
	Bandwidth (kbps).....	196-3
	BFD Enabled.....	196-3
	BSM Check Router Alert	196-3
	CBSR Address.....	196-3
	CBSR Address.....	196-3
	CBSR Admin State	196-4
	CBSR Admin State	196-4
	CBSR Hash Mask Length	196-4
	CBSR Hash Mask Length	196-4
	CBSR Priority	196-4
	CBSR Priority	196-5
	C-RP Address.....	196-5
	C-RP Address.....	196-5
	C-RP Hold Time (seconds)	196-5
	C-RP Hold Time (seconds)	196-5
	C-RP Priority	196-5
	C-RP Priority	196-6
	Data MDT Delay Interval	196-6
	Data MDT Prefix	196-6
	Data MDT Prefix Length	196-6
	Delay Interval (seconds).....	196-6
	Description	196-6
	DR Priority.....	196-6
	ECMP Balancing Enabled	196-7

ECMP Hashing Enabled.....	196-7
Embedded-RP Administrative State	196-7
Enable Embedded-RP	196-7
Group Address	196-8
Group IP Address	196-8
Group Prefix Length	196-8
Hello Interval (seconds)	196-8
Hello Multiplier	196-8
Hold Time (minutes)	196-9
Improved assert	196-9
Inclusive Tunnel Type	196-9
Infinity For Threshold.....	196-9
IPv4 Administrative State	196-9
IPv6 Administrative State	196-10
IPv4 RPF Lookup Sequence.....	196-10
IPv6 RPF Lookup Sequence.....	196-10
Lag Usage Optimization	196-10
Level ID	196-10
Level	196-11
Lsp Name	196-11
Mandatory Bandwidth (kbps)	196-11
Mask	196-11
Max Groups	196-11
MCast Signaling	196-11
MDT Default Group Address	196-12
Multicast Senders.....	196-12
Non DR Attract Traffic.....	196-12
Number of Ports Down	196-12
P2MP Administrative State.....	196-12
P2MP Administrative State.....	196-13
Pack Data Join TLV.....	196-13
Peer IP Address	196-13
PIM SSM Prefix	196-13
PIM SSM Prefix Length	196-13
Policy 1	196-14
Policy 2	196-14
Policy 3	196-14
Policy 4	196-14
Policy 5	196-14
Prefix.....	196-14
Provider Tunnel Inclusive PIM Mode	196-14
RP IP Address	196-15
RP Override	196-15
Sender Address	196-15
Sender Address Type.....	196-15
SSM Group IP Address.....	196-15
SSM Group Mask	196-16
Static Group IP Address	196-16
Static Group Mask	196-16
Static RP IP Address.....	196-16
Sticky DR.....	196-16
Sticky DR Priority.....	196-16

Three Way Hello.....	196-17
Threshold (kbps).....	196-17
Tracking Support	196-17
Unconstrained Bandwidth (kbps)	196-17

197 — RIP parameters **197-1**

197.1	RIP parameters	197-2
	Administrative State	197-2
	Check Zero	197-2
	Description	197-2
	Flush.....	197-2
	Inherit Value	197-2
	Key	197-2
	Message Size	197-3
	Metric In	197-3
	Metric Out.....	197-3
	Name	197-3
	Policy 1	197-4
	Policy 2	197-4
	Policy 3	197-4
	Policy 4	197-4
	Policy 5	197-4
	Preference	197-4
	Propagate RIP Metric	197-4
	Receive	197-4
	Select Locale.....	197-5
	Send	197-5
	Split Horizon	197-5
	Timeout.....	197-6
	Type	197-6
	Update	197-6

198 — RSVP parameters **198-1**

198.1	RSVP parameters	198-2
	Administrative State	198-2
	BFD Enabled.....	198-2
	Description	198-2
	Class Type 0 BW Percent	198-2
	Class Type 1 BW Percent	198-2
	Class Type 2 BW Percent	198-2
	Class Type 3 BW Percent	198-2
	Class Type 4 BW Percent	198-2
	Class Type 5 BW Percent	198-3
	Class Type 6 BW Percent	198-3
	Class Type 7 BW Percent	198-3
	Diff Serv Model	198-3
	Down Threshold (%)	198-4
	Enable Graceful Shutdown.....	198-4
	Enable Refresh Reduction.....	198-5
	Enable Reliable Delivery	198-5

FC Name	198-5
Hello Interval (milliseconds)	198-5
Include Node in RRO	198-6
Inherit SAM Class Type BW	198-6
Inherit TE Down Thresholds	198-6
Inherit TE Up Thresholds	198-6
Keep Multiplier	198-7
Key	198-7
Max Burst	198-7
Message Pacing	198-7
Period (milliseconds)	198-7
Priority	198-7
Rapid Retransmit Time (hundred-milliseconds)	198-7
Rapid Retry Limit	198-8
Refresh Time	198-8
Subscription Ratio	198-8
TE Class Type	198-8
TE Threshold Update Enabled	198-9
Up Threshold (%)	198-9
Update On CAC Failure Enabled	198-10
Update Timer (seconds)	198-10

199 — IS-IS parameters

199-1

199.1	IS-IS parameters	199-2
	Administrative State	199-2
	Advertise Only Passive Interfaces	199-2
	Area ID	199-2
	BFD Enabled	199-2
	CSNP Authentication	199-2
	CSNP Interval (seconds)	199-3
	Description	199-3
	Enable Authentication	199-3
	Enable IPv4	199-3
	Enable IPv6	199-3
	Enable LDP Synchronization	199-4
	Export Limit	199-4
	Export Limit Log Percent	199-4
	External	199-4
	Graceful Restart	199-4
	Hello Authentication	199-4
	Hello Interval (seconds)	199-4
	Hello Multiplier	199-5
	Helper Mode	199-5
	IID TLV	199-5
	Instance ID	199-5
	Internal	199-5
	IPv6 Routing TLV type	199-6
	IPv6 Unicast Multi-Topology	199-6
	Isis Default Route Tag	199-6
	Key	199-6
	L1 MAC Address	199-6

L2 MAC Address	199-6
LDP Over RSVP Include	199-7
Level Capability	199-7
LSP Initial Wait (seconds)	199-7
LSP Lifetime (seconds)	199-7
LSP Max Wait (seconds)	199-8
LSP Pacing Interval (seconds)	199-8
LSP Second Wait (seconds)	199-8
Mask	199-8
Mesh Group.....	199-9
Mesh Group Status	199-9
Metric	199-9
Multicast Import	199-9
Multi-Topology.....	199-9
Name	199-10
Network.....	199-10
Overload	199-10
Overload On Boot	199-10
Overload On Boot Timeout (seconds)	199-11
Overload Timeout (seconds).....	199-11
Passive	199-11
Policy 1	199-12
Policy 2	199-12
Policy 3	199-12
Policy 4	199-12
Policy 5	199-12
Priority.....	199-12
PSNP Authentication	199-13
Reference Bandwidth.....	199-13
Remove Key button	199-13
Retransmit Interval (seconds)	199-13
Route Tag.....	199-13
SPF Initial Wait (milliseconds)	199-13
SPF Max Wait (seconds)	199-14
SPF Second Wait (milliseconds)	199-14
Strict Adjacency Check.....	199-14
Summary Level	199-15
Summary Route Tag.....	199-15
Traffic Engineering.....	199-15
Type	199-15
Unicast Import	199-15
Wide Metrics Only	199-16

200 — OSPF parameters

200-1

200.1	OSPF parameters	200-2
	Administrative State	200-2
	Advertise Subnet	200-2
	Area ID	200-2
	Authentication Type	200-2
	Autonomous System Border Router.....	200-3
	BFD Enabled.....	200-3

Blackhole Range	200-3
Boot Overload Enabled	200-3
Boot Overload Interval (seconds)	200-4
Change Password button	200-4
Configured MTU (bytes)	200-4
Default Cost	200-4
Description	200-5
Domain ID	200-5
Enable LDP Synchronization	200-5
Effect	200-5
Exit Overflow Interval	200-5
External LSA Limit	200-6
External.....	200-6
Graceful Restart.....	200-6
Hello Interval (seconds)	200-6
Helper Mode	200-7
ID	200-7
Ignore DN Bit.....	200-7
Initial Wait (milliseconds).....	200-7
Initial Wait (milliseconds).....	200-7
Interface Base Reference Cost (kbps).....	200-8
Internal	200-8
Instance ID	200-8
Interface Name	200-8
IPsec In Static Security Association.....	200-9
IPsec Out Static Security Association	200-9
IPsec Security Association Name.....	200-9
Key	200-9
Key Index	200-9
LDP over RSVP Include.....	200-9
Link State DB Type.....	200-9
LSA Arrival Wait (milliseconds)	200-10
LSA Generate Max Wait (milliseconds).....	200-10
Metric	200-10
Multicast Import	200-11
Name	200-11
Network.....	200-11
Originate Default Route	200-11
OSPF Router ID.....	200-12
Overload Enabled	200-12
Overload Interval (seconds)	200-12
Overload Stubs.....	200-13
Passive	200-13
Password.....	200-13
Policy 1	200-13
Policy 2	200-14
Policy 3	200-14
Policy 4	200-14
Policy 5	200-14
Poll Interval (seconds).....	200-14
Prefix Length.....	200-14
Priority.....	200-14

Redistribute External Routes	200-15
Re-enter Key	200-15
Re-enter Password	200-15
Remote Neighbor IP Address	200-15
Retransmission Interval (seconds)	200-15
RFC1583 Compatible	200-16
Router Dead Interval (seconds)	200-16
Second Wait (milliseconds)	200-16
Second Wait (milliseconds)	200-17
SPF Max Wait (milliseconds)	200-17
Super-Backbone	200-18
Suppress DN Bit	200-18
Traffic Engineering Support	200-18
Transit Area	200-18
Transit Delay (seconds)	200-19
Transmit Interval	200-19
Type	200-19
Unicast Import	200-20
Version	200-20
Virtual Neighbor Router (Site) ID	200-20
VPN Domain ID (hex)	200-20
VPN Domain Type	200-21
VPN Tag	200-21

201 — Network Domain parameters **201-1**

201.1	Network Domain parameters	201-2
	Description	201-2
	Domain Name	201-2
	Interface Association Count	201-2
	Routing Instance ID	201-2
	Routing Instance Name	201-2
	SDP Association Count	201-2
	Site Name	201-2
	Site ID	201-2
	Network Interfaces tab	201-2
	Service Tunnels tab	201-3

202 — Static Routes parameters **202-1**

202.1	Static Routes parameters	202-2
	Administrative State	202-2
	Auto-Assign ID	202-2
	BFD Enabled	202-2
	Destination	202-2
	Disallow IGP	202-2
	Drop Count	202-2
	Enable CPE Check	202-2
	Interval (seconds)	202-2
	IP Address	202-3
	Log	202-3
	Mask	202-3

Metric	202-3
Multicast Capable Peers.....	202-4
Preference	202-4
Prefix Length.....	202-4
Static Route ID.....	202-4
Target IP Address.....	202-4
Type	202-4
Unnumbered Interface	202-5

203 – Common network navigation tree parameters 203-1

203.1	Common network navigation tree parameters	203-2
	Action	203-2
	Administrative State	203-2
	Advertise Tunnel Links Enabled	203-2
	Allow Directed Broadcasts	203-2
	Auto-Assign ID.....	203-3
	BFD Enabled.....	203-3
	Broadcast	203-3
	Broadcast Address Format	203-3
	Cflowd Type.....	203-4
	Class.....	203-4
	Constraint Admin State.....	203-5
	Description	203-5
	Disable Router Alert Check	203-5
	Disallow IGP.....	203-5
	DoD Label Distribution	203-6
	Egress Filter ID.....	203-6
	Enable DHCP Relay.....	203-6
	Enable Implicit Null Label	203-6
	Enable Ingress Flowspec	203-7
	Enable LDP Synchronization	203-7
	Family.....	203-8
	Force Q Tag Forwarding.....	203-8
	Graceful Restart.....	203-9
	Group IP Address	203-9
	Group IP Address	203-9
	Group IP Address	203-10
	Helper Mode	203-10
	IGP Inhibit	203-10
	IGP Shortcut.....	203-10
	Ingress Filter ID.....	203-11
	Inherit Value	203-11
	Interface Name	203-11
	IP Address	203-11
	IPv4 RPF Lookup Sequence.....	203-12
	IPv6 Allowed	203-12
	IPv6 BFD Enabled.....	203-12
	Key	203-12
	Lease Populate	203-13
	LDP	203-13
	LDP over RSVP Include.....	203-13

LDP Synchronization Timer	203-14
LSR IP Load Balancing	203-14
MAC Address	203-14
Mandatory Bandwidth (kbps)	203-14
Mask Reply	203-15
Minimum TTL Value	203-15
Maximum TTL	203-15
Multicast Import	203-16
Name	203-16
Network Policy ID	203-16
Number of Packet Too Big	203-16
Number of Param Problem	203-16
Number of Redirects	203-16
Number of Time Exceeded	203-17
Number of TTL Expired	203-17
Number of Unreachables	203-17
Packet Too Big	203-17
Packet Too Big Time (seconds)	203-17
Param Problem	203-18
Param Problem Time (seconds)	203-18
Path MTU Discovery Enabled	203-18
Physical Address	203-18
PIM RP Delayed Up Period	203-18
Policy 1	203-19
Policy 2	203-19
Policy 3	203-19
Policy 4	203-19
Policy 5	203-20
Populate Host Routes	203-20
Preference	203-20
Prefix Length	203-21
Prefix Length	203-21
Prefix Length	203-21
Prefix Length	203-21
Prefix Length	203-21
Prefix Length	203-21
Prefix Length	203-22
Prefix Length	203-22
Primary	203-22
Redirects	203-22
Redirects Time (seconds)	203-22
Router ID	203-22
RSVP Shortcut Enabled	203-23
Server 1	203-23
Server 2	203-23
Server 3	203-23
Server 4	203-23
Server 5	203-23
Server 6	203-24
Server 7	203-24
Server 8	203-24
Service ID	203-24
Subnet Mask	203-24

Tag	203-24
TE Metric	203-24
TE Metric Enabled	203-25
Time Exceeded	203-25
Time Exceeded Time (seconds)	203-25
Timeout (seconds)	203-25
TTL Expired	203-26
TTL Expired Time (seconds)	203-26
Type	203-26
Type	203-26
Type	203-27
Unconstrained Bandwidth (kbps)	203-27
Unicast Import	203-27
Unreachables	203-28
Unreachables Time (seconds)	203-28

Ring Group navigation tree parameters

204 — Network parameters	204-1
204.1 Network parameters	204-2
Description	204-2
Enabled	204-2
Ethertype	204-2
Group Name	204-2
Jumbo Frame	204-2
Mode	204-3
Query Response Time (seconds)	204-3
Ring Group Type	204-3

5620 SAM Parameter Guide overview

1 — 5620 SAM Parameter Guide overview

1 — 5620 SAM Parameter Guide overview

1.1 5620 SAM Parameter Guide overview 1-2

1.1 5620 SAM Parameter Guide overview

The *5620 SAM Parameter Guide* is intended for network planners, administrators, operators, OSS application developers, and technical support staff who use a 5620 SAM GUI or OSS client. The guide provides the following information for parameters that you can configure using the 5620 SAM:

- descriptions that include ranges and default values
- options and option descriptions
- dependencies on device types, device releases, and on other parameter settings
- equivalent OSS property names for use with the 5620 SAM-O

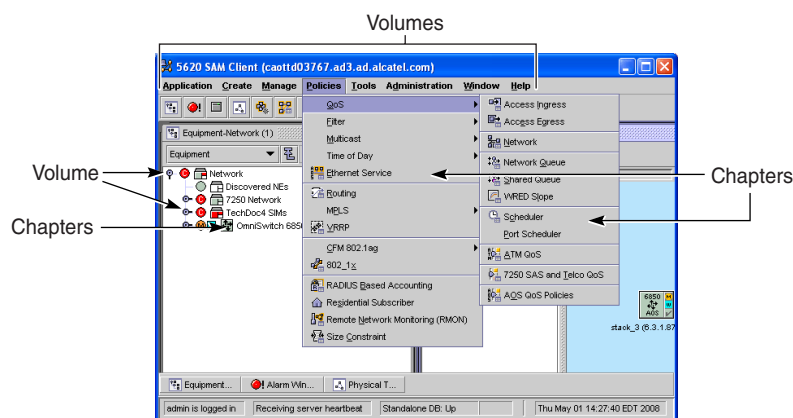


Note — A parameter that represents a percentage value may accept a non-integer value such as 48.15. This is not indicated in the parameter range description.

5620 SAM Parameter Guide structure

The *5620 SAM Parameter Guide* structure is based on the 5620 SAM GUI menu and navigation tree layouts, as shown in Figure 1-1.

Figure 1-1 GUI-based elements of *5620 SAM Parameter Guide* structure



17549

Each volume of this guide maps to a 5620 SAM main menu option or navigation tree view. For example, the “[Create menu parameters](#)” volume contains the configurable parameters on the forms and child forms that you can open using the Create menu option, and the “[Routing navigation tree parameters](#)” volume contains the configurable parameters on the forms and child forms that you can open using right-click contextual menu options in the Routing view of the navigation tree.



Note — The Help and Window 5620 SAM main menu options have no associated *5620 SAM Parameter Guide* chapters because the options provide no access to configurable parameters:

Each chapter maps to a submenu option and contains the configurable parameters on the forms and child forms that you can open using the submenu. The parameters in a chapter are listed in alphabetical order.

Each parameter is in the chapter associated with the most direct GUI path to the parent object. For example, although you can configure port parameters using a service creation form, the port parameters are described in the Physical port parameters chapter of the “[Equipment navigation tree parameters](#)” volume.

Searching for information

The *5620 SAM Parameter Guide* table of contents contains a live link to each parameter. In addition, you can use the following search mechanisms.

- In a PDF document, you can search for a parameter using the text search function.
- In an InfoPort document, you can search for a parameter using the InfoPort search Topic or Title option.

Procedure 1-1 To view *5620 SAM Parameter Guide* parameter descriptions from the *5620 SAM User Guide*

Perform this procedure to view the *5620 SAM Parameter Guide* description of a parameter in the *5620 SAM User Guide*.



Note 1 — The *5620 SAM Parameter Guide* and *5620 SAM User Guide* must be located in the same directory.

Note 2 — Adobe Reader Release 5.0 or later is required.

- 1 If the *5620 SAM User Guide* and the *5620 SAM Parameter Guide* are open, click on the parameter name in the *5620 SAM User Guide*. The parameter description in the *5620 SAM Parameter Guide* is displayed.
- 2 If only the *5620 SAM User Guide* is open, perform the following steps.
 - i Click on the parameter name in the *5620 SAM User Guide*. The *5620 SAM User Guide* closes, and the *5620 SAM Parameter Guide* opens to display the parameter description.
 - ii To reopen the *5620 SAM User Guide*, perform one of the following.
 - Choose View→Go To→Previous View from the Adobe Reader main menu.
 - Click on the Previous View button in the Adobe Reader tool bar.
 - Press ALT+←.

The *5620 SAM Parameter Guide* closes, and the *5620 SAM User Guide* opens to the previously viewed page.

5620 SAM-O OSS properties

A 5620 SAM GUI function typically has an equivalent OSS function, unless the function is GUI-specific, for example, display customization. The 5620 SAM design schema uses the following object hierarchy:

- package—a functional area, for example, L3 forwarding, which is called l3fwd in the 5620 SAM object model
- class—an object type in a package, for example, service site, which is called ServiceSite in the l3fwd package
- property—an attribute of an object, such as Service Name, which is called serviceName in the ServiceSite class

The *5620 SAM Parameter Guide* does not include references to OSS schema packages or classes, but does map the displayed name of each GUI parameter to the equivalent OSS property name using the following format:

GUI Displayed Name (equivalentOssPropertyName)

Table 1-1 lists the GUI and OSS elements of a 5620 SAM parameter as an example.

Table 1-1 Example mapping of 5620 SAM parameter to 5620 SAM-O property

5620 SAM GUI parameter	5620 SAM-O OSS property
Menu option: Tools→Statistics→Accounting Policies	Package name: accounting
Form name: Accounting Policy	Class name: Policy
Parameter name: Collection Interval (m)	Property name: collectionInterval

See the 5620 SAM-O XML Online Reference for information about OSS packages, classes, and properties.

Application menu parameters

2 – Task Manager parameters

3 – User Preferences parameters

2 – *Task Manager parameters*

2.1 Task Manager parameters 2-2

2.1 Task Manager parameters

This chapter describes the parameters on the Task Manager form and child forms.

autoRefreshInterval

The autoRefreshInterval parameter specifies how often, in s, the Task Manager searches for new tasks when the Task Manager is open. The range is 0, or 5 to 600. The default is 20. A value of 0 means the parameter is disabled. The parameter does not take effect until the client is restarted.

failedTasksPurgeInterval

The failedTasksPurgeInterval parameter specifies how often, in min, to remove all of the tasks that are not in the In Progress state. The range is 0, or 5 to 10 080. The default is 1440. A value of 0 means the parameter is disabled.

maxNumRetainedTasks

The maxNumRetainedTasks parameter specifies the maximum number of monitored tasks that the Task Manager displays. The count includes the top-level tasks and all sub-tasks. When the value is reached, the system automatically deletes successful tasks, starting with the earliest. The deleted tasks appear in XML format in the TaskTracker.log file, which is located in the log/taskmgmt directory on the 5620 SAM server. The range is 200 to 50 000 tasks. The default is 10 000.

numTasksToPurgeWhenFull

The numTasksToPurgeWhenFull parameter specifies the number of successful tasks to remove when the limit specified by the [maxNumRetainedTasks](#) parameter is reached. The range is 20 to 500 tasks. The default is 100.

successfulTasksPurgeInterval

The successfulTasksPurgeInterval parameter specifies, in min, the interval at which tasks that are in the Succeeded state are removed. For a specific interval, the tasks from the previous interval that have a Succeeded state are removed. The range is 0, or 2 to 2880. The default is 10. A value of 0 means the parameter is disabled.

3 — *User Preferences parameters*

3.1 User Preferences parameters 3-2

3.1 User Preferences parameters

This chapter describes the parameters on the User Preference form and its child forms.

Access Interface Encap Value (Dot1q only)

The Access Interface Encap Value (Dot1q only) parameter specifies whether the [Auto-Assign ID](#) parameter is the default parameter for dot1q encapsulation. The options are:

- Enabled
- Disabled (default)

Apply User Span of Control

The Apply User Span of Control parameters specifies whether the GUI automatically filters list forms, trees, and maps to display only the objects in the user Edit Access spans. The options are:

- Enabled
- Disabled (default)

Debug STM Mode

The Debug STM Mode parameter specifies the test objects that are available in the Service Test Manager (STM). When the parameter is enabled, you can select more tests. Table [3-1](#) lists the options.

Table 3-1 Debug STM Mode parameter

Parameter option	Service Test Manager (STM) form options
Disabled (default)	<ul style="list-style-type: none">• Test (Assurance)• Test Result (Assurance)• Test Suite (Assurance)• Test Policy (Assurance)• Aggregated Result (Assurance)
Enabled	<ul style="list-style-type: none">• NE Test Agent (Assurance)• Test (Assurance)• Deployed Test (Assurance)• Test Result (Assurance)• Test Suite (Assurance)• Test Policy (Assurance)• NE Schedulable Test (Assurance)• Aggregated Result (Assurance)

Default Client Time Zone

The Default Client Time Zone parameter specifies the time zone that is applied to the 5620 SAM client by default. Choose a time zone from the drop-down list. The default is the 5620 SAM server installation time zone. The Current Client Time Zone will automatically reflect any change made to the Default Client Time Zone.

Default Polling Interval (seconds)

The Default Polling Interval parameter specifies the default interval, in seconds, for the polling interval for real-time statistics in the Statistics Plotter form. The range is 10 to 3600. The default is 10.

Enable Confirmation for Bulk Change Actions

The Enable Confirmation for Bulk Change Actions parameter specifies whether a confirmation message is displayed before the 5620 SAM carries out a bulk change operation. The options are:

- false
- true (default)

Maximum Data Retention Time (seconds)

The Maximum Data Retention Time (Seconds) parameter specifies the number of seconds to keep statistics data in the Statistics Plotter form. The range is 3600 to 86400. The default is 43200.

Overlay Type

The Overlay Type parameter specifies the default type of overlay in topology maps. The options are:

- Hierarchy (default)
- Flat

Populate Entire Properties Form on Opening

The Populate Entire Properties Form on Opening parameter specifies whether all child objects of a service are immediately loaded. The options are:

- Enabled
- Disabled (default)

The 5620 SAM client GUI displays the service configuration form more quickly when child objects are not immediately loaded. When you click on a service configuration form tab button, such as Components or Sites, then the most recent information is loaded.

Show Alarm Flags

The Show Alarm Flags parameter specifies whether the monitoring flag panel toolbar at the top of the Dynamic alarm list Alarm Window is displayed. The options are:

- Enabled
- Disabled (default)

Show Alarm Flags

The Show Alarm Flags parameter specifies whether the monitoring flag panel toolbar at the top of the Dynamic alarm list Alarm Window is displayed. The options are:

- Enabled
- Disabled (default)

Show Correlated Alarms

The Show Correlated Alarms parameter specifies whether correlated alarms are displayed in the alarm window. The options are:

- Enabled
- Disabled (default)

Show Toolbar

The Show Toolbar parameter specifies whether the toolbar at the top of the window is displayed. The options are:

- Enabled
- Disabled (default)

Specify # of Items Per Page

The Specify # of Items Per Page parameter specifies the number of items returned per page by a search. The range is 1 to 9999. The default is 1000.

Suppress Containing Window Warning

The Show Alarm Flags parameter specifies whether containing window warnings are suppressed. The options are:

- Enabled
- Disabled (default)

When a child object configuration form is launched from a parent object, and the child object configuration is changed, a warning message opens. The warning message indicates that changes to the child form are not committed until they are applied in the parent object. You must acknowledge the message. You can use workspace preferences to turn off the warning message. You continue to receive a warning message that changes must be applied for parent objects before you can close the parent object configuration form.

Suppress Template Generation Message

The Suppress Template Generation Message parameter specifies whether template generation windows are suppressed. The options are:

- Enabled
- Disabled (default)

Turn on Audible Alarms

The Turn on Audible Alarms parameter specifies whether there is an alarm bell when an incoming alarm is registered. The options are:

- Enabled (default)
- Disabled

Create menu parameters

- 4 – VPLS parameters
- 5 – VLL parameters
- 6 – VPRN parameters
- 7 – IES parameters
- 8 – VLAN parameters
- 9 – Mirror parameters
- 10 – Service From Template parameters
- 11 – IPsec VPN parameters
- 12 – Topology Group parameters
- 13 – Physical Link parameters
- 14 – Common Create menu parameters

4 — VPLS parameters

4.1 VPLS parameters 4-2

4.1 VPLS parameters

This chapter describes the parameters on the VPLS cration form and child forms.



Note — This chapter also describes parameters common to the Service Template form and child forms. Service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent does not recommend using the 5620 SAM-O XML classes and methods associated with service templates.

AAL5 Encapsulation

See the [AAL5 Encapsulation](#) parameter in section [14.1](#).

Action

(infoAction)

The Action parameter specifies DHCP Option 82 processing on the L2 SAP. The parameter indicates to the DHCP relay agent what to do when it receives a DHCP request that already has an information option on the packet. Table [4-1](#) describes the parameter options.

Table 4-1 Action parameter

Option	Option description
Keep (default)	The existing information is kept on the packet and the device does not add any additional information. On egress, the information option is not removed and is sent to the downstream node. This setup is similar to not having configured DHCP relay at all. If the gateway IP address of the packet received is the same as the address on the device, the packet is dropped.
Drop	The packet is dropped.
Replace	On ingress, the existing information option is replaced with the information option from the device. On egress, the information option is removed.

Activation Timer (seconds)

(activationTimer)

The Activation Timer (seconds) parameter specifies the time (in seconds) that the system keeps the local site in standby status waiting for BGP updates from remote PEs. At the end of this period, the system runs the designated forwarder (DF) election algorithm to decide whether the site should be unblocked. When this parameter is set to its default value on the VPLS site, the global value configured for the [Site Activation Timer](#) parameter under BGP Multi-homing at the NE level will be used. The range is -1, and 1 to 100. The default is -1.

Administrative State

See the [Administrative State](#) parameter in section 14.1.

Administrative ISID

(**isid**)

The Administrative ISID parameter specifies a 24-bit service instance identifier for this service. As part of the Provider Backbone Bridging frames, it is used at the destination PE as a demultiplexor field. The default value of -1 is used to indicate that the value of this object is unspecified. The range is -1 to 16777215. The default is -1.

Address ID

See the [Address ID](#) parameter in section 14.1.

Aggregate Rate Limit (Kbps)

See the [Aggregate Rate Limit \(kbps\)](#) parameter in section 14.1.

Aggregation

See the [Aggregation](#) parameter in section 14.1.

Aging Enabled

(**agingEnabled**)

The Aging Enabled parameter specifies whether learned MAC addresses within a VPLS instance are aged out when no packets are sourced from the MAC address for a specified period of time. The specified time is determined by the Local Age Time (seconds) and the Remote Age Time (seconds) parameters. The options are:

- true (default)
- false

ANCP String

See the [ANCP String](#) parameter in section 14.1.

Application Profile

See the [Application Profile](#) parameter in section 14.1.

ARP Host Limit

See the [ARP Host Limit](#) parameter in section 14.1.

ARP Reply Agent

(arpReplyAgent)

The ARP Reply Agent parameter specifies whether an ARP response mechanism is enabled in the device for ARP requests destined for static or dynamic hosts associated with the SAP. The device responds to each ARP request using the host MAC address as both the source MAC address in the Ethernet header and the destination hardware address in the ARP header. In the event that both a static host and a dynamic host share the same IP address and MAC address, the device retains the host information until both the static and dynamic entries are removed.

Enabling the ARP Reply Agent parameter forces all the ARP request and reply messages received on the SAP to be evaluated according to the current anti-spoof filter rules.

After you enable the ARP Reply Agent parameter, you can configure only static hosts that have both an IP address and a MAC address.

The ARP Reply Agent parameter is configurable when all of the existing static hosts on the SAP have both an IP address and a MAC address specified. Table 4-2 describes the parameter options.

Table 4-2 ARP Reply Agent parameter

Option	Option description	Dependencies
disabled (default)	Disables the ARP response mechanism.	—
enabled	Enables the ARP response mechanism.	All existing static hosts on the SAP must have both an IP address and a MAC address specified. The SAP must support Ethernet encapsulation.
Enabled With Subscr Ident	Enables the ARP response mechanism and configures it to discard ARP requests that are targeted for a known host on the same SAP with the same subscriber identification. For DHCP subscriber hosts, the subscriber identification information is parsed from the Option 82 and remote ID suboptions. For static subscribers, the subscriber identification is part of the static host configuration.	The SAP must support Ethernet encapsulation.

ARP Timeout (seconds)

(arpTimeout)

The ARP Timeout (seconds) parameter specifies the minimum time, in seconds, that an ARP entry learned on the IP interface is stored in the ARP table. An ARP entry is automatically refreshed when an ARP request or gratuitous ARP is received from an IP host; otherwise the ARP entry is aged from the ARP table then this parameter is set to 0, and APR aging is disabled. The range is 0 to 65 535. The default is 14 400.

ARP Trigger Packet

(msapArpTrigger)

The ARP Trigger Packet parameter specifies whether the receipt of ARP trigger packets on the Capture SAP results in a RADIUS authentication that creates an MSAP.

ATM OAM Alarm Cell Handling

See the [ATM OAM Alarm Cell Handling](#) parameter in section 14.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Automatic Mesh SDP Binding Creation

(topologyAutoCompletion)

The Automatic Mesh SDP Binding Creation parameter specifies whether the service that you are creating is automatically bound to previously created service tunnels. The options are:

- Disabled (default)
- Enabled

If you plan to use BGP AD for all or part of the VPLS or BGP VPLS, you must not enable automatic mesh SDP binding creation.

Auto Select Tunnels

See the [Auto Select Tunnels](#) parameter in section 14.1.

Backbone STP

(backbonePipStp)

The Backbone STP parameter specifies whether STP is enabled on this Backbone VPLS site instance. The options are:

- Up
- Down (default)

BGP AD Administrative Status

(bgpAdAdminStatus)

The BGP AD Administrative Status parameter specifies the administrative state of the BGP AD function. When the parameter is set to Up, the option to set a BGP AD Service Identification VPLS ID is displayed. The parameter can be enabled only during service creation. The options are:

- Up
- Down (default)



Note — When you enable the parameter at the service level, you must also enable and configure the individual BGP AD objects at the site level.

Block On Mesh Failure

(blockOnMeshFail)

The Block On Mesh Failure parameter specifies that the operational status of this spoke SDP considers the operational status of associated mesh SDPs on this service site. If there are no mesh SDPs in the service, this parameter is ignored. When this parameter is enabled, then the operational status of this spoke SDP is Down, until the operational status of at least one mesh SDP in this service is Up. When this parameter is not enabled, the operational status of this spoke SDP does not consider the operational status of any mesh SDPs in the service.

The parameter is configurable only when the spoke is not under an endpoint. The parameter cannot be enabled when STP is enabled on the spoke. The options are:

- enabled
- disabled (default)

Boot Timer (seconds)

(bootTimer)

The Boot Timer (seconds) parameter specifies the time (in seconds) that the system waits after a network element reboot before running the designated forwarder (DF) election algorithm. When this parameter is set to its default value of -1 on the VPLS site, the global value configured at the NE level under BGP Multi-homing will be used.

At the VPLS site level, the range is -1, and 1 to 100 and the default is 1. At the NE level, the range is 0 to 100 and the default is 1.

Bridge Forward Delay (seconds)

(bridgeForwardDelay)

The Bridge Forward Delay (seconds) parameter specifies the number of seconds that a port or a SAP spends in the Listening and Learning states during the transition from the Disabled State to the Forwarding state. The range is 4 to 30. The default is 15.

The state transition flow for a SAP from a Disabled state to a point where the SAP is operational is:

Disabled > Listening > Learning > Forwarding

When the Forward Delay parameter is set to 15 s, the normal operation of the spanning tree state machine stays in the Listening state for 15 s and in the Learning state for 15 s. The Disabled and Forwarding states do not have transition times; they are steady-state conditions of a port or a SAP. This means that when operationally up, a SAP takes 30 s to reach the Forwarding state.

Modifying the bridge-level parameters must be done within the constraints of the following two formulas:

- $2 \times (\text{Bridge Forward Delay} - 1.0 \text{ s}) \geq \text{Bridge Max Age}$
- $\text{Bridge Max Age} \geq 2 \times (\text{Bridge Hello Time} + 1.0 \text{ s})$

Bridge Hello Time (seconds)

(bridgeHelloTime)

The Bridge Hello Time (seconds) parameter specifies the amount of time between the transmission of configuration BPDUs by the root bridge. The range is 1 to 10. The default is 2.



Note — Modifying the bridge-level parameters must be done within the constraints of the following two formulas:

- $2 \times (\text{Bridge Forward Delay} - 1.0 \text{ s}) \geq \text{Bridge Max Age}$
- $\text{Bridge Max Age} \geq 2 \times (\text{Bridge Hello Time} + 1.0 \text{ s})$

Bridge Max Age (seconds)

(bridgeMaxAge)

The Bridge Max Age (seconds) parameter specifies the number of seconds that a configuration BPDU is valid. The aging of BPDUs allows detection, at the protocol layer, of removed bridges or logical connectivity loss. The range is 6 to 40. The default is 20.



Note — Modifying the bridge-level parameters must be done within the constraints of the following two formulas:

- $2 \times (\text{Bridge Forward Delay} - 1.0 \text{ s}) \geq \text{Bridge Max Age}$
- $\text{Bridge Max Age} \geq 2 \times (\text{Bridge Hello Time} + 1.0 \text{ s})$

Bridge Max Hops

(bridgeMaxHops)

The Bridge Max Hops parameter specifies the maximum number of hops between bridges in the MSTP region before a BPDU times out and the device removes the port information. The range is 1 to 40. The default is 20.

Broadcast Address Format

See the [Broadcast Address Format](#) parameter in section 14.1.

Calling Station ID

See the [Calling Station ID](#) parameter in section 14.1.

Circuit ID

(infoCircuitId)

The Circuit ID parameter specifies whether the Option 82 circuit ID suboption is included in the DHCP relay packet and what format the suboption must take. The Option 82 circuit ID suboption contains information that uniquely identifies the device from which the packet was received. Table 4-3 describes the parameter options.

Table 4-3 Circuit-id Suboption parameter

Option	Option description
no circuit-id (default)	The suboption is left blank.
circuit-id	Links the following information in a tuple to be sent: <ul style="list-style-type: none">• access node ID• service ID• interface name• SAP ID

CCM Messages

See the [CCM Messages Enabled](#) parameter in section 14.1.

Clear Forced Switchover

The Clear Forced Switchover button allows you to clear a manual switchover from a redundant spoke SDP binding back to an active spoke SDP binding that was previously initiated by using the [Force Switchover](#) button. You must clear any such manually forced switchovers by using the Clear Forced Switchover button after the active spoke SDP binding has been restored. The system does not switch over automatically to other active spoke SDP bindings if this is not done, even if the redundant spoke SDP binding subsequently goes down.

The Active State read-only display indicates the change in status for the SDP binding when you press the Clear Forced Switchover button.

Collect Accounting Statistics

See the [Collect Accounting Statistics](#) parameter in section 14.1.

Control Word

(controlWord)

The Control Word parameter specifies the use of a control word to prevent VPLS packet hashing in ECMP-capable networks. The control word is exchanged with the LDP peer during pseudowire negotiation. This function also applies to MVPLS. The options are:

- Preferred
- Not Preferred (default)

Creation MSAP Policy

(creationMsapPolicyObjectPointer)

The Creation MSAP Policy parameter displays the unique identifier of the MSAP policy that was used to create the MSAP.

Creation MSAP Policy Re-evaluation

(creationPolicyReeval)

The Creation MSAP Policy Re-evaluation parameter allows you to re-apply the MSAP Policy that is associated with the MSAP. When you set the value to DoAction, MSAP policy re-evaluation is triggered, which synchronizes the MSAP properties to the new values of a changed MSAP policy. The options are:

- DoAction—choose this option to re-apply the MSAP Policy
- NotApplicable

Customer VID

See the [Customer VID](#) parameter in section [14.1](#).

Default Gateway IP Address

(defaultGatewayIpAddr)

The Default Gateway IP Address parameter specifies the IP address of the default gateway for this VPLS site. Specify an IPv4 address in dotted-decimal format. There is no default.

Default Gateway MAC Address

(defaultGatewayMacAddr)

The Default Gateway MAC Address parameter specifies the MAC address of the default gateway for this VPLS site. Specify a MAC address in the format xx-xx-xx-xx-xx-xx. The default is 00-00-00-00-00-00, which means that the parameter is not configured.

Default Mesh VC ID

See the [Default Mesh VC ID](#) parameter in section 14.1.

Default Service Priority

(svcPriority)

See the [Service Priority](#) parameter in section 14.1.

Description

See the [Description](#) parameter in section 14.1.

Destination Node ID

See the [Tunnel Termination Site](#) parameter in section 14.1.

DHCP Trigger Packet

(msapDhcpTrigger)

The DHCP Trigger Packet parameter specifies whether the receipt of DHCP trigger packets on the Capture SAP results in a RADIUS authentication that creates an MSAP.

Direction

See the [Direction](#) parameter in section 117.1.

Disable Fix Window

See the [Disable Fix Window](#) parameter in section 14.1.

Disable Revert Time (Infinite)

The Disable Revert Time (Infinite) parameter specifies whether or not to disable the “[Revert Time \(seconds\)](#)” parameter indefinitely. The options are:

- enabled
- disabled (default)

Discard Unknown Destinations

(discardUnknownDestinations)

The Discard Unknown Destinations parameter specifies whether packets with destination MAC addresses that are not learned are forwarded to all interfaces on the device. When the parameter is enabled, all unknown destination packets are forwarded on all LSPs to the participating devices of the service until the target responds and the MAC address is learned by the router that is associated with the service. The options are:

- enabled
- disabled (default)

Discard Unknown Source

(discardUnknownSource)

The Discard Unknown Source parameter specifies whether a packet with an unknown source MAC address is forwarded to all interfaces on the device. When the parameter is set to true, no unknown source packets are forwarded to the participating devices of the service. The options are:

- false (default)
- true

Displayed Name

See the [Displayed Name](#) parameter in section 14.1.

Dynamic Topology Discovery

See the [Dynamic Topology Discovery](#) parameter in section 14.1.

Edge Capability Detection

(autoEdge)

The Edge Capability Detection parameter specifies whether the edge port characteristics of the access interface are automatically detected. The options are:

- Enabled (default)
- Disabled

Edge Port

(rapidStart)

The Edge Port parameter specifies whether the access interface is an STP edge port. The options are:

- Enabled
- Disabled (default)

Egress Filter ID

See the [Egress Filter ID](#) parameter in section 14.1.

Egress Label

See the [Egress Label](#) parameter in section 14.1.

Egress Mark QinQ Top Bits Only

See the [Egress Mark QinQ Top Bits Only](#) parameter in section 14.1.

Egress Policy ID

See the [Egress Policy ID](#) parameter in section 14.1.

Egress Scheduler Name

See the [Egress Scheduler Name](#) parameter in section 14.1.

Enable

The Enable parameter specifies whether to enable or disable the configurability of the [Enable Lease Populate](#) parameter. The parameter is configurable when the [Snooping](#) parameter is enabled. The options are:

- enabled
- disabled (default)

When the parameter is enabled, you can configure the [Enable Lease Populate](#) parameter. Disabling the parameter is equivalent to configuring the [Enable Lease Populate](#) parameter with a value of 0.

Enable BGP AD

(bgpAdEnabled)

The Enable BGP AD parameter specifies whether or not BGP AD is enabled on the site. The options are:

- enabled
- disabled (default)

Enable BGP VPLS

(bgpVplsEnabled)

The Enable BGP VPLS parameter specifies whether or not BGP VPLS is enabled on the site. The options are:

- enabled
- disabled (default)

Enable DHCP Relay

See the [Enable DHCP Relay](#) parameter in section 14.1.

Enable IP Interface Binding

(enableIpItfBinding)

The Enable IP Interface Binding parameter specifies whether to allow IP interface binding on the service site. The options are:

- true
- false (default)

Enable Lease Populate

(leasePopulate)

The Enable Lease Populate parameter specifies the number of DHCP lease state entries allowed for the VPLS SAP. The Enable Lease Populate parameter is configurable when the Snooping parameter is enabled. The range is 0 to 8000. There is no default. Setting the parameter to 0 specifies that dynamic host lease state management for the interface is disabled.

Enable Multi-homing to

(bgpMhOption)

The Enable Multi-homing to parameter specifies which object associated with the site will be used for BGP VPLS multi-homing. The options are:

- SAP
- Spoke SDP
- Split Horizon Group
- Mesh SDP Binding
- None

If you select a Split Horizon Group associated with this site, all SAPs and PWs associated with this SHG will also be involved in the BGP multi-homing.



Note — In the 5620 SAM, you can only select one of these associated objects if it already exists. However, if BGP VPLS multi-homing is configured using CLI, it is possible to assign a non-existing object to this multi-homing site. In this case, 5620 SAM will simply resync the configuration on the network element and display it on the configuration form. If you click the Properties button beside the object's name in the form, the message "Object does not exist" will be displayed.

EndPoint ID

(multiChassisEndpointId)

The EndPoint ID parameter specifies the ID for the multichassis endpoint. The range is 0 to 4 294 967 295. The default is 0.

Endpoint Type

(type)

The Endpoint Type parameter specifies the type of VPLS endpoint. The options are:

- Single Chassis (default)
- Multi Chassis

Failed Threshold

(failedThreshold)

The Failed Threshold parameter specifies the number of objects which are required to be in the down state for this site itself to be declared in the down state. Setting the parameter to -1 indicates that all objects in this site should be down for the site to be declared in down. The range is -1 and 1 to 1000. The default is -1.

Fast Leave

(fastLeave)

The Fast Leave parameter specifies whether the status of IGMP or MLD fast leave processing is enabled, that is, whether fast leave is allowed on this SAP. If it is enabled, the system prunes the port on which an IGMP or MLD “leave” message has been received, without waiting for the Group Specific Query to timeout. The options are:

- enabled
- disabled (default)

Force L2PT on Managed L2 Access Interface

(forceL2Pt)

The Force L2PT on Managed L2 Access Interface parameter specifies whether L2PT is enforced for the managed SAPs of an M-VPLS L2 access interface. Setting the parameter to true forces the enabling of L2PT on the managed SAPs. If the access interface already has managed SAPs with L2PT disabled, you cannot set the parameter to true. The options are:

- false (default)
- true

Force Switchover

The Force Switchover button allows you to force a switchover of the active SDP binding to a redundant SDP binding under an endpoint of the VPLS. When you do this, the redundant SDP binding becomes active and the Active State indicator displays the status change.



Note — You must clear a manually forced switchover using the [Clear Forced Switchover](#) button after the active spoke SDP binding is restored. The 5620 SAM is unable to switch automatically to other active spoke SDP bindings if this is not done, even if the redundant spoke SDP binding subsequently goes down.

Force VLAN VC Forwarding

(forceVlanVcForwarding)

The Force VLAN VC Forwarding parameter specifies whether VLAN VC Forwarding is forced in the data path of an SDP that has the [VC Type](#) parameter set to Ethernet. The options are:

- False (default)
- True

Formatted VSI ID Prefix

(vsiIdPrefixIpFormat)

The Formatted VSI ID Prefix parameter is the VSI ID Prefix, but in an IP format for better readability. This is an IPv4 address in dotted-decimal format. If the value is set to 0.0.0.0, this is interpreted by the node as using the System IP Address of the NE. The default is 0.0.0.0.

Fragment Interleave

(frf12interleave)

See the [Fragment Interleave](#) parameter in section [14.1](#).

FRF-12 End-To-End Fragment Threshold

See the [FRF-12 End-To-End Fragment Threshold](#) parameter in section [14.1](#).

FRF-12 Mode

See the [FRF-12 Mode](#) parameter in section [14.1](#).

General Query Interval (seconds)

(genQueryInterval)

The General Query Interval (seconds) parameter specifies the interval at which the system sends general queries for the SAP or SDP. The range is 2 to 1024. The default is 125.

Group Address

(grpAddr)

The Group Address parameter specifies the IP multicast group address. For IGMP snooping this is an IPv4 address and the range is 224.0.0.0 to 239.255.255.255. For MLD snooping this is an IPv6 address that is not link-local or node-local. There is no default.

High Watermark (%)

Table 4-4 lists where to find more information about the High Watermark (%) parameter.

Table 4-4 High Watermark (%) parameter

Parameter	See
High Watermark for FIB	High Watermark (%) parameter in this section
High Watermark for MFIB	High Watermark (%) parameter in this section

High Watermark (%)

(highWatermark)

The High Watermark (%) parameter specifies the threshold percentage at which an alarm is raised based on whether the FIB reaches the maximum number of MAC addresses that it can contain. The maximum number of addresses for the FIB is determined by the value of the Size (entries) parameter. The range is 0 to 100. The default is 95.

High Watermark (%)

(mfibTableHighWatermark)

The High Watermark (%) parameter specifies the threshold percentage at which an alarm is raised based on whether the MFIB reaches the maximum number of MAC addresses that it can contain. The maximum number of addresses for the MFIB is determined by the value of the Table size (entries) parameter. The range is 0 to 100. The default is 95.

Hold Multiplier

See the [Hold Multiplier](#) parameter in section 14.1.

ID

See the **ID** parameter in section 14.1.

ID

See the **ID** parameter in section 14.1.

I/F MAC Address**(interfaceMacAddress)**

The I/F MAC Address parameter specifies the 48-bit MAC address for the static ARP in the form aa:bb:cc:dd:ee:ff or aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. Any non-broadcast, non-multicast MAC addresses and non-IEEE reserved MAC addresses are allowed values. The default is 00-00-00-00-00-00.

IGMP Version**(igmpVersion)**

The IGMP Version parameter specifies the version of IGMP that is running on the SAP or SDP binding. The options are:

- Version 1
- Version 2
- Version 3 (default)



Note — For IGMP snooping configuration on a 7210 SAS-E, Release 1.0 R4 or later, on a 7210 SAS-M24F, Release 1.1 R6 or later, on a 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or on a 7210 SAS-X24F2XFP, the options are Ver. 1 and Ver. 2 (default).

The 7210 SAS-E, Release 2.0 or later includes IGMP Ver. 3 support.

Ignore Standby Signalling**(ignoreStandbySignalling)**

The Ignore Standby Signalling parameter specifies whether the node ignores a standby bit received from an T-LDP peer. This parameter can also be set on a spoke SDP binding in VPLS. However, if the spoke SDP binding is associated with an endpoint, this parameter can only be changed at the endpoint level. You can not add a spoke SDP binding to an endpoint and have this parameter in conflict with its counterpart on the endpoint. Therefore, when you create a spoke SDP binding to an endpoint, this parameter automatically inherits its value from its endpoint counterpart.

Import Policy

(importPolicy)

The Import Policy parameter specifies the IGMP or MLD packet filter policy. The range is 0 to 32 characters.

Ingress Filter ID

See the [Ingress Filter ID](#) parameter in section 14.1.

Ingress Label

See the [Ingress Label](#) parameter in section 14.1.

Ingress Match Q in Q Dot1P

See the [Ingress Match QinQ Dot1P](#) parameter in section 14.1.

Ingress Policy ID

See the [Ingress Policy ID](#) parameter in section 14.1.

Ingress Scheduler Name

See the [Ingress Scheduler Name](#) parameter in section 14.1.

Inherit Value

See the [Inherit Service ID Value](#) parameter in section 14.1.

Inner Encapsulation Value

See the [Inner Encapsulation Value](#) parameter in section 14.1.

Inner Encapsulation Value

(VCI)

See the [Inner Encapsulation Value \(VCI\)](#) parameter in section 14.1.

Instance Index

(id)

The Instance Index parameter identifies the MST instance. The range is 1 to 4094. The default is 0.

Interface ID

See the [Interface ID](#) parameter in section 14.1.

IP Address

Table 4-5 lists where to find more information about the IP Address parameter.

Table 4-5 IP Address parameter

Parameter	See
IP Address for L2 management interface	IP Address parameter in this section
IP Address for GSMP neighbor	IP Address parameter in section 14.1

IP Address

(ipAddress)

The IP Address parameter specifies an IP address for the L2 management interface for VPLS. Specify an IPv4 address in dotted-decimal format. There is no default.

Keep Alive (seconds)

See the [Keep-Alive \(seconds\)](#) parameter in section 14.1.

Last Member Query Interval (tenths of seconds)

(lastMemberInterval)

The Last Member Query Interval (tenths of seconds) parameter specifies the interval at which group-specific query packets are sent. The range is 1 to 50. The default is 10.

Learning Enabled

(learningEnabled)

The Learning Enabled parameter specifies whether MAC address learning is enabled. MAC address learning is performed to reduce the amount of unknown destination MAC address flooding. When the parameter is enabled, each router learns the source MAC addresses of traffic that arrives on access and network ports and populates the learned addresses in a FIB for each VPLS instance. The options are:

- true (default)
- false

Limit Mac Move

(limitMacMove)

The Limit Mac Move parameter specifies whether the MAC relearn rate is blocked on the SAP. When the parameter is set to Blockable, the agent monitors the MAC relearn rate on this SAP, and it blocks it when the relearn rate exceeds the number defined by the Move Frequency parameter. When the value is Non-Blockable, the SAP is not blocked, and another SAP is blocked instead. The options are:

- Blockable (default)
- Non-Blockable

Limit Mac Move Level

(limitMacMoveLevel)

The Limit Mac Move level parameter specifies the hierarchy in which SAPs are blocked when a MAC move limit is exceeded. The parameter is configurable when the [Limit Mac Move](#) parameter on the port is set to blockable. The options are:

- Primary
- Secondary
- Tertiary (default)

Link Type

(linkType)

The Link Type parameter specifies the type of link used for the STP. The options are:

- Point To Point (default)
- Shared

Local Address

See the [Local Address](#) parameter in section [14.1](#).

Local Age Time (seconds)

(localAgeTime)

The Local Age Time (seconds) parameter specifies the number of seconds to age out FIB entries on access interfaces. Generally, the Remote Age Time (seconds) parameter is set to a longer period than the Local Age Time (seconds) parameter to reduce the amount of flooding required for destination unknown MAC addresses. The range is 60 to 86 400. The default is 300.

Low-priority Defect

See the [Low-priority Defect](#) parameter in section [117.1](#).

Low Watermark (%)

Table [4-6](#) lists where to find more information about the Low Watermark (%) parameter.

Table 4-6 Low Watermark (%) parameter

Parameter	See
Low Watermark for FIB	Low Watermark (%) parameter in this section
Low Watermark for MFIB	Low Watermark (%) parameter in this section

Low Watermark (%)

(lowWatermark)

The Low Watermark (%) parameter specifies the threshold percentage of the total FIB size limit at which an alarm that was previously raised by a “table full” condition is cleared by the system. The FIB size limit is specified by the Size (entries) parameter. For example, when an alarm is raised because the number of FIB entries exceeds the percentage set for the High Watermark parameter, and the number of FIB entries in the system drops to a value below the Low Watermark percentage, the alarm is cleared. The range is 0 to 100. The default is 90.

Low Watermark (%)

(mfibTableLowWatermark)

The Low Watermark (%) parameter specifies the threshold percentage of the total MFIB size limit at which an alarm that was previously raised by a “table full” condition is cleared by the system. The MFIB size limit is specified by the Table size (entries) parameter. For example, when an alarm is raised because the number of MFIB entries exceeds the percentage set for the High Watermark parameter, and the number of MFIB entries in the system drops to a value below the Low Watermark percentage, the alarm is cleared. The range is 0 to 100. The default is 90.

MAC Address

See the [MAC Address](#) parameter in section 14.1.

MAC Flush on fail

(macFlushOnFail)

The MAC Flush on fail parameter determines whether the VPLS site clears MAC entries if an interface fails. The options are:

- enabled
- disabled (default)

MAC Monitoring

See the [MAC Monitoring](#) parameter in section 14.1.

MAC Notification Count

(macNotifCount)

The MAC Notification Count parameter specifies how many MAC notification messages are sent. The range is 1 to 10. The default is 3.

MAC Notification Interval

(macNotifInterval)

The MAC Notification Interval parameter specifies the often the MAC notification messages are sent. The range is 100 ms to 10 s. The default is 100 ms.

MAC Pinning

(macPinning)

The MAC Pinning parameter specifies whether MAC pinning is active on the SAP, or the mesh or spoke circuit. The options are:

- disabled (default)
- enabled

For a SAP or mesh or spoke circuit that belongs to a residential split horizon group, the value is set to enabled by the 5620 SAM and cannot be changed by the operator. Setting the value to enabled disables the relearning of MAC addresses on other SAPs or mesh or spoke circuits within the same VPLS; the MAC address remains attached to the SAP for the duration of its age timer. This situation only affects the MAC addresses learned through the normal MAC address learning process and not the MAC address entries learned through DHCP.

MAC Subnet Length

(macSubnetLength)

The MAC Subnet Length parameter specifies how many bits, starting from the beginning of the MAC address, are used for MAC learning and switching. The range is 24 to 48. The default is 48.

Setting the MAC Subnet Length parameter to a value other than 48 enables the MAC subnetting feature. The following VPLS features are not supported when MAC subnetting is enabled:

- IGMP snooping
- MLD snooping
- PIM snooping
- MC LAG

Mandatory Bandwidth (kbps)

(preRsvdMandatoryBandwidth)

The Mandatory Bandwidth (kbps) parameter specifies the bandwidth pre-reserved for mandatory type BTV channels on an interface. The parameter combines with the [Unconstrained Bandwidth \(kbps\)](#) parameter to establish the bandwidth assigned to traffic on an interface using a multicast CAC policy. Table 4-7 describes the parameter options.

Table 4-7 Mandatory Bandwidth (kbps) parameter

Mandatory Bandwidth	Unconstrained Bandwidth	Result
0	0	No channels are allowed.
-1	-1	All mandatory and optional channels are allowed.
Equal to the value in the Unconstrained Bandwidth (kbps) parameter	—	All mandatory channels configured for the multicast CAC policy associated with the interface are allowed. Optional channels are not allowed.
Less than the value in the Unconstrained Bandwidth (kbps) parameter	—	All mandatory channels configured for the multicast CAC policy associated with the interface are allowed. Optional channels are allowed depending on bandwidth availability.

The range is –1 to 22 147 483 647. The default is –1. When the Unconstrained Bandwidth parameter is set to either –1 or 0, the Mandatory Bandwidth parameter defaults to the same value. The Mandatory Bandwidth value must be less than or equal to the Unconstrained Bandwidth value.

Max Number of Groups

(maxGroups)

The Max Number of Groups parameter specifies the maximum number of groups for which PIM snooping can have a downstream state based on the received PIM snooping joins on this interface. The range is 0 to 16000. The default is 0.

the maximum number of groups that can be statically or dynamically learned. The range is 1 to 1000. The default is 0, which means that no limit is imposed.

Maximum Number of Groups

(maxNbrGroups)

The Maximum Number of Groups parameter specifies the maximum number of groups that can be statically or dynamically learned. The range is 1 to 1000. The default is 0, which means that no limit is imposed.



Note — For IGMP snooping configuration on a 7210 SAS-E, Release 1.0 R4 or later, on a 7210 SAS-M24F, Release 1.1 R6 or later, on a 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or on a 7210 SAS-X24F2XFP, the range is 0 to 2047. The default is 0, which means that no limit is imposed.

Maximum Number of Sources per Group

(maxNbrSourcesPerGroup)

The Maximum Number of Sources per Group parameter specifies how many source addresses are allowed per group address for this SAP. The range is 0 to 1000, where 0 means that no limit is imposed. The default is 0.



Note — This parameter does not apply to the 7210 SAS-E, the 7210 SAS-M24F, the 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or 7210 SAS-X24F2XFP.

Maximum Response Interval (seconds)

(queryResponseInterval)

The Maximum Response Interval (seconds) parameter specifies the maximum time between IGMP or MLD queries. The range is 1 to 1023. The default is 10.

Max VE ID

(maxVeId)

The Max VE ID parameter specifies the allowed range for the [VE ID](#) parameter, locally configured and received in an NLRI. Configuration of a VE ID value higher than the value specified by this parameter is not allowed.

The range is 0 to 65 535. The default is 0, meaning it is disabled.

Max VLAN ID

(maxVlanId)

The Max Vlan ID parameter specifies the top end of the VLAN ID range. It specifies the maximum VPLS VC ID that can be associated with and managed by a specific MVPLS SAP. The range is 0 to 4094 or 2 to 4092, depending on the managed device. The 7250 SAS supports a range of 2 to 4092.

Max. VLAN Tag

(max)

The Max. VLAN Tag parameter specifies the maximum number of VLANs that can be associated with the MVPLS SAP. The range is 1 to 4094. The default is 0, which means that the parameter value is unspecified.

Maximum BPDUs (PDUs/Hello Interval)

(stpMaxBPDUs)

The Maximum BPDUs parameter specifies the hold count for the STP. The range is 1 to 10. The default is 6.

Maximum Entries

(maxEntries)

The Maximum Entries parameter specifies the maximum number of learned and static entries in the FIB. The range is 0 to 131 071 for the 7450 ESS. The range is 0 to 196 607 for the 7750 SR in chassis mode C. The range is 1 to 16 383 for the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, and 7210 SAS-E. The default is 0.

Maximum FIB Entries

(maxNumOfFibEntries)

The Maximum Entries parameter specifies the maximum number of learned and static entries allowed for this endpoint. The value 0 means no limit for this endpoint. The range is 0 to 196607, When the chassis mode is not 'C', the maximum value is 131071. The default is 0.

MC Ring Node

See the [MC Ring Node](#) parameter in section 14.1.

Member Group Name

(memberOperGroupName)

The Member Group Name parameter specifies the name of the operational group that a VPLS/MVPLS SAP, Spoke SDP Binding, or a PW Template Binding is assigned to as a member. Click on the Select button to choose an operational group.

Min VLAN ID

(minVlanId)

The Min Vlan ID parameter specifies the low end of the VLAN ID range. It specifies the minimum VPLS VC ID that can be associated with and managed by a specific MVPLS SAP. The range is 0 to 4094 or 2 to 4092, depending on the managed device. The 7250 SAS supports a range of 2 to 4092.

Min. VLAN Tag

(min)

The Min. VLAN Tag parameter specifies the minimum number of VLANs that can be associated with the MVPLS SAP. This parameter must be set to a value less than or equal to the Max. VLAN Tag parameter value. The range is 1 to 4094. The default is 0, which means that the parameter value is unspecified.

Minimum Authentication Interval (minutes)

See the [Minimum Authentication Interval \(minutes\)](#) parameter in section 14.1.

MIP

(mipEnabled)

The MIP parameter specifies whether a MIP is created on this specific SAP or spoke binding when the [MHF-Creation](#) parameter for the MEG is set to the value of “default”. The options are:

- enabled
- disabled (default)

MIP MAC Address

(mipMacAddress)

The MIP MAC Address parameter allows a user to associate a MAC address with the MIP created on this specific SAP or spoke binding. The default is 00-00-00-00-00-00.

MLD version

(mldVersion)

The MLD version parameter indicates the version (either 1 or 2) of the MLD protocol that is sent by the active MLD Querier.

Monitor Access Interface Operational State

See the [Monitor Access Interface Operational State](#) parameter in section 14.1.

Monitored Group Name

(monitorOperGroupName)

The Monitored Group Name parameter specifies the name of the operational group that a VPLS/MVPLS SAP, Spoke SDP Binding, or a BGP VPLS Multi-homing site is assigned to as a monitor. Click on the Select button to choose an operational group.

Move Frequency

(macMoveFrequency)

The Move Frequency parameter specifies the maximum rate at which MACs can be relearned in the service, before the SAP is disabled to protect the system against undetected loops or duplicate MACs. The rate is calculated as the maximum number of relearns allowed in a 5-second interval. The range is 1 to 10. The default is 2.

MRP Admin Status

(mrpAdminStatus)

The MRP Admin Status parameter specifies whether the Multiple Registration Protocol (MRP) is enabled in this B-VPLS. The options are:

- enabled
- disabled (default)

MRP Attribute-Table-High-Watermark

(mrpAttrTblHighWatermark)

The MRP Attribute-Table-High-Watermark parameter specifies the utilization of the MRP attribute table of this B-VPLS at which a Table Full alarm is raised by the agent. The range is 0 to 100. The default is 95.

MRP Attribute-Table-Low-Watermark

(mrpAttrTblLowWatermark)

The MRP Attribute-Table-Low-Watermark parameter specifies the utilization of the MRP attribute table of this B-VPLS at which a Table Full alarm is cleared by the agent. The range is 0 to 100. The default is 90.

MRP Flood Time (seconds)

(mrpFloodTime)

The MRP Flood Time (seconds) parameter specifies the amount of time in seconds after a status change in this B-VPLS during which traffic is flooded. After that time expires, traffic is delivered according to the MRP registrations which exist in the B-VPLS. The value of 0 indicates that no flooding occurs on state changes in the B-VPLS. The range is 0, 3 to 600. The default is 0.

MRP Join Time (tenths of a second)

(mrpJoinTime)

The MRP Join Time (tenths of a second) parameter specifies the amount of time in tenths of a second that is the maximum rate at which attribute join messages can be sent on the SDP. The range is 1 to 10. The default is 2.

MRP Leave All Time (tenths of a second)

(mrpLeaveAllTime)

The MRP Leave All Time (tenths of second) parameter specifies the amount of time in tenths of a second that is the frequency where all attribute declarations on the SDP are refreshed. The range is 60 to 300. The default is 100.

MRP Leave Time (tenths of a second)

(mrpLeaveTime)

The MRP Leave Time (tenths of second) parameter specifies the amount of time in tenths of a second that a registered attribute is held in the leave state before the registration is removed. The range is 30 to 60. The default is 30.

MRP Max Attributes

(mrpMaxAttributes)

The MRP Max Attributes parameter specifies the maximum number of MRP attributes supported in this B-VPLS. In most cases, the default value is 2048 MRP attributes. For some platform and chassis types, especially single slot chassis, the default value is lower due to resource constraints. An Inconsistent Value error is returned if an attempt is made to set this object to a value the platform cannot support. The range is 1 to 2048. The default is 2048.

MRP Periodic Enabled

(mrpPeriodicEnabled)

The MRP Periodic Enabled parameter specifies whether re-transmission of attribute declarations is enabled. The options are:

- enabled (default)
- disabled

MRP Periodic Time (tenths of a second)

(mrpPeriodicTime)

The MRP Periodic Time (tenths of second) parameter specifies the amount of time in tenths of a second that is the frequency of re-transmission of attribute declarations. The range is 10 to 100. The default is 10.

MTU

See the [MTU](#) parameter in section [14.1](#).

Multi-homing ID

(mhSiteId)

The Multi-homing ID parameter specifies a two-byte identifier for this site. To create several BGP multi-homing sites in the same group, the sites should all have the same RT and Multi-homing ID configured. The range is 0 to 65535. The default is 0. BGP multi-homing can only operate when the Multi-homing ID has a non-zero value.

Multi-homing Site Name

(mhSiteName)

The Multi-homing Site Name parameter specifies the name for this BGP VPLS multi-homing site. The range is 1 to 32 characters.

Mrouter attached

(mrouterAttached)

The Mrouter attached parameter specifies whether the port is connected to a subnet with a multicast router. The parameter is mutually exclusive with the Send queries parameter. When you select the parameter, the Send queries parameter is disabled. When the Send queries parameter is enabled, you cannot select the Multicast attached parameter. The options are:

- enabled
- disabled (default)

Name

See the [Name](#) parameter in section 14.1.

No Egress Aggregate Rate Limit

See the [No Egress Aggregate Rate Limit](#) parameter in section 14.1.

Number Of Retries

(macMoveNumRetries)

The Number Of Retries parameter specifies the number of times retries are performed for re-enabling the SAP/SDP. A value of zero indicates an unlimited number of retries. The range is 0 to 255. The default is 3.

OAM Administrative State

See the [OAM Administrative State](#) parameter in section 14.1.

Outer Encapsulation Value

See the [Outer Encapsulation Value](#) parameter in section 14.1.

Outer Encapsulation Value

(VPI)

See the [Outer Encapsulation Value \(VPI\)](#) parameter in section 14.1.

Path Cost

(pathCost)

The Path Cost parameter specifies the STP cost of the path to the root device as seen from this device. The range is 1 to 200 000 000. The default is 10.

Per Service Hashing for LAG Enabled

(perServiceHashing)

See the [Per Service Hashing for LAG Enabled](#) parameter in section 14.1.

Port

See the [Port](#) parameter in section 14.1.

Port Number

(portNum)

The Port Number parameter specifies the value of the port number field which is contained in the least significant 12 bits of the 16-bit Port ID parameter that is associated with the current SAP. The range is 0 to 4094 or 2 to 4092, depending on the managed device. The 7250 SAS supports a range of 2 to 4092. The default is 0.

PPPoE Circuit ID

(pppoeCircuitId)

The PPPoE Circuit ID parameter specifies whether PPPoE circuit ID tag processing is enabled on an L2 access interface on a VPLS site. The parameter is disabled by default.

The PPPoE Circuit ID parameter is applicable for ATM SAPs on an L2 access interface on a VPLS service. The parameter is supported on the 7705 SAR 4.0 R1 and later.

PPPoE Trigger Packet

(msapPppoeTrigger)

The PPPoE Trigger Packet parameter specifies whether the receipt of PPPoE trigger packets on the Capture SAP results in a RADIUS authentication that creates an MSAP.

Prefix Length

(prefixLength)

The Prefix Length parameter specifies the IPv4 prefix of the IP address of the L2 management interface. The range is 1 to 128. The default is 24.

Primary Ports Cumulative Factor

(macMovePrimaryPortsCumulativeFactor)

The Primary Ports Cumulative Factor parameter specifies the maximum periods at which MACs can be relearned in the service. Periods are used to measure the MAC-relearn rate. This rate must be exceeded during consecutive periods before the corresponding ports (SAP and/or spoke-SDP) are blocked. The value of this parameter must be larger than the [Secondary Ports Cumulative Factor](#). The range is 3 to 10. The default is 3.

Priority

Table 4-8 lists where to find more information about the Priority parameter.

Table 4-8 Priority parameter

Parameter	See
Priority for site	Priority parameter in this section
Priority for SAP	Priority parameter in this section

Priority

(priority)

The Priority parameter applies to site objects and specifies the priority portion of the Bridge ID field within outbound BPDUs. It also determines the best BPDU between sent and received messages. The range is 0 to 65 535. The default is 32 768.

Priority

(priority)

The Priority parameter applies to SAPs and specifies the value of the port priority field which is contained in the most significant 4 bits of the 16-bit Port ID that is associated with the current SAP. The range is 0 to 255. The default is 128.

Priority Dscp

See the [Priority Dscp](#) parameter in section 14.1.

Priority Level for CCM Messages

See the [Priority Level for CCM Messages](#) parameter in section 117.1.

Priority Precedence

See the [Priority Precedence](#) parameter in section 14.1.

Priority Type

See the [Priority Type](#) parameter in section 14.1.

Propagate MAC Flush

(propagateMacFlush)

The Propagate MAC Flush parameter specifies whether MAC flush messages received from the specific LDP are propagated to all spoke SDPs and mesh SDPs within the context of this VPLS or MVPLS service. The propagation follows the split-horizon principle and any data-path blocking is used to avoid the looping of these messages. The options are:

- enabled
- disabled (default)

Protected Mac Address

(protectedMac)

The Protected Mac Address parameter specifies a MAC address that is added to the list of protected MAC addresses. Specify a unicast MAC address in the form *xx-xx-xx-xx-xx-xx*. The default is 00-00-00-00-00-00.

Query Interval (seconds)

(queryInterval)

The Query Interval (seconds) parameter specifies how often, in s, the site sends query messages. The range is 1 to 65 535. The default is 125.

Query source address

(querySrcAddress)

The Query source address parameter specifies the source IP address used when generating IGMP or MLD queries. Table 4-9 describes the parameter options.

Table 4-9 Query source address parameter

Context	Option description
IGMP snooping	The Query source address parameter specifies the source IP address that is used when generating IGMP queries. This parameter can only be specified when the Use query source address parameter is enabled. This is an IPv4 address in dotted-decimal format. The default is 0.0.0.0.
MLD snooping	The Query source address parameter specifies the link local source IP address for the generation of MLD queries. Specify an IPv6 address in the form <i>x:x:x:x:x:x</i> or <i>x:x:x:x:x.d.d.d</i> , where <i>x</i> ranges from 0 to FFFF (hex) and <i>d</i> ranges from 0 to 255 (decimal). The default is 0:0:0:0:0:0:0:0.

Region Name

(regionName)

The Region Name parameter specifies a name for the MSTP region. An MSTP region consists of at least two bridges that run multiple MSTP instances. The region name, region revision, and VLAN-to-instance assignment define the MSTP region. The range is 0 to 32 characters.

Region Revision

(regionRevision)

The Region Revision parameter specifies an MSTP region configuration revision number. The region name, region revision, and VLAN-to-instance assignment define the MSTP region. The range is 0 to 65 535. The default is 0.

Remote Age Time (seconds)

(remoteAgeTime)

The Remote Age Time (seconds) parameter specifies the number of seconds to age out FIB entries on access interfaces. Generally, the Remote Age Time (seconds) parameter is set to a longer period than the Local Age Time (seconds) parameter to reduce the amount of flooding required for destination unknown MAC addresses. The range is 60 to 86 400. The default is 900.

Remote ID

(infoRemoteId)

The Remote ID parameter specifies whether the far-end MAC address is inserted in the remote ID suboption of DHCP Option 82. Inserting the MAC address in the suboption allows MAC-based authentication. The options are:

- false (default)
- true

Report source address

(reportSrcAddress)

The Report source address parameter specifies the IP address for the generation of IGMP or MLD reports. For IGMP, specify a unicast IPv4 address in dotted-decimal format. For MLD, specify an IPv6 address in the form x:x:x:x:x:x:x or x:x:x:x:x.d.d.d, where x ranges from 0 to FFFF (hex) and d ranges from 0 to 255 (decimal). There is no default.

Residential

(residential)

The Residential parameter indicates whether the split horizon group is a residential split horizon group. A residential split horizon group supports lightweight SAPs. The options are:

- enabled
- disabled (default)

Restrict Protected Source

(restrictProtectedSource)

The Restrict Protected Source parameter specifies whether packets that enter a SAP are checked for a protected source MAC address. Packets that contain a protected source MAC address are discarded, a trap is generated, and the SAP is put in an operationally down state. The options are:

- true
- false (default)

All the SAPs that belong to a split horizon group that has the Restrict Protected Source parameter set to True are restricted.

Restrict Protected Source Action

(restrictProtectedSourceAction)

The Restrict Protected Source Action parameter specifies the action to be taken when packets that contain a protected source MAC address are detected. The options are:

- disable (default)
- alarm only

Restrict Unprotected Destination

(restrictUnprotectedDestination)

The Restrict Unprotected Destination parameter specifies whether packets that enter a SAP are checked for an unprotected destination MAC address. Packets that contain an unprotected destination MAC address are discarded. The options are:

- true
- false (default)

Retry Timeout

(macMoveRetryTimeout)

The Retry Timeout parameter specifies the time in seconds that elapses before a SAP that is disabled after exceeding the maximum relearn rate is re-enabled. A value of zero indicates that the SAP does not automatically re-enabled after being disabled. If the SAP is disabled again after the SAP is re-enabled, the effective retry timeout is doubled to avoid thrashing. The range is 0 to 120. The default is 10.

Return Tunnel Auto-Selection Transport Preference

See the [Return Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Return Tunnel Transport

See the [Return Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Revert Time (seconds)

(revertTime)

The Revert Time (seconds) parameter specifies the time to wait before trying to revert to the primary spoke SDP defined on the service endpoint, after having failed over to a backup spoke SDP. The range is -1, or 1 to 600 s. The default is 0. Selecting the Disable Revert Time (Infinite) check box means the parameter is set to a value of -1, or disabled.

Root Guard

(rootGuard)

The Root Guard parameter specifies whether a port is allowed to become an STP root port. The parameter corresponds to the parameter restrictedRole in 802.1Q. The enabled parameter can affect spanning tree connectivity. The options are:

- selected
- not selected (default)

Robust Count

(robustCount)

The Robust Count parameter specifies a variable that allows tuning for the expected packet loss on a SAP, an SDP or a site. If a SAP or an SDP is expected to have high packet loss, increase the Robust count parameter value. Packet loss for IGMP or MLD snooping is calculated by subtracting 1 from the Robust count parameter value. Table lists the parameter ranges for different objects. The default is 2 for all object types. Table 4-10 describes the parameter options.

Table 4-10 Robust count parameter

Object	Range
SAP or SDP	2 to 7
Service site	1 to 255

Route Distinguisher

(vsiRdCli)

The Route Distinguisher parameter is the VsiRd parameter, but in a CLI readable format, [ip-addr:comm-val] or [as-number:ext-comm-val]. Setting this to 0:0 means that the node uses the same value as the VPLS ID. The default is 0:0.

Routing Policy Name

(policyStatementName)

The Routing Policy Name parameter specifies the name of the multicast routing policy associated with a VPLS site. This parameter is enabled if the Use Component Package Policy parameter is disabled. You can enter a multicast routing policy name if no multicast routing policy has been configured. The range is 0 to 32 characters. There is no default.

SAP Sub Type

(sapSubType)

The SAP Sub Type parameter specifies the subtype for the SAP that is to be created. The options are:

- Regular (default)
- Capture
- Managed

When you configure the SAP, this parameter can be set to either Regular or Capture. Use Regular to configure a Regular SAP, and Capture to configure a Capture SAP. The Capture SAP is created to enable the creation of an MSAP. After MSAPs have been created, this parameter displays the read-only value of Managed for the MSAP.

SAP Type

See the [SAP Type](#) parameter in section 14.1.

Scheduling Class

See the [Scheduling Class](#) parameter in section 14.1.

Secondary Ports Cumulative Factor

(macMoveSecondaryPortsCumulativeFactor)

The Secondary Ports Cumulative Factor parameter specifies the maximum periods at which MACs are relearned. Periods are used to measure the MAC-relearn rate, which must be exceeded during consecutive periods before the corresponding ports are blocked. The parameter value must be less than the [Primary Ports Cumulative Factor](#) value. The range is 2 to 9. The default is 2.

Send Flush All But Mine

(IdpMacFlushNotMine)

The Send Flush All But Mine parameter specifies whether an “LDP MAC withdraw all but mine” message received in the I-VPLS domain should attempt to generate a new “LDP MAC withdraw all but mine” message in the B-VPLS domain. The message is generated when the parameter is enabled.

The net effect of receiving this message in the B-VPLS domain is to instruct the B-site to flush all the VPLS MACs, except for those learned from the I-VPLS sender. However, the final implementation of such flushing is still governed by the [MAC Flush on fail](#) parameter that you set on the B-VPLS service site. This functionality complies with the RFC4762 and its behavior is equivalent to the Topology Change Notification in RSTP. The default is not enabled.

Send Flush All From Me

(IdpMacFlush)

The Send Flush All From Me parameter specifies whether an “LDP MAC withdraw all from me” message received in the I-VPLS domain should attempt to generate a new “LDP MAC withdraw all from me” message in the B-VPLS domain. The message is generated when the parameter is enabled.

The net effect of receiving this new message in the B-VPLS domain is to instruct the B-site to flush all the VPLS MACs learned from the I-VPLS sender. However, the final implementation of such flushing is still governed by the [MAC Flush on fail](#) parameter that you set on the B-VPLS service site. The default is not enabled.

Send Queries

(sendQueries)

The Send Queries parameter specifies whether the generation of queries on the SAP is enabled. The parameter is mutually exclusive with the Multicast attached parameter. When you enable the parameter, the Multicast attached parameter is disabled. When the Multicast attached parameter is enabled, the Send queries parameter is disabled. The options are:

- enabled
- disabled (default)

Service ID

See the [Service ID](#) parameter in section 14.1.

Service Name

See the [Service Name](#) parameter in section 14.1.

Service Tier

See the [Service Tier](#) parameter in section 14.1.

Service Site Pointer

(serviceSitePointer)

The Service Site Pointer parameter specifies the site with which the virtual MEP is associated.

Site Activation Timer

(seconds)

The Site Activation Timer (seconds) parameter specifies the time (in seconds) that the system keeps the network element in standby status waiting for BGP updates from remote PEs. At the end of this period, the system runs the designated forwarder (DF) election algorithm to decide whether the network element should be unblocked. The range is 1 to 100. The default is 1.

Site ID

See the [Site ID](#) parameter in section 14.1.

Size (entries)

(size)

The Size (entries) parameter specifies the maximum number of learned and static entries in the FIB. The range is 0 to 196 607. The default is 250.

Snooping

(snooping)

The Snooping parameter specifies whether DHCP snooping is enabled for DHCP messages. The default is determined by the managed device. The options are:

- Enabled
- Disabled (default)

The BSA can copy DHCP packets and inspect them to help secure the system. For example, if malicious user A sends an IP packet requesting a video stream intended for user B, any return packets sent to user B could jam B's connection.

Configure DHCP snooping for two purposes.

- Insert Option 82 information when the system is not configured for DHCP relay by enabling DHCP snooping on the SAP closest to the subscriber.
- Build a DHCP lease-state table by enabling snooping on the service tunnel nearest the network egress and on the SAP closest to the subscriber.

Source Address

(srcAddr)

The Source Address parameter specifies the IP address of the multicast traffic source. Specify a unicast IP address. For IGMP snooping, this is an IPv4 address in dotted-decimal format. For MLD snooping, this is an IPv6 address in colon-hexadecimal format. There is no default.



Note — The Source Address parameter is not supported for Static Mcast groups on the 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], or the 7210 SAS-X24F2XFP.

Source MAC Address

(backboneSrcMac)

The Source MAC Address parameter specifies the Backbone Source MAC-Address for PBB packets. If not provisioned, it defaults to the loopback chassis MAC-Address. The default is 00-00-00-00-00-00.

Split Horizon Group

(splitHorizonGroup)

The Split Horizon Group parameter specifies the name of the Split Horizon Group to be used to the control the traffic that flows through SAPs or spoke SDPs for the VPLS site.

STP Mode

(rstpProtocol)

The STP Mode parameter specifies the STP variant used by the VPLS. Table 4-11 describes the parameter options.

Table 4-11 STP Mode parameter

Option	Option description	Dependencies
RSTP (default)	Specifies compliance with IEEE 802.1D-2004	—
CompDot1w	Specifies that the variant operates as RSTP but is backward compatible with IEEE 802.1w-2001	—
Dot1w	Specifies that the variant is compliant with IEEE 802.1w-2001	—
MSTP	Specifies compliance with IEEE 802.1Q-REV/D3.0-04/2005	Configurable for MVPLS only

Subscriber ID

See the [Subscriber ID](#) parameter in section 36.1.

Suppress Standby Signalling

(suppressStandbySignalling)

The Suppress Standby Signalling parameter specifies whether the pseudowire forwarding standby bit is sent to the LDP peer.

When the Suppress Standby Signalling parameter is enabled, the pseudo-wire standby bit is not sent to T-LDP peer when a specific spoke is selected as a standby. This allows faster switchover, as the traffic is sent over this SDP binding and discarded at blocking side of the connection. This is especially applicable to multicast traffic.

SVC Mgr Service ID

(id)

See the [SVC Mgr Service ID](#) parameter in section 14.1.

Table size (entries)

(mfibTableSize)

The Table size (entries) parameter specifies the maximum number of learned and static entries in the multicast FIB. The range is 0 to 16 383. A value of 0 specifies that there is no limit to the number of entries.

Tunnel Auto-Selection Transport Preference

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Tunnel Fault Notification

See the “[Tunnel Fault Notification](#)” parameter in section 14.1.

Tunnel Transport

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Unconstrained Bandwidth (kbps)

(unconstrainedBandwidth)

The Unconstrained Bandwidth parameter specifies the bandwidth assigned to BTV traffic on an interface using a multicast CAC policy. If the default value of –1 is set, then the value is set to the physical bandwidth available for the interface. If a value of 0 is set, and if a multicast CAC policy is assigned to the interface, BTV traffic from that policy is not allowed on the interface. The range is 0 to 2 147 483 647. The default is –1.

Use Bandwidth-Reserved Paths

See the [Use Bandwidth-Reserved Paths](#) parameter in section 14.1.

Use Component Package Policy

(useComponentPackagePolicy)

The Use Component Package Policy parameter specifies whether the multicast package policy configured as part of the VPLS component is associated with the VPLS site. If the parameter is disabled, the user can specify a multicast routing policy to associate with the VPLS site in the Routing Policy Name parameter field. The options are:

- enabled (default)
- disabled

Use Node Level Boot Timer

(useSysBootTimer)

The Use Node Level Boot Timer parameter specifies whether or not to use the value set for the [Boot Timer \(seconds\)](#) parameter on the network element. When it is enabled, the value set for the Boot Timer (seconds) parameter on the network element will be used. When it is disabled, the value set for the Boot Timer (seconds) parameter on the VPLS site will be used. The options are:

- disabled (default)
- enabled

Use Node Level Site Activation Timer

(useSysActivationTimer)

The Use Node Level Site Activation Timer parameter specifies whether or not to use the value set for the [Site Activation Timer](#) parameter on the network element. When it is enabled, the value set for the Site Activation Timer parameter on the network element will be used. When it is disabled, the value set for the [Activation Timer \(seconds\)](#) parameter on the VPLS site will be used. The options are:

- disabled (default)
- enabled

Use query source address

(useQuerySrcAddress)

The Use query source address parameter, together with the value of the [Query source address](#) parameter, specifies the source IPv4 address used when generating IGMP queries. When the parameter is enabled, the [Query source address](#) value is used as the query source address. When this parameter is disabled, the system interface IP address is used. The options are:

- disabled (default)
- enabled

Use SAP Backbone MAC Address

(backboneUseSapBMac)

The Use SAP Backbone MAC Address parameter specifies the use of the source B-MACs allocated to multi-homed SAPs that are assigned to an MC LAG in the related I-VPLS. The parameter is configurable only on an NE configured with an IOM 3 MDA.

The following restrictions are enforced:

- The Use SAP Backbone MAC Address parameter will only be configurable when the B-SAPs and network interfaces are on IOM 3 MDAs
- If the Use SAP Backbone MAC Address parameter is enabled under at least one B-VPLS, then its B-SAPs and network interfaces must be on an IOM 3 MDA
- If the Use SAP Backbone MAC Address parameter is enabled in a B-VPLS, then any new network interfaces or B-SAPs created in that B-VPLS must be on an IOM 3 MDA or their addition is rejected
- MC-LAG SAPs for the PBB Epipe local switching must be on an IOM 3 MDA for the capability to function properly
- Other SAPs can be on IOM 1 or IOM 2 MDAs

Validation regarding these restrictions originates from the NE and/or the 5620 SAM.

The restrictions for MC-LAG dual-homing in a PBB Epipe do not apply until the Use SAP Backbone MAC Address parameter is enabled.

The options are:

- disabled (default)
- enabled

Use Shared Queue

See the [Use SAP ID as Subscriber ID](#) parameter in section 14.1.

VC ID

See the [VC ID](#) parameter in section 36.1.

VC Type

See the [VC Type](#) parameter in section 21.1.

VE ID

(veId)

The VE ID parameter specifies the VE ID value for this BGP VPLS site. The VE ID is advertised by the BGP update message as part of NLRI, and used to calculate the pseudowire label to other VPLS members. This parameter must be lower than or equal to the [Max VE ID](#) parameter and it should be unique within the VPLS, except for multi-home scenario. The range is 0 to 65 535. The default is 0, meaning it is disabled.

If you need to change this value, be aware of the following:

- The VE ID can be changed without shutting down the VPLS Instance as long as it is smaller than [Max VE ID](#).
- When the VE-ID changes, BGP withdraws its own previously advertised routes and sends a route refresh to all the peers. This results in reception of all the remote routes again. The old PWs are removed and new ones are instantiated for the new VE ID value.

VE Name

([veName](#))

The VE Name parameter specifies a name for a BGP VPLS instance under a VPLS. The range is 0 to 32 ASCII characters. The default is 0, meaning it is disabled.

VLAN VC Tag

See the [VLAN VC Tag](#) parameter in section [36.1](#).

VPLS ID

([vplsIdCli](#))

The value of the VPLS ID parameter specifies the globally-unique VPLS ID for BGP Auto-Discovery in this VPLS service. The [Administrative State](#) parameter cannot be enabled until a VPLS ID is assigned which is not all zeros. The default is 0:0.

VPLS Mode

([vplsMode](#))

The VPLS Mode parameter, which is applicable only to the 7250 SAS-ES and, Release 3.0 R4 or later, specifies the VPLS mode on an Ethernet port or CES card. The parameter can be configured when there is no other SAP configured on the selected Ethernet port or CES card. The options are:

- Qualified (default)
- Unqualified

VPLS Tag

([vplsTag](#))

The VPLS Tag parameter specifies the outer encapsulation value for a VPLS SAP on a 7250 SAS-ES or 7250 SAS-ESA when the **VPLS Mode** parameter is set to Qualified for Release 2.0 to Release 3.0 R3.1 inclusive, or Enabled for Release 3.0 R4 or later.

The VPLS Tag parameter is also used to create a VLAN object and bind the SAP to the object on a 7250 SAS-ES or 7250 SAS-ESA for either of the following conditions:

- **VPLS Mode** parameter is set to Qualified or Unqualified for a 7250 SAS-ES or 7250 SAS-ESA Release 2.0, to Release 3.0 R3.1 inclusive
- **VPLS Mode** parameter is set to Enabled and the **VPLS Mode** parameter is set to Qualified or Unqualified for a 7250 SAS-ES or 7250 SAS-ESA, Release 3.0 R4 or later

Table 4-12 describes the effect of this parameter on the VPLS SAP outer encapsulation and VLAN ID for Qualified and Unqualified modes.

Table 4-12 Effect of the VPLS Tag parameter value on modes

VPLS component	Qualified mode	Unqualified mode
SAP outer encapsulation	VPLS Tag parameter value	Fixed internal value assigned by the 7250 SAS-ES or 7250 SAS-ESA
7250 SAS-ES or 7250 SAS-ESA VLAN ID	VPLS Tag parameter value	VPLS Tag parameter value

The range is 2 to 4092. The default is 0.

5 — VLL parameters

5.1 VLL parameters 5-2

5.1 VLL parameters

This chapter describes the parameters on the VLL service creation form and child forms.



Note — This chapter also describes parameters common to the Service Template forms. Service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent does not recommend using the 5620 SAM-O XML classes and methods associated with service templates.

AAL5 Encapsulation

See the [AAL5 Encapsulation](#) parameter in section [14.1](#).

AAL5 Frame Aware

(concatCellAal5Fr)

The AAL5 Frame Aware parameter specifies whether to complete ATM cell concatenation into MPLS packets based on a AAL5 end of message. The options are:

- enabled
- disabled (default)

Concatenation controls how ATM cells terminate into MPLS frames.

Active Hold Delay (100s of milliseconds)

(activeHoldDelay)

The Active Hold Delay (100s of milliseconds) parameter specifies the amount of time to hold the active state before switching from active to the standby state after the operational failure of a local MC-LAG SAP or MC-APS SAP. LAG and APS subgroup changes that trigger the switch include:

- endpoint changes from active to standby
- object in the endpoint, for example, SAP, ICB, or regular spoke SDP, changes operation state

The range is 0 to 60. The default is 0.

Admin Concat Limit

(maxAdminCells)

The Admin Concat Limit parameter specifies the maximum number of ATM cells that are put into an MPLS packet for transmission. The range is 1 to 128 cells. The default is 1, indicating that no concatenation is done. Concatenation controls how ATM cells terminate into MPLS frames.

You can view the number of ATM cells the far end of the connection in the read-only Peer Concat Limit parameter. When the lesser of the two parameter values is reached, the MPLS packet is ready for transmission. The MPLS packet MTU size always conforms to the service MTU packet size.

Administrative State

See the [Administrative State](#) parameter in section 14.1.

Administrative State

(administrativeState)

The Administrative State parameter specifies the administrative state of the resiliency. When enabled, activity automatically switches between primary and secondary services as required. When disabled, activity can be manually switched from the 5620 SAM interface. The options are:

- Enabled (default)
- Disabled

Aggregate Rate Limit (Kbps)

See the [Aggregate Rate Limit \(kbps\)](#) parameter in section 14.1.

Aggregation

See the [Aggregation](#) parameter in section 14.1.

ANCP String

See the [ANCP String](#) parameter in section 14.1.

Application Profile

See the [Application Profile](#) parameter in section 14.1.

ATM Connection Type

(connectionType)

The ATM Connection Type parameter specifies the type of ATM connection. This parameter is configurable only when the VC Type parameter for the Apipe service is set to Atm-cell. The options are:

- PVT (default)
- PVC
- Port

If the VC Type parameter for the Apipe service is set to Atm-sdu or Atm-vcc, the ATM Connection Type parameter is set automatically to PVC and is not configurable. If the VC Type parameter for the Apipe service is set to Atm-vpc, the ATM Connection Type parameter is set automatically to PVT and is not configurable.

If the PVC connection type is selected, only a connection profile SAP can be created on an ATM cell Apipe service.

ATM OAM Alarm Cell Handling

See the [ATM OAM Alarm Cell Handling](#) parameter in section 14.1.

ATM OAM Terminate

(atmOamTerminate)

The ATM OAM Terminate parameter specifies whether the SAP acts as an OAM termination point. When the parameter is enabled, the SAP does not pass OAM cells. When the parameter is disabled, OAM cells pass into the APIPE service. This object is only configurable for ATM SAPs that are part of an SDU-mode or VCC-mode Apipe service. The options are:

- Up
- Down (default)

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Auto-Generate ID

The Auto-Generate ID parameter specifies the value used by each end of a service tunnel to identify the VC. The range is 0 to 4 294 967 295. The options are:

- Enabled (default)
- Disabled

Automatic SDP Binding/PBB Tunnel Creation

(topologyAutoCompletion)

The Automatic SDP Binding/PBB Tunnel Creation parameter specifies whether the service that you are creating is automatically bound to previously created service tunnels. The options are:

- Enabled
- Disabled (default)

Enabling the parameter displays the [Transport Type](#) and [Use Bandwidth-Reserved Paths](#) parameters.

Auto Select Return Transport Tunnel

See the [Auto Select Return Transport Tunnel](#) parameter in section 14.1.

Auto Select Transport Tunnel

See the [Auto-Select Transport Tunnel](#) parameter in section 14.1.

CCM Messages Enabled

See the [CCM Messages Enabled](#) parameter in section 117.1.

CE IP Address

(ceInetAddress)

The CE IP Address parameter specifies the IPv4 address of the local end host, in dotted-decimal format. This parameter is not configurable when the [Enable CE IP Address Discovery](#) parameter is enabled. The default is 0.0.0.0.

Clock Source

(pwCTDMCfgClockSource)

The Clock Source parameter specifies the type of clock recovery used by a 9500 MPR CEM-to-Eth or SDH to SDH Cpipe service. Table 5-1 describes the parameter options.

Table 5-1 Clock Source parameter

Option	Description	Dependencies
Differential (default)	Differential clock recovery is used when there is a common timing source at each end of an emulated circuit. Common timing sources include GPS signals and SONET/SDH clock signals.	—
Adaptive	Adaptive clock recovery is used when a common timing reference source is not available at each end of an emulated circuit. Adaptive clock recovery typically uses sequence numbers or timestamps in the header of the data packets.	—
Node Timing	Timing from the network clock as defined in G.8261.	—

CLP Change

(concatCellClp)

The CLP Change parameter specifies whether to complete ATM cell concatenation into MPLS packets based on a change to the CLP value of an ATM traffic descriptor. The options are:

- enabled
- disabled (default)

Concatenation controls how ATM cells terminate into MPLS frames.

Collect Accounting Statistics

See the [Collect Accounting Statistics](#) parameter in section 14.1.

Control Word

(controlWord)

The Control Word parameter specifies the use of a control word for the PW OAM. The control word is negotiated with the peer. The options are:

- Preferred
- Not Preferred (default)

The Preferred setting is required for a multi-hop VCC ping. The Not Preferred setting is required for a single-hop VCC ping.

Customer VID

See the [Customer VID](#) parameter in section 14.1.

Default VC ID

(defaultVcId)

The Default VC ID parameter specifies the virtual circuit identifier for the spoke SDP binding. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 4 294 967 295. The default is 0.

Description

See the [Description](#) parameter in section 14.1.

Destination MAC Address

(backboneDestMac)

The Destination MAC Address parameter specifies the Backbone Destination MAC-Address for PBB packets. It must be a valid unicast MAC address. The default is 00-00-00-00-00-00.

Destination Node ID

See the [Tunnel Termination Site](#) parameter in section 14.1.

Direction

See the [Direction](#) parameter in section 117.1.

Disable Fix Window

See the [Disable Fix Window](#) parameter in section 36.1.

EC ID Rx

(ecIdReceive)

The EC ID Rx parameter specifies the emulated circuit identifier in the received direction for a 9500 MPR CEM-to-Eth Cpipe service. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 1 048 576. There is no default value.

EC ID Tx

(ecidTransmit)

The EC ID Rx parameter specifies the emulated circuit identifier in the transmit direction for a 9500 MPR CEM-to-Eth Cpipe service. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 1 048 576. There is no default value.

Egress Filter ID

See the [Egress Filter ID](#) parameter in section 14.1.

Egress Label

See the [Egress Label](#) parameter in section 14.1.

Egress Policy ID

See the [Egress Policy ID](#) parameter in section 14.1.

Egress Scheduler Name

See the [Egress Scheduler Name](#) parameter in section 14.1.

Enable AIS

(aisEnable)

The Enable AIS parameter specifies whether AIS frames are generated by the MEG. The options are:

- Enabled
- Disabled (default)

Enable CE IP Address Discovery

(ceAddressDiscovery)

The Enable CE IP Address Discovery parameter specifies whether the Ipipe service automatically discovers the CE router IP addresses. When the parameter is enabled, the Ipipe service automatically discovers the IP address of each SAP or spoke SDP that supports address discovery, and manual configuration of the addresses on an Ipipe SAP using the [CE IP Address](#) parameter, or on a spoke SDP using the [Peer CE IP Address](#) parameter, is not allowed. If the parameter is disabled, you must manually configure the CE IP address before a SAP can be operationally Up. The options are:

- Enabled
- Disabled (default)

Enable IPv6

(enableIpv6)

The Enable IPv6 parameter specifies whether the service automatically discovers CE IPv6 addresses. When the parameter is enabled, the addresses are automatically discovered on SAPs that support address discovery, and on spoke SDPs. The Enable IPv6 parameter can only be configured when the [Enable CE IP Address Discovery](#) parameter is enabled. The options are:

- Enabled
- Disabled (default)

Enable PW Standby Signaling Master

(enableStandbySignaling)

The Enable PW Standby Signaling Master parameter specifies whether or not to enable T-LDP status messaging in a configuration between a VLL Epipe/Ipipe and IES/VP RN service. T-LDP status messaging provides the ability to propagate faults in the SAP or PW to the PE where the IES/VP RN service is configured, without withdrawing the PW labels. There are also implications for redundant configurations.

In a redundant configuration, consider an example where Release 8.0 or later NE PE1 terminates two spoke SDPs into a VPRN, via devices PE2 and PE3. PE1 chooses to forward traffic on one of the spoke SDPs (active to PE2), while blocking traffic on the other (standby to PE3). With the implementation of T-LDP status messaging, PE1 now has two methods available for switching between these active and standby SDP bindings when needed.

For compatibility with NEs at releases earlier than 8.0, which do not have T-LDP status messaging capability, device PE1 must be able to perform the switchover using either T-LDP status messaging or the older method of PW label withdrawal. To accommodate this, the Enable PW Standby Signaling Master parameter is configured accordingly, to indicate whether or not T-LDP status messaging should be used in the redundant setup.

The ability to enable Standby Signaling on a VLL Epipe endpoint is blocked under the following conditions:

- If vc-switching is enabled on the VLL site
- If Inter-Chassis Backup (ICB) is enabled on any spoke SDP bindings configured to use this endpoint
- If a SAP under this endpoint belongs to an MC-LAG/MC-APS

In addition, when a PE that belongs to the VPRN/IES receives the T-LDP standby message, the L3 Access Interface associated with that spoke SDP will go operationally down. Therefore, the spoke SDP using this interface will be assigned the color purple in the 5620 SAM topology map, signifying that this is the backup spoke SDP.

The options are:

- enabled
- disabled (default)

Enable PW Standby Signaling Slave

(enableStandbySignalingSlave)

The Enable PW Standby Signaling Slave parameter specifies whether transmission of any spoke in a VLL Epipe endpoint is blocked when the spoke receives standby status notification from its peer.

When the Enable PW Standby Signaling Slave parameter is enabled, the node blocks the transmit forwarding direction of a spoke SDP binding, based on the setting of the standby bit received from a T-LDP peer.

A newly-created spoke SDP binding which is part of an explicit VLL Epipe endpoint inherits the setting of this parameter from the endpoint configuration.

If the Enable PW Standby Signaling Slave parameter is disabled, the node assumes the existing independent mode of forwarding behaviour on the spoke SDP binding.

The Enable PW Standby Signaling Slave parameter is blocked on an endpoint under the following conditions:

- If vc-switching is enabled on the VLL site
- If Inter-Chassis Backup (ICB) is enabled on any spoke SDP bindings configured to use this endpoint
- If a SAP under this endpoint belongs to an MC-LAG/MC-APS

The options are:

- Enabled
- Disabled (default)

Encapsulation Value

(End VPI)

The Encapsulation Value (End VPI) parameter specifies the encapsulation value for the port. The parameter is equivalent to the VPI of the PVT connection on the port at the end of a hop. When the ATM Interface Cell Format parameter is set to UNI, the range is 0 to 255. When the ATM Interface Cell Format parameter is set to NNI, the range is 0 to 1024. The default is 0.

Encapsulation Value

(Start VPI)

The Encapsulation Value (Start VPI) parameter specifies the encapsulation value for the port. The parameter is equivalent to the VPI of the PVT connection on the port at the start of a hop. When the ATM Interface Cell Format parameter is set to UNI, the range is 0 to 255. When the ATM Interface Cell Format parameter is set to NNI, the range is 0 to 1024. The default is 0.

Encapsulation Value

(VPI)

The Encapsulation Value (VPI) parameter specifies the encapsulation value for the port. The parameter is equivalent to the VPI of the PVP connection on the port. When the ATM Interface Cell Format parameter is set to UNI, the range is 0 to 255. When the ATM Interface Cell Format parameter is set to NNI, the range is 0 to 1024. The default is 0.

Fragment Interleave

(interleave)

See the [Fragment Interleave](#) parameter in section 14.1.

FRF-12 End-To-End Fragment Threshold

See the [FRF-12 End-To-End Fragment Threshold](#) parameter in section 14.1.

FRF-12 Mode

See the [FRF-12 Mode](#) parameter in section 14.1.

ID

(mepId)

The ID parameter specifies the ID of the remote MEP being tested. The range is 1-8191. The default is 0.

Ingress Filter ID

See the [Ingress Filter ID](#) parameter in section 14.1.

Ingress Label

See the [Ingress Label](#) parameter in section 14.1.

Ingress Match QinQ Dot1P

See the [Ingress Match QinQ Dot1P](#) parameter in section 14.1.

Ingress Policy ID

See the [Ingress Policy ID](#) parameter in section 14.1.

Ingress Scheduler Name

See the [Ingress Scheduler Name](#) parameter in section 14.1.

Inherit Service ID Value

See the [Inherit Service ID Value](#) parameter in section 14.1.

Inner Encapsulation Value

See the [Inner Encapsulation Value](#) parameter in section 14.1.

Inner Encapsulation Value (VCI)

(pwAtmInboundNto1MappedVci)

The Inner Encapsulation Value parameter specifies the ingress generated VCI of the associated ATM PW. The range is 32 to 65 535. The default is 32.

Inner Encapsulation Value (VCI)

(pwAtmOutboundNto1MappedVci)

The Inner Encapsulation Value parameter specifies the egress generated VCI of the associated ATM PW. The range is 32 to 65 535. The default is 32.

Inner Encapsulation Value

(VCI)

See the [Inner Encapsulation Value \(VCI\)](#) parameter in section 14.1.

Inter-Chassis Backup

(isIcb)

The Inter-Chassis Backup specifies the spoke SDP as an inter-chassis backup SDP binding. The options are:

- Enabled
- Disabled (default)

Interworking Type

(interworking)

The Interworking Type parameter specifies the type of interworking that is required for the endpoints of the VLL to communicate. The options are:

- None (default)
- FR-ATM Network Interworking (Frf-5)

ISID

(isid)

The ISID parameter specifies a 24-bit service instance identifier for this service. As part of the Provider Backbone Bridging frames, it is used at the destination PE as a demultiplexor field. The default value of -1 is used to indicate that the value of this object is unspecified. The range is -1 to 16 777 215. The default is -1.

Jitter Buffer (ms)

(cemJitterBuffer)

The Jitter Buffer (ms) parameter specifies the jitter buffer size for Cpipe L2 access interfaces and Epipe L2 access interfaces with CEM encapsulation. The range is 0 to 250. The default value depends on the endpoint type. See the Table 5-2 for the default values.

Table 5-2 Jitter Buffer parameter

Endpoint type	Default Value (ms)	Dependencies
Unstructured E1	5	—
Unstructured T1	5	—
Unstructured E3	5	—
Unstructured T3	5	—
NxDS0 (E1/T1)	32	Timeslot is set to 1
	16	Timeslot is set to between 2 and 4
	8	Timeslot is set to between 5 and 15
	5	Timeslot is set to 16 or higher
NxDS0 with CAS signalling (E1)	8	—
NxDS0 with CAS signalling (T1)	12	—

Jitter Buffer Depth

(pwCTDMCfgJtrBfrDepth)

The Jitter Buffer Depth parameter specifies the Jitter Buffer size in ms, for 9500 MPR Cpipe L2 access interface creation using an SDH port on an STM card (ETSI 3.0.0 only). The options are:

- Low (default)
- High

Low represents 100 ms and High represents 200 ms.

LLF Enabled

(llfEnabled)

The LLF Enabled parameter specifies whether the link loss forwarding forces the operational status of the port on the L2 access interface to be down when a VLL becomes operationally down. If this parameter is enabled and the service goes down, the SAP port will shut down, thereby signaling the connected equipment that the VLL is down. A switch over to a redundant service can then be made. For Epipe, the port must be a null-encapsulated Ethernet port that is used as a SAP for the VLL. For Apipe, the Terminating Port must be a clear channel on 4 port OC3-STM1 ASAP MDA. The options are:

- Enabled
- Disabled (default)

A read-only Ethernet Down Reason parameter on the port configuration form indicates whether the port is down because of Link Loss Forwarding.

Local ECID

(cemLocalEcid)

The Local ECID parameter specifies the 20-bit unsigned binary field which contains an identifier for the circuit that is emulated. The ECID is associated with a specific MAC address. The range is 0 to 1 048 575. The default is 0.

Low-priority Defect

See the [Low-priority Defect](#) parameter in section [117.1](#).

MAC Address

See the [MAC Address](#) parameter in section [14.1](#).

Mac Address

(pwPeerMacAddress)

The Mac Address parameter specifies the destination MAC address for a 9500 MPR CEM-to-Eth Cpipe service, a 9500 MPR ATM-to-Eth Apipe service, or a 9500 MPR Epipe service. The default is 00-00-00-00-00-00.

MAC Refresh Interval

(macRefreshInterval)

The MAC Refresh Interval parameter specifies the amount of time between successive attempts to refresh the MAC address of the CE device associated with an IP VLL (Ipipe) Ethernet SAP. The range is 0 to 65535 s. The default is 14400 s.

Max Concat Delay

(maxDelay)

The Max Concat Limit parameter specifies the maximum amount of time, in hundreds of microseconds, to wait before transmitting the MPLS packet while ATM cells are concatenated into an MPLS packet. Use the parameter to prevent delays in transmitting MPLS packets. The range is 1 to 400 hundreds of microseconds. The time is rounded up to one of the following numbers: 1, 5, 10, 50, 100, 200, 300, or 400. Concatenation controls how ATM cells terminate into MPLS frames.

MC Ring Node

See the [MC Ring Node](#) parameter in section 14.1.

Monitor Access Interface Operational State

See the [Monitor Access Interface Operational State](#) parameter in section 14.1.

MTU

See the [MTU](#) parameter in section 14.1.

Name

See the [Name](#) parameter in section 14.1.

Name

(primaryServiceSitePointer)

The Primary Service Name parameter specifies the primary Apipe service used for the HSDPA configuration. This service:

- must be configured on the site specified for this HSDPA configuration
- the site specified for this HSDPA configuration must have the [VC Type](#) parameter set to either ATM-VCC

- cannot be part of any other resiliency relationship
- must have only one SAP and either one SDP or one Endpoint with at least one SDP

There is no default.

Name

(secondaryServiceSitePointer)

The Secondary Service Name parameter specifies the secondary Apipe service used for the HSDPA configuration. This service:

- must be configured on the site specified for this HSDPA configuration
- the site specified for this HSDPA configuration must have the [VC Type](#) parameter set to either ATM-VCC
- cannot be part of any other resiliency relationship
- must be a different service from the Primary Service specified for this HSDPA configuration
- must have only one SAP

There is no default.

Name

(sitePointer)

The Name parameter specifies the site used for the HSDPA offload resiliency configuration. This must be a site utilizing a 7705 SAR chassis, version 1.1 or later. This field is typically populated by using the Select Site - HSDPA Resiliency form. There is no default.

No Egress Aggregate Rate Limit

See the [No Egress Aggregate Rate Limit](#) parameter in section 14.1.

No Revert

The No Revert parameter specifies whether the VLL returns the primary spoke SDP to service after a failure. When the parameter is enabled, the VLL does not return the primary spoke SDP to service after a failure. The options are:

- disabled (default)
- enabled

Outer Encapsulation Value

See the [Outer Encapsulation Value](#) parameter in section 14.1.

Outer Encapsulation Value

(VPI)

See the [Outer Encapsulation Value \(VPI\)](#) parameter in section 14.1.

Outer Encapsulation Value (VPI)

(pwAtmInboundNto1MappedVpi)

The Outer Encapsulation Value parameter specifies the ingress generated VPI of the associated ATM PW. The range is 0 to 255. The default is 0.

Outer Encapsulation Value (VPI)

(pwAtmOutboundNto1MappedVpi)

The Outer Encapsulation Value parameter specifies the egress generated VPI of the associated ATM PW. The range is 0 to 255. The default is 0.

Payload Size (octets)

(cemPayloadSize)

The Payload Size (octets) parameter specifies the payload size of traffic transmitted to the Packet Service Network (PSN) by the CEM SAP. The payload size is the size of the data that is transmitted over the service. If the size of the data received is not equal to the payload size, the packet is considered defective. The range is 0 and 16 to 2048. The default value depends on the CEM SAP endpoint type, and if applicable, the number of timeslots. See the Table 5-3 for the default values.

Table 5-3 Payload Size parameter

Endpoint type	Default Value (ms)	Dependencies
Unstructured E1	256	—
Unstructured T1	192	—
Unstructured E3	1024	—
Unstructured T3	1024	—
NxDS0 (E1/T1)	64	Timeslot is set to 1
	16	Timeslot is set to between 2 and 4
	Timeslot x 168	Timeslot is set to between 5 and 15
	Timeslot x 8	Timeslot is set to 16 or higher
NxDS0 with CAS signalling (E1)	Timeslot x 16	—
NxDS0 with CAS signalling (T1)	Timeslot x 24	—

Peer CE IP Address

(ceInetAddress)

The Peer CE IP Address parameter specifies the IPv4 address, in dotted-decimal format, of the CE device that is reachable through the IP VLL (Ipipe) SDP binding. This parameter is not be configurable when the [Enable CE IP Address Discovery](#) parameter is enabled. The default is 0.0.0.0.

Per Service Hashing for LAG Enabled

(perServiceHashing)

See the [Per Service Hashing for LAG Enabled](#) parameter in section 14.1.

Port

See the [Port](#) parameter in section 14.1.

Precedence

(endpointPrecedence)

The Precedence parameter specifies the precedence of the SDP binding when there are multiple SDP bindings attached to one service endpoint.

The numeric precedence designation controls the SDP binding responsible for forwarding traffic. A value of 0 defines the primary SDP binding and can only be assigned to one binding. In the event of a failure on a binding with a precedence of 0, traffic forwarding responsibilities move to a binding with a precedence of 1. The range is 0 to 4. The default is 4.

Priority Level for CCM Messages

See the [Priority Level for CCM Messages](#) parameter in section 117.1.

PW Label

(pwLabel)

The PW Label parameter specifies the value to be assigned to Inbound and Outbound PW Labels for the associated ATM PW. Since de-multiplexing of ATM PW flows towards ATM interface is based on the Inbound PW Label value, a check on all Inbound values configured on the same NE must be done in order to avoid duplications. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 16 to 65535. There is no default value.

Remote ECID

(cemRemoteEcid)

The Remote ECID parameter specifies the remote ECID for the circuit that is emulated. The ECID is associated with a specific MAC address. The range is 0 to 1 048 575. The default is 0.

Remote MAC Address

(cemRemoteMacAddr)

The Remote MAC Address parameter specifies the remote MAC address of the CEM-encapsulated Epipe L2 access interface form aa-bb-cc-dd-ee-ff where aa, bb, cc, dd, ee, and ff are hexadecimal numbers. The default is 00-00-00-00-00-00.

Report Alarm

(cemReportAlarm)

The Report Alarms parameter specifies the CEM alarms to monitor and report. A check mark beside the alarm option enables the alarm to be logged. Table 5-4 lists the parameter options.

Table 5-4 Report Alarm parameter

Option	Default
Stray Packets	Alarm monitored and reported
Packet Loss	
Buffer Underrun	
Malformed Packets	
Buffer Overrun	
Remote TDM Fault	Alarm not monitored or reported
Remote Packet Loss	
Remote RDI	

Return Tunnel Auto-Selection Transport Preference

See the [Return Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Return Tunnel Transport

See the “[Return Tunnel Auto-Selection Transport Preference](#)” parameter in section 14.1.

Revert Time (second)

(revertTime)

The Revert Time (second) parameter specifies the time to wait before trying to revert to the primary spoke SDP defined on the service endpoint. The range is -1 to 600 seconds. Setting the parameter to -1 specifies that there is no revert to the primary spoke SDP after a failure to the backup spoke SDP. You can also set the parameter to -1 by selecting the Disable Revert Time (Infinite) check box. The default is 0.

RTP Header

(cemUseRtpHeader)

The RTP Header parameter specifies whether an RTP header is used when packets are transmitted to the PSN by the CEM SAP. The options are:

- Enabled
- Disabled (default)

SAP Type

See the [SAP Type](#) parameter in section 14.1.

Scheduling Class

See the [Scheduling Class](#) parameter in section 14.1.

SDP Admin Bandwidth

(sdpBindAdminBandwidth)

The SDP Admin Bandwidth parameter specifies the bandwidth that needs to be reserved for this SDP binding in kilo-bits per second. The parameter only applies to the SDP bindings under the Epipe, Apipe, Fpipe, Ipipe and Cpipe services. It is linked to the State Cause indicator named “Insufficient Bandwidth to allocate to SDP binding” shown in the States tab of the VLL Spoke-SDP Binding form. The range is 0 to 100 000 000. The default is 0.

The following conditions on the use of this parameter should be observed:

- The SR service manager keeps track of the available bandwidth for each RSVP SDP. The initial value, and maximum value, is the sum of the bandwidths of all constituent LSPs in the SDP. The SDP available bandwidth is adjusted by the user-configured SDP Bandwidth Booking Factor. The relationship is:
$$\text{Max-SDP-available-bw} = \text{Sum}(\text{LSP-bw}) \times \text{SDP-booking-factor}$$

If an LSP consists of a primary and many secondary standby LSPs, then the bandwidth used in the maximum SDP available bandwidth is that of the active path.
- A change to the LSP active path bandwidth updates the maximum SDP available bandwidth, but the activation of a bypass or detour LSP in the path of the primary LSP does not change the maximum SDP available bandwidth. A change to a constituent of the LSP bandwidth that causes overbooking of the maximum SDP available bandwidth raises a warning alarm. This can happen, for example, because the primary LSP path is resignalled or a secondary path is activated, and means that the operational SDP capacity may be greater than the administrative

capacity. The spoke SDPs on the SDP before the change are kept in the operationally Up state and are unaffected. The 5620 SAM does not automatically clear an overbooking alarm when an SDP is no longer overbooked.

- If a static LSP is added to an MPLS SDP, then the maximum SDP available bandwidth is not modified, since a static LSP does not have a bandwidth parameter. This means that PWs may not be admitted because the sum of bandwidth of the constituent dynamic LSPs is too small while the static LSP is available.
- The value you assign to the administrative bandwidth of the spoke SDP in a VLL service may or may not reflect the actual traffic offered to this VLL service. When you bind a VLL service to this SDP, the amount of bandwidth (VLL-bw) configured under the spoke SDP is subtracted from the SDP available bandwidth adjusted by the Booking Factor. If you delete a VLL service binding from this SDP, the amount of bandwidth (VLL-bw) configured under the spoke SDP is added back into the SDP available bandwidth. The relationship is:
$$SDP\text{-}Available\text{-}bw = Max\text{-}SDP\text{-}available\text{-}bw - Sum(VLL\text{-}bw)$$
- If you overbook the total SDP available bandwidth when adding a VLL service, a warning is issued and the bandwidth reservation is rejected. This means that the spoke SDP bandwidth does not update the maximum SDP available bandwidth. In this case, the spoke SDP is put in operational Down state and a status message of “PW not forwarding” is sent to the remote 7x50 PE node. A “CAC failure” trap is also generated. The local 7x50 PE also triggers the appropriate OAM actions on the SAP. That is, it generates an RDI for the ATM SAP and set the Active-bit to zero in the LMI for FR SAP. The same is true for the remote 7x50 PE when it receives the (T-)LDP status message.
- For spoke termination on IES/VP RN, you can specify bandwidth for the spoke SDP on the VLL side only. T-LDP status bits are not supported on the IES/VP RN PE. Therefore, if CAC fails, the spoke SDP goes down and the label is withdrawn from the VLL PE side. The IES/VP RN PE side brings down the spoke SDP since there is no egress PW label. It also brings down the IP interface and the service.
- In the case of spoke termination on VPLS, you can specify bandwidth for the spoke SDP on the VLL side only. The VLL PE puts the spoke SDP in the operational Down state and sends a status message of “PW not forwarding” VPLS PE.
- When CAC admission fails, the service manager does not put the spoke SDP back into the operational Up state until you perform one of the following:
 - A shutdown/no-shutdown of the spoke SDP resulting in a subsequent successful bandwidth check. The service manager does not automatically audit spoke SDPs after their creation to check if bandwidth is available.
 - An in-service modification of the spoke SDP bandwidth parameter that causes the service manager to re-check admission, resulting in a subsequent successful bandwidth check.
- If the VLL service contains an endpoint with multiple redundant spoke SDPs, each spoke SDP has its bandwidth checked against the available bandwidth of the corresponding SDP. If bandwidth reservation is rejected for a spoke SDP, that spoke SDP is put into the operationally Down state and a status message of “PW not forwarding” is sent to the remote 7x50 PE node. A trap is also generated for this spoke SDP, not for the endpoint. This status notification is used by both this 7x50 PE node and the remote 7x50 PE node in determining the Active-tx spoke SDP. The endpoint does not go into the operationally Down state until all constituent spoke SDPs are down.

- If the VLL service performs a PW switching function, each spoke SDP is separately checked for bandwidth against the corresponding SDP. If any spoke SDP is rejected, it is put into the operationally Down state and a status message of “PW not forwarding” is sent upstream and downstream to the 7x50 T-PE and S-PE nodes attached over a signaled PW segment.
- If class-forwarding is enabled on the SDP, VLL service packets are forwarded to the SDP LSP that the packet forwarding class maps to, or if this is Down, then to the default LSP. However, the VLL bandwidth is not checked against the selected LSP available bandwidth, but instead, on the total SDP available bandwidth. If there is a single LSP for each SDP, these two figures match.
- If the same RSVP LSP is part of multiple SDPs, then the bandwidth of this LSP is counted separately in each SDP’s available bandwidth. The bandwidth consumption across SDPs is not updated.
- For multiple RSVP LSPs that are part of the same SDP, load balancing of service packets occurs over the SDP LSPs, based either on service-id or on a hash of the packet header if ingress SAP shared queuing is enabled. In both cases, the VLL bandwidth is not checked against the selected LSP(s) available bandwidth, but instead, on the total SDP available bandwidth. If there is a single LSP for each SDP, these two figures match.
- If you specify a non-zero bandwidth for a VLL service and attempt to bind the service to an LDP or a GRE SDP, a warning is issued that CAC failed. However, the VLL is established and is operationally Up, assuming no other condition prevents this from occurring.

Service Class

(serviceProfile)

The Service Class parameter specifies the service profile used for 9500 MPR Cpipe Apipe, and Epipe services. Table 5-5 describes the parameter options:

Table 5-5 Service Class parameter

Option	Dependencies
CEM to CEM (default)	Cpipe
CEM to Eth	Cpipe, Epipe
SDH to SDH	Cpipe
ATM to ATM (default)	Apipe
ATM to Eth	Apipe

Service ID

See the [Service ID](#) parameter in section 14.1.

Service Name

See the [Service Name](#) parameter in section 14.1.

Service Priority

(svcPriority)

See the [Service Priority](#) parameter in section 14.1.

Service Tier

See the [Service Tier](#) parameter in section 14.1.

Signalling VC Type Override

(signaledOverride)

The Signalling VC Type Override parameter specifies the type of pseudo-wire signaling for the service site of an Apipe of service type ATM cell. The options are:

- None (default)
- ATM-VCC

When you choose None, you must set the [ATM Connection Type](#) parameter to PVC before setting the [Connection Profile ID](#) parameter.

When you choose ATM-VCC, the [ATM Connection Type](#) parameter is set to PVC and cannot be changed.

When an SAP/SDP is configured after you configure this parameter, you cannot change the parameter setting unless the SAP/SDP is deleted.

Site ID

See the [Site ID](#) parameter in section 14.1.

Specify VLAN Path

(specifyVlanPath)

See the [Specify VLAN Path](#) parameter in section 14.1.

Stack Capability Signaling

(stackCapabilitySignaling)

The Stack Capability Signaling parameter specifies whether the service sends the IPv6 stack capability, and verifies whether the IPv6 capability is received from the peer via LDP interface parameters. When the [Enable CE IP Address Discovery](#) parameter and the [Enable IPv6](#) parameter are enabled, the Stack Capability Signaling parameter is sent via LDP to the far end peer. However, if the capability is not received from the peer, the label for the service is released. When the parameter is disabled, the capability is not advertised to the peer, and the presence or absence of the capability from the peer is ignored. The options are:

- Enabled
- Disabled (default)

Subscriber Identification

See the [Subscriber Identification](#) parameter in section 14.1.

SVC Mgr Service ID

(id)

See the [SVC Mgr Service ID](#) parameter in section 14.1.

Transport Type

See the [Transport Type](#) parameter in section 14.1.

Tunnel Auto-Selection Transport Preference

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Tunnel Fault Notification

See the “[Tunnel Fault Notification](#)” parameter in section 14.1.

Tunnel Transport

See the “[Tunnel Auto-Selection Transport Preference](#)” parameter in section 14.1.

Use Bandwidth-Reserved Paths

See the [Use Bandwidth-Reserved Paths](#) parameter in section 14.1.

Use Broadcast MAC Address

(useBroadcastMacAddress)

The Use Broadcast MAC Address parameter specifies whether to use a broadcast MAC address to forward traffic from the Ethernet Ipipe SAP when arpedMacAddress is not a valid MAC address (no ARPed MAC address). The options are:

- true
- false (default)

Use Shared Queue

See the [Use SAP ID as Subscriber ID](#) parameter in section 14.1.

VC Type

(vcType)

The VC Type parameter specifies the type of pseudowire signaling for the service. Table 5-6 describes the parameter options.

Table 5-6 VC Type parameter

Option	Option description	Dependencies
Ethernet	Specifies Ethernet signaling	Applies to Epipe service
VLAN	Specifies VLAN signaling	Applies to Epipe service
ATM-SDU	Specifies ATM-SDU signaling	Applies to Apipe service
ATM-cell	Specifies ATM-cell signaling	Applies to Apipe service
ATM-VCC	Specifies VCC signaling	Applies to Apipe service
ATM-VPC	Specifies ATM-VPC signaling	Applies to Apipe service
FR-DLCI	Specifies FR-DLCI signaling	Applies to Fpipe service
SAToP E1	Specifies SAToP E1 emulation.	Applies to Cpipe service
SAToP T1	Specifies SAToP T1 emulation.	Applies to Cpipe service
CESoPSN	Specifies CESoPSN emulation.	Applies to Cpipe service
CESoPSN-CAS	Specifies CESoPSN-CAS emulation.	Applies to Cpipe service

VLAN ID

(vlanId)

The VLAN ID parameter specifies the identification number of the VLAN associated with a 9500 MPR Cpipe or Apipe service. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 2 to 4080. There is no default value.

VLAN VC Tag

See the [VLAN VC Tag](#) parameter in section 36.1.

VLL Site Type

(vllSiteType)

The VLL Site Type parameter specifies whether the VLL site is a PW switching or terminating site. Table 5-7 describes the parameter options.

Table 5-7 VLL Site Type parameter

Option	Option description
Terminating	Specifies a VLL terminating site.
Switching	Specifies pseudowire switching signaling for the spoke SDPs configured in a VLL service.

6 — *VPRN parameters*

6.1 VPRN parameters 6-2

6.1 VPRN parameters

This chapter describes the parameters on the VPRN service creation forms.



Note — This chapter also describes parameters common to the Service Template form and child forms. Service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent does not recommend using the 5620 SAM-O XML classes and methods associated with service templates.

AAL5 Encapsulation

See the [AAL5 Encapsulation](#) parameter in section 14.1.

Action

(action)

The Action parameter specifies whether the IP address range configured in the [Start Address](#) parameter and the [End Address](#) parameter is included in the subnetwork's free IP address pool. The options are:

- Included (default)
- Excluded

Administrative State

See the [Administrative State](#) parameter in section 14.1.

Administration Status

(adminStatus)

The Administration Status parameter specifies whether Bi-directional Forwarding Detection is enabled. This parameter must be configured before BFD parameters are accessible on router interfaces. The options are:

- Up
- Down (default)

Aggregate Rate Limit (kbps)

See the [Aggregate Rate Limit \(kbps\)](#) parameter in section 14.1.

Aggregation

See the [Aggregation](#) parameter in section 14.1.

Allow Directed Broadcasts

See the [Allow Directed Broadcasts](#) parameter in section 14.1.

Allow Send Force Renews

(allowSendForceRenews)

The Allow Send Force Renews parameter specifies whether the server sends a DHCP force renew message to DHCP clients. When the parameter is enabled, the server sends a force renew message to DHCP clients if it detects a configuration change that affects the lease configuration. The options are:

- enabled
- disabled (default)

ANCP String

See the [ANCP String](#) parameter in section 14.1.

Anti-Spoof MAC Address

See the [Anti-Spoof MAC Address](#) parameter in section 14.1.

Application Profile

See the [Application Profile](#) parameter in section 14.1.

Application Profile String

(appProfileString)

The Application Profile String parameter specifies a string that categorizes an application profile. Specify a text string for the parameter. The range is 0 to 16 characters. There is no default.

ARP Host Limit

See the [ARP Host Limit](#) parameter in section 14.1.

ATM OAM Alarm Cell Handling

See the [ATM OAM Alarm Cell Handling](#) parameter in section 14.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Automatic SDP Binding Creation

(topologyAutoCompletion)

The Automatic SDP Binding Creation parameter specifies whether the VPRN service is base off the VRF Target configuration in the VPRN. The options are:

- Disabled (default)
- Enabled

Autonomous Address Configuration

See the [Autonomous Address Configuration](#) parameter in section 14.1.

Autonomous System

(autonomousSystemNumber)

The Autonomous System parameter specifies the CE-to-PE AS. The range is 1 to 65 535. The default is 0.

Auto Select Return Transport Tunnel

See the [Auto Select Return Transport Tunnel](#) parameter in section 14.1.

Auto Select Transport Tunnel

See the [Auto-Select Transport Tunnel](#) parameter in section 14.1.

BFD Enabled

(bfdEnabled)

The BFD Enabled parameter specifies whether bi-directional forwarding detection is enabled for the interface. When the value is configured to true, the interface can establish BFD sessions and use a BFD for signaling. When the value is configured to false, the interface cannot use BFD. The options are:

- True
- False (default)

BGP Enabled

(bgpEnabled)

The BGP Enabled parameter specifies whether BGP is enabled for the device. The options are:

- Enabled
- Disabled (default)

Broadcast Address Format

See the [Broadcast Address Format](#) parameter in section 14.1.

Calling Station ID

See the [Calling Station ID](#) parameter in section 14.1.

Carrier Carrier VPN

(carrierCarrierVpn)

The Carrier Carrier VPN parameter specifies whether a Carrier Supporting Carrier model is supported on a VPRN service. The parameter must be enabled in order to configure a network interface on a VPRN site. The options are:

- Enabled
- Disabled (default)



Note — You cannot configure the Carrier Carrier VPN parameter on a VPRN site if there are any pre-existing interfaces configured on the site.

Collect Accounting Statistics

See the [Collect Accounting Statistics](#) parameter in section 14.1.

Context Value

(contextValue)

The Context Value parameter specifies the unique context value for IP packet reassembly. The Context Value parameter is configurable only when the [Reassemble](#) parameter is enabled. The range is 1 to 31.

Client Applications

See the [Client Applications](#) parameter in section 14.1.

Current Hop Limit

See the [Current Hop Limit](#) parameter in section 14.1.

Days

(days)

The Days parameter specifies the number of days for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 3650. The default is 0.

Table 6-1 lists and describes the [Option](#) parameter values that require a time specification.

Table 6-1 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCP OFFER response, the DHCP server uses this option to specify the offered lease time.
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

Days**(leaseHoldTimeDay)**

The Days parameter specifies the minimum number of days that a leased IPv6 prefix is valid. The range is 0 to 3650. The default is 0.

Days**(maxLeaseDay)**

The Days parameter specifies the maximum number of days that a leased IP address is valid. The range is 0 to 3650. The default is 10.

Days**(minLeaseDay)**

The Days parameter specifies the minimum number of days that a leased IP address is valid. The range is 0 to 3650. The default is 0.

Days**(preferredLifeTimeDay)**

The Days parameter specifies the minimum number of days that an assigned IP prefix is valid. The range is 0 to 3650. The default is 0.

Days**(rebindTimerDay)**

The Days parameter specifies the number of days between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 14. The default is 0.

Days

(renewTimerDay)

The Days parameter specifies the number of days between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 7. The default is 0.

Days

(validLifeTimeDay)

The Days parameter specifies the minimum number of days that an assigned IP prefix is valid. The range is 0 to 3650. The default is 1.

Default Subscriber Identification String

See the [Default Subscriber Identification String](#) parameter in section 14.1.

Description

See the [Description](#) parameter in section 14.1.

Destination

(destination)

The Destination parameter specifies the destination IP address of a static route for an L3 interface. Specify one of the following:

- an IPv4 address in dotted-decimal format
- an IPv6 address in colon-hexadecimal format; IPv6 must be enabled

There is no default.

Direction

See the [Direction](#) parameter in section 117.1.

Disable Fix Window

See the [Disable Fix Window](#) parameter in section 36.1.

Display Name

See the [Displayed Name](#) parameter in section 14.1.

Displayed Name

See the [Displayed Name](#) parameter in section 14.1.

dot1p

(dot1p)

The dot1p (dot1p) parameter specifies a dot1p class to self-generated traffic on a VPRN site. When a packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the IEEE 802.1p value specified by the Dot1p parameter. The range is 0 to 7, or default. The default is default. Specifying 0 is equivalent to removing the explicit marking.

DSCP

(dscp)

The DSCP parameter specifies the DiffServ Code Point value to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. On a VPRN site, self-generated traffic is assigned a DSCP which is mapped to a forwarding class.

When a packet is marked with the value specified by the DSCP parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter. Table 6-2 lists the parameter options.

Table 6-2 DSCP parameter

Options			
be (default)	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43

Dynamic Topology Discovery

See the [Dynamic Topology Discovery](#) parameter in section 14.1.

Echo Interval

(bfdEchoInterval)

The Echo Interval parameter specifies the minimum echo receive interval, in milliseconds, for the BFD session. The range is 100 to 100 000. The default is 100.

Egress Filter ID

See the [Egress Filter ID](#) parameter in section 14.1.

Egress Mark QinQ Top Bits Only

See the [Egress Mark QinQ Top Bits Only](#) parameter in section 14.1.

Egress Policy ID

See the [Egress Policy ID](#) parameter in section 14.1.

Egress Scheduler Name

See the [Egress Scheduler Name](#) parameter in section 14.1.

Enable DHCP Relay

See the [Enable DHCP Relay](#) parameter in section 14.1.

Enable GRT Lookup

(enableGrtLookup)

The Enable GRT Lookup parameter specifies if a route lookup is performed in the Global Route Table (GRT) when the lookup in the local VRF fails. When this parameter is not enabled, route lookup in the GRT is disabled. The options are:

- Enabled
- Disabled (default)

Enable Local Proxy

See the [Enable Local Proxy](#) parameter in section 14.1.

Enable Local Proxy ARP

See the [Enable Local Proxy ARP](#) parameter in section 14.1.

End Address

(endAddress)

The End Address parameter specifies the last IP address for a range of IP addresses to be configured for a subnetwork. You must also set the [End Address](#) parameter. The default is 0.0.0.0.

Enforce Maximum Number Of Multicast Routes

(`enforceMaxNumberOfMcastRoutes`)

The Enforce Maximum Number Of Multicast Routes parameter specifies whether to enforce a maximum number of multicast routes on an interface when you configure routing properties for a service. The options are:

- Enabled
- Disabled (default)

Enforce Maximum Number Of Routes

(`enforceMaxNumberOfRoutes`)

The Enforce Maximum Number Of Routes parameter specifies whether to enforce a maximum number of routes on an interface when you configure routing properties for a service. The options are:

- Enabled
- Disabled (default)

Export Target AS Value

(`vrfExportTargetASValue`)

The Export Target AS Value parameter specifies the two-byte AS value of the default export VRF target for the site. This parameter is configurable when the Target Format parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 1 to 65 535. The default is 1.

Export Target AS Value

(`vrfMVPNExportTargetASValue`)

The Export Target AS Value parameter specifies the two-byte AS value of the default export VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 0 to 65 535. The default is 1.

Export Target AS Value (4Byte)

(`vrfExportTargetASValue4Byte`)

The Export Target AS Value (4Byte) parameter specifies the four-byte AS value of the default export VRF target for the site. This parameter is configurable when the Target Format parameter is set to Define Import and Export, and the Export Target Format parameter is set to AS-4Byte. The range is 65 536 to 4 294 967 295. The default is 65 536.

Export Target AS Value (4Byte)

(vrfMVPNExportTargetASValue4Byte)

The Export Target AS Value (4Byte) parameter specifies the four-byte AS value of the default export VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to Define Import and Export, and the Export Target Format parameter is set to AS-4Byte. The range is 65 536 to 4 294 967 295. The default is 65 536.

Export Target Community Value

(vrfExportTargetCommunityValue)

The Export Target Community Value parameter specifies a BGP community to use for the default export VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export and the Import Target Format is set to IP Address. The range is 0 to 65 535. The default is 0.

Export Target Community Value

(vrfMVPNExportTargetCommunityValue)

The Export Target Community Value parameter specifies a BGP community to use for the default export VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export and the Import Target Format is set to IP Address. The range is 0 to 65 535. The default is 0.

Export Target Extended Community Value

(vrfExportTargetExtendedCommunityValue)

The Export Target Extended Community Value parameter specifies the extended BGP community of the default export VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 0 to 4 294 967 295. The default is 0.

Export Target Extended Community Value

(vrfMVPNExportTargetExtendedCommunityValue)

The Export Target Extended Community Value parameter specifies the extended BGP community of the default export VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 0 to 4 294 967 295. The default is 0.

Export Target Format

(vrfExportTargetFormat)

The Export Target Format parameter specifies the export target format to use for the default VRF export target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export. Table 6-3 describes the parameter options.

Table 6-3 Export Target Format parameter

Option	Option description
None (default)	—
AS	Specifies that you want to configure a two-byte AS number for the default export target
IP Address	Specifies that you want to configure an IP address for the default export target
AS-4Byte	Specifies that you want to configure a four-byte AS number for the default export target

Export Target Format

(vrfMVPNExportTargetFormat)

The Export Target Format parameter specifies the export target format to use for the default VRF export target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export. Table 6-4 describes the parameter options.

Table 6-4 Export Target Format parameter for MVPN

Option	Option description
None (default)	—
AS	Specifies that you want to configure a two-byte AS number for the default export target
IP Address	Specifies that you want to configure an IP address for the default export target
AS-4Byte	Specifies that you want to configure a four-byte AS number for the default export target
Unicast	Specifies that you want to configure a unicast address for the default export target

Export Target IP Address

(vrfExportTargetIpAddress)

The Export Target IP Address parameter specifies the IP address of the default export VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to IP Address. The default is 0.0.0.0.

Export Target IP Address

(vrfMVPNExportTargetIpAddress)

The Export Target IP Address parameter specifies the IP address of the default export VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to IP Address. The default is 0.0.0.0.

Export Unicast

(exportUnicast)

The Export Unicast parameter specifies the export policies to control MVPN routes exported by the local VRF to other VRFs on the same or remote PE routers. Setting the value to False allows you to specify the policies. The options are:

- True
- False (default)

FIB Priority

(fibPriority)

The FIB Priority parameter specifies the priority level for updating FIB routes into the forwarding plane. Table 6-5 describes the parameter options.

Table 6-5 FIB Priority parameter

Option	Option description
Standard (default)	The FIB entries have no priority over other routes.
High	The FIB entries are given priority over all other routes.

Forwarding Class

(forwardingClass)

The Forwarding Class parameter specifies the forwarding class value to be used as the match criterion for mapping packets that egress the access interface which uses the policy to a queue and Dot1p value. When a packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the queue specified by the Queue ID parameter, and the Dot1p value specified by the dot1p parameter. The options are:

- be (default)
- l2
- l1
- af
- h1
- ll
- nc

Fragment Interleave

(interleave)

See the [Fragment Interleave](#) parameter in section 14.1.

Free Addresses Minimum Threshold

(minFree)

The Free Addresses Minimum Threshold parameter specifies the minimum number of available IP addresses for a specific subnetwork. These IP addresses can be offered to DHCP clients belonging to the subnetwork. When the value is set to 0, there is no minimum specified. The range is 0 to 255. The default is 1.

FRF-12 End-To-End Fragment Threshold

See the [FRF-12 End-To-End Fragment Threshold](#) parameter in section 14.1.

FRF-12 Mode

See the [FRF-12 Mode](#) parameter in section 14.1.

GSMP Administrative State

See the [GSMP Administrative State](#) parameter in section 14.1.

Hold Multiplier

See the [Hold Multiplier](#) parameter in section 14.1.

Hours

(hours)

The Hours parameter specifies the number of hours for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 23. The default is 0.

Table 6-6 lists and describes the [Option](#) parameter values that require a time specification.

Table 6-6 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCPPOFFER response, the DHCP server uses this option to specify the offered lease time.
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.

(1 of 2)

Value	Value description
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

(2 of 2)

Hold-Off Time (seconds)

(singleSfmOverloadHldOffTime)

The Hold-Off Time (seconds) parameter specifies the delay time between the detection of the single SFM failure condition and the IGP entering the overload state. The range is 0 to 600 seconds. The default is 0 seconds.

Hours

(leaseHoldTimeHour)

The Hour parameter specifies the minimum number of hours that a leased IPv6 prefix is valid. The range is 0 to 23. The default is 0.

Hours

(maxLeaseHour)

The Hours parameter specifies the maximum number of hours that a leased proxy IP address is valid. The range is 0 to 23. The default is 0.

Hours

(minLeaseHour)

The Hours parameter specifies the minimum number of hours that a leased proxy IP address is valid. The range is 0 to 23. The default is 0.

Hours

(preferredLifeTimeHour)

The Hours parameter specifies the minimum number of hours that an assigned IP prefix is valid. The range is 0 to 23. The default is 1.

Hours

(rebindTimerHour)

The Hours parameter specifies the number of hours between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 23. The default is 0.

Hours

(renewTimerHour)

The Hours parameter specifies the number of hours between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 23. The default is 0.

Hours

(validLifeTimeHour)

The Hours parameter specifies the minimum number of hours that an assigned IP prefix is valid. The range is 0 to 23. The default is 0.

ID

See the [ID](#) parameter in section [14.1](#).

IGMP Enabled

(igmpEnabled)

The IGMP Enabled parameter specifies whether IGMP is enabled on the site. The options are:

- Enabled
- Disabled (default)

Import Target AS Value

(vrfImportTargetASValue)

The Import Target AS Value parameter specifies the two-byte AS value for the default import VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 1 to 65 535. The default is 1.

Import Target AS Value

(vrfMVPNImportTargetASValue)

The Import Target AS Value parameter specifies the two-byte AS value for the default import VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 0 to 65 535. The default is 1.

Import Target AS Value (4Byte)

(vrfImportTargetASValue4Byte)

The Import Target AS Value (4Byte) parameter specifies the four-byte AS value of the default import VRF target for the site. This parameter is configurable when the Target Format parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS-4Byte. The range is 65 536 to 4 294 967 295. The default is 65 536.

Import Target AS Value (4Byte)

(vrfMVPNImportTargetASValue4Byte)

The Import Target AS Value (4Byte) parameter specifies the four-byte AS value of the default import VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS-4Byte. The range is 65 536 to 4 294 967 295. The default is 65 536.

Import Target Community Value

(vrfImportTargetCommunityValue)

The Import Target Community Value parameter specifies the BGP community of the default import VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to IP Address. The range is 0 to 65 535. The default is 0.

Import Target Community Value

(vrfMVPNImportTargetCommunityValue)

The Import Target Community Value parameter specifies the BGP community of the default import VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to IP Address. The range is 0 to 65 535. The default is 0.

Import Target Extended Community Value

(vrfImportTargetExtendedCommunityValue)

The Import Target Extended Community Value parameter specifies the extended BGP community of the default import VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 0 to 4 294 967 295. The default is 0.

Import Target Extended Community Value

(vrfMVPNImportTargetExtendedCommunityValue)

The Import Target Extended Community Value parameter specifies the extended BGP community of the default import VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to AS. The range is 0 to 4 294 967 295. The default is 0.

Import Target Format

(vrfImportTargetFormat)

The Import Target Format parameter specifies the import target format to use for the default VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export. Table 6-7 describes the parameter options.

Table 6-7 Import Target Format parameter

Option	Option description
None (default)	—
AS	Specifies that you want to configure a two-byte AS number for the default import target
IP Address	Specifies that you want to configure an IP address for the default import target
AS-4Byte	Specifies that you want to configure a four-byte AS number for the default import target

Import Target Format

(vrfMVPNImportTargetFormat)

The Import Target Format parameter specifies the import target format to use for the default VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export. Table 6-8 describes the parameter options.

Table 6-8 Import Target Format parameter for MVPN

Option	Option description
None (default)	—
AS	Specifies that you want to configure a two-byte AS number for the default import target
IP Address	Specifies that you want to configure an IP address for the default import target
AS-4Byte	Specifies that you want to configure a four-byte AS number for the default import target
Unicast	Specifies that you want to configure a unicast address for the default import target

Import Target IP Address

(vrfImportTargetIpAddress)

The Import Target IP Address parameter specifies the IP address of the default import VRF target for the site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to IP Address. The default is 0.0.0.0.

Import Target IP Address

(vrfMVPNImportTargetIpAddress)

The Import Target IP Address parameter specifies the IP address of the default import VRF target for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Import and Export, and the Import Target Format parameter is set to IP Address. The default is 0.0.0.0.

Import Unicast

(importUnicast)

The Import Unicast parameter specifies the import policies to control MVPN routes imported by the local VRF from other VRFs on the same or remote PE routers. Setting the value to False allows you to specify the policies. The options are:

- True
- False (default)

Ingress Filter ID

See the [Ingress Filter ID](#) parameter in section 14.1.

Ingress Match QinQ Dot1P

See the [Ingress Match QinQ Dot1P](#) parameter in section 14.1.

Ingress Policy ID

See the [Ingress Policy ID](#) parameter in section 14.1.

Ingress Scheduler Name

See the [Ingress Scheduler Name](#) parameter in section 14.1.

Inner Encapsulation Value

See the [Inner Encapsulation Value](#) parameter in section 14.1.

Inner Encapsulation Value

(VCI)

See the [Inner Encapsulation Value \(VCI\)](#) parameter in section 14.1.

Interface ID

See the [Interface ID](#) parameter in section 14.1.

Intermediate Destination ID

(interDestIdString)

The Intermediate Destination ID parameter specifies a string that identifies an Intermediate Destination. Specify a text string for the parameter. The range is 0 to 32 characters. There is no default.

IP Address

Table 6-9 lists where to find information about the IP Address parameter.

Table 6-9 IP Address parameter

Parameter	See
IP Address for L3 interface, or IES or VPRN routing-instance neighbor	IP Address parameter in section 14.1
IP Address for destination node of static route	IP Address parameter in section 14.1

IP Address 1

(address1)

The IP Address 1 parameter specifies an IP address for the Subnet Option in dotted-decimal format for an IPv4 address. The default is 0.0.0.0. The parameter is configurable when the [Type](#) parameter is set to IP Address.

IP Address 2

(address2)

See the [IP Address 1](#) in this section.

IP Address 3

(address3)

See the [IP Address 1](#) in this section.

IP Address 4

(address4)

See the [IP Address 1](#) in this section.

IP Address Overlap Avoidance Enabled

(ipAddrOverlapAvoidanceEnabled)

The IP Address Overlap Avoidance Enabled parameter specifies whether to enable or disable checking for duplicate IP addresses on different VPRN sites within the same VPRN service. When the parameter is set to enabled, and a duplicate IP address is used within the same VPRN service for the same customer, an IpAddressOverlap alarm notifies users of this condition.

IPv6 Address

(address)

The IP Address parameter specifies the IP address for the object. An IP address must be assigned to each IP interface. An IP address and a subnet mask create an IP prefix. The defined IP prefix must be unique within the context of the routing instance. The prefix must not overlap with other IP prefixes that are defined as local subnets on other IPv6 prefixes that exist on any local DHCPv6 servers in the same routing context within the device. Specify an IPv6 address in colon-hexadecimal format. There is no default

IPv6 Delegated Prefix Length

See the [IPv6 Delegated Prefix Length](#) parameter in section [14.1](#).

IPv6 Prefix

See the [IPv6 Prefix](#) parameter in section [14.1](#).

Keep Alive

See the [Keep-Alive \(seconds\)](#) parameter in section [14.1](#).

L2 Header

See the [L2 Header](#) parameter in section [14.1](#).

L2TP Enabled

(l2tpEnabled)

The L2TP Enabled parameter specifies whether L2TP is enabled on the site. The options are:

- Enabled
- Disabled (default)

Label Mode

(labelMode)

The Label Mode parameter specifies the mode of allocation of service labels to the routes exported by the VPRN as BGP-VPN routes. Table 6-10 describes the parameter options.

Table 6-10 Label Mode parameter

Option	Option description
VRF (default)	The service labels are allocated per-VRF basis. All BGP-VPN routes exported from a VPRN service have the same service label.
Next Hop	The service labels are allocated on a per-next-hop basis. One unique (platform-wide) service label is allocated to each next-hop IP interface of the VPRN.

Lease Populate

See the [Lease Populate](#) parameter in section 14.1.

Lifetime (seconds)

Table 6-11 lists where to find information about the Lifetime (seconds) parameter.

Table 6-11 Lifetime (seconds) parameter

Parameter	See
Lifetime (seconds) for general router advertisement	Lifetime (seconds) parameter in section 14.1
Lifetime (seconds) to specify preferred routing prefix lifetime	Lifetime (seconds) parameter in section 14.1
Lifetime (seconds) to specify valid routing prefix lifetime	Lifetime (seconds) parameter in section 14.1

Link MTU

(linkMTU)

See the [Link MTU](#) parameter in section 14.1.

LNS

See the [LNS](#) parameter in section 14.1.

Local Address

See the [Local Address](#) parameter in section 14.1.

Log Only

Table 6-12 lists where to find information about the Log Only parameter.

Table 6-12 Log Only parameter

Parameter	See
Log Only in Maximum Number of IPv6 Routes panel	Log Only parameter in this section
Log Only in Maximum Number of Multicast Routes panel	Log Only parameter in this section
Log Only in Maximum Number of Routes panel	Log Only parameter in this section

Log Only

(ipv6MaxNumRoutesLogOnly)

The Log Only parameter specifies whether to disable the learning of new routes when the limit set by the [Maximum Number Of IPv6 Routes](#) parameter is exceeded. The parameter setting does not affect the logging of events. When the parameter is set to true, the learning of new routes is not disabled. The options are:

- false (default)
- true

Log Only

(maxNumberOfMcastRoutesLogOnly)

The Log Only parameter specifies whether to disable the learning of new routes when the limit set by the [Maximum Number Of Multicast Routes](#) parameter is exceeded. The parameter setting does not affect the logging of events. When the parameter is set to true, the learning of new routes is not disabled. The options are:

- false (default)
- true

Log Only

(maxNumberOfRoutesLogOnly)

The Log Only parameter specifies whether to disable the learning of new routes when the limit set by the [Maximum Number Of Routes](#) parameter is exceeded. The parameter setting does not affect the logging of events. When the parameter is set to true, the learning of new routes is not disabled. The options are:

- false (default)
- true

Loopback Enabled

See the [Loopback Enabled](#) parameter in section 186.1.

Low-priority Defect

See the [Low-priority Defect](#) parameter in section 117.1.

MAC Address

See the [MAC Address](#) parameter in section 14.1.

MAC Monitoring

See the [MAC Monitoring](#) parameter in section 14.1.

Managed Address Config

See the [Managed Address Config](#) parameter in section 14.1.

Mask

(mask)

The Mask parameter specifies the IP address subnet mask in dotted-decimal format or as a 32-bit integer.

Mask Reply

See the [Mask Reply](#) parameter in section 14.1.

Maximum Declined Addresses Stored

(maxDeclined)

The Maximum Declined Addresses Stored parameter specifies the maximum number of declined IP address that can be stored. After the maximum is reached, the oldest declined IP address is moved back to the free IP address pool. The range is 0 to 4 294 967 295. The default is 64.

Maximum Number Of Equal Cost Routes

(maxNumberOfEqualCostRoutes)

The Maximum Number Of Equal Cost Routes parameter specifies the number of equal cost routes to use for path sharing. When there are more equal cost routes than the configured value, routes with the lowest next-hop value are chosen. When you set the parameter value to 1, multipath routing is disabled. In this case, the route with the lowest next-hop IP address is used. The range is 0 to 16. The default is 1.

Maximum Number Of IPv6 Routes

(maxIPv6RouteNumber)

The Maximum Number Of IPv6 Routes parameter specifies the maximum number of IPv6 routes in the VRF table. To configure the parameter, you must first deselect the No Maximum check box beside the parameter. The range is 1 to 2 147 483 647. The default is -1, which specifies that there is no maximum.

Maximum Number Of Multicast Routes

(maxNumberOfMcastRoutes)

The Maximum Number Of Multicast Routes parameter specifies the maximum number of multicast routes that are held in the VRF. This parameter is configurable when the [Enforce Maximum Number Of Multicast Routes](#) parameter is enabled. The range is 1 to 2 147 483 647. The default is -1, which specifies that there is no maximum.

You must disable the [Enforce Maximum Number Of Multicast Routes](#) parameter if the Maximum Number Of Multicast Routes parameter is set to the default of -1 on an NE. You must enable the [Enforce Maximum Number Of Multicast Routes](#) parameter if the Maximum Number Of Multicast Routes parameter is set to a non-default value.

Maximum Number Of Routes

(maxNumberOfRoutes)

The Maximum Number Of Routes parameter specifies the maximum number of routes that are held in the VRF. This parameter is configurable when the [Enforce Maximum Number Of Routes](#) parameter is enabled. The range is 1 to 2 147 483 647. The default is -1, which specifies that there is no maximum.

Max Interval (seconds)

See the [Max Interval \(seconds\)](#) parameter in section [14.1](#).

Max Number of Exported Policies

(maxExportedGrtRoutes)

The Max Number of Exported Policies parameter is used in determining the maximum number of routes that can be exported from a specific VRF to populate the GRT. Specifically, the GRT is populated by defining export policies for each participating VPRN service. The range is 0 to 1000. The default is 5.

Metric

(metric)

The Metric parameter specifies the cost metric for the static route. This value is used when the static route is exported to other protocols such as OSPF. The range is 0 to 65 535. The default is 1.

Minimum Authentication Interval (minutes)

See the [Minimum Authentication Interval \(minutes\)](#) parameter in section 14.1.

Min Interval (seconds)

See the [Min Interval \(seconds\)](#) parameter in section 14.1.

Minutes

(leaseHoldTimeMinute)

The Minutes parameter specifies the minimum number of minutes that a leased proxy IPv6 prefix is valid. The range is 0 to 59. The default is 0.

Minutes

(maxLeaseMinute)

The Minutes parameter specifies the maximum number of minutes that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

Minutes

(minLeaseMinute)

The Minutes parameter specifies the minimum number of minutes that a leased proxy IP address is valid. The range is 0 to 59. The default is 10.

Minutes

(minutes)

The Minutes parameter specifies the number of minutes for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 59. The default is 10.

Table 6-13 lists and describes the [Option](#) parameter values that require a time specification.

Table 6-13 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCPPOFFER response, the DHCP server uses this option to specify the offered lease time.

(1 of 2)

Value	Value description
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

(2 of 2)

Minutes

(offerMinute)

The Minutes parameter specifies the number of minutes the DHCP client can consider the IP address before the offer is withdrawn. The range is 0 to 10. The default is 1.

Minutes

(preferredLifeTimeMinute)

The Minutes parameter specifies the minimum number of minutes that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

Minutes

(rebindTimerMinute)

The Minutes parameter specifies the number of minutes between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 59. The default is 48.

Minutes

(renewTimerMinute)

The Minutes parameter specifies the number of minutes between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 59. The default is 30.

Minutes

(validLifeTimeMinute)

The Minutes parameter specifies the minimum number of minutes that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

Monitor Access Interface Operational State

See the [Monitor Access Interface Operational State](#) parameter in section 14.1.

MTU

See the [MTU](#) parameter in section 14.1.

Multicast Capable Peers

(multicastCapablePeers)

The Multicast Capable Peers parameter specifies whether multicast capable BGP peers are displayed. The options are:

- Enabled
- Disabled (default)

Multiplier

(bfdMultiplier)

The Multiplier parameter specifies the number of consecutive BFD messages that must be missed before the BFD session state is changed to the down state. OSPF, IS-IS and PIM are notified of the fault. The range is 3 to 20. The default is 3.

MVPN VRF Target Type

(vrfMVPNTargetType)

The VRF Target Type parameter specifies how to configure the VRF target for the MVPN site. Table 6-27 describes the parameter options.

Table 6-14 VRF Target Type parameter

Option	Option description
None (default)	Specifies that you do not want to configure a VRF target for the MVPN site
Define Default	Specifies that you want to configure a default VRF target for the MVPN site
Define Import and Export	Specifies that you want to configure import and export VRF targets for the MVPN site

Name

See the [Name](#) parameter in section 14.1.

Netbios Node Type

(netbiosNodetype)

The Netbios Node Type parameter specifies the order and method to resolve a Netbios name into an IP address. Table 6-15 lists the parameter options and the option numbers.

Table 6-15 Netbios parameter options

Option	Option Description
B	The DHCP server uses broadcast for name resolution and registration.
P	The DHCP server uses peer to peer for name resolution and registration.
M	The DHCP server uses a combination of broadcast and peer to peer. If broadcast cannot resolve the name, it uses peer to peer.
H	The DHCP server uses a combination of peer to peer and broadcast. If peer to peer cannot resolve the name, it uses broadcast.

No Expiry

Table 6-16 lists where to find information about the No Expiry parameter.

Table 6-16 No Expiry parameter

Parameter	See the
No Expiry for preferred routing prefix lifetime	No Expiry parameter in section 14.1
No Expiry for valid routing prefix lifetime	No Expiry parameter in section 14.1

Number

(optionNumber)

The Number parameter specifies a DHCP option number defined in RFC 2131. The parameter is configurable when the [Option](#) parameter is set to Custom Option. The range is 1 to 254. The default is 0, which means the parameter is not configured.

Number of Packet Too Big

See the [Number of Packet Too Big](#) parameter in section 14.1.

Number of Param Problem

See the [Number of Redirects](#) parameter in section 14.1.

Number of Redirects

See the [Number of Redirects](#) parameter in section 14.1.

Number of Time Exceeded

See the [Number of Time Exceeded](#) parameter in section 14.1.

Number of TTL Expired

See the [Number of TTL Expired](#) parameter in section 14.1.

Number of Unreachables

See the [Number of Unreachables](#) parameter in section 14.1.

OAM Administrative State

See the [OAM Administrative State](#) parameter in section 14.1.

On-link Determination

See the [On-Link Determination](#) parameter in section 14.1.

Option

(option)

The Option parameter specifies the information that a DHCP client receives from the DHCP server. Depending on the parameter value, a DHCP client can receive network service or network configuration information. If no option is specified, a DHCP client is identified using the client MAC Address. The following options are available when you configure the parameter in a subnet:

- Custom Option (default)
- Default Routers
- Subnet Mask

The following options are available for IP address pools:

- Custom Option (default)
- DNS Name Servers
- Netbios Name Server
- Domain Name
- Lease Rebind Time
- Lease Renew Time
- Lease Time
- Netbios Name Server
- Netbios Node Type

You can specify a different DHCP option by setting the parameter to Custom Option and setting the [Number](#) parameter using a DHCP option number defined in RFC 2131.

OSPFv2 Enabled

(ospfEnabled)

The OSPFv2 Enabled parameter specifies whether OSPFv2 is enabled on the device. The options are:

- Enabled
- Disabled (default)

OSPFv3 Enabled

(ospfv3Enabled)

The OSPFv3 Enabled parameter specifies whether OSPFv3 is enabled on the device. The options are:

- Enabled
- Disabled (default)

Other Stateful Config

See the [Other Stateful Config](#) parameter in section 14.1.

Outer Encapsulation Value

See the [Outer Encapsulation Value](#) parameter in section 14.1.

Outer Encapsulation Value

(VPI)

See the [Outer Encapsulation Value \(VPI\)](#) parameter in section 14.1.

Packet Too Big

See the [Packet Too Big](#) parameter in section 14.1.

Packet Too Big Time (seconds)

See the [Packet Too Big Time \(seconds\)](#) parameter in section 14.1.

Param Problem

See the [Param Problem](#) parameter in section 14.1.

Param Problem Time (seconds)

See the [Param Problem Time \(seconds\)](#) parameter in section 14.1.

Physical Address

See the [Physical Address](#) parameter in section 14.1.

PIM Enabled

(pimEnabled)

The PIM Enabled parameter specifies whether PIM is enabled on the site. The options are:

- Enabled
- Disabled (default)

Periodic Atm Oam LoopBack

See the [Periodic ATM OAM Loopback](#) parameter in section 14.1.

Policy 1

See the [Policy 1](#) parameter in section 14.1.

Policy 2

See the [Policy 1](#) parameter in section 14.1.

Policy 3

See the [Policy 1](#) parameter in section 14.1.

Policy 4

See the [Policy 1](#) parameter in section 14.1.

Policy 5

See the [Policy 1](#) parameter in section 14.1.

Pool Name

(displayName)

The Pool Name parameter specifies the name of an IP address pool. The range is 0 to 32 characters. There is no default.

Port

See the [Port](#) parameter in section 14.1.

Preference

(preference)

The Preference parameter specifies the preference of the current static route (as opposed to the routes from different sources such as BGP or OSPF), expressed as a decimal integer. When you modify the preference value of an existing static route, unless specified, the metric does not change. The range is 1 to 255. The default is 5.

When multiple routes are learned with the same preference using the same protocol, the lowest cost route is used. When multiple routes are learned with the same preference using the same protocol and the costs are equal, the route is determined by ECMP configuration.

Preferred Life Time

See the [Preferred Life Time](#) parameter in section 14.1.

Prefix Length

See the [Prefix Length](#) parameter in section 14.1.

Prefix Delegation

See the [Prefix Delegation](#) parameter in section 14.1.

Priority Dscp

See the [Priority Dscp](#) parameter in section 14.1.

Priority Precedence

See the [Priority Precedence](#) parameter in section 14.1.

Priority Type

See the [Priority Type](#) parameter in section 14.1.

Private Retail Subnet

(privateRetailSubnets)

The Private Retail Subnet parameter specifies whether overlapping IP address may exist between different retailers referring to the same wholesale interface. This property is only applicable to Foredoing Subscriber Interfaces. If IP addresses are defined for the retail interface, they must be cleared before modification of this property is allowed. If VPRN type is Hub, this property must be set to True. The options are:

- True
- False (default)

Proxy ARP Policy 1

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy ARP Policy 2

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy ARP Policy 3

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy ARP Policy 4

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy ARP Policy 5

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Reachable Time (milliseconds)

See the [Reachable Time \(milliseconds\)](#) parameter in section 14.1.

Reassemble

(reassemble)

The Reassemble parameter enables IP Packet Reassembly on a VPRN L3 access interface or a network interface. The options are:

- Enabled
- Disabled (default)

Rebind Timer

See the [Rebind Timer](#) parameter in section 14.1.

Receive Interval

(bfdRxInterval)

The Receive Interval parameter specifies the receive interval in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Redirects

See the [Redirects](#) parameter in section 14.1.

Redirects Time (seconds)

See the [Redirects Time \(seconds\)](#) parameter in section 14.1.

Remote Proxy ARP

See the [Remote Proxy ARP](#) parameter in section 14.1.

Renew Timer

See the [Renew Timer](#) parameter in section 14.1.

Retransmit Time (milliseconds)

See the [Retransmit Time \(milliseconds\)](#) parameter in section 14.1.

Return Tunnel Auto-Selection Transport Preference

See the [Return Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Return Tunnel Transport

See the “[Return Tunnel Auto-Selection Transport Preference](#)” parameter in section 14.1.

RIP Enabled

(ripEnabled)

The RIP Enabled parameter specifies whether RIP is enabled on the site. The options are:

- Enabled
- Disabled (default)

Route Distinguisher Type

(routeDistinguisherType)

The Route Distinguisher Type parameter specifies the identifier attached to routes that indicates the VPRN to which it belongs. Each routing instance must have a unique route distinguisher within the carrier’s domain associated with it. A route distinguisher must be defined for a VPRN to be operationally active. Table 6-17 describes the parameter options.

Table 6-17 Route Distinguisher Type parameter

Option	Option description
Type 0	Specifies that you want to assign a 2-byte AS number for the route distinguisher
Type 1	Specifies that you want to assign an IP address for the route distinguisher
Type 2	Specifies that you want to assign a 4-byte AS number for the route distinguisher
None (default)	Specifies that you do not want to assign a route distinguisher

Router ID

(routerId)

The Router ID parameter specifies the IP address of the routing instance. The default is the value of the Site ID parameter that you specify when you create a service site. Specify a unicast IP address in dotted-decimal format for the Server 1 parameter.

Router Lifetime (seconds)

See the [Router Lifetime \(seconds\)](#) parameter in section 14.1.

SAP ARP Host Limit

See the [SAP ARP Host Limit](#) parameter in section 14.1.

Scheduling Class

See the [Scheduling Class](#) parameter in section 14.1.

Seconds

(leaseHoldTimeSecond)

The Seconds parameter specifies the minimum number of seconds that a leased proxy IPv6 prefix is valid. The range is 0 to 59. The default is 0.

Seconds

(maxLeaseSecond)

The Second parameter specifies the maximum number of seconds that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

Seconds

(minLeaseSecond)

The Seconds parameter specifies the minimum number of seconds that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

Seconds

(offerSecond)

The Seconds parameter specifies the number of seconds the DHCP client can consider the IP address before the offer is withdrawn. The range is 0 to 59. The default is 0.

Seconds

(preferredLifeTimeSecond)

The Seconds parameter specifies the minimum number of seconds that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

Seconds

(rebindTimerSecond)

The Seconds parameter specifies the number of seconds between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 59. The default is 0.

Seconds

(renewTimerSecond)

The Seconds parameter specifies the number of seconds between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 59. The default is 0.

Seconds

(seconds)

The Seconds parameter specifies the number of seconds for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 3650. The default is 0.

Table 6-18 lists and describes the [Option](#) parameter values that require a time specification.

Table 6-18 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCPPOFFER response, the DHCP server uses this option to specify the offered lease time.
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

Seconds

(validLifeTimeSecond)

The Seconds parameter specifies the minimum number of seconds that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

Send Advertisement

See the [Send Advertisement](#) parameter in section 14.1.

Server 1

See the [Server 1](#) parameter in section 14.1.

Server 2

See the [Server 1](#) parameter in section 14.1.

Server 3

See the [Server 1](#) parameter in section 14.1.

Server 4

See the [Server 1](#) parameter in section 14.1.

Server 5

See the [Server 1](#) parameter in section 14.1.

Server 6

See the [Server 1](#) parameter in section 14.1.

Server 7

See the [Server 1](#) parameter in section 14.1.

Server 8

See the [Server 1](#) parameter in section 14.1.

Service ID

See the [Service ID](#) parameter in section 14.1.

Service Name

See the [Service Name](#) parameter in section 14.1.

Service Priority

(svcPriority)

See the [Service Priority](#) parameter in section 14.1.

Service Tier

See the [Service Tier](#) parameter in section 14.1.

Session Limit

(ifSessionLimit)

The Session Limit parameter specifies the maximum number of PPPoE sessions allowed on the interface. The range is 1 to 8000. The default is 1.

Session Limit per SAP

(sapSessionLimit)

The Session Limit per SAP parameter specifies the maximum number of PPPoE sessions allowed on the SAP belonging to the interface. The range is 1 to 8000. The default is 1.

Single SFM Overload Admin State

(singleSfmOverloadAdminState)

The Single SFM Overload Admin State parameter specifies the administrative state of the IGP single SFM overload behavior in this virtual router instance. When the parameter is set to Up, the IGP protocols (either IS-IS or OSPF) enter an overload state when the NE has only a single functional Switch Fabric Module.

In a typical system in the event of a SFM failure, multicast traffic must be rerouted around the NE. The defined failure scenarios include:

- There is only one SFM installed in the system
- One Switch Fabric Module (active or standby) fails in a dual SFM configuration
- The system is in the process of an in-service software upgrade

The overload state in IGP is used to trigger the traffic reroute by setting the overload bit in IS-IS, or setting the metric to maximum in OSPF. Since PIM uses IGP, a next-hop change in IGP will cause PIM to join the new path and destroy the old path, which effectively reroutes the multicast traffic. When the problem is resolved, the overload condition is cleared and traffic is directed back to the router.

The options are:

- Up
- Down (default)

The Hold-Off Time (seconds) parameter and read-only attributes Overload State, Overload Start, and Overload Duration are displayed when the Single SFM Overload Admin State parameter is set to Up.

The read-only attributes associated with the function indicate the following:

- Overload State, will display one of the following:
 - Not Applicable - the IGP overload reaction to the single SFM failure condition is disabled.
 - Normal - the full system multicast capacity of a dual SFM chassis is available.
 - Overload - only reduced system multicast capacity is available, and IGP protocols are in an overload state.

- **Overload Start:** indicates the total time this system has been in overload. If this has never occurred, this attribute displays a zero value.
- **Overload Duration:** indicates the duration of the most recent overload condition.

SLA Profile Mapped String

(**subscrProfileString**)

The SLA Profile Mapped String parameter specifies the mapped string to the subscriber SLA profile assigned to the subscriber host. The range is 0 to 16 characters. There is no default.

SNMP Community String

(**snmpCommunityName**)

The SNMP Community String parameter specifies an SNMP community string for the mediation of IPv6 objects on the VPRN site. The range is 1 to 32 characters. There is no default.

Source Address Termination

(**ipOrInterfaceIndex**)

The Source Address Termination parameter specifies whether the source address used by the IP application to send unsolicited packets to a managed node is a user-specified IP address or the primary address of the L3 access interface (referred to on the Source Address form as Interface Index). The L3 interface must be created on the routing instance of the selected router for the VPRN before it can be used as the source address.

The options are:

- IP Address
- Interface Index

Source IP Address

(**sourceIpAddress**)

The Source IP Address parameter specifies the IP address, in dotted-decimal format for IPv4, or colon-hexidecimal format for IPv6, that is used by the IP application to send unsolicited packets to an NE. An IPv6 IP address is configurable when the following are true:

- The [Source Address Termination](#) parameter is set to IP Address.
- The [IPv6 Allowed](#) parameter is enabled on the L3 access interface; see chapter [28](#) for information about enabling IPv6.
- The [IPv6 Allowed](#) parameter is enabled for the VPRN service; see chapter [73](#) for information about enabling IPv6.

Source IP Application

(sourceIpApplication)

The Source IP Application parameter specifies the application for which the source IP or interface index is specified. Table 6-19 describes the parameter options.

Table 6-19 IP Source Application Parameter

Option	Dependencies
Telnet	Selectable when the Source IP Address is set to an IPv4 address.
FTP	
SSH	
RADIUS	
TACACS+	
SNMP Traps	
Syslog	
ICMP Ping	
Trace Route	
DNS	
SNTP	
NTP	
Telnet IPv6	Selectable when the Source IP Address is set to an IPv6 address.
FTP IPv6	
RADIUS IPv6	
TACACS+ IPv6	
SNMP Traps IPv6	
Syslog IPv6	
ICMP Ping IPv6	
Trace Route IPv6	
DNSIPv6	

Static Route ID

(id)

The Static Route ID parameter specifies a unique identifier for the static route in the service domain. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 2 147 483 647. The default is 0.

Start Address

(startAddress)

The Start Address parameter specifies the first IP address for a range of IP addresses to be configured for a subnetwork. You must also set the [End Address](#) parameter. The default is 0.0.0.0.

Subscriber Identification

(subscrIdent)

The Subscriber Identification parameter specifies an identifier for the subscriber for a PPPoE session. The range is 1 to 32 characters. There is no default.

Subscriber Mapped Profile String

(subscrProfileString)

The Subscriber Mapped Profile String parameter specifies the mapped string to the subscriber profile assigned to the subscriber host. The range is 0 to 16 characters. There is no default.

Subscriber Identification

See the [Subscriber Identification](#) parameter in section 14.1.

SVC Mgr Service ID

(id)

See the [SVC Mgr Service ID](#) parameter in section 14.1.

Tag

See the [Tag](#) parameter in section 203.1.

Target AS Value

(vrfMVPNTargetASValue)

The Target AS Value parameter specifies the two-byte AS number of the default VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to AS. The range is 0 to 65 535. The default is 1.

Target AS Value

(vrfTargetASValue)

The Target AS Value parameter specifies the two-byte AS number of the default VRF target for the site. This parameter is configurable when the Target Format parameter is set to AS. The range is 1 to 65 535. The default is 1.

Target AS Value (4Byte)

(vrfMVPNTargetASValue4Byte)

The Target AS Value (4Byte) parameter specifies the four-byte AS number of the default VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to AS-4Byte. The range is 65 536 to 4 294 967 295. The default is 65 536.

Target AS Value (4Byte)

(vrfTargetASValue4Byte)

The Target AS Value (4Byte) parameter specifies the four-byte AS number of the default VRF target for the site. This parameter is configurable when the Target Format parameter is set to AS-4Byte. The range is 65 536 to 4 294 967 295. The default is 65 536.

Target Community Value

(vrfMVPNTargetCommunityValue)

The Target Community Value parameter specifies the BGP community value of the default VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to IP address. The range is 0 to 65 535. The default is 0.

Target Community Value

(vrfTargetCommunityValue)

The Target Community Value parameter specifies the BGP community value of the default VRF target for the site. This parameter is configurable when the Target Format parameter is set to IP address. The range is 0 to 65 535. The default is 0.

Target Extended Community Value

(vrfMVPNTargetExtendedCommunityValue)

The Target Extended Community Value parameter specifies the BGP community value of the default VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to AS. The range is 4 294 967 295. The default is 0.

Target Extended Community Value

(vrfTargetExtendedCommunityValue)

The Target Extended Community Value parameter specifies the BGP community value of the default VRF target for the site. This parameter is configurable when the Target Format parameter is set to AS. The range is 4 294 967 295. The default is 0.

Target Format

(vrfMVPNTargetFormat)

The Target Format parameter specifies the VRF target format to use for the MVPN site. This parameter is configurable when the VRF Target Type parameter is set to Define Default. Table 6-20 describes the parameter options.

Table 6-20 Target Format parameter for MVPN

Option	Option description
None (default)	—
AS	Specifies that you want to configure a two-byte AS number for the default target
IP Address	Specifies that you want to configure an IP address for the default target
AS-4Byte	Specifies that you want to configure a four-byte AS number for the default target
Unicast	Specifies that you want to configure a unicast address for the default target

Target Format

(vrfTargetFormat)

The Target Format parameter specifies the VRF target format to use. This parameter is configurable when the VRF Target Type parameter is set to Define Default. Table 6-21 describes the parameter options.

Table 6-21 Target Format parameter

Option	Option description
None (default)	—
AS	Specifies that you want to configure a two-byte AS number for the default target
IP Address	Specifies that you want to configure an IP address for the default target
AS-4Byte	Specifies that you want to configure a four-byte AS number for the default target

Target IP Address

(vrfMVPNTargetIpAddress)

The Target IP Address parameter specifies the IP address of the default VRF target for the MVPN site. This parameter is configurable when the Target Format parameter is set to IP Address. The default is 0.0.0.0.

Target IP Address

(vrfTargetIpAddress)

The Target IP Address parameter specifies the IP address of the default VRF target for the site. This parameter is configurable when the Target Format parameter is set to IP Address. The default is 0.0.0.0.

Transmit Interval

(bfdTxInterval)

The Transmit Interval parameter specifies the time in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Threshold (%)

Table 6-22 lists where to find information about the Threshold (%) parameter.

Table 6-22 Threshold (%) parameter

Parameter	See
Threshold (%) in Maximum Number of IPv6 Routes panel	Threshold (%) parameter in this section
Threshold (%) in Maximum Number of Multicast Routes panel	Threshold (%) parameter in this section
Threshold (%) in Maximum Number of Routes panel	Threshold (%) parameter in this section

Threshold (%)

(ipv6MaxNumRoutesThresHold)

The Threshold (%) parameter specifies the percentage of the value configured for the [Maximum Number Of IPv6 Routes](#) parameter at which the NE logs a warning message and sends an SNMP trap to the 5620 SAM, which generates an alarm. To configure the parameter, you must first deselect the Infinity check box beside the parameter. The range is 0 to 100. The default is 0, which specifies that the threshold is infinity and no associated threshold-crossing event is generated.

Threshold (%)

(midRouteMcastThreshold)

The Threshold (%) parameter specifies the percentage of the value configured for the [Maximum Number Of Multicast Routes](#) parameter at which the NE logs a warning message and sends an SNMP trap to the 5620 SAM, which generates an alarm. The range is 0 to 100. The default is 0, which specifies that the threshold is infinity and no associated threshold-crossing event is generated.

Threshold (%)

(midRouteThreshold)

The Threshold (%) parameter specifies the percentage of the value configured for the [Maximum Number Of Routes](#) parameter at which the NE logs a warning message and sends an SNMP trap to the 5620 SAM, which generates an alarm. The range is 0 to 100. The default is 0, which specifies that the threshold is infinity and no associated threshold-crossing event is generated.

Time Exceeded

See the [Time Exceeded](#) parameter in section [14.1](#).

Time Exceeded Time (seconds)

See the [Time Exceeded Time \(seconds\)](#) parameter in section [14.1](#).

Timeout (seconds)

See the [Timeout \(seconds\)](#) parameter in section [14.1](#).

Transport

(circuitTransport)

The Transport parameter specifies whether the VPRN sites are to be automatically bound to previously created service tunnels. Table [6-23](#) describes the parameter options.

Table 6-23 Transport parameter

Option	Option description
None (default)	Specifies that you want to manually configure service tunnels and circuits for the service
GRE	Specifies that you want the service to be automatically bound to GRE service tunnels
MPLS RSVP-LSP	Specifies that you want the service to be automatically bound to MPLS service tunnels utilizing RSVP-LSP. It provides the capability to include RSVP-TE based LSPs, in which the paths use static metrics by default. This option is available only on a 7710 SR or 7750 SR.
MPLS LDP	Specifies that you want the service to be automatically bound to MPLS service tunnels utilizing LDP
MPLS RSVP or LDP	Specifies that you want the service to be automatically bound to MPLS service tunnels utilizing either RSVP or LDP. 5620 SAM tries to resolve the VPN route by using RSVP-LSP tunnels first. If no RSVP-LSP service tunnels are available, then tunnels configured for LDP are used. If RSVP-LSP tunnels subsequently become available, then the route resolution automatically falls back to RSVP-LSP. This option is available only on a Release 7.0 R3 or later 7710 SR or 7750 SR.

Trusted

Table [6-24](#) lists where to find information about the Trusted parameter.

Table 6-24 Trusted parameter

Parameter	See
Trusted for L3 interface	Trusted parameter in section 14.1
Trusted for DHCP	Trusted parameter in section 14.1

TTL Expired

See the [TTL Expired](#) parameter in section 14.1.

TTL Expired Time (seconds)

See the [TTL Expired Time \(seconds\)](#) parameter in section 14.1.

Tunnel Auto-Selection Transport Preference

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Tunnel Fault Notification

See the [“Tunnel Fault Notification”](#) parameter in section 14.1.

Tunnel Transport

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Type

(type)

The Type parameter specifies the hop type for the static route. Table 6-25 describes the parameter options.

Table 6-25 Type parameter

Option	Option description
Next Hop (default)	Specifies the directly connected next-hop IP address used to reach the destination. This address must be associated with a network that is directly connected to a network configured on this node.
Indirect	The configured IP address is not directly connected to a network configured on this node. The destination can be reachable using multiple paths. The static route remains valid when the address configured as the indirect address is a valid entry in the routing table. Indirect static routes cannot use an IP prefix and mask to another indirect static route.
Black Hole	Specifies a black hole route. This means that if the destination address on a packet matches this static route, it is discarded without notification.

(1 of 2)

Option	Option description
Global Route Table	Specifies a route selected from the Global Route Table due to a lookup failure in the local VRF table. Note that not all of the properties typically associated with static routes are applicable to this type. When the Global Route Table type is selected, the non-applicable properties are hidden in the 5620 SAM GUI.

(2 of 2)

Type

(optionType)

The Type parameter specifies the format of the DHCP option that the DHCP server sends to the DHCP client. The options are:

- IP Address (default)
- ASCII String
- Hex String

Type

(vprnType)

The Type parameter specifies the type of VPRN instance being configured for a hub and spoke configuration. Table 6-26 describes the parameter options.

Table 6-26 Type parameter

Option	Option description
Regular (default)	Specifies a fully meshed VPRN.
Hub	Specifies a hub VPRN, which allows all traffic from the hub SAPs to be routed to the destination directly, while all traffic from spoke VPRNs or network interfaces can only be routed to a hub SAP.
Subscriber Split Horizon	Specifies a subscriber split horizon VPRN, which controls the flow of traffic for wholesale subscriber applications.

Type 0 Administrative Value

(type0AdministrativeValue)

The Type 0 Administrative Value parameter specifies the AS number for the RD. You can set the AS number to 0 when you use static routing or RIP between the PE and CE routers. The AS number can also be the AS of the PE router (base router instance). Alcatel-Lucent recommends that you do not use private AS numbers. This parameter is configurable when the Route Distinguisher Type parameter is set to Type 0. The range is 1 to 65 535. The default is 1.

Type 0 Assigned Value

(type0AssignedValue)

The Type 0 Assigned Value parameter specifies a 4 byte integer for the route distinguisher. This parameter is configurable when the Route Distinguisher Type parameter is set to Type 0. The range is 1 to 4 294 967 295. The default is 0.

Type 1 Assigned Value

(type1AssignedValue)

The Type 1 Assigned Value parameter specifies a 2 byte integer of the RD. This parameter is configurable when the Route Distinguisher Type parameter is set to Type 1. The range is 1 to 65 535. The default is 1.

Type 1 IP Address

(type1IpAddress)

The Type 1 IP Address parameter specifies the IP address of the RD. Alcatel-Lucent recommends that you do not use a private IP address. This parameter is configurable when the Route Distinguisher Type parameter is set to Type 1. The default is 0.0.0.0.

Type 2 Administrative Value

(type2AdministrativeValue)

The Type 2 Administrative Value parameter specifies the AS number for the RD. The AS number can also be the AS of the PE router (base router instance). Alcatel-Lucent recommends that you do not use private AS numbers. This parameter is configurable when the Route Distinguisher Type parameter is set to Type 2. The range is 65 535 to 4 294 967 295. The default is 65 535.

Type 2 Assigned Value

(type2AssignedValue)

The Type 2 Assigned Value parameter specifies a 4 byte integer for the route distinguisher. This parameter is configurable when the Route Distinguisher Type parameter is set to Type 2. The range is 0 to 65 535. The default is 0.

Unreachables

See the [Unreachables](#) parameter in section 14.1.

Unreachables Time (seconds)

See the [Unreachables Time \(seconds\)](#) parameter in section 14.1.

URPF Check Mode

See the [URPF Check Mode](#) parameter in section 14.1.

URPF Check State

See the [URPF Check State](#) parameter in section 14.1.

Use GI Address

(useGiAddress)

The Use GI Address parameter specifies whether a gateway IP address is used. When the value is set to true, the IP address is set based on an available gateway IP address. The address is offered even if authentication fails or there is no local user database configured. When the value is set to false, the IP address must be specified and included in the local database. The options are:

- True
- False (default)

Use Pool From Client

(usePoolFromClient)

The Use Pool From Client parameter specifies whether the DHCP server uses the pool name in vendor-specific DHCP-attributes. The options are:

- enabled
- disabled (default)

Use Shared Queue

See the [Use SAP ID as Subscriber ID](#) parameter in section 14.1.

Valid Life Time

See the [Valid Life Time](#) parameter in section 14.1.

Value

(optionValue)

The Value parameter specifies additional values for the DHCP option. For example Option 42 specifies the list of network time protocol servers available to the DHCP client. Option 12, the host name option, specifies the name of the DHCP client. All DHCP protocol options and values are defined in RFC 2131.

Version

(version)

The Version parameter specifies whether the OSPF routing instance uses OSPFv2 or OSPFv3. The options are:

- 2 (default)
- 3

VRF Target Type

(vrfTargetType)

The VRF Target Type parameter specifies how to configure the VRF target for the site. Table 6-27 describes the parameter options.

Table 6-27 VRF Target Type parameter

Option	Option description
None (default)	Specifies that you do not want to configure a VRF target for the site
Define Default	Specifies that you want to configure a default VRF target for the site
Define Import and Export	Specifies that you want to configure import and export VRF targets for the site

WAN Host

See the [WAN Host](#) parameter in section 14.1.

7 – *IES parameters*

7.1 IES parameters 7-2

7.1 IES parameters

This chapter describes the parameters on the IES creation forms.



Note — This chapter also describes parameters common to the Service Template form and child forms. Service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent does not recommend using the 5620 SAM-O XML classes and methods associated with service templates.

AAL5 Encapsulation

See the [AAL5 Encapsulation](#) parameter in section 14.1.

Administrative State

See the [Administrative State](#) parameter in section 14.1.

Administration Status

(adminStatus)

The Administration Status parameter specifies whether Bi-directional Forwarding Detection is enabled. This parameter must be configured before BFD parameters are accessible on router interfaces. The options are:

- Up
- Down (default)

Aggregate Rate Limit (Kbps)

See the [Aggregate Rate Limit \(kbps\)](#) parameter in section 14.1.

Aggregation

See the [Aggregation](#) parameter in section 14.1.

Allow Directed Broadcasts

See the [Allow Directed Broadcasts](#) parameter in section 14.1.

ANCP String

See the [ANCP String](#) parameter in section 14.1.

Anti-Spoof Mac Address

See the [Anti-Spoof MAC Address](#) parameter in section 14.1.

Application Profile

See the [Application Profile](#) parameter in section 14.1.

ARP Host Limit

See the [ARP Host Limit](#) parameter in section 14.1.

ATM OAM Alarm Cell Handling

See the [ATM OAM Alarm Cell Handling](#) parameter in section 14.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Autonomous Address Configuration

See the [Autonomous Address Configuration](#) parameter in section 14.1.

Auto Select Transport Tunnel

See the [Auto-Select Transport Tunnel](#) parameter in section 14.1.

Broadcast Address Format

See the [Broadcast Address Format](#) parameter in section 14.1.

Calling Station ID

See the [Calling Station ID](#) parameter in section 14.1.

CCM Messages Enabled

See the [CCM Messages Enabled](#) parameter in section 117.1.

Client Applications

See the [Client Applications](#) parameter in section 14.1.

Collect Accounting Statistics

See the [Collect Accounting Statistics](#) parameter in section 14.1.

Current Hop Limit

See the [Current Hop Limit](#) parameter in section 14.1.

Default Subscriber Identification String

See the [Default Subscriber Identification String](#) parameter in section 14.1.

Description

See the [Description](#) parameter in section 14.1.

Direction

See the [Direction](#) parameter in section 117.1.

Echo Interval

(bfdEchoInterval)

The Echo Interval parameter specifies the minimum echo receive interval, in ms, for the BFD session. The range is 100 to 100 000. The default is 100.

Egress Filter ID

See the [Egress Filter ID](#) parameter in section 14.1.

Egress Mark QinQ Top Bits Only

See the [Egress Mark QinQ Top Bits Only](#) parameter in section 14.1.

Egress Policy ID

See the [Egress Policy ID](#) parameter in section 14.1.

Egress Scheduler Name

See the [Egress Scheduler Name](#) parameter in section 14.1.

Enable DHCP Relay

See the [Enable DHCP Relay](#) parameter in section 14.1.

Enable DHCPv6 Relay

See the [Enable DHCPv6 Relay](#) parameter in section 14.1.

Enable Local Proxy

See the [Enable Local Proxy](#) parameter in section 14.1.

Enable Local Proxy ARP

See the [Enable Local Proxy ARP](#) parameter in section 14.1.

Enable Proxy ARP

See the [Remote Proxy ARP](#) parameter in section 14.1.

Fragment Interleave

See the [Fragment Interleave](#) parameter in section 14.1.

FRF-12 End-To-End Fragment Threshold

See the [FRF-12 End-To-End Fragment Threshold](#) parameter in section 14.1.

FRF-12 Mode

See the [FRF-12 Mode](#) parameter in section 14.1.

ID

See the [ID](#) parameter in section 14.1.

ID

See the [ID](#) parameter in section 116.1.

Ingress Filter ID

See the [Ingress Filter ID](#) parameter in section 14.1.

Ingress Match Q in Q Dot1P

([ingressMatchQinqDot1pBits](#))

The Ingress Match Q in Q Dot1P parameter specifies which set of 802.1p bits in a QinQ-encapsulated packet are used as the match criterion for a QoS or MAC filter policy. The parameter is configurable when the port encapsulation type is null, dot1q, or QinQ, but the parameter affects only QinQ packets. Table 7-1 describes the parameter options.

Table 7-1 Ingress Match Q in Q Dot1P parameter

Option	Option description
None (default)	Uses default 802.1P behavior
Bottom	Uses 802.1P prioritization bits in the inner VLAN tag
Top	Uses 802.1P prioritization bits in the outer VLAN tag

Ingress Policy ID

See the [Ingress Policy ID](#) parameter in section 14.1.

Ingress Scheduler Name

See the [Ingress Scheduler Name](#) parameter in section 14.1.

Inner Encapsulation Value

See the [Inner Encapsulation Value](#) parameter in section 14.1.

Inner Encapsulation Value

(VCI)

See the [Inner Encapsulation Value \(VCI\)](#) parameter in section 14.1.

Interface ID

See the [Interface ID](#) parameter in section 14.1.

Interface Id Option

See the [Interface Id Option](#) parameter in section 14.1.

Interface Id String

See the [Interface Id String](#) parameter in section 14.1.

IP Address

See the [IP Address](#) parameter in section 14.1.

IPv6 Allowed

See the [IPv6 Allowed](#) parameter in section 14.1.

IPv6 Delegated Prefix Length

See the [IPv6 Delegated Prefix Length](#) parameter in section 14.1.

IPv6 Prefix

See the [IPv6 Prefix](#) parameter in section 14.1.

L2 Header

See the [L2 Header](#) parameter in section 14.1.

Lease Populate

See the [Lease Populate](#) parameter in section 14.1.

Lifetime (seconds)

Table 7-2 lists where to find more information about the Lifetime (seconds) parameter.

Table 7-2 Lifetime (seconds) parameter

Parameter	See
Lifetime (seconds) for general router advertisement	Lifetime (seconds) parameter in section 14.1
Lifetime (seconds) to specify preferred routing prefix lifetime	Lifetime (seconds) parameter in section 14.1
Lifetime (seconds) to specify valid routing prefix lifetime	Lifetime (seconds) parameter in section 14.1

Link MTU**(linkMTU)**

See the [Link MTU](#) parameter in section 14.1.

LNS

See the [LNS](#) parameter in section 14.1.

Loopback Enabled

See the [Loopback Enabled](#) parameter in section 186.1.

Low-priority Defect

See the [Low-priority Defect](#) parameter in section 117.1.

MAC Address

See the [MAC Address](#) parameter in section 14.1.

MAC Monitoring

See the [MAC Monitoring](#) parameter in section 14.1.

Managed Address Config

See the [Managed Address Config](#) parameter in section 14.1.

Mask Reply

See the [Mask Reply](#) parameter in section 14.1.

Maximum Number of Leases

See the [Maximum Number of Leases](#) parameter in section 14.1.

Max Interval (seconds)

See the [Max Interval \(seconds\)](#) parameter in section 14.1.

Minimum Authentication Interval (minutes)

See the [Minimum Authentication Interval \(minutes\)](#) parameter in section 14.1.

Min Interval (seconds)

See the [Min Interval \(seconds\)](#) parameter in section 14.1.

Monitor Access Interface Operational State

See the [Monitor Access Interface Operational State](#) parameter in section 14.1.

Multiplier**(bfdMultiplier)**

The Multiplier parameter specifies the number of consecutive BFD messages that must be missed before the BFD session state is changed to the down state. OSPF, IS-IS and PIM are notified of the fault. The range is 3 to 20. The default is 3.

MTU

See the [MTU](#) parameter in section 14.1.

Name

See the [Name](#) parameter in section 14.1.

Neighbor Resolution

See the [Neighbor Resolution](#) parameter in section 14.1.

No Expiry

Table 7-3 lists where to find more information about the No Expiry parameter.

Table 7-3 No Expiry parameter

Parameter	See
No Expiry for preferred routing prefix lifetime	No Expiry parameter in section 14.1
No Expiry for valid routing prefix lifetime	No Expiry parameter in section 14.1

Number of Packet Too Big

See the [Number of Packet Too Big](#) parameter in section 14.1.

Number of Param Problem

See the [Number of Redirects](#) parameter in section 14.1.

Number of Redirects

See the [Number of Redirects](#) parameter in section 14.1.

Number of Time Exceeded

See the [Number of Time Exceeded](#) parameter in section 14.1.

Number of TTL Expired

See the [Number of TTL Expired](#) parameter in section 14.1.

Number of Unreachables

See the [Number of Unreachables](#) parameter in section 14.1.

On-Link Determination

See the [On-Link Determination](#) parameter in section 14.1.

Other Stateful Config

See the [Other Stateful Config](#) parameter in section 14.1.

Outer Encapsulation Value

See the [Outer Encapsulation Value](#) parameter in section 14.1.

Outer Encapsulation Value

(VPI)

See the [Outer Encapsulation Value \(VPI\)](#) parameter in section 14.1.

Packet Too Big

See the [Packet Too Big](#) parameter in section 14.1.

Packet Too Big Time (seconds)

See the [Packet Too Big Time \(seconds\)](#) parameter in section 14.1.

Param Problem

See the [Param Problem](#) parameter in section 14.1.

Param Problem Time (seconds)

See the [Param Problem Time \(seconds\)](#) parameter in section 14.1.

Periodic Atm Oam LoopBack

See the [Periodic ATM OAM Loopback](#) parameter in section 14.1.

Physical Address

See the [Physical Address](#) parameter in section 14.1.

Policy 1

See the [Policy 1](#) parameter in section 14.1.

Policy 2

See the [Policy 1](#) parameter in section 14.1.

Policy 3

See the [Policy 1](#) parameter in section 14.1.

Policy 4

See the [Policy 1](#) parameter in section 14.1.

Policy 5

See the [Policy 1](#) parameter in section 14.1.

Port

See the [Port](#) parameter in section 14.1.

Preferred Life Time

See the [Preferred Life Time](#) parameter in section 14.1.

Prefix Address

See the [Prefix Address](#) parameter in section 14.1.

Prefix DUID

See the [Prefix DUID](#) parameter in section 14.1.

Prefix Delegation

See the [Prefix Delegation](#) parameter in section 14.1.

Prefix IAID

See the [Prefix IAID](#) parameter in section 14.1.

Prefix Length

See the [Prefix Length](#) parameter in section 14.1.

Prefix Life Time (seconds)

See the [Prefix Life Time \(seconds\)](#) parameter in section 14.1.

Prefix Option

See the [Prefix Option](#) parameter in section 14.1.

Prefix Valid Life Time (seconds)

See the [Prefix Valid Life Time \(seconds\)](#) parameter in section 14.1.

Priority Level for CCM Messages

See the [Priority Level for CCM Messages](#) parameter in section 117.1.

Proxy Arp Policy 1

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy Arp Policy 2

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy Arp Policy 3

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy Arp Policy 4

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Proxy Arp Policy 5

See the [Proxy ARP Policy 1](#) parameter in section 14.1.

Reachable Time (milliseconds)

See the [Reachable Time \(milliseconds\)](#) parameter in section 14.1.

Rebind Timer

See the [Rebind Timer](#) parameter in section 14.1.

Receive Interval

(bfdRxInterval)

The Receive Interval parameter specifies the receive interval in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Redirects

See the [Redirects](#) parameter in section 14.1.

Redirects Time (seconds)

See the [Redirects Time \(seconds\)](#) parameter in section 14.1.

Renew Timer

See the [Renew Timer](#) parameter in section 14.1.

Retransmit Time

See the [Retransmit Time \(milliseconds\)](#) parameter in section 14.1.

Return Tunnel Transport

See the “[Return Tunnel Auto-Selection Transport Preference](#)” parameter in section 14.1.

Router Lifetime (seconds)

See the [Router Lifetime \(seconds\)](#) parameter in section 14.1.

SAP ARP Host Limit

See the [SAP ARP Host Limit](#) parameter in section 14.1.

Scheduling Class

See the [Scheduling Class](#) parameter in section 14.1.

Send Advertisement

See the [Send Advertisement](#) parameter in section 14.1.

Server 1

See the [Server 1](#) parameter in section 14.1.

Server 1

(server1IpAddress)

The Server 1 parameter specifies a DHCPv6 server for the interface. The DHCPv6 server stores network addresses and delivers configuration parameters to DHCP clients. Specify an IPv6 address in colon-hexadecimal format for the Server 1 parameter. The default is 0:0:0:0:0:0:0:0.

Server 2

See the [Server 1](#) parameter in section 14.1.

Server 2

See the [Server 1](#) in this section for more information.

Server 3

See the [Server 1](#) parameter in section 14.1.

Server 3

See the [Server 1](#) in this section for more information.

Server 4

See the [Server 1](#) parameter in section 14.1.

Server 4

See the [Server 1](#) parameter in this section for more information.

Server 5

See the [Server 1](#) parameter in section 14.1.

Server 5

See the [Server 1](#) parameter in this section for more information.

Server 6

See the [Server 1](#) parameter in section 14.1.

Server 6

See the [Server 1](#) parameter in this section for more information.

Server 7

See the [Server 1](#) parameter in section 14.1.

Server 7

See the [Server 1](#) parameter in this section for more information.

Server 8

See the [Server 1](#) parameter in section 14.1.

Server 8

See the [Server 1](#) parameter in this section for more information.

Service ID

See the [Service ID](#) parameter in section 14.1.

Service Name

See the [Service Name](#) parameter in section 14.1.

Service Priority

(svcPriority)

See the [Service Priority](#) parameter in section 14.1.

Service Tier

See the [Service Tier](#) parameter in section 14.1.

Session Limit

(ifSessionLimit)

The Session Limit parameter specifies the maximum number of PPPoE sessions allowed on the IES interface. The range is 1 to 8000. The default is 1.

Session Limit per SAP

(sapSessionLimit)

The Session Limit per SAP parameter specifies the maximum number of PPPoE sessions allowed on the IES SAP. The range is 1 to 8000. The default is 1.

Source IP Address

See the [Source IP Address](#) parameter in section 14.1.

Subscriber Identification

See the [Subscriber Identification](#) parameter in section 14.1.

SVC Mgr Service ID

(id)

See the [SVC Mgr Service ID](#) parameter in section 14.1.

Time Exceeded

See the [Time Exceeded](#) parameter in section 14.1.

Time Exceeded Time (seconds)

See the [Time Exceeded Time \(seconds\)](#) parameter in section 14.1.

Timeout

See the [Timeout \(seconds\)](#) parameter in section 14.1.

Transmit Interval

(bfdTxInterval)

The Transmit Interval parameter specifies the time in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Trusted

Table 7-4 lists where to find more information about the Trusted parameter.

Table 7-4 Trusted parameter

Parameter	See
Trusted for L3 interface	Trusted parameter in section 14.1
Trusted for DHCP	Trusted parameter in section 14.1

TTL Expired

See the [TTL Expired](#) parameter in section 14.1.

TTL Expired Time (seconds)

See the [TTL Expired Time \(seconds\)](#) parameter in section 14.1.

Tunnel Auto-Selection Transport Preference

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Tunnel Fault Notification

See the [“Tunnel Fault Notification”](#) parameter in section 14.1.

Tunnel Transport

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

Unreachables

See the [Unreachables](#) parameter in section 14.1.

Unreachables Time (seconds)

See the [Unreachables Time \(seconds\)](#) parameter in section 14.1.

URPF Check Mode

See the [URPF Check Mode](#) parameter in section 14.1.

URPF Check State

See the [URPF Check State](#) parameter in section 14.1.

Use Shared Queue

See the [Use SAP ID as Subscriber ID](#) parameter in section 14.1.

Valid Life Time

See the [Valid Life Time](#) parameter in section 14.1.

WAN Host

See the [WAN Host](#) parameter in section 14.1.

8 — *VLAN parameters*

8.1 VLAN parameters 8-2

8.1 VLAN parameters

This chapter describes the parameters on the VLAN service creation forms.



Note — This chapter also describes parameters common to the Service Template form and child forms. Service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent does not recommend using the 5620 SAM-O XML classes and methods associated with service templates.

Administrative State

See the [Administrative State](#) parameter in section 14.1.

Application

(vlanSubType)

The Application parameter specifies the VLAN type. Table 8-1 describes the parameter options.

Table 8-1 Application parameter

Option	Option description	Dependencies
unspecified (default)	You must choose a VLAN application.	—
Broadcast TV (MVR/IPMV)	Specifies that the VLAN is used for BTM (7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco) or IP multicast (OmniSwitch)	The VLAN ID for the SAP endpoints in the service used to carry the broadcast channels on the 7450 ESS must match the VLAN ID of the VLAN service.
L2-VPN (TLS/VLAN-Stacking)	Specifies that the VLAN is used for TLS (7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, and Telco) or stacked VLANs (OmniSwitch)	TLS must be configured for the ring group for the VLAN. Configure and apply to the Telco devices the appropriate QoS and ACL templates to specify the QoS delivered to subscribers.
Internet Access (Super-VLAN)	Specifies that the VLAN is used for Internet access	The 7450 ESS devices that connect to the ring group must have at least two IESs ready, one for internet traffic and one for DHCP relays on each Telco device. End customer devices must be assigned an IP address from the DHCP server.
Standard VLAN	Standard VLANs can be configured on 7250 SAS, 7250 SAS-ES, 7250 SAS-ESA, Telco, and OmniSwitch	You cannot configure a standard VLAN, however an existing standard VLAN on a Telco device, for example a management VLAN, can be resynchronized from the managed device.
Management VLAN	Specifies that the VLAN is to be used in conjunction with a ring group	The 7450 ESS must be part of a management VPLS used to relay SNMP and CLI messages to the Telco devices.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Customer VLAN ID

(custVlanID)

The Customer VLAN ID parameter associates a CVLAN service with a service access multipoint. The range is 0 to 4094. The default is 0.

Customer VLAN Tag

(custVlanTag)

The Customer VLAN Tag parameter specifies the mapping between an IP multicast VLAN and a customer VLAN ID. The range is 1 to 4094. The default is 0.

Description

See the [Description](#) parameter in section 14.1.

Enable 1x1 STP

(enable1x1Stp)

The Enable 1x1 STP parameter specifies whether the STP status for the VLAN applies when the switch is running in the 1x1 spanning tree mode. The options are:

- True (default)
- False

Enable Authentication

(enableAuthentication)

The Enable Authentication parameter specifies whether authentication is enabled for a VLAN. The options are:

- True
- False (default)

Enable Flat STP

(enableFlatStp)

The Enable Flat STP parameter whether the STP status for the VLAN applies when the switch is running in the flat spanning tree mode. The options are:

- True (default)
- False

Enable Mobile-Tag

(enableMobileTag)

The Enable Mobile-Tag parameter specifies whether classification of tagged packets received on mobile ports is enabled or disabled. If a mobile port receives a tagged packet with a VLAN ID that matches the specified VLAN ID, the port and packet are dynamically assigned to the VLAN. If the Enable Mobile-Tag parameter is set to False, when packets are tagged with a VLAN ID that does not match the mobile port default VLAN or a rule VLAN that the traffic qualifies for, the packet is dropped. The options are:

- True
- False (default)

Enable STP

(enableStp)

The Enable STP parameter specifies whether the STP for a VLAN is enabled or disabled. The options are:

- True (default)
- False

Ethernet Service Name

(ethernetServiceName)

The Ethernet Service Name parameter specifies a name for the Ethernet service. The range is 1 to 32 characters.

IP Address

(bindingIpAddress)

The IP Address parameter specifies the IP address that the DHCP server offered to the client. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Lease Time

(bindingLeaseTime)

The Lease Time parameter specifies the IP address lease time assigned by the DHCP server. The range is - 2 147 483 648 to 2 147 483 647. The default is 0.

MAC Address

(bindingMacAddress)

The MAC Address parameter specifies the MAC address of a client connected to a local untrusted port belonging to the VLAN. The default is 00-00-00-00-00-00.

Map Type

(cVlanMapType)

The Map Type parameter is applied to frames that are received on all SAP UNI ports of an Ethernet service. The parameter determines the type of customer traffic that is accepted on the UNI ports and processed by the service. Table 8-2 describes the parameter options.

Table 8-2 Map Type parameter

Option	Description
Single (default)	Applies the SAP profile to frames tagged with one CVLAN value; see Customer VLAN ID in this section for more information
All	Applies the SAP profile to tagged and untagged frames
Untagged Only	Applies the SAP profile only to untagged frames

Mode

See the [Mode](#) parameter in section 187.1.

Multicast Address

(address)

The Multicast Address parameter specifies an IPv4 multicast address for an IP multicast VLAN site. You can add the same multicast group address to several IP multicast VLANs as long as the VLANs do not share access interfaces. The default is 0.0.0.0.

Name

See the [Name](#) parameter in section 14.1.

Port

See the [Port](#) parameter in section 14.1.

Query Response Time (seconds)

See the [Query Response Time \(seconds\)](#) parameter in section 204.1.

Service ID

See the [Service ID](#) parameter in section 14.1.

Service Name

See the [Service Name](#) parameter in section 14.1.

Service Priority

(svcPriority)

See the [Service Priority](#) parameter in section 14.1.

Service Tier

See the [Service Tier](#) parameter in section 14.1.

Service Access Multi-Point ID

(sapId)

The Service Access Multi-Point ID parameter specifies a unique ID for the service. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 1024. The default is 0, which indicates that the parameter is not set.

Specify VLAN Path

(specifyVLANPath)

See the [Specify VLAN Path](#) parameter in section 14.1.

Subscriber Identification

See the [Subscriber Identification](#) parameter in section 14.1.

SVC Mgr Service ID

(id)

See the [SVC Mgr Service ID](#) parameter in section 14.1.

Type

(ipmVlanSubType)

This parameter specifies whether the IP multicast VLAN is associated with a stacking or Enterprise configuration, and is configurable only if the [Application](#) parameter value is set to Broadcast TV(MVR/IPMV). The options are:

- Stacking (default)
- Enterprise

VLAN ID

(vlanId)

The VLAN ID parameter specifies the VLAN ID of a 9500 VLAN service. The range is 2 to 4080. The default is 0.

VLAN Level MAC Address Verification

(**dhcpSnoopingVlanMacAddrVerificationStatus**)

The VLAN Level MAC Address Verification parameter specifies whether the source MAC address in DHCP packets received on ports belonging to a VLAN that has DHCP snooping enabled on it are compared to the client hardware MAC address. If the MAC addresses do not match, the DHCP packet is dropped. The options are:

- Disabled
- Enabled (default)

VLAN Level Option-82 Data Insertion

(**dhcpSnoopingVlanOpt82DataInsertionStatus**)

The VLAN Level Option-82 Data Insertion parameter specifies whether Option-82 information is inserted into DHCP packets received on ports belonging to a VLAN that has DHCP snooping enabled on it. The options are:

- Disabled
- Enabled (default)

VLAN Tagging

(**tagging**)

The VLAN Tagging parameter specifies the type of encapsulation allowed on a VLAN access port. The options are:

- Untagged (default)
- Tagged

The VLAN Tagging parameter should always be set to Tagged on CES interfaces.

See Table 17-4 parameter in section 17.17 for a description of tagged and untagged traffic behavior.

9 — *Mirror parameters*

9.1 Mirror parameters 9-2

9.1 Mirror parameters

This chapter describes the parameters on the Mirror service creation forms.



Note — This chapter also describes parameters common to the Service Template form and child forms. Service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent does not recommend using the 5620 SAM-O XML classes and methods associated with service templates.

Administrative State

See the [Administrative State](#) parameter in section 14.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Automatic SDP Binding Creation

See the [Automatic SDP Binding Creation](#) parameter in section 6.1.

Auto Select Transport Tunnel

See the [Auto-Select Transport Tunnel](#) parameter in section 14.1.

Description

See the [Description](#) parameter in section 14.1.

Destination MAC Address

(ipMirrorDestinationMacAddress)

The Destination MAC Address parameter specifies the MAC address to be used for the destination MAC Address field in the mirrored packets.

An error message is displayed if an attempt is made to set the value of this parameter to other than the default of 00-00-00-00-00-00, if the encapsulation type is not set to IP Only. When the encapsulation type is set to IP Only, all zeroes are not allowed.

Destination MAC Address

(destinationMacAddress)

The Destination MAC Address specifies the Destination MAC Address field of the ethernet encapsulation that is used for NAT subscribers associated with this mirror source. Specify a MAC address in colon-hexadecimal format. The default is the Base MAC address of the individual machine.

Disable Revert Time

(Infinite)

The Disable Revert Time parameter specifies whether you can configure the [Revert Time \(seconds\)](#) parameter. Select the check box to set the value to -1, which means that the [Revert Time \(seconds\)](#) parameter cannot be changed.

Egress Aggregate Rate Limit

See the [Aggregate Rate Limit \(kbps\)](#) parameter in section 14.1.

Egress Mark QinQ Top Bits Only

See the [Egress Mark QinQ Top Bits Only](#) parameter in section 14.1.

Enable Egress

(egressEnabled)

The Enable Egress parameter specifies whether to enable the mirroring of packets that egress the selected SAP or port. The options are:

- true (default)
- false

Enable Ingress

(ingressEnabled)

The Enable Ingress parameter specifies whether to enable the mirroring of packets that ingress the selected SAP or port. The options are:

- true (default)
- false

Enable Port ID Mirroring

(enablePortId)

The Enable Port ID Mirroring parameter indicates whether a port identifier is included in the mirrored packets. The parameter is only displayed and can only be set when the [Encapsulation Type](#) parameter on the mirror site is set to PPP. The options are:

- false (default)
- true

Encapsulation Type

(encapsulationType)

The Encapsulation Type parameter specifies the type of encapsulation configured on the mirror service site. The encapsulation type must be the same for all the mirror sites associated with a service. The options are:

- Ethernet (default)
- FrameRelay
- PPP
- ATM-SDU
- IP Only

EtherType

(etherType)

The EtherType parameter specifies the ethertype of the ethernet encapsulation used for NAT subscribers associated with this mirror source that have an intercept identifier. If a NAT subscriber's intercept identifier is unavailable, the value of the EtherType parameter is ignored. The range is 1536 to 65 535. The default is 1792.

Forwarding Class

(forwardingClass)

The Forwarding Class parameter specifies the forwarding class that the mirror service assigns to packets that it forwards to the mirror destination. A mirrored packet does not inherit the forwarding class of the original packet. The options are:

- | | |
|----------------|------|
| • be (default) | • h2 |
| • l2 | • ef |
| • af | • h1 |
| • l1 | • nc |

Forwarding Classes

(forwardingClass)

The Forwarding Classes parameter specifies the forwarding classes that are to be used as match criteria for the mirrored subscriber packets. There is no default. The options are:

- | | |
|------|------|
| • nc | • h1 |
| • ef | • h2 |
| • l1 | • af |
| • l2 | • be |

Host IP Address

(ipAddress)

The Host IP Address parameter specifies an IP address range for subscriber hosts on the SAP as a match criterion for the mirrored subscriber packets. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured and an IP address is not used as a match criterion for the subscriber traffic.

Host MAC Address

(macAddress)

The Host MAC Address parameter specifies a MAC address range for subscriber hosts on the SAP as a match criterion for the mirrored subscriber packets. The default is 00-00-00-00-00-00, which means that the parameter is not configured and a MAC address is not used as a match criterion for the subscriber traffic.

Ingress Label

(ingressLabel)

The Ingress Label parameter specifies the ingress service label. The parameter value identifies a remote source that is bound to the mirror-service destination. The parameter value is obtained manually or through signalling with the far-end device. A parameter value of 0 represents a T-LDP configuration; the label value is obtained from signaling using the LSP. The range is 2048 to 18 431. The default is 0, which means that the parameter is not configured.

You must ensure that the parameter value meets the following criteria:

- It is unique to the service.
- It is not in use by another label.
- It matches the expected egress value.

Intercept ID

(interceptId)

The Intercept ID parameter specifies the intercept identifier. The range is 0 to 4 294 967 295. The default is 0.

IP Address

(ipAddress)

The IP Address parameter specifies the IPv6 B4 address for DS Lite subscribers and the IPv4 inside address for Classic LSN subscribers. Specify an IPv4 address in dotted-decimal format, or, if IPv6 is enabled, an IPv6 address in colon-hexadecimal format. The default is 0.0.0.0.

Monitor Access Interface Operational State

See the [Monitor Access Interface Operational State](#) parameter in section 14.1.

Name

See the [Name](#) parameter in section 14.1.

Port

See the [Port](#) parameter in section 14.1.

Prefix Length

(prefixLength)

The Prefix Length parameter specifies the prefix length of the subscriber. The range is 1 to 128. The default is 32. For DS Lite LSN subscribers, entering any value other than 128 will produce an error.

Remote ICB

(remoteSourceICBackup)

The Remote ICB parameter specifies whether the source is an inter-chassis backup remote source. The options are:

- enabled
- disabled (default)

Remote Site ID

(remoteSourceSiteId)

The Remote Site ID parameter specifies the service IP address (system IP address) of the remote node sending mirrored traffic to the mirror destination service. A parameter value of 0.0.0.0 configures support for the mirror destination service to receive mirrored traffic from any remote 7750 SR. The default is 0.0.0.0.

Remote VC ID

(remoteSourceVCId)

The Remote VC ID parameter specifies the virtual circuit that is associated with the remote source. The range is 1 to 4294 967 295. The default is the value of the [Service ID](#) parameter.

Revert Time (seconds)

(revertTime)

The Revert Time (seconds) parameter specifies the amount of time to wait before trying to revert to the primary spoke SDP defined on the endpoint, after having failed over to a backup spoke SDP. The range is -1 to 600 s. The default is 0.

Routing Instance ID

(routerId)

The Routing Instance ID parameter specifies the ID of the router to be used. Specify an integer between 1 to 10 240 or click on the Select button to choose a router.

Service ID

See the [Service ID](#) parameter in section 14.1.

Service Name

See the [Service Name](#) parameter in section 14.1.

Service Priority

(svcPriority)

See the [Service Priority](#) parameter in section 14.1.

Service Tier

See the [Service Tier](#) parameter in section 14.1.

Slice Size

(sliceSize)

The Slice Size parameter specifies how much of the mirrored packet, in bytes, to send to the mirror destination. For example, when you specify a parameter value of 256, the first 256 bytes of a packet are sent to the mirror destination. The original packet is not affected. The range is 128 to 9216. The default is 0, which specifies that the entire packet is mirrored and no packet slicing occurs.

Source Administrative State

(sourceAdministrativeState)

The Source Administrative State parameter specifies whether mirror sources on the site are enabled. The options are:

- Up (default)
- Down

Source MAC Address

(ipMirrorSourceMacAddress)

The Source MAC Address parameter specifies the MAC address to be used for the source MAC Address field in the mirrored packets. This MAC address must not be a broadcast or multicast address.

When the [Encapsulation Type](#) parameter value is other than IP Only, an error message is displayed if an attempt is made to configure the parameter.

Source MAC Address

(sourceMacAddress)

The Source MAC Address parameter specifies the Source MAC Address field of the ethernet encapsulation that is used for NAT subscribers associated with this mirror source. Specify a MAC address in colon-hexadecimal format. The default is the Base MAC address of the individual machine.

Subscriber ID

(subscriberId)

The Subscriber ID parameter specifies a specific L2 Aware Residential Subscriber. The range is 1 to 32 characters. There is no default.

Subscriber Identification String

(subscriberIdent)

The Subscriber Identification String parameter specifies the subscriber identification string that identifies the subscriber for which to mirror traffic. If no other match criteria are specified, all of the host packets from all of the SAPs on the NE that belong to the subscriber are mirrored. The range is 1 to 32 characters. There is no default.

SVC Mgr Service ID

(id)

See the [SVC Mgr Service ID](#) parameter in section 14.1.

Tunnel Auto-Selection Transport Preference

See the [Tunnel Auto-Selection Transport Preference](#) parameter in section 14.1.

10 – Service From Template parameters

10.1 Service From Template parameters 10-2

10.1 Service From Template parameters

See chapters [4](#) to [14](#) for descriptions of the parameters on the Service Template and Create Service forms and child forms.

11 — IPsec VPN parameters

11.1 IPsec VPN parameters 11-2

11.1 IPsec VPN parameters

This chapter describes the parameters on the IPsec VPN form and child forms.

Authentication Key

Table 11-1 lists where to find more information about the Authentication Key parameter.

Table 11-1 Authentication Key parameter

Parameter	See
Inbound Authentication key for IPsec VPN	Authentication Key parameter in this section
Outbound Authentication key for IPsec VPN	Authentication Key parameter in this section

Authentication Key

(authenticationKeyInbound)

The Authentication Key parameter specifies the key that is used for the inbound authentication algorithm defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters.

Authentication Key

(authenticationKeyOutbound)

The Authentication Key parameter specifies the key that is used for the outbound authentication algorithm defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Auto Establish

(autoEstablish)

The Auto Establish parameter specifies whether there is an automatic attempt to establish a phase 1 exchange. The options are:

- Enabled
- Disabled (default)

Delivery Service Interface Address

The Delivery Service Interface Address parameter specifies the IPv4 address, in dotted-decimal format, of the delivery service interface. The subnet for the parameter must be the same subnet as the [Local Gateway Address](#) parameter.

Description

See the [Description](#) parameter in section 14.1.

Encryption Key

Table 11-2 lists where to find more information about the Encryption Key parameter.

Table 11-2 Encryption Key parameter

Parameter	See
Inbound encryption key for IPsec VPN	Encryption Key parameter in this section
Outbound encryption key for IPsec VPN	Encryption Key parameter in this section

Encryption Key

(`encryptionKeyInbound`)

The Encryption Key parameter specifies the key that is used for the inbound encryption algorithm that is defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters.

Encryption Key

(`encryptionKeyOutbound`)

The Encryption Key parameter specifies the key that is used for the outbound encryption algorithm that is defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters.

IPsec VPN Name

(`displayName`)

The IPsec VPN Name parameter specifies the name of the IPsec VPN. The range is 0 to 80 characters.

ISA-IPSEC Group

The ISA-IPSEC Group parameter specifies the ISA-IPSEC group for the IPSEC VPN.

Keying

(keying)

The Keying parameter specifies the keying type that the IPsec tunnel uses. The Keying parameter specifies whether the SA entry is created manually by the user or dynamically by the IPsec sub-system. The options are:

- None (default)
- Manual
- Dynamic

Keying Type

Table 11-2 lists where to find more information about the Keying Type parameter.

Table 11-3 Keying Type parameter

Parameter	See
Inbound keying type for IPsec VPN	Keying Type parameter in this section
Outbound keying type for IPsec VPN	Keying Type parameter in this section

Keying Type

(keyTypeOptionInbound)

The Keying Type parameter specifies the inbound key type. The options are:

- String (default)
- Hex

Keying Type

(keyTypeOptionOutbound)

The Keying Type parameter specifies the outbound key type. The options are:

- String (default)
- Hex

Link Corporate and Secured Service

(createCompositeService)

The Link Corporate and Secured Service parameter specifies whether corporate and secure services are associated with each other in the IPsec VPN. The options are:

- Enabled
- Disabled (default)

Local Gateway Address

The Local Gateway Address parameter specifies the IPv4 address, in dotted-decimal format, of the local NE of the IPsec tunnel. The subnet for the parameter must be the same subnet as the [Delivery Service Interface Address](#) parameter.

Pre Shared Key

(preSharedKey)

The Pre Shared Key parameter specifies the secret key that is shared by the two peers that form the IPsec tunnel. The range is 0 to 32 characters. There is no default.

Remote Gateway Address

The Remote Gateway Address parameter specifies the IPv4 address, in dotted-decimal format, of the remote gateway.

Replay Window

(replayWindow)

The Replay Window parameter specifies the size of the anti-replay window for the IPsec tunnel. The anti-replay window protocol secures IP against an entity that can inject messages in a message stream from a source to a destination computer on the Internet. If the value is set to 0, anti-replay is disabled. The options are:

- 0 (default)
- 32
- 64
- 128
- 256
- 512

Secure Service Interface Address

The Secure Service Interface Address parameter specifies the IPv4 address for the secure service interface. The parameter is mandatory when the [Tunnel Type](#) parameter is set to the Dynamic (Soft Client) option.

Service Type

(serviceType)

The Service Type parameter specifies the type of service for the IPsec VPN. The options are:

- Apipe
- Cpipe
- Epipe
- Fpipe
- IES
- VLAN
- VPLS
- VPRN (default)

SPI Inbound

(spiInbound)

The SPI Inbound parameter specifies the Security Parameter Index that is used to select the security association to verify and decrypt the incoming IPsec VPN. The Security Parameter Index is an identification tag that is added to the header. The range is 256 to 16 383. The default is 0.

SPI Outbound

(spiOutbound)

The SPI Outbound parameter specifies the Security Parameter Index that is used to select the security association to verify and decrypt the outgoing IPsec VPN. The Security Parameter Index is an identification tag that is added to the header. The range is 256 to 16 383. The default is 0.

Static Route Address

The Static Route Address parameter specifies the IPv4 address, in dotted-decimal format, of the static route.

Static Route Prefix

The Static Route Prefix parameter specifies the prefix for the static route. Table 11-4 describes the parameter options.

Table 11-4 Static Route Prefix parameter

Option	Option description
24	Choose when the Tunnel Type parameter is set to Dynamic (Site-to-Site) or Dynamic (Soft Client)
32	Choose when the Tunnel Type parameter is set to Static

Tunnel Type

The Tunnel Type parameter specifies the tunnel type for the IPsec group. The options are:

- Dynamic (Site-to-Site)
- Dynamic (Soft Client)
- Static

12 – Topology Group parameters

12.1 Topology Group parameters 12-2

12.1 Topology Group parameters

This chapter describes the parameters on the topology group creation form.

Background Image

(backgroundImage)

The Background Image parameter specifies a background map image for a topology group, for example, a map image of North America. You can position device icons and topology group icons in the map of the network to reflect their relative geographic locations.

The range is 0 to 254 characters, including the file extension; for example, n_america.gif. The default background image is defaultBackgroundImage.gif. The position of the background image defaults to the upper left corner of the map panel.

To view the list of example images provided by 5620 SAM, navigate to the background directory in the 5620 SAM client Installation directory; for example, /nms/images/map/background.

When adding your own map image to the directory, ensure that the file type is GIF and that the size is a maximum of 2000 × 2000 pixels.

Configuration Name

The Configuration Name parameter specifies the name of the global information table configuration.

Description

The Description parameter specifies a description for the filter. The range is 0 to 80 characters.

Description

See the [Description](#) parameter in section 14.1.

Filter Name

The Filter Name parameter specifies a unique name of the saved filter. You can use the saved filter for future searches. When a filter is applied, the name of the filter is displayed on the screen beside the filter button.

Group Name

See the [Name](#) parameter in section 14.1.

Public

The Public parameter specifies if a filter can be accessed by other users. When the value is enabled the filter is public. When the value is disabled the filter is private and cannot be accessed by other users. The options are:

- Enabled
- Disabled

Span

The Span parameter specifies whether span of control filtering is enabled. Table [12-1](#) describes the parameter options.

Table 12-1 Span parameter

Option	Description
Span Off (default, if span filtering is disabled on the User Preferences form)	Span of control filtering is disabled; objects in the View Access and Edit Access spans of the current user are displayed.
Span On (default, if span filtering is enabled on the User Preferences form)	Span of control filtering is enabled; only objects in the Edit Access spans of the current user are displayed.
User Preference	Span of control filtering is enabled or disabled, as configured on the User Preferences form.

13 – Physical Link parameters

13.1 Physical Link parameters 13-2

13.1 Physical Link parameters

This chapter describes the parameters on the physical link creation form.

Bandwidth (Mbps)

The Bandwidth parameter specifies the maximum bandwidth allowed for each specified CoS. The default value is derived from the speed of the physical port. Because there are eight classes of service, the default value for each CoS is the speed of the port divided by eight. The XML values are shown in Table 13-1.



Note — This parameter is only available if service CAC is configured. See the *5620 SAM User Guide* for more information.

Table 13-1 Bandwidth (Mbps) parameters

Bandwidth (Mbps) parameter name	XML string	Maximum bandwidth allowed for:
Bandwidth (Mbps) first field in column	cos0BW	CoS 0
Bandwidth (Mbps) second field in column	cos1BW	CoS 1
Bandwidth (Mbps) third field in column	cos2BW	CoS 2
Bandwidth (Mbps) fourth field in column	cos3BW	CoS 3
Bandwidth (Mbps) fifth field in column	cos4BW	CoS 4
Bandwidth (Mbps) sixth field in column	cos5BW	CoS 5
Bandwidth (Mbps) seventh field in column	cos6BW	CoS 6
Bandwidth (Mbps) eighth field in column	cos7BW	CoS 7

Bandwidth (%)

(endPtTotalBW)

The endpoint Bandwidth parameter specifies the total maximum allowed bandwidth for the port. By default, it is derived from the speed of the physical port. This value is not necessarily the sum of the CoS bandwidth parameters.



Note — This parameter is only available if service CAC is configured. See the *5620 SAM User Guide* for information.

Booking Factor (%)

The Booking Factor parameter specifies the actual amount of bandwidth being booked on the physical link. For example, if a service requests 10 Mbps on CoS 0 and the booking factor on CoS 0 is 50%, then the actual amount of booked bandwidth is 5Mbps. The XML values are shown in Table 13-2.



Note — This parameter is only available if service CAC is configured. See the *5620 SAM User Guide* for information.

Table 13-2 Booking Factor (%) parameters

Booking Factor (%) parameter name	XML string	Bandwidth being booked for:	Default value
Booking Factor (%) first field in column	cos0BookFactor	CoS 0	100
Booking Factor (%) second field in column	cos1BookFactor	CoS 1	100
Booking Factor (%) third field in column	cos2BookFactor	CoS 2	100
Booking Factor (%) fourth field in column	cos3BookFactor	CoS 3	100
Booking Factor (%) fifth field in column	cos4BookFactor	CoS 4	100
Booking Factor (%) sixth field in column	cos5BookFactor	CoS 5	100
Booking Factor (%) seventh field in column	cos6BookFactor	CoS 6	100
Booking Factor (%) eighth field in column	cos7BookFactor	CoS 7	100

Description

See the [Description](#) parameter in section 14.1.

Endpoint A Type

(endPointAType)

The Endpoint A Type parameter specifies the type of physical link for endpoint A. The options are:

- Port (default)
- Network Element
- Generic NE Interface

Endpoint B Type

(endPointBType)

The Endpoint B Type parameter specifies the type of physical link for endpoint B. The options are:

- Port (default)
- Network Element
- Unmanaged NE
- Generic NE Interface

The Unmanaged NE option specifies that the physical port at endpoint B of the link is not managed by the 5620 SAM.

Name

See the [Name](#) parameter in section 14.1.

Name

(cos#Name)

The Name parameter specifies a name for the CoS whose bandwidth parameters are defined for service CAC. The XML values are shown in Table 13-3.

Table 13-3 Name parameters

Name parameter name	XML string	Default value
Name first field in column	cos0Name	CoS0
Name second field in column	cos1Name	CoS1
Name third field in column	cos2Name	CoS2
Name fourth field in column	cos3Name	CoS3
Name fifth field in column	cos4Name	CoS4
Name sixth field in column	cos5Name	CoS5
Name seventh field in column	cos6Name	CoS6
Name eighth field in column	cos7Name	CoS7

Notes

(notes)

The Notes parameter specifies additional information about the physical link. The range is 0 to 254 characters.

Unmanaged - Description

(unmanagedEndpointBDescription)

The Unmanaged - Description parameter specifies a description for the physical port that is not managed by the 5620 SAM and is endpoint B of the link. The range is 0 to 64 characters.

Unmanaged - Management Address

(unmanagedEndpointBIPAddr)

The Unmanaged - Management Address parameter specifies the IP address for the location of the physical port that is not managed by the 5620 SAM and is endpoint B of the link. The default is 0.0.0.0.

Unmanaged - Name

(unmanagedEndpointB)

The Unmanaged - Name parameter specifies a name for the physical port that is not managed by the 5620 SAM and is endpoint B of the link. The range is 1 to 32 characters.

Used Bandwidth (Mbps)

(Mbps)

The Used Bandwidth parameter specifies the total amount of bandwidth per CoS currently being used on the links. When the used bandwidth value is reached, no additional bandwidth is accepted on the link. The XML values are shown in Table 13-4.



Note — This parameter is only available if service CAC is configured. See the *5620 SAM User Guide* for information.

Table 13-4 Used Bandwidth (Mbps) parameters

Used Bandwidth (Mbps) parameter name	XML string	Bandwidth currently being used for:
Used Bandwidth (Mbps) first field in column	cos0UsedBW	CoS 0
Used Bandwidth (Mbps) second field in column	cos1UsedBW	CoS 1
Used Bandwidth (Mbps) third field in column	cos2UsedBW	CoS 2
Used Bandwidth (Mbps) fourth field in column	cos3UsedBW	CoS 3
Used Bandwidth (Mbps) fifth field in column	cos4UsedBW	CoS 4
Used Bandwidth (Mbps) sixth field in column	cos5UsedBW	CoS 5
Used Bandwidth (Mbps) seventh field in column	cos6UsedBW	CoS 6
Used Bandwidth (Mbps) eighth field in column	cos7UsedBW	CoS 7

Used Bandwidth (Mbps)

(endPtTotalUsedBW)

The endpoint Used Bandwidth parameter specifies the total amount of bandwidth currently being used on the port. The total Endpoint Used Bandwidth value can exceed the Endpoint Bandwidth value.



Note — This parameter is only available if service CAC is configured. See the *5620 SAM User Guide* for information.

Utilization Threshold (%)

The Utilization Threshold parameter specifies the percentage of bandwidth that, when exceeded, raises an alarm indicating that the used bandwidth has exceeded the maximum allowed bandwidth on the link. For example, if the threshold is set to 75% and the maximum allowed bandwidth is 20 Mbps, then an alarm will be raised when the used bandwidth value exceeds 15 Mbps. The XML values are shown in Table 13-5.



Note — This parameter is only available if service CAC is configured. See the *5620 SAM User Guide* for information.

Table 13-5 Utilization Threshold (%) parameters

Utilization Threshold (%) parameter name	XML string	Bandwidth currently being used for:
Utilization Threshold (%) first field in column	cos0BWThreshold	CoS 0
Utilization Threshold (%) second field in column	cos1BWThreshold	CoS 1
Utilization Threshold (%) third field in column	cos2BWThreshold	CoS 2
Utilization Threshold (%) fourth field in column	cos3BWThreshold	CoS 3
Utilization Threshold (%) fifth field in column	cos4BWThreshold	CoS 4
Utilization Threshold (%) sixth field in column	cos5BWThreshold	CoS 5
Utilization Threshold (%) seventh field in column	cos6BWThreshold	CoS 6
Utilization Threshold (%) eighth field in column	cos7BWThreshold	CoS 7

Utilization Threshold (%)

(endPtBwUtilThreshold)

The endpoint Utilization Threshold parameter specifies the percentage of bandwidth that, when exceeded, raises an alarm indicating that the used bandwidth has exceeded the maximum allowed bandwidth on the port.



Note — This parameter is only available if service CAC is configured. See the *5620 SAM User Guide* for information.

14 – Common Create menu parameters

14.1 Common Create menu parameters 14-2

14.1 Common Create menu parameters

This chapter describes the parameters that are common to the 5620 SAM Create menu forms and child forms.

AAL5 Encapsulation

(atmAal5Encapsulation)

The AAL5 Encapsulation parameter specifies the type of AAL-5 data on the port. AAL-5 supports the conversion of VBR, delay-tolerant, connection-oriented traffic such as signaling and control data and network management data. This traffic requires minimal sequencing and minimal error detection support. Table 14-1 lists the parameter options.

Table 14-1 AAL5 Encapsulation parameter

Parameter	Options	Interfaces		Description
		L2	L3	
AAL5 Encapsulation	• AAL5 mux IP		✓	A routed IP encapsulation for VC multiplexed circuits as defined in RFC 2684. VC multiplexing creates a binding between an ATM VC and the type of network protocol carried on the VC. As a result, protocol identification is unnecessary in the payload of the AAL5 PDU.
	• AAL5 mux bridged ETH no FCS	✓	✓	An Ethernet bridged encapsulation without frame checksum that is used for bridging by the PVC.
	• AAL5 SNAP routed		✓	A routed IP encapsulation that identifies the protocol type of routed PDUs by prefixing an IEEE 802.2 LLC header to each PDU. In some cases, the LLC header must be followed by an IEEE 802.1a SNAP header.
	• AAL5 SNAP bridged	✓	✓	A bridged encapsulation that provides the necessary ARP capability to bind and maintain MAC addresses for the IP nodes on the remote LAN segment.

Action

(action)

The Action parameter specifies DHCP Option 82 processing on an interface. The parameter tells the DHCP relay agent what to do when it receives a DHCP request that already has an information option on the packet. Table 14-2 describes the parameter options.

Table 14-2 Action parameter

Option	Option description
Keep (default)	The existing information is kept on the packet and the device does not add any additional information. On egress, the information option is not removed and is sent to the downstream node. This setup is similar to not having configured DHCP relay at all. If the gateway IP address of the packet received is the same as the address on the device, the packet is dropped.
Drop	The packet is dropped.
Replace	On ingress, the existing information option is replaced with the information option from the device. On egress, the information option is removed.

Active State

(txActiveState)

The Active State parameter specifies an active or backup mode designation for redundant SDP bindings. The options are:

- Active (default)
- Backup

Address ID

(index)

The Address ID parameter specifies a numeric identifier for the IP address. The range is 1 to 16. The default is 1, which is reserved for the primary interface address.

The Address ID parameter can be configured for the 7705 SAR, but only the default value is allowed. The default is 1.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled.

The options are:

- Up (default)
- Down (default for IGMP snooping on a 7210 SAS-E, Release 1.0 R4 or later, or on a 7210 SAS-M, Release 1.1 R6 or later).

Admin Status

(adminStatus)

The AdminStatus parameter specifies whether residential subscriber management is enabled on the SAP. The options are:

- Enabled
- Disabled (default)

Aggregated Service Site Operational State

The Aggregated Service Site Operational State parameter cannot be configured. The value is derived from the operational states of the sites that are part of the service. The values are:

- Up—All sites are operationally up
- Partially Down—At least one site is operationally down
- Down—All sites are operationally down
- Unknown—The service has no provisioned sites

When the Aggregated Service Site Operational State is Partially Down or Down, a check mark appears beside the appropriate State Cause indicator to identify the type of fault to the 5620 SAM admin or mirror service management user. You can view alarms on the Faults page.

Aggregate Rate Limit (kbps)

Table 14-3 lists where to find information about the Aggregate Rate Limit (kbps) parameter.

Table 14-3 Aggregate Rate Limit parameter

Parameter Value	See
Aggregation rate limit for egress queues	Aggregate Rate Limit (kbps) parameter in this section
Aggregation rate limit for egress HSMDA queues	Aggregate Rate Limit (kbps) parameter in this section

Aggregate Rate Limit (kbps)

(egressAggRateLimit)

The Aggregate Rate Limit (kbps) parameter specifies, in kb/s, the maximum transmission rate of all egress queues for the access interface. You must select Assign Aggregate Rate Limit before you can configure the parameter. The range is –1, which means unlimited, or 1 to 100 000 000. When the parameter value is greater than zero, you cannot specify an egress scheduler.

Aggregate Rate Limit (kbps)

(hsmdaEgressAggRateLimit)

The Aggregate Rate Limit (kbps) parameter specifies the maximum total rate of all HSMDA egress queues for the access interface. You must select the Assign Aggregate Rate Limit check box before you configure the Aggregate Rate Limit (kbps) parameter. When the parameter is set to a value greater than 0, you cannot specify an egress scheduler. The range is 1 to 100 000 000. When you specify –1, the rate is unlimited.

Aggregation

(aggregation)

The Aggregation parameter specifies whether aggregation scheduling is used for the access interface. The options are:

- on
- off (default)

Allow Directed Broadcasts

(directedBroadcast)

The Allow Directed Broadcasts parameter specifies whether direct broadcast forwarding from the interface is permitted. The options are:

- Enabled
- Disabled (default)

ANCP String

(ancpKeyString)

The ANCP String parameter specifies the ASCII representation of the DSLAM circuit ID. This parameter is associated with an ANCP policy. The range is 1 to 63 characters. There is no default.

Anti-Spoofing

(antiSpoofing)

The Anti-Spoofing parameter specifies whether anti-spoof filtering is enabled and defines the type of anti-spoof filter to use. Anti-spoof filtering is an automatic filter mechanism that is used to improve network security. Anti-spoof filters guard the managed network against packets generated by an external network to falsely appear as originating from an internal device.

When anti-spoof filtering is enabled on a service SAP, the anti-spoof table is populated with all the static and dynamic host information available on the SAP. For the device to be able to forward the IP packets that enter the SAP, the packets must successfully match the entries in the anti-spoof table. Ingress packets that match an anti-spoof filter entry are forwarded by the system and may be subject to additional forwarding criteria. Ingress packets that do not match any entries in the table are discarded. Not all ingress packets are subject to anti-spoof filtering when it is enabled; for example, non-IP packets, such as DHCP and ARP requests and replies, are not subject to anti-spoofing filtering.

You can configure anti-spoofing for the following service objects:

- VPLS SAPs
- IES SAP-based IP interfaces
- VPRN SAP-based IP interfaces

There are three types of anti-spoof filters that the SAP can use to filter packets:

- source IP
- source MAC
- combination source IP and source MAC
- next hop IP and MAC address

For example, if you want only the incoming source MAC address to be verified, the SAP anti-spoof type must be set to Source MAC Address, which results in the MAC anti-spoof table being defined and maintained.

Table 14-4 describes the parameter options.

Table 14-4 Anti-Spoofing parameter

Option	Option description	Dependencies
disabled (default)	Disables anti-spoof filtering on the SAP	—
Source IP Address	Configures SAP anti-spoof filtering to use only the source IP address as a match criterion.	Each static host requires an IP address. The DHCP lease state table must be up and populated. This is the default option for a group interface SAP and cannot be changed.
Source Mac Address	Configures SAP anti-spoof filtering to use only the source MAC address as a match criterion.	Each static host requires a MAC address. The DHCP lease state table must be up and populated. The SAP must support Ethernet encapsulation.
Source IP and MAC Address	Configures SAP anti-spoof filtering to use both the source IP address and the source MAC address as match criteria.	Each static host requires an IP address and a MAC address. The DHCP lease state table must be up and populated. The SAP must support Ethernet encapsulation.

(1 of 2)

Option	Option description	Dependencies
Next Hop IP and MAC Address	Enables a SAP to accept SRRP advertisements when anti-spoofing is enabled for subscriber hosts on the SAP. Required for each SAP on a group IP interface that receives SRRP advertisements.	The option is available on VPRN and IES group-interface SAPs. Each static host requires an IP address and a MAC address. This option is supported on the 7710 SR, and only on the IOM 2 cards of the 7750 SR-7, and 7750 SR-12. If the group interface SAP is associated with a LAG, all ports in the LAG must reside on an IOM 2 card.

(2 of 2)

Anti-Spoof MAC Address

(antiSpoofMacAddr)

The Anti-Spoof MAC Address parameter specifies, with the [L2 Header](#) parameter, the MAC address that is used in anti-spoof configuration for the lease state on the interface. When the [L2 Header](#) parameter is set to False, the client hardware address stored in the DHCP server is used. When the [L2 Header](#) parameter is set to True and the value of the Anti-Spoof Mac Address parameter value is 0.0.0.0, the source MAC address in the Layer 2 header of the DHCP packet is used. When a valid MAC address is entered, the MAC address is used. The default is 00-00-00-00-00.

Application Profile

(aaApplicationProfile)

The Application Profile parameter specifies the application profile to be used by a SAP or spoke SDP. Click on the Select button to choose a profile from the list of Application profiles.

ARP Host Limit

(maxNumHosts)

The ARP Host Limit parameter specifies the maximum number of ARP hosts allowed on the interface. The range is 1 to 32 767. The default is 1.



Note — The default is 1 for L2 access interfaces, but 32 767 for VPRN retailer subscriber interfaces.

ARP Populate

(arpPopulate)

The ARP Populate parameter specifies whether IP addresses and MAC addresses of the static and dynamic hosts are placed in the ARP cache of the device. Both a MAC address and an IP address are required to populate an ARP entry. In the event that both a static host and a dynamic host share the same IP address and MAC address, the ARP cache retains the host information until both the static and dynamic host information is removed. The options are:

- disabled (default)
- enabled

When the ARP Populate parameter is enabled, the system does not send out ARP requests for hosts that are not in the ARP cache.

After you enable the ARP Populate parameter, you can configure only static hosts that have both an IP address and a MAC address.



Note — Do not enable the ARP Populate parameter for routed ATM interfaces.

ATM OAM Alarm Cell Handling

(atmOamAlarmCellHandling)

The ATM OAM Alarm Cell Handling parameter specifies whether OAM cells are used to provide ATM network maintenance functions, such as connectivity verification, alarm surveillance, continuity checking, and performance monitoring. The options are:

- Up (default)
- Down

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

When you create a VLAN with access ports on a 7250 SAS or Telco device, disable the parameter and use the [Service ID](#) parameter to configure the VLAN service ID that matches the VLAN ID that you want to use.

Autonomous Address Configuration

(autonomous)

The Autonomous Address Creation parameter specifies whether the routing prefix is used for stateless autoconfiguration. The options are:

- true (default)
- false

Auto Select Return Transport Tunnel

(autoSelectReturnTunnel)

The Auto Select Return Transport Tunnel parameter specifies the automatic selection of the transport encapsulation type for the return service tunnel by the 5620 SAM. The 5620 SAM automatically binds the return tunnel to a circuit. The options are:

- Enabled
- Disabled (default)

You must also define the [Return Tunnel Auto-Selection Transport Preference](#) parameter when you enable the Auto Select Return Transport Tunnel parameter.

Auto-Select Transport Tunnel

(autoSelectTunnel)

The Auto-Select Transport Tunnel parameter specifies the automatic selection of the transport encapsulation type for the service tunnel by the 5620 SAM. The 5620 SAM automatically binds the tunnel to a circuit. The options are:

- Enabled
- Disabled (default)

You must also define the [Return Tunnel Auto-Selection Transport Preference](#) parameter when you enable the Auto Select Transport Tunnel parameter.

Auto Select Tunnels

(autoSelectTunnel)

The Auto Select Tunnels parameter specifies whether the spoke connector is automatically bound to previously created service tunnels. The options are:

- Enabled (default)
- Disabled

BPDU Translation

(bpdTranslation)

The BPDU Translation parameter enables BPDU translation to PVST or STP or to a format that is automatically detected, based on the type of BPDU received on a specific SAP or spoke SDP binding. The options are:

- Auto
- Disabled (default)
- PVST
- STP
- PVST-RW
- Auto-RW

BPDU translation is supported only for Ethernet and ATM MDAs on the 7250 SAS, 7750 SR, and 7450 ESS.

Broadcast Address Format

(bcastAddrFormat)

The Broadcast Address Format parameter overrides the default broadcast address that is used when the IP interface acts as a source of IP broadcasts. Table 14-5 describes the parameter options.

Table 14-5 Broadcast Address Format parameter

Option	Option description	Notes
Host Ones (default)	Specifies that the broadcast address used by the IP interface for this IP address is the subnet broadcast address. This is an IP address that corresponds to the local subnet with all the host bits set to binary one.	—
All Ones	Specifies that the broadcast address used by the IP interface for this IP address is 255.255.255.255, (also called the local broadcast).	This option is not available for IES 7750 SR subscriber interfaces. If the option is configured on a device using CLI, the 5620 SAM displays no value for the parameter.

Calling Station ID

(callingStationId)

The Calling Station ID parameter specifies the calling station ID to be included in all RADIUS authentication and accounting requests. The range is 0 to 64 characters. There is no default. If no value is provided, no calling station ID is included.

Circuit ID

(circuitId)

The Circuit ID parameter specifies whether the Option 82 circuit ID suboption is included in the DHCP relay packet and what format the suboption takes. The circuit ID suboption contains information that uniquely identifies the device from which the packet was received. Table 14-6 describes the parameter options.

Table 14-6 Circuit ID parameter

Option	Option description
For L3 interfaces	
None	The suboption is left blank.
Ascii Tuple (default)	<p>Links the following information in a tuple to be sent:</p> <ul style="list-style-type: none"> • access node ID • service ID • interface name • SAP ID <p>The format of the tuple for VPRN, IES, or network interface is <i>system-name service-ID interface-name</i>. The format of the tuple for VPLS is <i>system-name service-ID SAP-ID</i>.</p>
Interface Index	<p>Called ifindex on the managed device, this option indicates the index for the IP interface in which the policy is applied.</p> <p>For VPRN, the option is unique only within the VRF. When DHCP relay is performed, the VRF ID is automatically added before the DHCP request is relayed to the DHCP server.</p>
SAP ID	This option indicates the SAP-id of the interface.
VLAN ASCII Tuple	Includes the VLAN-id and dot1p bits in addition to the default ASCII tuple information. The format is supported on Dot1 Q- and QinQ-encapsulated ports only.
Port ID	This option indicates the port ID of the interface.
Interface Name	This option indicates the name of the interface.
For L2 interfaces	
false (default) true	—
VLAN ASCII Tuple	Includes the VLAN-id and dot1p bits in addition to the default ASCII tuple information. The format is supported on Dot1 Q- and QinQ-encapsulated ports only.

When a device is not configured for DHCP relay, and if a VPLS SAP is configured for DHCP snooping, Option 82 information is added.



Note — The maximum DHCP relay packet size is 1500 bytes. If adding option 82 information to the packet causes the packet to exceed 1500 bytes, the DHCP relay request is forwarded without including the Option 82 information.

Class

(interfaceClass)

The Class parameter specifies whether the IP interface is a numbered or an unnumbered interface. Table 14-7 describes the parameter options:

Table 14-7 Class parameter

Option	Description	Dependencies
Numbered (default)	The interface is a numbered interface.	—
Unnumbered	This option is selectable only when the interface port encapsulation type is routed ATM, FR, or IPCP.	You must configure the Unnumbered Type parameter.

Client Applications

(clientApplications)

The Client Applications parameter specifies the client applications that can use the DHCP relay functionality. The options are:

- DHCP (default)
- PPPoE

Collect Accounting Statistics

(accountingOn)

The Collect Accounting Statistics parameter specifies whether the collection of accounting statistics on the interface is enabled. The options are:

- Enabled (default)
- Disabled

Composite ID

(compositeSvcId)

The Composite ID parameter specifies a unique ID for the composite service. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 2 147 483 647. The default is 0, which specifies that the parameter is not set.

Configured IP MTU (Octets)

(ipMtu)

The parameter specifies the maximum IP MTU size, in bytes, that the interface transmits. The range is 0, or 512 to 9000. A value of zero specifies that the value is set to the interface default, which is calculated by subtracting the DLC header size from the physical MTU size of the interface.

The Operational IP MTU value for the interface is displayed on the interface configuration form after interface creation. This value indicates the size of the largest IP MTU that this interface transmits. It is the lesser of the [Configured IP MTU \(Octets\)](#) value and the operational MTU value of the physical port to which the interface is bound.

Current Hop Limit

(currentHopLimit)

The Current Hop Limit parameter specifies the hop limit value that the interface includes in router advertisement messages. The interface informs the nodes on the subnet about the hop limit when it sends IPv6 packets. The range is 0 to 255. The default is 64. A value of zero means that the interface includes no hop limit value in a router advertisement message.

Customer VID

(svcCustomerVcId)

This parameter specifies the encapsulation value when the [SAP Type](#) is dot1q-preserve. This value must match the [Inner Encapsulation Value](#) of the [L2Uplink](#) SAP, and must match the [Outer Encapsulation Value](#) of the Dot1Q SAP.

Default Mesh VC ID

(defaultMeshVcId)

The Default Mesh VC ID parameter specifies the default virtual circuit identifier used for the mesh SDP bindings for the service. It inherits the value of the Service ID parameter by default. The Default Mesh VC ID parameter is configurable when the Inherit Value parameter is disabled. The range is 0 to 4 294 967 295. The default is 0, which specifies that the Default Mesh VC ID parameter is set to the same value as the Service ID parameter.

Default Primary DNS Server Address

(defaultPrimaryDnsIPv4Addr)

The Default Primary DNS Server Address parameter specifies the IPv4 address of the default primary DNS server for subscribers. Subscribers that cannot obtain an IPv4 DNS server address can use the default primary server address of 0.0.0.0 for DNS name resolution.

Default Secondary DNS Server Address

(defaultSecondaryDnsIPv4Addr)

The Default Secondary DNS Server Address parameter specifies the IPv4 address of the default secondary DNS server for subscribers. Subscribers that cannot obtain an IPv4 DNS server address can use the default secondary server address of 0.0.0.0 for DNS name resolution.

Default Subscriber Id

(defSubscriberIdString)

The Default Subscriber Id parameter specifies the default subscriber identification string for each host on the SAP. The parameter is configurable when the [Default Subscriber Identification Type](#) parameter is set to String. The range is 0 to 32 characters. There is no default.

Default Subscriber Identification String

(defaultSubIdentString)

The Default Subscriber Identification String parameter specifies the default subscriber identification string applicable on the subscribers of the LNS interface. The range is 0 to 32 characters. There is no default.

Default Subscriber Identification Type

(defSubscriberIdType)

The Default Subscriber Identification Type parameter specifies the type of information for the default subscriber identification string for hosts on the SAP. The default subscriber identification string is assigned to hosts that cannot be associated with a subscriber in any other way. Table 14-8 describes the parameter options.

Table 14-8 Default Subscriber Identification Type parameter

Option	Description	Dependencies
SAP ID	The SAP ID is used as the subscriber identification string.	—
String (default)	The Default Subscriber Id parameter value is used as the subscriber identification string.	You must configure the Default Subscriber Id parameter.
None	A default subscriber identifier is not assigned to hosts.	—

Default VC ID

(vcId)

The Default VC ID parameter specifies the virtual circuit identifier for a spoke SDP binding that originates from a 7250 SAS-ES. The parameter is configurable when the [Inherit Service ID Value](#) parameter is Disabled. The range is 0 to 4 294 967 295. The default is 0, which specifies that the Default VC ID parameter value is the same as the [Service ID](#) value.

Description

(description)

The Description parameter specifies a description for the created object. The range is 0 to 80 characters for all objects except topology groups, physical links, and discovered physical links.

For a topology group, the range is 0 to 252 characters. For a physical link or a discovered physical link, the range is 0 to 254 characters.

Displayed Name

(displayedName)

The Displayed Name parameter specifies the name for the created object. The range is 1 to 32.

Dynamic Topology Discovery

(dynamicTopDiscAdminState)

The Dynamic Topology Discovery parameter specifies whether the GSMP ANCP dynamic topology discovery capability is negotiated at the startup of the GSMP connection. The options are:

- Up (default)
- Down

Egress Filter ID

(egressFilterId)

The Egress Filter ID parameter specifies the egress filter to use for a circuit or interface. Click on the Select button to choose an egress ACL IP or ACL MAC filter.

Egress Label

(egressLabel)

The Egress Label parameter specifies an MPLS egress label for the SDP binding. A parameter value of 0 represents a T-LDP configuration. The range is 16 to 1 048 575. The default is 0.

You must ensure that the configuration of the Egress Label parameter meets the following configuration criteria:

- label must be unique to the service and not previously used
- label must match the ingress label value

See the [“Ingress Label”](#) parameter in section 9.1 for more information.

Egress Mark QinQ Top Bits Only

(egressQinqMarkTopBitsOnly)

The Egress Mark QinQ Top Bits Only parameter specifies which 802.1p bits to mark during packet egress when the port encapsulation type for the SAP is set to Q in Q. Table 14-9 describes the parameter options:

Table 14-9 Egress Mark QinQ Top Bits Only parameter

Option	Option description
disabled (default)	The top and bottom 802.1p bits in the Q in Q-encapsulated packet are marked.
enabled	The top 802.1p bits in the Q in Q-encapsulated packet are marked.

Egress Policy ID

(egressPolicyId)

The Egress Policy ID parameter specifies the egress policy to use for an L2 or L3 interface. Click on the Select button to choose an egress policy.

Egress Scheduler Name

(egressSchedulerName)

The Egress Schedule Name parameter specifies the egress scheduler to use for an L2 or L3 interface. Click on the Select button to choose an egress scheduler.

Emulated Server IP Address

(emulatedServerAddr)

The Emulated Server IP Address specifies the source address for the emulated DHCP server of the interface. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

The local proxy server is not operational unless you configure the Emulated Server IP Address parameter.

Enable

The Enable parameter specifies whether the [Lease Populate](#) parameter is configurable. The options are:

- Enabled
- Disabled (default)

Enable DHCP Relay

(administrativeState)

The Enable DHCP Relay parameter specifies the administrative state for DHCP relay. DHCP discover messages are broadcast packets that typically do not leave the IP subnet. DHCP relay agents are used to intercept the requests and forward them as unicast messages to a DHCP server. Table 14-10 lists the Enable DHCP Relay parameter options.

Table 14-10 Enable DHCP Relay parameter

Parameter	Options
Enable DHCP Relay for IES, VPRN, or network interface	<ul style="list-style-type: none">• Up (default)• Down
Enable DHCP Relay for VPLS	<ul style="list-style-type: none">• Enabled• Disabled (default)

Enable DHCPv6 Relay

(administrativeState)

The Enable DHCPv6 Relay parameter specifies the administrative state for DHCPv6 relay. DHCP discover messages are broadcast packets that typically do not leave the IP subnet. DHCP relay agents are used to intercept the requests and forward them as unicast messages to a DHCP server. The options are:

- Up (default)
- Down

Enable Egress Forwarding

(sapEgressStatsEnable)

The Enable Egress Forwarding parameter specifies whether or not to enable collection of the egress related statistics on the SAP. When the check box is enabled, egress accounting records like the service-egress-octets can be assigned to the SAP. The options are:

- enabled
- disabled (default)

This parameter is only applicable to the 7210 SAS-D-6F-4T (ETR).

Enable Ingress Forwarding

(sapIngressStatsEnable)

The Enable Ingress Forwarding parameter specifies whether or not to enable collection of the ingress related statistics on the SAP. When the check box is enabled, ingress accounting records like the service-ingress-octets can be assigned to the SAP. The options are:

- enabled
- disabled (default)

This parameter is only applicable to the 7210 SAS-D-6F-4T (ETR).

Enable Egress Packets Forwarding

(sapEgressStatsPktsMode)

The Enable Egress Packets Forwarding parameter specifies whether or not to enable a counter to monitor the traffic on the SAP. The total number of forwarded packets in the SAP egress queue are tallied. The options are:

- enabled
- disabled (default)

This parameter is only applicable to the 7210 SAS-E.

Enable Hash Label

(hashLabel)

The Enable Hash Label parameter specifies whether to enable an MPLS hash label. The MPLS hash label allows LSR nodes in a network to load balance labelled packets in a more granular fashion than allowed by simply hashing on the standard label stack. It removes the need to have an LSR inspect the payload below the label stack to check for an IPv4 or IPv6 header. Hash labels can only be enabled on an SDP binding if the underlying transport of the service tunnel is of MPLS type, and they must be enabled on both sides of the SDP binding for proper operation.

Hash labeling is supported for the following chassis types:

- 7750 SR-c4, 7750 SR-7, and 7750 SR-12 NEs in chassis mode B, C or D
- 7450 ESS NEs in chassis mode D
- 7710 SR-c4 and 7710 SR-c12

Chassis mode B is only supported for the hash label on the SDP binding.

Hash labeling is supported on VLL Epipes, Fpipes, and Ipipes, VPLS mesh and spoke SDPs, IES and VPRN L2 SDP spoke terminations.

When hash labelling is enabled on a VPRN site, it is included on packets forwarded on the following objects of the VPRN service:

- All RSVP or LDP LSPs to BGP next-hops when the service is configured in LDP, MPLS, or RSVP auto-bind modes
- All user-specified SDPs

Setting the Enable Hash Label parameter on the VPRN site does not control the use of the hash label on an interface terminated spoke-SDP binding. The hash label for this type of binding can be enabled individually on the spoke access interface.

Hash labeling is supported in the creation of PW templates. This requires chassis mode C or D.

The options are:

- Disabled (default)
- Enabled

Enable Local Proxy

(localProxy)

The Enable Local Proxy parameter specifies whether local proxy neighbor discovery can be used on the interface. Proxy neighbor discovery allows an interface, such as an L3 access interface, to respond to neighbor discovery queries that are intended for another interface. The options are:

- true
- false (default)

Enable Local Proxy ARP

(proxyArpLocal)

The Enable Local Proxy ARP parameter specifies whether local proxy ARP is in effect on the interface. The options are:

- true
- false (default)

Proxy ARP allows a device, such as a router, to answer ARP requests intended for another device. This allows a device reach a remote subnet without configuring routes to the subnet or a default gateway device.

Enable Secure SAPs

(enableSecureSaps)

The Enable Secure SAPs parameter specifies that all traffic entering a VPLS from a SAP is forwarded directly to the Spoke-SDP and is not propagated to the other SAP members of the VPLS. The options are:

- Disabled (default)
- Enabled

Enable Signal Capability

(hashLabelSignalCapability)

The Enable Signal Capability parameter specifies whether or not the Local PE should signal the hash label capability to the Remote PE. This parameter operates in conjunction with the [Enable Hash Label](#) parameter, and together, they determine if data traffic can be hashed between the two units. Alarms are raised if a mismatch in this capability is configured between the PEs.

The Enable Signal Capability parameter can only be enabled when the Enable Hash Label parameter is enabled.

Each row in Table 14-11 shows a possible configuration state of both parameters on the Local and Remote PEs and whether or not an alarm will be raised to indicate a mismatched configuration.

Table 14-11 Enable Signal Capability and Enable Hash Label configurations

Local PE parameter configuration		Remote PE parameter configuration		Hash Label alarm raised?	Signal Capability alarm raised?
Enable HL	Enable SC	Enable HL	Enable SC		
enabled	enabled	enabled	enabled	No	No
enabled	enabled	enabled	disabled	No	On Local PE
enabled	enabled	disabled	disabled	On Local PE	On Local PE
enabled	disabled	enabled	enabled	No	On Remote PE
enabled	disabled	enabled	disabled	No	No
enabled	disabled	disabled	disabled	On Local PE	No
disabled	disabled	enabled	enabled	On Remote PE	On Remote PE
disabled	disabled	enabled	disabled	On Remote PE	No
disabled	disabled	disabled	disabled	No	No

Only a VLL, VPLS, or VPRN service bound to an SDP of type MPLS (LDP or RSVP) support the Hash Label and Signal Capability parameters.

The Enable Signal Capability parameter is also supported in the creation of PW templates.

A configuration alarm (SignalCapabilityMismatch) operates in conjunction with the Enable Signal Capability parameter. This alarm is raised when an SDP binding hash label is enabled and the return SDP binding hash label is disabled. If this misconfiguration causes the mismatch of the operational hash label on both sides, the receiving site will drop the data packets as a result. This alarm is cleared when the hash label is either enabled or disabled on both sides.

The parameter options are:

- disabled (default)
- enabled

Enable PW Status Signaling (pwStatusSignaling)

The Enable PW Status Signaling parameter specifies whether or not PW Status Signalling is enabled. The options are:

- disabled
- enabled (default)

Encapsulation Tagging

(encapTagging)

The Encapsulation Tagging parameter specifies whether a 7250 SAS-ES VPLS SAP is tagged or untagged, which affects how traffic passes through the SAP. You can configure the Encapsulation Tagging parameter when the [VPLS Mode](#) parameter is set to Qualified. Table 17-4 describes the parameter options:

Table 14-12 Encapsulation Tagging parameter

Option	Description
Tagged	The SAP accepts only traffic that is encapsulated with the VPLS Tag parameter value.
Untagged	The SAP accepts untagged traffic, or traffic that is encapsulated with the VPLS Tag parameter value.

Ethernet Tunnel Endpoint Control SAP

(ethTunnelControlSap)

The Ethernet Tunnel Endpoint Control SAP parameter specifies if this is a Control SAP. It is only applicable for SAPs that have an Ethernet Tunnel Endpoint as the Terminating Port. If the parameter is enabled, then the value of the [Outer Encapsulation Value](#) parameter is automatically set to 8191. The options are:

- enabled
- disabled (default)

Expiry Time

(expiryTime)

The Expiry Time parameter specifies the time, in seconds, that the 5620 SAM tracks inactive hosts. The default is 260. The range is 1 to 65 535.

FlowSpec Validate Enabled

(flowSpecValidate)

The FlowSpec Validate Enabled parameter specifies whether received flow specifications are subject to validation. If the parameter is disabled, all received flow routes are considered valid. The parameter is enabled by default.

Forwarding Service ID

(fwdServiceId)

The Forwarding Service ID parameter specifies the ID of a forwarding service (i.e., a service other than the parent VPRN service) that contains a group interface that is intended for use with the current service. The default is 0.

If the parameter value is 0, group interfaces from the parent IES or VPRN service are listed. If the parent service is an IES, the parameter is set to 0 and cannot be edited.

If the parameter value is other than 0, group interfaces from the specified forwarding service ID are listed. The remote group interface must have IGMP enabled locally in order for the remote activation to function.

Fragment Interleave

(interleave)

The Fragment Interleave parameter specifies a mode of operation for the fragmentation of the FR SAP in the transmit direction. The parameter is configurable only in a VLL Epipe or Ipipe service. The options are:

- Enabled
- Disabled (default)

When the parameter is set to Enabled, only frames of the FR SAP non-expedited forwarding class queues are fragmented. The frames of the FR SAP expedited queues are interleaved among the fragmented frames with no fragmentation header.

Frame-Based Accounting

(egressFrameBaseAccounting)

The Frame-Based Accounting parameter specifies whether to use Frame-Based Accounting or packet-based accounting. Frame-Based Accounting uses inter-frame gap and instructions to calculate overhead. The options are:

- Enabled
- Disabled (default)

FRF-12 End-To-End Fragment Threshold

(frf12FragmentThreshold)

The Fragment Threshold parameter specifies the maximum length of a fragment transmitted across an FRF.12 link with UNI/NNI fragmentation enabled. The range is 128 to 512. The default is 128.

FRF-12 Mode

(frf12Mode)

The FRF-12 Mode parameter specifies whether a channel uses FRF.12 UNI/NNI fragmentation. The options are:

- Enabled
- Disabled (default)

Gateway IP Address

(gatewayIpAddress)

The Gateway IP Address parameter specifies the IP address that the CES module uses as a default gateway. The default is the [IP Address](#) value.

GSMP Administrative State

(gsmpAdministrativeState)

The GSMP Administrative State parameter specifies whether GSMP is enabled for the site. The options are:

- enabled
- disabled (default)

Hold Multiplier

(holdMultiplier)

The Hold Multiplier parameter specifies the GSMP hold multiplier value. The range is 1 to 100. The default is 3.

ID

Table [14-13](#) lists where to find more information about the ID parameter.

Table 14-13 ID parameter

Parameter	See
ID for generic object	ID parameter in this section
ID for subscriber	ID parameter in this section
ID for service tunnel	ID parameter in this section
ID for address rule	ID parameter in this section

ID

(id)

The ID parameter specifies a unique ID for the created object. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 65 535. The default is 0.

ID

(id)

The ID parameter specifies the unique ID for the address rule. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 10. The default is 0.

ID

(mepId)

The ID parameter specifies the ID of the remote MEP being tested. The range is 1-8191. The default is 0.

ID

(subscriberId)

The ID parameter specifies a unique ID for the subscriber. The range is 0 to 2 147 483 647. The default is 0.

ID

(pathId)

The ID parameter specifies a unique, automatically generated ID for the service tunnel. Click on the Select button to choose a service tunnel for the SDP binding.

Import Policy

(importPolicy)

The Import Policy parameter specifies the import policy to be used to filter IGMP packets. Click on the Select button to choose a policy from the list of import policies.

Ingress Counter Mode

(sapIngressCounterMode)

The Ingress Counter Mode parameter allows you to configure the mode of the counter used in service ingress statistics monitoring on a SAP. The options are:

- Packet (default)
- Octet

This parameter is only applicable to the 7210 SAS-E.

Ingress Filter ID

(`ingressFilterId`)

The Ingress Filter ID parameter specifies an ACL IP or ACL MAC ingress filter to use for a circuit, L2, or L3 interface. Click on the Select button to choose an ingress filter.

Ingress Label

(`ingressLabel`)

The Ingress Label parameter specifies an MPLS ingress label for the SDP binding. The range is 0 to 131 071. The default is 0.

Ingress Match QinQ Dot1P

(`ingressMatchQinqDot1pBits`)

The Ingress Match QinQ Dot1P parameter specifies which set of IEEE 802.1p bits in a QinQ-encapsulated packet are used to match a QoS or MAC filter policy. The parameter is configurable when the port encapsulation is null, dot1q, or QinQ, but affects only QinQ-encapsulated packets. Table 14-14 describes the parameter options.

Table 14-14 Ingress Match QinQ Dot1P parameter

Option	Option description
None (default)	Uses default 802.1p behavior
Top	Uses 802.1p prioritization bits in the outer VLAN tag
Bottom	Uses 802.1p prioritization bits in the inner VLAN tag

Ingress Policy ID

(`ingressPolicyId`)

The Ingress Policy ID parameter specifies the ingress policy to use for an L2 or L3 interface. Click on the Select button to choose an ingress policy.

Ingress Scheduler Name

(`ingressSchedulerName`)

The Ingress Schedule Name parameter specifies the ingress scheduler to use for an L2 or L3 interface. Click on the Select button to choose an ingress scheduler.

Inherit Service ID Value

The Inherit Service ID Value parameter specifies whether the [Default VC ID](#) value for a VPLS on a 7250 SAS-ESA service site is the same as the [Service ID](#) value. The options are:

- Enabled (default)
- Disabled

Inherit Service ID Value

(inheritanceMask)

The Inherit Service ID Value parameter specifies whether the default virtual circuit identifier used for the mesh SDP bindings is the same as the Service ID parameter value for the service. If enabled, the Inherit Service ID Value parameter specifies that the Default Mesh VC ID parameter is set to the value of the Service ID parameter. The options are:

- Enabled (default)
- Disabled

Inner Encapsulation Value

(innerEncapValue)

The Inner Encapsulation Value parameter specifies the inner encapsulation value for the port. This parameter is configurable when the Encap Type parameter value for the port is Q in Q. The range is 0 to 4094, or 4095 to indicate *. The default is 0. A value of 4095 is equivalent to * using CLI, which indicates that all tags are accepted, regardless of value. You can also use an asterisk (*). A value of 0 indicates that the port has no tag.

Inner Encapsulation Value (VCI)

(vci)

The Inner Encapsulation Value (VCI) parameter specifies the inner encapsulation value for the port. The parameter is equivalent to the VCI of the PVC connection on the port. The range is 1 to 65 535. The default is 0.

Inter-Chassis Backup

(isIcb)

The Inter-Chassis Backup parameter specifies whether the endpoint is enabled for ICB. The options are:

- enabled
- disabled (default)

Interface ID

(id)

The Interface ID parameter specifies a unique ID for the interface. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 5119. The default is 0.

Interface Id Option

(relayItfIdOption)

The Interface ID Option parameter specifies the interface ID option that is encoded in the DHCPv6 relay packet. Table 14-15 describes the options.

Table 14-15 Interface ID Option parameter

Option	Description	Dependencies
None	Disables the sending of interface ID options in the DHCPv6 relay packet	—
Interface Index	Called ifindex on the managed device, this option indicates the index for the IP interface in which the policy is applied.	—
ASCII Tuple	Links the following information in a tuple to be sent: <ul style="list-style-type: none"> access node ID service ID interface name SAP ID <p>The format of the tuple for IES is <i>system-name service-ID interface-name</i>.</p>	—
SAP-ID	This option indicates the SAP-id of the interface.	—
String	Specifies an alpha-numeric string that is included in the DHCPv6 relay packet	0 to 32 characters

Interface Id String

(dhcp6ItfIdString)

The Interface Id String parameter specifies the alpha-numeric string that is included in the DHCPv6 relay packet. The parameter is configurable when the [Interface Id Option](#) parameter is set to String. The range is 0 to 32 characters.

Interface Name

(unnumberedInterfaceName)

The Interface Name parameter specifies a unique name for the interface. The parameter is configurable when the [Unnumbered Type](#) parameter is set to Name. The range is 0 to 32 characters. There is no default.

Interface Type

(sapOrBinding)

The Interface Type parameter specifies the type of object that the MEP is associated with. The options are:

- SAP (default)
- SdpBinding
- Ethernet Tunnel Path Endpoint
- Ethernet Ring Path Endpoint
- Network Interface
- Port
- LAG

Intermediate Destination ID

(intermediateDestId)

The Intermediate Destination ID parameter specifies the identifier of an intermediate node, such as a DSLAM, between the SAP and the static host. The range is 0 to 32 characters. There is no default.

Interworking Type

(interworking)

The Interworking Type parameter specifies the type of interworking function that is applied to packets that ingress or egress the SAPs that are part of the VLL service. The options are:

- None
- FR-ATM Network Interworking (Frf-5)

IP Address

Table 14-16 lists where to find more information about the IP Address parameter.

Table 14-16 IP Address parameter

Parameter	See
IP Address for DHCP network gateway	IP address parameter in this section
IP Address for static subscriber host	IP Address parameter in this section
IP Address for neighbor or numbered L3 interface	IP Address parameter in this section
IP Address for destination node of static route	IP Address parameter in this section
IP Address for GSMP neighbor	IP Address in this section

(1 of 2)

Parameter	See
IP Address for unnumbered L3 interface	IP Address in this section

(2 of 2)

IP address

(giIpAddress)

The IP address parameter specifies the IP address of the network gateway that DHCP relay uses. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

IP Address

(ipAddr)

The IP Address parameter specifies the IP address of a static subscriber host. The IP Address parameter must be configured when the Anti-Spoofing parameter is enabled with the Source Ip Addr or the Source Ip And Mac Addr option, or the ARP Reply Agent parameter is enabled. Only one static host with a specified IP address can be configured on the SAP. Defining a static host with the same IP address as a previous static host overwrites the previous static host. The default is 0.0.0.0.

IP Address

(ipAddress)

The IP Address parameter specifies the IP address for an IES or VPRN neighbor, or for a numbered L3 interface. Specify an IP address in dotted-decimal format for IPv4, or in colon-hexadecimal format for IPv6. There is no default.

IP Address

(targetIpAddress)

The IP Address parameter specifies the IP address for the destination node of a static route. The parameter is configurable when the [Type](#) parameter is set to Next Hop or Indirect. Specify an IPv4 address in dotted-decimal format, or, if IPv6 is enabled, an IPv6 address in colon-hexadecimal format. The default is 0.0.0.0, which means that the parameter is not configured.

IP Address

(ipAddress)

The IP Address parameter specifies an IP address for the GSMP neighbor in dotted-decimal format for an IPv4 address, or in colon-hexadecimal format for an IPv6 address. The default is 0.0.0.0.

IP Address

(unnumberedIpAddress)

The IP Address parameter specifies an IP address for the unnumbered L3 interface in dotted-decimal format. The parameter is configurable when the [Unnumbered Type](#) parameter is set to IP Address. The default is 0.0.0.0.

IPv6 Allowed

(ipv6Allowed)

The IPv6 Allowed parameter specifies whether an IPv6 addressing scheme is valid for the interface. The options are:

- enabled
- disabled (default)

IPv6 Delegated Prefix Length

(delegatedPrefixLength)

The IPv6 Delegated Prefix Length parameter specifies the number of bits that can be allocated to a delegated prefix for IPv6. The range is 48 to 64. The default is 64.

IPv6 Prefix

(prefix)

The IPv6 Prefix parameter specifies the IP prefix for router advertisement messages. The range is 0 to 128. The default is 32.

Keep-Alive (seconds)

(keepAlive)

The Keep-Alive (seconds) parameter specifies the GSMP keep alive timer value. The range is 1 to 25. The default is 10.

L2 Header

(l2header)

The L2 Header and [Anti-Spoof MAC Address](#) parameters specify which MAC address is used in the anti-spoofing configuration for the lease state on the interface. If the parameter value is set to False, the client hardware address stored in the DHCP server is used. When the parameter value is set to True, and the [Anti-Spoof MAC Address](#) is set to 0.0.0.0, the source MAC address in the Layer 2 header of the DHCP packet is used. The options are:

- True
- False (default)

L2 Protocol Termination

(l2ptTermination)

The L2 Protocol Termination parameter enables L2 protocol termination on a specific SAP or spoke SDP binding. L2 protocol termination is only supported for STP BDPUs. All other PDUs are discarded. The options are:

- Enabled
- Disabled (default)

L2 protocol termination is only supported by Ethernet and ATM MDAs on the 7250 SAS, 7750 SR, and 7450 ESS.

L2Uplink

(isl2UplinkMode)

The L2Uplink parameter specifies whether a port or LAG is configured in access uplink mode. Access uplink ports and LAGs behave like network ports and LAGs on the 7210 SAS nodes, 7750 SR, 7450 ESS, and 7710 SR routers. When a port or LAG is configured in access uplink mode, the encapsulation is set to Q-in-Q and cannot be changed. All members of an access uplink LAG must be access uplink ports. The options are:

- Disabled (default)
- Enabled

LAG link selection

(macDestAddrHashing)

The LAG link selection parameter specifies whether subscriber traffic that egresses a LAG SAP chooses an egress LAG link using a function of the MAC destination address or the subscriber ID. The parameter is configurable when the underlying port for the SAP is a LAG. The options are:

- Subscriber ID (default)
- MAC dest addr

Lease Populate

(leasePopulate)

The Lease Populate parameter specifies the number of DHCP lease state entries that are allowed for the IES or VPRN SAP. Enabling the parameter also enables DHCP snooping. The range is 0 to 8000. There is no default. Setting the parameter to 0 specifies that dynamic host lease state management for the interface is disabled and disables the [Enable](#) parameter.

DHCP snooping on the SAP obtains the lease state information for a host from a DHCP ACK message that is sent by a DHCP server to the host. Entries in the DHCP lease state table remain valid for the duration of the IP address lease.

You cannot configure the Lease Populate parameter if the [Use ARP](#) parameter is configured.

Lease Time

(leaseTime)

The Lease Time parameter specifies whether the DHCP client can use an IP address. When you set the parameter to disabled, the local proxy server uses the lease time information provided by a RADIUS server or upstream DHCP server. The options are:

- Disabled (default)
- Specified Time Period

When you set the Lease Time parameter to Specified Time Period, you can specify how long the DHCP client can use an IP address by configuring the following parameters:

- [Number of Days](#)
- [Number of Hours](#)
- [Number of Minutes](#)
- [Number of Seconds](#)

Lease Time RADIUS Override

(proxyLTRadiusOverride)

The Lease Time RADIUS Override parameter specifies whether the DHCP client uses the proxy server lease time information provided by the RADIUS server. The options are:

- false (default)
- true

Lifetime (seconds)

(defaultLifetime)

The Lifetime (seconds) parameter specifies the router lifetime in seconds. The range is 0 or 4 to 9000. The default is 1800. A value of zero means that the router is not to be a default router.

Lifetime (seconds)

(preferredLifetime)

The Lifetime (seconds) parameter specifies the length of time, in seconds, that a router advertisement prefix remains preferred. The parameter is configurable when the [No Expiry](#) parameter is disabled. The range is 0 to 4 294 967 295. The default is 604 800. The 4 294 967 295 value represents infinity.

A preferred lifetime must not be longer than a valid lifetime. See the “[Lifetime \(seconds\)](#)” in this section for more information.

Lifetime (seconds)

(validLifetime)

The Lifetime (seconds) parameter specifies the length of time, in seconds, that a router advertisement prefix remains valid. The parameter is configurable when the [No Expiry](#) parameter is disabled. The range is 0 to 4 294 967 295. The default is 2 592 000. The 4 294 967 295 value represents infinity.

A valid lifetime must be longer than a preferred lifetime. See the “[Lifetime \(seconds\)](#)” in this section for more information.

Link MTU

(linkMTU)

The Link MTU parameter specifies the value to be placed in link MTU options sent by the node on an interface. The range is 1280 to 9212. The default is 0. A value of 0 means that the interface sends no MTU option information in router advertisements.

LNS

(lns)

The LNS parameter specifies the type of group interface. The parameter can only be set at creation. The options are:

- false (default)
- true

Local Address

(localAddress)

The Local Address parameter specifies the source IP address that is defined in the GSMP group. This parameter is connected to the neighbor that is configured for each group.

Loopback Enabled

See the “[Loopback Enabled](#)” parameter in section [186.1](#).

MAC Address

Table [14-17](#) lists where to find more information about the MAC Address parameter.

Table 14-17 MAC Address parameter

Parameter	See
MAC Address for static subscriber host	MAC Address parameter in this section
MAC Address for IP interface	MAC Address parameter in this section

MAC Address

(macAddr)

The MAC Address parameter specifies the MAC address of a static subscriber host. The MAC Address parameter must be configured when the Anti-Spoofing parameter is enabled with either the Source Mac Addr or the Source Ip And Mac Addr option, or the ARP Reply Agent parameter is enabled. Multiple static hosts can be configured with the same MAC address when each definition is distinguished by a unique IP address. Defining a static host with the same MAC address as but a different IP address from that of an existing host creates a new static host. The default is 00-00-00-00-00-00.

MAC Address

(macAddress)

The MAC Address parameter specifies the unicast MAC address. The default is 00-00-00-00-00-00.

MAC Address

(macNameAddress)

The MAC Address parameter specifies the IEEE MAC address for the PBB MAC name. The default is 00-00-00-00-00-00.

MAC Address

(physicalAddress)

The MAC Address parameter specifies a 48-bit MAC address for the object in the unicast MAC address format. Only one MAC address can be assigned to an IP interface. The default is 00-00-00-00-00-00.

MAC Monitoring

(macMonitoring)

The MAC Monitoring parameter specifies whether the packet rate limit in the NE DoS protection policy is in effect. The parameter is configurable on multiple-slot 7450 ESS and 7750 SR NEs. Table [14-18](#) describes the parameter options.

Table 14-18 MAC Monitoring parameter

Option	Description
disabled (default)	The interface ignores the packet rate limit specified in the NE DoS protection policy.
enabled	The interface applies the packet rate limit specified in the NE DoS protection policy.

MAC Name

(macName)

The MAC Name parameter specifies an ASCII name for the PBB MAC name.

MAC Notification Count

(macNotifCount)

The MAC Notification Count parameter specifies how many MAC notification messages are sent. The range is 1 to 10. The default is 3.

MAC Notification Interval (seconds)

(macNotifInterval)

The MAC Notification (seconds) parameter specifies how often the MAC notification messages are sent.

Managed Address Config

(managedAddrConfigFlag)

The Managed Address Config parameter sets the managed address configuration flag. This flag indicates that DHCPv6 is available for address configuration in addition to any address that has been automatically configured using stateless address autoconfiguration. The options are:

- false (default)
- true

Mask Reply

(maskReply)

The Mask Reply parameter specifies whether responses to ICMP mask requests are enabled on the interface. The options are:

- Enabled (default)
- Disabled

Match Circuit ID

(matchCircuitId)

The Match Circuit ID parameter specifies whether DHCP relay uses the information in the Option 82 circuit ID field to identify a host. The options are:

- false (default)
- true

Maximum Number of Leases

(maxLeaseStates)

The Maximum Number of Leases parameter specifies the maximum number of DHCPv6 lease state entries that are installed by the DHCPv6 server on the IES interface. The range is 0 to 8000. The default is 8000.

Max Interval (seconds)

(maxInterval)

The Max Interval (seconds) parameter specifies the maximum interval, in seconds, between router advertisement messages sent on the interface. The range is 4 to 1800. The default is 600.

Max Number of Groups

(maxNumberGroup)

The Max Number of Groups parameter specifies the maximum number of multicast groups to be tracked. The default is 0, which means that there is no limit on the number of tracked multicast groups. The range is 1 to 1 000.

Max Number of Sources per Group

(maxNumberSources)

The Max Number of Sources per Group parameter specifies the maximum number of sources per multicast group to be tracked. The default is 0, which means that there is no limit on the number of tracked multicast sources. The range is 1 to 1 000.

MC Ring Node

(ringNodeName)

The MC Ring Node parameter specifies the unique name of an access node in an MC ring. The range is 32 characters. You can type in the name, or click on the Select button to choose a ring node. There is no default.

Min Interval (seconds)

(minInterval)

The Min Interval (seconds) parameter specifies, in seconds, the minimum interval between router advertisement messages sent on the interface. The range is 3 to 1350. The default is 200.

Minimum Authentication Interval (minutes)

(minAuthInterval)

The Minimum Authentication Interval (minutes) parameter specifies the minimum interval between two consecutive authentication attempts for the same ARP host. The range is 1 to 6000. The default is 15.

Monitor Access Interface Operational State

(monitorAccessInterfaceOper)

The Monitor Access Interface Operational State parameter specifies whether the service operational flags are affected by the operational state of the service SAPs. Alcatel-Lucent recommends enabling this parameter for VPLS and VPRN services, and disabling this parameter for services with a large number of SAPs, such as BTV multicast configurations.

MTU

(mtu)

The MTU parameter specifies the MTU size, in bytes, for nodes on the link. The range is 0 to 9212. The default is 1280. A value of zero means that the interface sends no MTU option information in router advertisements.

MTU

(mtuValue)

The MTU parameter specifies the MTU size, in bytes, for a configured service site. The range is 0 to 9194. The default is 1514. The default is 1508 for the VLL Apipe service. The default is 1500 for the VLL Fpipe and Ipipe services.

MTU Check

(isMtuCheck)

The MTU Check parameter specifies whether or not to pass on packets to the egress based on the packet length MTU configured for the port. When the parameter is enabled, the system will pass on packets that are less than or equal to the configured MTU. In other words, the length of the packet sent out of a SAP is limited by the access port MTU and the length of the packet sent out of a PW is limited by the network port MTU (minus the MPLS encapsulation). When the parameter is not enabled, the configured service MTU value is not enforced.

The options are:

- disabled
- enabled (default)

Name

Table 14-19 lists where to find more information about the Name parameter.

Table 14-19 Name parameter

Parameter	See
Name for generic object	Name parameter in this section
Name for subscriber	Name parameter in this section

Name

([displayedName](#))

The Name parameter specifies a name for the object. The range depends on the type of object being configured. Table 14-20 lists the Name parameter ranges for different objects.

Table 14-20 Name parameter

Object	Range (characters)
Site	0 to 32 or 0 to 64
L2 access interface or SAP on IES group interface	0 to 40
L3 access interface	1 to 32
Composite service and related objects	1 to 32
Topology group	1 to 25
Service template	1 to 255
Physical link	1 to 32
Discovered Physical link	1 to 32
IP mirror interface (must begin with an alphabetic character)	1 to 32
Mirror service endpoint	1 to 32

Additional notes when using the Name parameter at the service site level:



Note 1 – On 7710 SR, 7750 SR, and 7750 SR-c12 NEs at releases earlier than 8.0, services that are created using a CLI are assigned a Service ID. You can optionally configure a service name on Release 8.0 or later NEs of these types.

Note 2 – If you configure a site on a Release 8.0 or later NE using a CLI and specify a service name, the 5620 SAM does not subsequently overwrite the name or supply a default name, as in Release 7.0.

Note 3 – If the Name parameter is configured on a service site, then it is linked to the Service Name property on the associated NE. There are a number of CLI commands on these platforms that accept the Service Name as a service identifier in place of the Service ID. If a naming conflict arises from NEs at earlier release versions, then the upgrade script you run will append an underscore character to the beginning of the name.

Note 4 – If the Name field is created in 5620 SAM but is left blank, then 5620 SAM generates a default name that is sent to the device. (Service sites created by CLI do not get a default name).

Note 5 – The following are the restrictions for the Name parameter:

- The maximum number of characters is 64.
- The name must not begin with a number or an underscore character; special characters are valid anywhere in the name except as the first character.
- The name must be unique among the 5620 SAM services.

Name

(subscriberName)

The Name parameter specifies a name for the subscriber. The range is 1 to 32 characters. Click on the Select button to choose a subscriber.

Neighbor Resolution

(ngbrResolution)

The Neighbor Resolution parameter specifies whether neighbor resolution is enabled through the DHCPv6 relay. The options are:

- true
- false (default)

No Egress Aggregate Rate Limit

The No Egress Aggregate Rate Limit parameter specifies that the transmission rate of all egress queues for the access interface is unlimited. The options are:

- Enabled (default)
- Disabled

No Expiry

(preferredLifetimeNoExpiry)

The No Expiry parameter sets the preferred lifetime of a router advertisement prefix to infinity, which is represented by the 4 294 967 295 value. The options are:

- enabled
- disabled (default)

See the “[Lifetime \(seconds\)](#)” in this section for more information.

No Expiry

(validLifetimeNoExpiry)

The No Expiry parameter sets the valid lifetime of a router advertisement prefix to infinity, which is represented by the 4 294 967 295 value. The options are:

- enabled
- disabled (default)

See the “[Lifetime \(seconds\)](#)” in this section for more information.

Non-Subscriber Traffic Identification

(nonSubTrafficIdent)

The Non-Subscriber Traffic Identification parameter specifies a string that identifies a host packet as originating from a non-subscriber host. The string can have 0 to 32 characters. There is no default.

Number of Days

(leaseTimeDays)

The Number of Days parameter specifies the number of days that a leased proxy IP address is valid. The range is 0 to 3650. The default is 0.

The parameter is configurable only when the [Lease Time](#) parameter is set to Specified Time Period.

Number of Hours

(leaseTimeHours)

The Number of Hours parameter specifies the number of hours that a leased proxy IP address is valid. The range is 0 to 23. The default is 0.

The parameter is configurable only when the [Lease Time](#) parameter is set to Specified Time Period.

Number of Minutes

(leaseTimeMinutes)

The Number of Minutes parameter specifies the number of minutes that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

The parameter is configurable only when the [Lease Time](#) parameter is set to Specified Time Period.

Number of Packet Too Big

(numberOfPacketTooBig)

The Number of Packet Too Big parameter specifies the number of ICMP Packet Too Big messages that the interface issues in the interval specified by the [Packet Too Big Time \(seconds\)](#) parameter. The parameter is configurable when the [Packet Too Big](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Param Problem

(numberOfParamProblem)

The Number of Param Problem parameter specifies the number of ICMP Param Problem messages that the interface issues in the interval specified by the [Param Problem Time \(seconds\)](#) parameter. The parameter is configurable when the [Param Problem](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Redirects

(numberOfRedirects)

The Number of Redirects parameter specifies the maximum number of ICMP Redirect messages that the interface issues in the time specified by the [Redirects Time \(seconds\)](#) parameter. The parameter is configurable when the [Redirects](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Seconds

(leaseTimeSeconds)

The Number of Seconds parameter specifies the number of seconds that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

The parameter is configurable only when the [Lease Time](#) parameter is set to Specified Time Period.

Number of Time Exceeded

(numberOfTimeExceeded)

The Number of Time Exceeded parameter specifies the number of ICMP Time Exceeded messages that the interface issues in the interval specified by the [Time Exceeded Time \(seconds\)](#) parameter. The parameter is configurable when the [Time Exceeded](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of TTL Expired

(numberOfTtlExpired)

The Number of TTL Expired parameter specifies the maximum number of ICMP TTL Expired messages that the interface can issue in the time specified by the [TTL Expired Time \(seconds\)](#) parameter. The parameter is configurable when the [TTL Expired](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Unreachables

(numberOfUnreachables)

The Number of Unreachables parameter specifies the maximum number of ICMP Unreachable messages that the interface can issue in the time specified by the [Unreachables Time \(seconds\)](#) parameter. The parameter is configurable when the [Unreachables](#) parameter is enabled. The range is 10 to 1000. The default is 100.

OAM Administrative State

(oamAdminState)

The OAM Administrative State parameter specifies whether the GSMP ANCP OAM capability is negotiated at the startup of the GSMP connection. The options are:

- Up
- Down (default)

OLC State

(olcState)

The OLC State parameter specifies whether an object or service is in-service or maintenance to filter alarms in the Alarms Window. Alarms are generated for objects and services regardless of the OLC State parameter setting. The parameter setting is not sent to the objects or services.

You can set the OLC state for the following objects and services:

- network element
- card slot
- daughter card
- port
- composite service
- service
- site
- LAG
- SAPs (L2 access interfaces and L3 access interfaces)

See the chapter 26 of the *5620 SAM User Guide* for information about the OLC.

Table 14-21 describes the options.

Table 14-21 OLC State parameter

Option	Option description	Default
Maintenance	For objects and services that are in maintenance	The default is Maintenance for services. The default value for objects can be specified in the discovery rules.
In Service	For objects and services that are in service	The default is In Service for objects. The default value for services can be specified using the nms-server.xml file.

On-Link Determination

(onLink)

The On-Link Determination parameter specifies whether the routing prefix is used for on-link determination. The options are:

- true (default)
- false

Operational State UP While Empty

(operationalStateWhileEmpty)

The Operational State UP While Empty parameter specifies whether the operational status of the group interface is up when there are no SAPs on the group interface.

- true
- false (default)

Other Stateful Config

(otherStatefulConfigFlag)

The Other Stateful Config parameter specifies whether DHCPv6lite is available for the autoconfiguration of other non-address information, such as DNS parameters or information about other servers in the network. The options are:

- false (default)
- true

Outer Encapsulation Value

(outerEncapValue)

The Outer Encapsulation Value parameter specifies the outer encapsulation value for the port. This parameter is configurable when the port encapsulation is dot1q, QinQ, BCP dot 1q, or FR. Table 14-22 lists the ranges for different encapsulation types. The default is 0.

Table 14-22 Outer Encapsulation Value parameter

Encapsulation type	Range	Range description
dot1q	0 to 4094, 8191	8191 indicates an Ethernet Tunnel Endpoint Control SAP
QinQ	0 to 4094	—
Q1.Q2	0 to 4094	—
BCP dot1q	0 to 4094	—
FR	16 to 1022	—
Default SAP	4095 or *	<ul style="list-style-type: none">• Ethernet ports only• Dot1Q ports• VPLS and Epipe VLL• Null encapsulated port cannot exist on the same port as a default SAP

Outer Encapsulation Value (VPI)

(vpi)

The Outer Encapsulation Value (VPI) parameter specifies the outer encapsulation value for the port. The parameter is equivalent to the VPI of the PVC connection on the port. When the ATM Interface Cell Format parameter is set to UNI, the range is 0 to 255. When the ATM Interface Cell Format parameter is set to NNI, the range is 0 to 4095. The default is 0.

Packet Too Big

(packetTooBig)

The Packet Too Big parameter specifies whether the rate at which the interface issues ICMP Packet Too Big messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Packet Too Big](#) and [Packet Too Big Time \(seconds\)](#) parameters.

Packet Too Big Time (seconds)

(packetTooBigTime)

The Packet Too Big Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Packet Too Big messages specified by the [Number of Packet Too Big](#) parameter. The parameter is configurable when the [Packet Too Big](#) parameter is enabled. The range is 1 to 60. The default is 10.

Param Problem

(paramProblem)

The Param Problem parameter specifies whether the rate at which the interface issues ICMP Packet Too Big messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Param Problem](#) and [Param Problem Time \(seconds\)](#) parameters.

Param Problem Time (seconds)

(paramProblemTime)

The Param Problem Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Packet Too Big messages specified by the [Number of Param Problem](#) parameter. The parameter is configurable when the [Param Problem](#) parameter is enabled. The range is 1 to 60. The default is 10.

Path ID

(sdpBindingPathId)

The Path ID parameter specifies an SDP binding identifier. Click on the Select button to choose an SDP binding.

PBB Source Backbone MAC Address

(pbbSrcBVplsMacAddr)

The PBB Source Backbone MAC Address parameter specifies the chassis-level BMAC address. The default is 00-00-00-00-00-00.

Peer Address

(peerAddress)

The Peer Address parameter specifies the IP address that is exchanged by IPCP to configure the IP address of the remote peer. The default is 0.0.0.0.

Periodic ATM OAM Loopback

(periodicAtmOamLoopBack)

The Periodic ATM OAM Loopback parameter specifies whether ATM OAM loopback is enabled on the current L3 access interface using ATM port encapsulation. ATM OAM loopback is configured globally on the 7750 SR. The options are:

- Disabled (default)
- Enabled

Per Service Hashing for LAG Enabled

(perServiceHashing)

The Per Service Hashing for LAG Enabled parameter specifies service-level hashing for Ethernet services on the 7750 SR-7, 7750 SR-12, 7450 ESS-6v, 7450 ESS-7 and 7450 ESS-12.

You can configure this parameter only in chassis mode D.

The options are:

- Disabled (default)
- Enabled

Physical Address

(physicalAddress)

The Physical Address parameter specifies the physical address in MAC address format. The default is 00-00-00-00-00-00.

PIM Snooping Enabled

(pimSnpgEnabled)

The PIM Snooping Enabled parameter specifies whether PIM snooping is enabled for this site of the VPLS service. The options are:

- Disabled (default)
- Enabled

Policy ID

(transitIpPolicyPointer)

The Policy ID parameter specifies the AA transit IP policy that is to be associated with the L3 access interface.

Policy 1

(policy1)

The Policy 1 to Policy 5 parameters specify the names of routing policies used to determine the interfaces that respond to neighbor discovery queries intended for other interfaces. When you specify multiple policies, the policies are evaluated in the order in which they are specified. The routing instance applies the first policy that matches. Use the Select button beside the parameter to choose a policy.

Policy 2

(policy2)

See the [“Policy 1”](#) in this section.

Policy 3

(policy3)

See the [“Policy 1”](#) in this section.

Policy 4

(policy4)

See the [“Policy 1”](#) in this section.

Policy 5

(policy5)

See the [“Policy 1”](#) in this section.

Port

(portId)

The Port parameter specifies the port or channel to use on the source or destination node of an L2 or L3 interface. Click on the Select button to choose an access port or channel.

Precedence

(endpointPrecedence)

The Precedence parameter specifies the precedence of the SDP binding when there are multiple bindings attached to one service endpoint. The range is 0 to 4. You can set the parameter to 0 for only one SDP binding, which makes that SDP binding the primary. If an SDP binding goes down, the SDP binding with the next highest precedence starts forwarding traffic.

Preferred Life Time

(preferredLifeTime)

The Preferred Life Time parameter specifies (in seconds) the preferred lifetime for an IPv6 prefix or address in an option. When the preferred lifetime expires, any derived addresses are deprecated. The range is 300 to 4 294 967 295. The default is 3600. A value of 4 294 967 295 represents an infinite preferred lifetime.

The preferred lifetime should not be longer than a valid lifetime. See [Valid Life Time](#) in this section for more information.

Prefix Address

(pfxdPrefix)

The Prefix Address parameter specifies the IPv6 address that is delegated by the router to a requesting DHCP client. Specify an IPv6 address in colon-hexadecimal format.

Prefix Delegation

(pd)

The Prefix Delegation parameter specifies whether a subscriber prefix is used by IPv6 ESM hosts for DHCPv6 prefix delegation. The default is True.

Prefix DUID

(pfxdDUID)

The Prefix DUID parameter specifies the DHCP Unique Identifier of the requesting DHCP client. If you set this parameter to a non-zero value, the prefix that is defined is delegated only to this DHCP client. If you set this parameter to zero, the prefix is delegated to any requesting DHCP client. The range is 0 to 64 characters.

Prefix IAID

(pfxIAID)

The Prefix IAID parameter specifies the Identity Association Identification (IAID) from the requesting DHCP client that must be matched on this DHCP client to delegate the prefix defined for the entry. If the Prefix IAID is set to 0, no matching on the received IAID is performed. The range is 0 to 4 294 967 295 characters. The default is 0.

The Prefix IAID parameter is configurable only when the [Prefix DUID](#) parameter is configured.

Prefix Length

(pfxdPrefixLen)

The Prefix Length parameter, along with the [Prefix Address](#) parameter, specifies the prefix of the IPv6 address that is delegated by the router to a requesting DHCP client. The range is 0 to 128. The default is 0.

Prefix Length

(prefixLength)

When combined with an IP address value, the Prefix Length parameter specifies a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. The prefix must not overlap with other existing IP prefixes that are defined as local subnets on other IP interfaces in the same routing context within the device or service. The range is 1 to 32 for an IPv4 address and 1 to 128 for an IPv6 address. A value of 32 is typically reserved for an IPv4 system address, but is available for general use in IPv6. The IPv4 default is 24; the IPv6 default is 64.

Prefix Life Time (seconds)

(pfxdPrefLifetime)

The Prefix Life Time (seconds) parameter specifies the time that the prefix is a preferred prefix. The range is 0 to 4 294 967 295. The default is 604 800.

Prefix Option

(pfxdAdminState)

The Prefix Option parameter specifies the administrative state of the prefix delegation options for delegating a long-lived prefix from a delegating DHCP client to a requesting DHCP client, where the delegating DHCP client does not require knowledge about the topology of the links in the network to which the prefixes are assigned. The options are:

- Enabled (default)
- Disabled

Prefix Valid Life Time (seconds)

(pfxdValidLifetime)

The Prefix Valid Life Time (seconds) parameter specifies the time that the prefix is valid. The range is 60 to 4 294 967 295. The default is 2 592 000.

Primary DNS Address

(primaryDnsAddress)

The Primary DNS Address parameter specifies the IP address that is exchanged by IPCP to configure the primary DNS IP address on the remote peer. The default is 0.0.0.0.

Priority Level for CCM Messages

(ccmLtmPriority)

The Priority Level for CCM Messages parameter specifies the CCM interval for the MEP. The range is 0 to 7. The default is 7.

Priority Dscp

(priorityMarkDscp)

The Priority Dscp parameter specifies whether the Dscp is used when remarking is performed on the in-profile packets. This parameter is configurable when the [Priority Type](#) parameter is set to Dscp. The range is 0 to 32. There is no default.

Priority Precedence

(priorityMarkPrec)

The Priority Precedence parameter specifies the precedence priority marking used when remarking the in profile packets. It is configurable when the [Priority Type](#) parameter is set to Precedence. The range is 0 to 7. There is no default.

Priority Type

(priorityMarkType)

The Priority Type parameter specifies the remarking type to be used. The options are:

- None (default)
- Dscp
- Precedence

Profiled Traffic only

(profiledTrafficOnly)

The Profiled Traffic only parameter specifies whether the SAP allows traffic that is not associated with a subscriber profile. The options are:

- true
- false (default)

Profile Name

(profileName)

The Profile Name parameter specifies the tunnel selection profile to use when automatic SDP binding creation is enabled. It contains steering parameters configured by the user that are used by the system to determine the tunnel selection. The range is 1 to 32 characters.

Proxy ARP Policy 1

(policy1)

The Proxy ARP Policy 1 parameter specifies the name of the first proxy ARP policy that a device is to use. Enter a proxy ARP policy name. The proxy ARP policies are applied in order, from policy 1 to policy 5. Proxy ARP enables a device to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without a default gateway or a route to the subnet.

Proxy ARP Policy 2

(policy2)

The Proxy ARP Policy 2 parameter specifies the name of the second proxy ARP policy that a device is to use. Enter a proxy ARP policy name. The proxy ARP policies are applied in order, from policy 1 to policy 5. Proxy ARP enables a device to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without a default gateway or a route to the subnet.

Proxy ARP Policy 3

(policy3)

The Proxy ARP Policy 3 parameter specifies the name of the third proxy ARP policy that a device is to use. Enter a proxy ARP policy name. The proxy ARP policies are applied in order, from policy 1 to policy 5. Proxy ARP enables a device to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without a default gateway or a route to the subnet.

Proxy ARP Policy 4

(policy4)

The Proxy ARP Policy 4 parameter specifies the name of the fourth proxy ARP policy that a device is to use. Enter a proxy ARP policy name. The proxy ARP policies are applied in order, from policy 1 to policy 5. Proxy ARP enables a device to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without a default gateway or a route to the subnet.

Proxy ARP Policy 5

(policy5)

The Proxy ARP Policy 5 parameter specifies the name of the fifth proxy ARP policy that a device is to use. Enter a proxy ARP policy name. The proxy ARP policies are applied in order, from policy 1 to policy 5. Proxy ARP enables a device to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without a default gateway or a route to the subnet.

Reachable Time (milliseconds)

(reachableTime)

The Reachable Time (milliseconds) parameter specifies how long, in milliseconds, this router should be considered reachable by other nodes on the link after the router receives a reachability confirmation. The range is 0 to 3 600 000. The default is 0.

Rebind Timer

(rebindTimer)

The Rebind Timer parameter specifies the time (in seconds) after which the client contacts any available server to extend the lifetimes of the addresses or prefixes assigned to the client. The range is 0 to 1209600. The default is 2880. A value of 0 leaves the rebind time at the discretion of the client.

Receive Interval

(bfdRxInterval)

The Receive Interval parameter specifies the receive interval in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Redirects

(redirects)

The Redirects parameter specifies whether the rate at which the interface issues ICMP Redirect messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Redirects](#) and [Redirects Time \(seconds\)](#) parameters.

Redirects Time (seconds)

(redirectsTime)

The Redirects Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Redirect messages specified by the [Number of Redirects](#) parameter. The parameter is configurable when the [Redirects](#) parameter is enabled. The range is 1 to 60. The default is 10.

Relay Plain BOOTP

(dhcpRelayPlainBootp)

The Relay Plain BOOTP parameter specifies whether plain BOOTP messages is relayed. If the value is set to disabled the system considers plain BOOTP packets as malformed DHCP packets and does not relay the messages. The options are:

- Enabled
- Disabled

Remote ID

(infoRemoteId)

The Remote ID parameter specifies whether the far-end MAC address is inserted in the remote ID suboption of DHCP Option 82. Inserting the MAC address in the suboption allows MAC-based authentication by identifying the host at the other end of the service tunnel binding. The options are:

- false (default)
- true
- Remote IDString

The Remote IDString is not available for DHCPv6.

When a device is not configured for DHCP relay, if a VPLS SAP is configured for DHCP snooping, Option 82 information is added.



Note — The maximum DHCP relay packet size is 1500 bytes. If adding Option 82 information to the packet causes the packet to exceed 1500 bytes, the DHCP relay request is forwarded without including the Option 82 information.

Remote ID String

(remoteIdString)

The Remote ID String parameter specifies the remote ID of DHCP Option 82. The range is 0 to 32 characters.

The Remote ID String parameter is configurable only when the [Remote ID](#) parameter is set to Remote IDString.

Remote Proxy ARP

(proxyArp)

The Remote Proxy ARP parameter specifies whether remote proxy ARP is in effect on the interface. The options are:

- true
- false (default)

Proxy ARP allows a device, such as a router, to answer ARP requests intended for another device. This allows a device to reach a remote subnet without configuring routes to the subnet or a default gateway device.

Renew Timer

(renewTimer)

The Renew Timer parameter specifies the time (in seconds) after which the client contacts the server from which the addresses were obtained to extend the lifetimes of the addresses or prefixes assigned to the client. The range is 0 to 604800. The default is 1800. A value of 0 leaves the renew time at the discretion of the client.

Retransmit Time (milliseconds)

(retransmitTime)

The Retransmit Time (milliseconds) parameter specifies, in milliseconds, the frequency of neighbor solicitation messages that are sent on the interface. The range is 0 to 1 800 000. The default is 0.

Return Tunnel Auto-Selection Transport Preference

(tunnelAutoselectionReturnTunnelTransportPreference)

The Return Tunnel Auto-Selection Transport Preference parameter specifies the transport encapsulation type preference for the return service tunnel. The 5620 SAM chooses an existing service tunnel based on the value of this parameter. A new tunnel is created for GRE and MPLS:LDP encapsulation types if a tunnel does not exist. The 5620 SAM automatically binds the return tunnel to a circuit. The options are:

- GRE
- MPLS:RSVP
- MPLS:BGP
- MPLS:LDP
- Any (default)



Note — The available options vary by NE type and release. The Any option is available for all NE types and releases.

The Return Tunnel Auto-Selection Transport Preference parameter is configurable when the [Auto Select Return Transport Tunnel](#) parameter is enabled.

Router Lifetime (seconds)

(routerLifetime)

The Router Lifetime parameter specifies the value (in seconds) to be placed in the router lifetime field of router advertisements sent from an interface. The range is 2700 to 9000. The default is 4500. A value of 0 indicates that the router is not used as a default router.

SAP Administrative State

See the [Administrative State](#) in this section.

SAP ARP Host Limit

(maxNumHostsSap)

The SAP ARP Host Limit parameter specifies the maximum number of ARP hosts per SAP allowed on the interface. The range is 1 to 32 767. The default is 1.

SAP Description

See the [Description](#) in this section.

SAP Type

(svcSapType)

This parameter specifies the type of SAPs which can be configured in the service supported by the 7210 SAS-E and 7210 SAS-D-6F-4T(ETR). This parameter specifies the generic encapsulation at the site level. The options are:

- null-star (default)
- dot1q (7210 SAS-E only)
- dot1q-preserve
- any (7210 SAS-D-6F-4T (ETR) only)

Table [14-23](#) lists for each service (site level) SAP type, the permitted combinations of access SAP types for the 7210 SAS-E and 7210 SAS-D-6F-4T(ETR).

Table 14-23 Service SAP Type/Access SAP Type Permitted Combinations

Service SAP Type	Access SAP Type	Uplink SAPs	Limitations
null-star	Null SAP, dot1QDefault SAP, Q.*(Supported for SAS-D only) O.*(Supported for SAS-D only)	Q.* SAP O.* SAP	—
dot1q (Supported for 7210 SAS-E only)	Null Dot 1Q Q1.Q2	Q.* SAP	—
dot1q-preserve	dot1q-preserve Q1.Q2(Supported for SAS-D only)	Q1.Q2	The outer tag of the dot1q-preserve SAP and the inner tag of the Q1.Q2 SAP (for example, Q1 tag) should be the same
any (Supported for SAS-D only)	Null dot1q SAP dot1q E.N SAP Q1.Q2 SAP Q.*SAP O.*SAP	Q1.Q2 SAP Q.* SAP O.* SAP	—



Note 1 — null-star requires access SAPs to be Null.

Note 2 — dot1q requires access SAPs to be Dot1 Q.

Note 3 — dot1q-preserve requires access SAPs to be Dot1 Q and [L2Uplink](#) SAPs are always be Q in Q.

Scheduling Class

(schedulingClass)

The Scheduling Class parameter specifies the Frame Relay class for a SAP with FRF.12 end-to-end fragmentation enabled. The range is 0 to 3. The default is 3.

Secondary DNS Address

(secondaryDnsAddress)

The Secondary DNS Address parameter specifies the IP address that is exchanged by IPCP to configure the secondary DNS IP address on the remote peer. The default is 0.0.0.0.

Send Advertisement

(sendAdvertisement)

The Send Advertisement parameter specifies whether the interface sends routing advertisement messages. The options are:

- false (default)
- true

Server 1

(server1)

The Server 1 parameter specifies the first DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server 2

(server2)

The Server 1 parameter specifies the second DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server 3

(server3)

The Server 1 parameter specifies the third DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server 4

(server4)

The Server 1 parameter specifies the fourth DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server 5

(server5)

The Server 1 parameter specifies the fifth DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server 6

(server6)

The Server 1 parameter specifies the sixth DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server 7

(server7)

The Server 1 parameter specifies the seventh DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server 8

(server8)

The Server 1 parameter specifies the eighth DHCP server for the interface. A DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format. There is no default.

Server Name

(displayedName)

The Server Name parameter specifies a name for the local DHCP server instance. The range is 0 to 32. There is no default.

Service ID

(serviceId)

The Service ID parameter specifies an ID for the service. This parameter is configurable when the [Auto-Assign ID](#) parameter is disabled.

If you are creating a new service for the purpose of service size reduction, then the services that you are moving sites to and from must have the same Service ID. Refer to Procedure [65-7](#) for detailed information.

The range is 1 to 2 147 483 647. The default is 0, which indicates that the parameter is not set.

Service Model

(serviceModel)

The Service Model parameter specifies the intended service model for the SAP. Configure the parameter to facilitate 5620 SAM and 5750 SSC comanagement of the SAP. The options are:

- Not specified (default)
- VLAN per Subscriber Routed
- VLAN per Subscriber Bridged
- VLAN per Service Routed
- VLAN per Service Bridged
- VLAN per Subscriber per Service Routed
- VLAN per Subscriber per Service Bridged

- VLAN for all Services Routed
- VLAN for all Services Bridged

Service Name

(serviceName)

The Service Name parameter specifies a name for the service. The range is 1 to 32 characters. The range is 0 to 32 characters for the VLL Apipe, Epipe, Ipipe, and Fpipe services.

For VLAN services, the name cannot start with “vlan_” or “VLAN_”. For example, a VLAN service can be named “company_x_vlan” or “companyvlan_x”, but it cannot be named “vlan_company_x”.

Service Priority

(svcPriority)

The Service Priority (svcPriority) parameter specifies the default priority of the service. The options are Low, Medium, and High priority. The default value is Low priority.

Service Tier

(tier)

The Service Tier parameter specifies the tier that the service occupies in the composite service hierarchy. The range is 1 to 10. The value is relevant only in the context of a composite service. See chapter 74 for more information about the hierarchical organization of composite services.

Set Default VLAN to VPLS Tag

(defaultVlan)

The Set Default VLAN to VPLS Tag parameter specifies whether the default VLAN of the port is the same as the VPLS service tag. The options are:

- Enabled
- Disabled (default)

SHCV Action

(shcvAction)

The SHCV Action parameter specifies the action to take for a host on the interface when checking the host indicates a connectivity failure. The parameter is configurable when the SHCV Enabled parameter is selected. Table 14-24 describes the parameter options.

Table 14-24 SHCV Action parameter

Option	Description
Raise Event	The 5620 SAM raises an alarm to indicate that host connectivity on the SAP is lost.
Remove And Raise Event	The 5620 SAM raises an alarm to indicate that host connectivity on the SAP is lost, removes the DHCP state information, and releases the resources allocated to the host.

SHCV Enabled

The SHCV Enabled parameter specifies whether SHCV is enabled on the interface. The options are:

- Enabled
- Disabled (default)

SHCV Interval (minutes)

(shcvInterval)

The SHCV Interval parameter specifies how often, in minutes, the node verifies connectivity for a host on the SAP. The range is 0 to 6000. The default is 0, which specifies that SHCV is disabled.

SHCV Retry Count

(shcvRetryCount)

The SHCV Retry Count parameter specifies the number of connectivity check retransmissions. Setting the value to (n) specifies that, for any given host, (n+1) probes are done each interval, and (n+1) missed replies are considered as a connectivity failure. The range is 2 to 29. The default is 2.

SHCV Retry Timeout (seconds)

(shcvRetryTimeout)

The SHCV Retry Timeout (seconds) parameter specifies the timeout in seconds before a connectivity check retransmission. The range is 10 to 60 (seconds). The default is 10.

SHCV Source

(shcvSource)

The SHCV Source parameter specifies the source of the source IP and MAC addresses in the unicast ARP packets that SHCV sends to hosts for connectivity verification. Table [14-25](#) describes the parameter options.

Table 14-25 SHCV Source parameter

Option	Description	Dependencies
Interface (default)	Specifies the L3 interface as the source of the source IP and MAC addresses that SHCV uses Because multiple subnets may exist on the interface, SHCV uses the host subnet. For IES group interfaces, SHCV uses the subscriber interface address.	Configurable on IES and VPRN L3 interfaces
VRRP	Specifies the VRRP state as the source of the source IP and MAC addresses that SHCV uses. The IP and MAC address are selected as follows. <ul style="list-style-type: none"> SHCV packets from a master VRRP IP interface use the VRRP VRID IP and MAC addresses as the source addresses. SHCV packets from a backup VRRP IP interface use the L3 interface IP and MAC addresses as the source addresses to avoid corrupting the host ARP cache. 	Configurable on IES and VPRN L3 interfaces Not configurable on IES group interfaces

SHCV Source IP Address

(shcvSourceIpAddress)

The SHCV Source IP Address parameter specifies the IP address that is inserted as the source IP address for the unicast ARP packets that SHCV sends to hosts for connectivity verification. The default is 0.0.0.0, which is valid and specifies that the host does not record the ARP entry in the ARP cache.

SHCV Source MAC Address

(shcvSourceMacAddress)

The SHCV Source MAC Address parameter specifies the MAC address that is inserted as the source MAC address for the unicast ARP packets that SHCV sends to hosts for connectivity verification. The default is 00-00-00-00-00-00, which specifies that the device uses the MAC address of the CPM that issues the packet.

Site ID

(siteId)

Table 14-26 describes the parameter options. Click on the Select button to choose a site. You can select filters to view specific sites; for example you can choose the apply span of control filter to view only sites that are in your span of control.

Table 14-26 Site ID parameter

For	Option
LSP Ping LSP Trace LDP Tree Trace	IP address of the MPLS path. Click on the Select button and choose an MPLS path from the list. Click on the Clear button to remove the MPLS path. The read-only name parameter is populated with the configured name of the MPLS path.
Multicast Router Information	IP address of the VPRN PIM site or the core routing PIM site.
Multicast Trace	IP address of the VPRN or core routing PIM site. IP address of the multicast group.
MEP	IP address of the MEP.

Snooping

(snooping)

The Snooping parameter specifies whether DHCP snooping is enabled for DHCP messages. The default depends on the type of managed device. The options are:

- Enabled
- Disabled

Source IP Address

(sourceAddress)

The Source IP Address specifies the IPv6 address that is used by the DHCPv6 relay agent as a source IP address in all the DHCPv6 relay messages that are sent to the DHCPv6 servers. The default is 0:0:0:0:0:0:0:0.

Specify VLAN Path

(specifyVlanPath)

The Specify VLAN Path parameter specifies whether the 5620 SAM will create a single hop VLAN path during service creation. When this parameter is disabled, the 5620 SAM will create a VLAN path with a single hop as part of service creation. This service is called an Aggregator (single hop) service. When Specify VLAN path is enabled, the user must select a VLAN path. The options are:

- Enabled (default)
- Disabled

Subscriber Authentication Policy

(subscrAuthPolicyPointer)

The Subscriber Authentication Policy defines the subscriber authentication policy applied when a DHCP message is received on the interface. The authentication policy must be previously defined. The policy is only applied when the DHCP Lease Populate parameter is set to a non-zero value for this interface.

Subscriber Identification

(subscriberIdent)

The Subscriber Identification parameter specifies an identifier with which to identify the static subscriber host. The parameter is configurable when the [Use SAP ID as Subscriber ID](#) parameter is disabled. The range is 0 to 32 characters. There is no default.

Subscriber Limit

(subscriberLimit)

The Subscriber Limit parameter specifies the maximum number of subscribers that the SAP allows. The range is 0, or 1 to 20 000. The default is 1, which can be specified by selecting the Single check box. Selecting the Unlimited check box or setting the parameter to a value of 0 means that no limit is enforced.

SVC Mgr Service ID

(id)

The SVC Mgr Service ID (id) parameter specifies the service component ID for this service. This parameter is configurable when the [Auto-Assign ID](#) parameter is disabled.

Tag (Inner Encapsulation Value)

(tunnelSapPathInnerTagValue)

The Tag (Inner Encapsulation Value) parameter specifies a VLAN tag for fate-sharing. It is used for the Path Endpoints of the fate-sharing Ethernet Tunnel Endpoint SAP. The range is 0 to 4095. The default is 0.

Tag (Outer Encapsulation Value)

(tunnelSapPathOuterTagValue)

The Tag (Outer Encapsulation Value) parameter specifies a VLAN tag for fate-sharing. It is used for the Path Endpoints of the fate-sharing Ethernet Tunnel Endpoint SAP. The range is -1, and 0 to 4094. The default is -1.

Template Description

The Template Description parameter specifies a description for the template type. The range is an interface name of 0 to 80 characters. The default is an empty string.

Time Exceeded

(timeExceeded)

The Time Exceeded parameter specifies whether the rate at which the interface issues ICMP Time Exceeded messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which ICMP redirects are issued is controlled by the [Number of Time Exceeded](#) and [Time Exceeded Time \(seconds\)](#) parameters.

Time Exceeded Time (seconds)

(timeExceededTime)

The Time Exceeded Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Time Exceeded messages specified by the [Number of Time Exceeded](#) parameter. The parameter is configurable when the [Time Exceeded](#) parameter is enabled. The range is 1 to 60. The default is 10.

Timeout (seconds)

(timeOut)

The Timeout (seconds) parameter specifies the minimum time, in seconds, that an ARP entry learned on the IP interface is stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is seen from an IP host, otherwise the ARP entry is aged from the ARP table. When the parameter is set to 0, ARP aging is disabled. The range is 0 to 65 535. The default is 14 400.

Translation

(vlanTranslation)

The Translation parameter specifies the desired Ingress VLAN Translation mode.

The options are:

- VLAN ID: specifies that the value of the [Translation ID](#) parameter is to be used to overwrite the preserved VLAN ID in a packet. This setting is only applicable to dot1q encapsulated SAPs.
- Copy Outer: specifies that the outer VLAN ID should be used to overwrite the preserved VLAN ID in the packet. This setting is only applicable to QinQ SAPs.
- None: specifies that Ingress VLAN Translation is disabled.

The default is None.

Translation ID

(vlanTranslationId)

The Translation ID parameter specifies the VLAN ID to be used to overwrite the preserved VLAN ID in a packet. The parameter is disabled if [Translation](#) is not set to VLAN ID. The range is -1 or 4094. The default is -1.

Transmit Interval

(bfdTxInterval)

The Transmit Interval parameter specifies the time in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Transport Type

(transportPreference)

The Transport Type parameter specifies the type of transport to use when you configure SDP bindings for a service. The options are:

- GRE
- MPLS:RSVP
- MPLS:BGP
- MPLS:LDP
- PBB
- Mixed LSP Mode
- Any (default)

The Transport Type parameter is configurable only when the [Automatic Mesh SDP Binding Creation](#) parameter, [Automatic SDP Binding/PBB Tunnel Creation](#), or [Automatic Mesh SDP Binding Creation](#) parameter is enabled.



Note 1 – The available options vary by NE type and release. The Any option is available for all NE types and releases.

Note 2 – If a transport type other than PBB is selected, the 5620 SAM attempts to find the optimal service tunnels by type which are using TDLP signaling, and then will create SDP bindings over them.

MPLS:BGP

When MPLS:BGP is selected, 5620 SAM creates SDP bindings between sites that support BGP tunnels by associating them with SDPs that have [Enable BGP-Tunnel](#) set to true and that are operationally up.

If no SDP with [Enable BGP-Tunnel](#) exists, 5620 SAM will create the missing BGP tunnels. If the [Enable BGP-Tunnel](#) parameter is not applicable to a site as a source of the SDP binding, then no mesh SDP bindings will be created for that site. Note that the BGP route tunnel method is excluded if multi-mode transport is enabled for an SDP.

Refer to the [Enable BGP-Tunnel](#) parameter for further information on the MPLS:BGP selection.

Mixed LSP Mode

When Mixed LSP Mode is selected, 5620 SAM creates SDP bindings between sites by associating them with SDPs that have their Mixed LSP Mode parameter set to true and that are operationally up.

Alternatively, 5620 SAM will choose operational RSVP SDPs first, then operational LDP SDPs if:

- the Mixed LSP Mode parameter is not applicable to a site as a source of an SDP binding
- none of the SDPs have their Mixed LSP Mode parameter set to true
- none of the SDPs that have their Mixed LSP Mode parameter set to true are operationally up

If none of the SDPs with their Transport Type set to Mixed LSP Mode, MPLS:RSVP, or MPLS:LDP are operationally up, 5620 SAM will alternatively choose operationally-down SDPs in the following order:

- an operationally-down SDP set to Mixed LSP Mode, and at the least cost
- an operationally-down SDP set to MPLS:RSVP, and at the least cost
- an operationally-down SDP set to MPLS:LDP, and at the least cost

In addition, if there are no RSVP or LDP SDPs, then no mesh SDP bindings will be created.

See the [Mixed Lsp Mode](#) parameter for further information on Mixed LSP Mode selection.

Trusted

(isTrusted)

The Trusted parameter specifies whether the ToS bits of packets that ingress an IP interface can be trusted by the system. Packets received on a trusted interface are only remarked at network egress when the network egress Remark function is enabled, except for VPRN packets, which are not affected. A packet that ingresses a non-trusted IP interface is always remarked at egress network interfaces regardless of the Remark parameter value of the egress network interface. The options are:

- true (default for VPRN and network IP interfaces)
- false (default for IES IP interfaces)

Trusted

(trusted)

The Trusted parameter specifies that the router forward the DHCP request even if the request has a giaddr value of 0 and attached Option 82 information. Table [14-27](#) describes the parameter.

Table 14-27 Trusted parameter

Option	Option description
false	The device discards the DHCP request.
true (default)	The device forwards the DHCP request. The device acting as the DHCP relay agent modifies the giaddr value to be equal to that of the ingress interface. Use this option when the Action parameter is set to Keep and the affected service is IES or VPRN.

TTL Expired

(ttlExpired)

The TTL Expired parameter specifies whether the rate at which the interface issues TTL Expired messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of TTL Expired](#) and [TTL Expired Time \(seconds\)](#) parameters.

TTL Expired Time (seconds)

(ttlExpiredTime)

The TTL Expired Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP TTL Expired messages specified by the [Number of TTL Expired](#) parameter. The parameter is configurable when the [TTL Expired](#) parameter is enabled. The range is 1 to 60. The default is 10.

Tunnel Auto-Selection Transport Preference

(tunnelAutoselectionTunnelTransportPreference)

The Tunnel Auto-Selection Transport Preference parameter specifies the transport encapsulation type preference for the originating service tunnel. The 5620 SAM chooses an existing service tunnel based on the value of this parameter. A new tunnel is created for GRE, MPLS:LDP, and MPLS:BGP encapsulation types if a tunnel does not exist. The 5620 SAM automatically binds the tunnel to a circuit. The options are:

- GRE
- MPLS:RSVP
- MPLS:LDP
- MPLS:BGP
- Mixed LSP Mode
- Any (default)

The Tunnel Auto-Selection Transport Preference parameter is configurable when the [Auto-Select Transport Tunnel](#) parameter is enabled.

Refer to the [Transport Type](#) parameter for further information on the MPLS:BGP and Mixed LSP Mode selections.

Tunnel Fault Notification

([tunnelFaultNotification](#))

The Tunnel Fault Notification parameter specifies whether the service site will accept CFM fault notification from a Tunnel MEP. The options are:

- Accept
- Ignore (default)

Tunnel Termination Site

([tunnelSelectionTerminationSiteId](#))

The Destination Node ID parameter specifies the endpoint for a created circuit. Click the Select button to choose a destination node, or specify a unicast IP address in dotted-decimal format. For an IES or VPRN service, this can be an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format.

Unnumbered Type

([unnumberedReferenceType](#))

The Unnumbered Type parameter specifies the type of information that identifies the unnumbered interface. Table [14-28](#) describes the parameter options:

Table 14-28 Unnumbered Type parameter

Option	Description	Dependencies
System (default for IES)	The interface uses the router system address to identify itself.	—
IP Address (default for VPRN)	The interface uses the IP Address specified by the IP Address parameter to identify itself.	You must configure the IP Address parameter.
Name	The interface uses the character string specified by the Interface Name parameter to identify itself.	You must configure the Interface Name parameter.

Unreachables

([unreachables](#))

The Unreachables parameter specifies whether the rate at which the interface issues ICMP Unreachable messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Unreachables](#) and [Unreachables Time \(seconds\)](#) parameters.

Unreachables Time (seconds)

(unreachablesTime)

The Unreachables Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Unreachable messages specified by the [Number of Unreachables](#) parameter. The parameter is configurable when the [Unreachables](#) parameter is enabled. The range is 1 to 60. The default is 10.

URPF Check Mode

(uRPFCheckMode)

This parameter is used to help limit the malicious traffic on an enterprise network. The options are:

- Strict
- Loose (default)

The URPF Check Mode parameter is configurable when the [URPF Check State](#) parameter is enabled.

In Strict mode, the Unicast RPF checks whether the incoming packet has a source address which matches a prefix in the routing table, and whether the interface expects to receive a packet with this source address prefix.

In Loose mode, the Unicast RPF checks whether the incoming packet has a source address which matches a prefix in the routing table, but there is no check whether the interface expects to receive a packet with this source address prefix.

URPF Check State

(uRPFCheckState)

The URPF Check State parameter specifies whether Unicast Reverse Path Forwarding is enabled on the interface. This parameter is supported on a 2 x XP MDA IOM3 in a 7450 ESS or 7750 SR. The options are:

- Enabled
- Disabled (default)

Use ARP

(useArpForReply)

The Use ARP parameter specifies how the system determines the hardware address for outgoing IP packets. The options are:

- false (default)
- true

You cannot configure the Use ARP parameter if the [Lease Populate](#) parameter is configured.

Use as source

(giAddressAsSrc)

The Use as source parameter specifies whether DHCP relay uses the value specified for the IP address parameter as the source address. The options are:

- false (default)
- true

Use Bandwidth-Reserved Paths

(useBwReservedPath)

The Use Bandwidth-Reserved Paths parameter specifies whether to configure bandwidth allocation for a mesh SDP binding. The options are:

- Never
- No Preference (default)
- Always

The parameter is configurable when the [Automatic Mesh SDP Binding Creation](#) parameter is enabled.

Use Multipoint Shared Queue

(usesMultipointShared)

The Use Multipoint Shared Queue parameter specifies whether the access interface uses a multipoint shared queue on the device. The options are:

- false (default)
- true

The 5620 SAM automatically enables the Use Shared Queue parameter when the Use Multipoint Shared Queue parameter is set to true.

Use SAP ID as Subscriber ID

(subIdIsSapId)

The Use SAP ID as Subscriber ID parameter specifies whether the static host uses the SAP ID as the subscriber ID. When the parameter is enabled, the [Subscriber Identification](#) parameter is not configurable. The options are:

- enabled
- disabled (default)

Use Shared Queue

(sharedQueueOn)

The Use Shared Queue parameter specifies whether the access interface uses the shared queue on the device. The options are:

- enabled
- disabled (default)

The 5620 SAM automatically enables the Use Shared Queue parameter when the Use Multipoint Shared Queue parameter is set to true.

Valid Life Time

(validLifeTime)

The Valid Life Time parameter specifies (in seconds) the valid lifetime for an IPv6 prefix or address in an option. The range is 300 to 4 294 967 295. The default is 86400. A value of 4294 967 295 represents an infinite valid lifetime.

A valid lifetime must be longer than a preferred lifetime. See [Preferred Life Time](#) in this section for more information.

VC ID

(vcId)

The VC ID parameter specifies the value used by each end of a service tunnel to identify the VC. The range is 0 to 4 294 967 295. The default is 0.

VC Type

(svcVcType)

The VC Type parameter specifies the type of VC for a VPLS service. It is only applicable to a Telco 7250. The options are:

- Ethernet (default)
- VLAN

VC Type

(vcType)

The VC Type parameter allows termination of an Epipe or Ipipe into an IES or VPRN service. The parameter can only be set during the creation of the spoke SDP binding.

The options are:

- Ethernet (default)
- Ipipe

The Ipipe option is only available in chassis mode C or D.

As a configuration example for this parameter, suppose your setup involves a customer edge device running ATM, FR, Ethernet, or PPP traffic to a provider edge device (PE-1). Furthermore, you want to terminate this into a VPRN (or IES) service on another provider edge device (PE-2). You would therefore create a spoke SDP binding from an Ipipe on PE-1 and terminate it on the VPRN (or IES) service on PE-2. On the PE-2 VPRN (or IES) service, a spoke SDP binding is then required with the VC Type set as Ipipe. Alternatively, if the PE-1 VLL is an Epipe, then the VPRN (or IES) service on PE-2 is required to use a VC Type of Ethernet.

When this type of setup is configured within 5620 SAM, a composite service is automatically created for the involved Epipe/Ipipe and VPRN/IES.

Vendor Specific Options

(vendorIncludeOptions)

The Vendor Specific Options parameter specifies what is included in the Alcatel-Lucent vendor specific sub-option of DHCP Option 82. Table [14-29](#) describes the parameter options.

Table 14-29 Vendor Specific Options parameter

Option	Description	Dependencies
SAP ID	Specifies that the SAP ID is encoded in the vendor specific sub-option of DHCP Option 82.	—
Service ID	Specifies that the Service ID is encoded in the vendor specific sub-option of DHCP Option 82.	—
Client MAC	Specifies that the Client MAC address is encoded in the vendor specific sub-option of DHCP Option 82.	—
System ID	Specifies that the system ID is encoded in the vendor specific sub-option of DHCP Option 82.	—

Vendor String

(vendorOptionString)

The Vendor String parameter specifies the string that is included in the Alcatel-Lucent vendor specific sub-option of the DHCP Option 82.

VLAN VC Tag

(vlanVcTag)

The VLAN VC Tag parameter specifies a dot1q value for encapsulation to the far end of the service tunnel. The range is 0 to 4095. The default is None.

VPLS Name

(vplsName)

The VPLS Name parameter specifies the name of the VPLS site routed by the interface. The range is 0 to 64 characters. There is no default.

WAN Host

(wanhost)

The WAN Host parameter specifies that the subscriber prefix is used by IPv6 ESM hosts for local addressing or by a routing gateway's WAN interface. The default is False.

Manage menu parameters

- 15 – Templates parameters
- 16 – Services parameters
- 17 – Mirror Services parameters
- 18 – Customers parameters
- 19 – LSPs parameters
- 20 – MPLS Paths parameters
- 21 – Service Tunnels parameters
- 22 – IPsec VPN parameters
- 23 – VLAN group and path parameters
- 24 – Node Redundancy parameters
- 25 – Routing Instances parameters
- 26 – VRRP Virtual Routers parameters
- 27 – Virtual Anycast RP parameters
- 28 – FIB Entries parameters
- 29 – Snapshot Instances parameters
- 30 – Activation parameters

- 31 – Gateway configuration parameters
- 32 – Mobile Regions parameters
- 33 – LTE User Stats parameters
- 34 – LTE EPS Path Drill Down Hints parameters
- 35 – Call Trace parameters
- 36 – Common Manage menu parameters

15 – Templates parameters

15.1 Templates parameters 15-2

15.1 Templates parameters

This chapter describes the parameters on the Manage Service Templates form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Command Type

The Command Type parameter specifies the command type for the template. The options are:

- Create (default)
- Modify

When you choose the Create option, the template is used to create new objects. When you choose the Modify option, the template is used to modify an existing object.

Description

See the [Description](#) parameter in section 14.1.

Generate First (Base) Version

The Generate First (Base) Version parameter specifies whether a Velocity UI header is generated in the XML API configuration template script at template creation. The options are:

- Enabled (default)
- Disabled

Generate Velocity Properties

The Generate Velocity Properties parameter specifies whether a Velocity UI header is generated in the XML API configuration template script. The options are:

- Enabled (default)
- Disabled

Mode

The Mode parameter is used to specify the state of the template. The options are:

- Draft (default)
- Released

Name

(scriptName)

The Name parameter specifies a name for the XML API configuration script. The range is 1 to 255 characters.

Script ID

(id)

The Script ID parameter specifies a unique numeric identifier for the created XML API configuration template script. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 65 535. The default is 0.

Show created object

The Show created object parameter specifies whether to open the properties form for the object that you are creating from the template. The options are:

- Enabled (default)
- Disabled

State

(state)

The State parameter specifies whether the XML API configuration template script appears in the list of templates and can be executed. The options are:

- Enabled (default)
- Disabled

Templated Object Categories

(configuredClassCategories)

The Templated Object Categories parameter specifies the object categories for which the template is created. Click on the Select button to choose from a list of templatable object categories.

Templated Object Class Name

(configuredClass)

The Templated Object Class Name parameter specifies the object class for which the template is created. Click on the Select button to choose from a list of templatable object classes.

Type

The Type parameter specifies a user-defined description of the XML API configuration templated category. The range is 0 to 255 characters.

16 – *Services parameters*

16.1 Services parameters 16-2

16.1 Services parameters

This chapter describes the parameters on the Manage Services form and its child forms.

Administrative State

(administrativeState)

The Administrative State parameter specifies the current state of the OAM diagnostic test. The options are:

- clear
- go
- cleared (read-only)

Age (seconds)

(age)

The Age (seconds) parameter specifies the interval, in seconds, that an OAM MAC address is aged. The default is 3600.

Inhibit Learning

(inhibitLearning)

The Inhibit Learning parameter specifies whether MAC entries are learned (created in the router table) during an OAM MAC purge diagnostic activity. The options are:

- Enabled
- Disabled (default)

Last Member Query Interval (tenths of seconds)

(genLastMembQueryIntvl)

The Last Member Query Interval (tenths of seconds) parameter specifies the IGMP last member query interval on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to set the parameter on the system or the specified VLAN.

The IGMP last member query interval refers to the amount of time to reply to an IGMP query message that has been sent in response to a leave group message. The range is 1 to 65 535. The default is 10.

Max Group

(igmpMaxGroupLimit)

The Max Group parameter specifies the maximum number of IGMP groups that can be dynamically learned by the OmniSwitch. The range is 0 to 4 294 967 295. The default is 0.

Max Group Action

(igmpMaxGroupExceedAction)

The Max Group Action parameter specifies the action performed if the dynamically learned IGMP group addresses exceed the value specified by the [Max Group](#) parameter. Table 16-1 describes the parameter options.

Table 16-1 Max Group Action parameter

Option	Description
None (default)	When the Max Group parameter is 0, the number of dynamically learned IGMP group addresses is not limited. When the Max Group parameter is not 0, any IGMP group addresses that are dynamically learned after the Max Group value is exceeded are dropped.
Drop	IGMP group addresses that are dynamically learned after the Max Group value is exceeded are dropped.
Replace	IGMP group addresses that are dynamically learned after the Max Group value is exceeded replace the oldest learned group address.

Multicast Group IP Address

(groupAddress)

The Group IP Address parameter specifies the multicast group IP address. Specify an IPv4 multicast address in dotted-decimal format, or an IPv6 multicast address in colon-hexadecimal format.

Protocol Version

(igmpVersion)

The Protocol Version parameter specifies the default version of the IGMP on the specified VLAN or on the system when a VLAN is not specified. The options are:

- Version 1
- Version 2 (default)
- Version 3

Proxying

(igmpProxying)

The Proxying parameter specifies whether IGMP proxying is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP proxying refers to the processing of membership information on behalf of client systems and the reporting of the membership on their behalf. The options are:

- Disabled (default)
- Enabled

Querier Forwarding

(igmpQuerierForwarding)

The Querier Forwarding parameter specifies whether IGMP querier forwarding is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP querier forwarding refers to the promotion of detected IGMP queriers to receive all IP multicast data traffic. The options are:

- Disable (default)
- Enable

Query Interval (seconds)

(genQueryInterval)

The Query Interval (seconds) parameter specifies the time period between IGMP query messages. Table 16-2 lists the default and range values for the parameter.

Table 16-2 Query Interval (seconds) parameter

Object	Default	Range
OmniSwitch system or VLAN	125	1 to 65 535
Other	125	2 to 1024

Query Response Interval (tenths of seconds)

(genQueryResponseIntvl)

The Query Response Interval (tenths of seconds) parameter specifies the IGMP query response interval on the specified VLAN or on the system when a VLAN is not specified.

The query response interval refers to the amount of time to wait before replying to an IGMP query message. The range is 1 to 65 535. The default is 100.

Querying

(igmpQuerying)

The Querying parameter specifies whether IGMP querying is enabled on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to configure the parameter on the system or the specified VLAN.

IGMP querying refers to the requesting of the network IGMP group membership information by sending IGMP queries. IGMP querying also involves participation in IGMP querier elections. The options are:

- Disable (default)
- Enable

Robust Count

(genRobustCount)

The Robust Count parameter sets the IGMP robustness variable on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to set the parameter on the system or the specified VLAN.

The robustness variable allows you to fine-tune a network that is expected to have high packet loss. The range is 1 to 7. The default is 2.

Router Timeout (seconds)

(igmpRouterTimeout)

The Router Timeout (seconds) parameter specifies the expiry time of IP multicast routers on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to set the parameter. The range is 1 to 65 635. The default is 90.

Source Timeout (seconds)

(igmpSourceTimeout)

The Source Timeout (seconds) parameter specifies the expiry time of IP multicast sources on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to configure the parameter. The range is 1 to 65 635. The default is 30.

Spoofing

(igmpSpoofing)

The Spoofing parameter specifies whether IGMP spoofing is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP spoofing refers to replacing a client MAC and IP address with the system MAC and IP address when proxying aggregated IGMP group membership information. The options are:

- Disable (default)
- Enable

Target MAC Address

(targetMacAddress)

The Target MAC Address parameter specifies the MAC address of the specified router. By default, this parameter is populated automatically with the configured address.

Unsolicited Report Interval (seconds)

(igmpUnsolicitedReportInterval)

The Unsolicited Report Interval (seconds) parameter sets the value of the IGMP unsolicited report interval on the specified VLAN or on the system when a VLAN is not specified. The unsolicited report interval refers to the amount of time to proxy any changed IGMP membership state. The range is 1 to 65 635. The default is 1.

What type of interface would you like to create?

The What type of interface would you like to create? parameter specifies the:

- type of multicast interface that is added to an existing IES
- type of protocol that is applied to an existing IES or IES SAP

Table 16-3 describes the objects to which the parameter applies and the options for each object:

Table 16-3 What type of interface would you like to create? parameter

Object	Options
IES	<ul style="list-style-type: none">• PIM (default)• IGMP
IES or IES SAP	<ul style="list-style-type: none">• OSPFv2 (default)• OSPFv3• RIP• ISIS

Zapping

(igmpZapping)

The Zapping parameter specifies whether IGMP zapping is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP zapping refers to processing membership and source filter removals immediately without waiting for the protocol specified time period. This mode facilitates IP TV applications that need to change quickly between IP multicast groups. The options are:

- Disabled (default)
- Enabled

17 – Mirror Services parameters

17.1 Mirror Services parameters 17-2

17.1 Mirror Services parameters

This chapter describes the unique parameters on the Manage Mirror Service Templates form and child forms.



Note — The mirror service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent recommends that you do not use the 5620 SAM-O XML classes and methods that are associated with the service templates.

Allow Binding Of Templates Not Associated With Any Customer

See the [Allow Binding Of Templates Not Associated With Any Subscriber](#) parameter in section [36.1](#).

Automatic SDP Binding Creation

(**topologyAutoCompletion**)

The Automatic Mesh SDP Binding Creation parameter specifies whether the service that you are creating is automatically bound to previously created service tunnels. The options are:

- Enabled
- Disabled (default)

Enabling the parameter displays the Transport Type and Use Bandwidth-Reserved Paths parameters.

Collect Accounting Statistics

(**accountingOn**)

The Collect Accounting Statistics parameter specifies whether the collection of accounting statistics on the interface is enabled. The options are:

- Enabled (default)
- Disabled

Customer ID

(**subscriberId**)

Click on the Select button to specify the subscriber that the template is associated with. The default is 0.

Description

See the [Description](#) parameter in section [36.1](#).

Encapsulation Type

(encapsulationType)

The Encapsulation Type parameter specifies the type of encapsulation configured on the service mirror site. The encapsulation type must be the same for all the mirror sites associated with a service. The options are:

- Ethernet (default)
- Frame Relay
- PPP

Forwarding Class

(forwardingClass)

The Forwarding Class parameter specifies a default forwarding class for mirrored packets that are part of the mirrored service. Forwarding classes provide network elements with a method to establish the priority of packets. All packets for a mirrored service use the same forwarding class. For example, when the destination of a mirrored packet is on a SAP, a single egress queue is created using the buffers from the pool of buffers that is associated with the forwarding class. Table 17-1 describes the parameter options.

Table 17-1 Forwarding Class parameter

Option	Option description
be (default)	Specifies that packets are treated, at best, as out-of-profile assured service packets. There are no delivery guarantees. The best-effort and low-2 options are intended for best effort traffic.
l2	
af	Specifies that packets are forwarded or discarded based on the availability of bandwidth on NEs. The assured and low-1 options are intended for assured traffic. Assured forwarding classes provide services with a CIR and PIR. Transmitted packets that are at or below the CIR are marked in-profile. If the core service network has sufficient bandwidth along the path for the assured traffic, all aggregate in-profile service packets reach the destination. Transmitted packets that are above the CIR are marked out-of-profile. When an assured out-of-profile packet is received at a congestion point in the network, it is discarded before in-profile assured-service packets.
l1	
h2	Specifies that packets in the class are always serviced at congestion points over other forwarding classes. These options are intended for high-priority traffic. <ul style="list-style-type: none"> • The h2 and ef options are intended for delay- or jitter-sensitive traffic, such as voice or video. • The h1 option is intended for secondary network control traffic or delay- and jitter-sensitive traffic. • The nc option is intended for network control traffic. With a strict PHB at each network hop, service latency is mainly affected by the amount of high-priority traffic at each hop. When the core network has sufficient bandwidth, delay and jitter characteristics of high-priority traffic can be supported without using traffic-engineered paths, as long as the core treats high-priority traffic with the appropriate PHB.
ef	
h1	
nc	

ID

See the “ID” parameter in section 36.1.

Inner Encap Value**(innerEncapValue)**

The Inner Encap Value parameter specifies the inner encapsulation value for the port. The range is 0 to 4095. The default is 0.

Name

See the [Name](#) parameter in section 36.1.

Outer Encap Value**(outerEncapValue)**

The Outer Encap Value parameter specifies the outer encapsulation value of the port. The range is 0 to 4094. The default is 0.

Return Tunnel Transport**(tunnelAutoselectionReturnTunnelTransportPreference)**

The Return Tunnel Transport parameter specifies the transport encapsulation type preference for the return service tunnel. The 5620 SAM chooses an existing service tunnel based on the value of this parameter, or creates a new tunnel when one does not exist. The 5620 SAM automatically binds the return tunnel to a circuit. The options are:

- GRE
- MPLS:RSVP
- MPLS:LDP
- Any (default)

The Return Tunnel Transport parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.

Service Description

See the [Service Description](#) parameter in section 36.1.

Service Name**(displayName)**

The Service Name parameter specifies a name for the service. The range is 1 to 32 characters.

Site ID

(siteId)

The Site ID parameter specifies the site on which the terminating port of the L2 access interface mirror service template is located. Click on the Select button to list and choose a site.

Site Type

(mirrorSiteType)

The Site Type parameter specifies the type of site in the mirror site service template. The options are:

- Source (default)
- Destination

Slice Size

(sliceSize)

The Slice Size parameter specifies how much of the mirrored packet, in bytes, to send to the mirror destination. For example, when you specify a parameter value of 256, the first 256 bytes of a packet are sent to the mirror destination. The original packet is not affected. The range is 0 to 9216. The default is 0, which specifies that the entire packet is mirrored and no packet slicing occurs.

Source Administrative State

(sourceAdministrativeState)

The Source Administrative State parameter specifies whether mirror sources on the site are enabled. The options are:

- Up (default)
- Down

Template Description

The Template Description parameter specifies a description for the template type. The range is an interface name of 0 to 80 characters. The default is an empty string.

Transport Type

(transportPreference)

The Transport Type parameter specifies the type of transport to use when you configure SDP bindings for a service. The options are:

- GRE
- MPLS:RSVP

- MPLS:LDP
- Any (default)

The Transport Type parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.

Tunnel Source Site ID

(fromNodeId)

Click on the Select button to list and choose the source site of the tunnel.

Tunnel Transport

(tunnelAutoselectionTunnelTransportPreference)

The Tunnel Transport parameter specifies the transport encapsulation type preference for the service tunnel. The 5620 SAM chooses an existing tunnel based on the value of this parameter, or creates a new tunnel when one does not exist.

The 5620 SAM automatically binds the service tunnel to a circuit. The options are:

- GRE
- MPLS:RSVP
- MPLS:LDP
- Any (default)

The Tunnel Transport parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.

Use Bandwidth-Reserved Paths

(topologyAutoCompletion)

The Use Bandwidth-Reserved Paths parameter specifies whether to configure bandwidth allocation for an SDP binding when you configure service transport preferences. The options are:

- Never
- No Preference (default)
- Always

The Use Bandwidth-Reserved Paths parameter is configurable when the Automatic Mesh SDP Binding Creation parameter is enabled.

18 – Customers parameters

18.1 Customers parameters 18-2

18.1 Customers parameters

This chapter describes the parameters on the Manage Customers form and its child forms.

Address

(address)

The Address parameter specifies the mailing address of the customer.

Apdex scores below this threshold are unacceptable quality

The Apdex scores below this threshold are unacceptable quality, the parameter range is 0 to 1 in 0.01 increments. The default value is 0.5.

Apdex scores below this threshold are poor quality

The Apdex scores below this threshold are poor quality, the parameter range is 0 to 1 in 0.01 increments. The default value is 0.7.

Apdex scores below this threshold are fair quality

The Apdex scores below this threshold are fair quality, the parameter range is 0 to 1 in 0.01 increments. The default value is 0.85.

Apdex scores below this threshold are good quality

The Apdex scores below this threshold are good quality, the parameter range is 0 to 1 in 0.01 increments. The default value is 0.94.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 36.1.

Contact

(contact)

The Contact parameter specifies the primary point of contact for the customer.

Description

See the [Description](#) parameter in section 36.1.

Email

(email)

The Email parameter specifies the e-mail address of the primary contact for the customer.

Equipment Type

(scope)

The Equipment Type parameter specifies the type of object across which an aggregation scheduler can be applied. The options are:

- Port (default)
- Card

ID

(subscriberId)

The ID parameter specifies a unique ID for the customer. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 2 147 483 647. The default is 0.

MOS scores below this threshold are bad quality

The MOS scores below this threshold are bad quality, the parameter range is 0 to 5 in 0.01 increments. The default value is 1.0.

MOS scores below this threshold are poor quality

The MOS scores below this threshold are poor quality, the parameter range is 0 to 5 in 0.01 increments. The default value is 2.0.

MOS scores below this threshold are fair quality

The MOS scores below this threshold are fair quality, the parameter range is 0 to 5 in 0.01 increments. The default value is 3.0.

MOS scores below this threshold are good quality

The MOS scores below this threshold are good quality, the parameter range is 0 to 5 in 0.01 increments. The default value is 4.0.

Name

(subscriberName)

The Name parameter specifies a name of the customer. The range is 0 to 32 characters. There is no default.

Phone Number

(phoneNumber)

The Phone Number parameter specifies the phone number for the customer.

Scheduler Name

(aggregationSchedulerName)

The Scheduler Name parameter specifies a name for the aggregation scheduler. The range is 1 to 32 characters. There is no default.

19 – LSPs parameters

19.1 LSPs parameters 19-2

19.1 LSPs parameters

This chapter describes the parameters on the Manage LSP Path form and child forms.

Adjust Down Bandwidth (mbps)

(autoBWAdjDNMbps)

The Adjust Down Bandwidth (mbps) parameter specifies the minimum difference between the current bandwidth reservation of the LSP and the measured maximum average data rate, expressed as an absolute bandwidth, to decrease the bandwidth. The range is 0 to 100 000. The default is 0.

Adjust Down Threshold (percent)

(autoBWAdjDNPercent)

The Adjust Down Threshold (percent) parameter specifies the minimum difference between the current bandwidth reservation of the LSP and the measured maximum average data rate, expressed as a percentage of the current bandwidth, for decreasing the bandwidth of the LSP. A value of 0 indicates that the threshold check is always true for any measured bandwidth less than the current bandwidth. The range is 0 to 100. The default is 5.

Adjust Multiplier

(autoBWAdjMul)

The Adjust Multiplier parameter specifies the number of collection intervals in the adjust interval. The range is 1 to 16 383. The default is 288.

Adjust Up Bandwidth (mbps)

(autoBWAdjUPMbps)

The Adjust Up Bandwidth (mbps) parameter specifies the minimum difference between the current bandwidth reservation of the LSP and the measured maximum average data rate, expressed as an absolute bandwidth, to increase the bandwidth of the LSP. The range is 0 to 100 000. The default is 0.

Adjust Up Threshold (percent)

(autoBWAdjUPPercent)

The Adjust Up Threshold (percent) parameter specifies the minimum difference between the current bandwidth reservation of the LSP and the measured maximum average data rate, expressed as a percentage of the current bandwidth, to increase the bandwidth of the LSP. A value of 0 indicates that the threshold check is always true for any measured bandwidth greater than the current bandwidth. The range is 0 to 100. The default is 5.

Administrative

See the [Administrative State](#) parameter in section 36.1.

Administrative

(administrativeState)

The Administrative parameter specifies whether the point-to-multipoint LSP is administratively enabled. The options are:

- Up (default)
- Down

Administrative State

See the [Administrative State](#) parameter in section 36.1.

Administrative State

(egrAccountingAdminState)

The Administrative State parameter specifies whether the object is administratively enabled. The options are:

- Up
- Down (default)

Auto Bandwidth

(autoBandWidth)

The Auto Bandwidth parameter specifies whether automatic bandwidth adjustment is enabled for the LSP. The options are:

- true
- false (default)

Auto Select Hop-less Path

The Auto Select Hop-less Path parameter specifies whether MPLS paths are explicitly specified during LSP creation or the LSP uses a completely loose path and the 5620 SAM selects the MPLS paths for the LSP. Table 19-1 describes the parameter options:

Table 19-1 Auto Select Hop-less Path parameter

Option	Option description
Disabled (default)	Specifies that you must manually choose or create the MPLS paths during LSP creation based on the source NE. IGP is used to identify the next hop.

(1 of 2)

Option	Option description
Enabled	Specifies a loose path. The 5620 SAM chooses the MPLS paths for the LSP. If no hopless path to the destination exists, the 5620 SAM creates one.

(2 of 2)

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 36.1.

Backup Hold Priority

(backupHoldPriority)

The priority of the backup session with respect to holding resources. The value 0 is the highest priority. Backup Holding Priority is used in deciding whether this session can be preempted by another session. The range is 0 to 7. The default is 0.

Backup Setup Priority

(backupSetupPriority)

The priority of the backup session with respect to taking resources. The value 0 is the highest priority. The Backup Setup Priority is used in deciding whether this session can preempt another session. The range is 0 to 7. The default is 0.

Backup Type

(fastRerouteBackupType)

The Backup Type parameter specifies the type of backup route associated with a failed link or LSP. Table 19-2 describes the parameter options.

Table 19-2 Backup Type parameter

Option	Option description	Dependencies
One To One	Specifies a backup LSP that intersects the original LSP downstream of the point of link or node failure. A separate backup LSP is established for each LSP that is backed up.	The parameter is configurable when the Fast Reroute parameter is set to true.
Many To One	Specifies that a single backup LSP is used to backup multiple original LSPs. This type of LSP is often called a bypass tunnel.	
facility	Specifies that a single backup LSP is used to backup multiple original LSPs. This type of LSP is often called a bypass tunnel.	

Collect Accounting Statistics

(accountingOn)

The Collect Accounting Statistics parameter specifies whether the collection of accounting statistics for the LSP is enabled. The options are:

- Enabled (default)
- Disabled

Collect Accounting Statistics

(egrAccountingOn)

The Collect Accounting Statistics parameter specifies whether the collection of egress accounting statistics for the dynamic LSP is enabled. The options are:

- Enabled (default)
- Disabled

Committed Rate

(committedRate)

The Committed Rate parameter specifies the mean traffic rate supported by the LSP. The committed rate is expressed in multiples of 1 Kb/s. The range is 1 to 1,000,000. The default is 100.

Description

See the [Description](#) parameter in section [36.1](#).

Destination IP Address

(destinationIpAddress)

The Destination IP Address parameter specifies the IP address of a path that is associated with the hop.

Destination Site ID

(destinationNodeId)

The Destination Site ID parameter specifies a destination interface for the LSP based on the site ID associated with the interface. The LSP must terminate on the system interface. You can manually configure the parameter or use the Select button to choose an NE.

Diff-Serv Backup Class Type

(teBackUpClassType)

The Diff-Serv Backup Class Type parameter specifies the backup Class Type associated with the LSP. It is only applicable to Dynamic LSPs.

When an LSP primary fails, MPLS will try a new path for the LSP using the main Class Type. If the first attempt fails, the head-end node performs subsequent retries using the backup Class Type. This applies to both CSPF and non-CSPF LSPs. It will retry up to the limit set in [Main Class Type Retry Limit](#).

When an unmapped LSP primary path goes into retry, it uses the main Class Type until the number of retries reaches the value configured for the [Main Class Type Retry Limit](#) parameter. If the path does come up, it starts using the backup Class Type.

The default value of -1 indicates that no backup Class Type has been configured for the LSP. The range is -1 to 7.

Diff-Serv Class Type

(teClassType)

The Diff-Serv Class Type parameter specifies the differentiated services class type to which the LSP or LSP path belongs. A differentiated services class type specifies the precedence that one type of traffic has over other traffic types. For example, voice traffic, which requires uninterrupted data flow, may have a higher precedence than other data. The range is 0 to 7, where 1 is the highest priority and 7 is the lowest priority. An LSP or LSP path belongs to class type 0 by default, which means that no class is configured.



Note — The parameter value at the LSP path level overrides the parameter value at the LSP level.

Displayed Name

(displayName)

The Displayed Name parameter specifies the LSP template name. The length is 1 to 32. There is no default.

Dynamic Bypass

(dynamicBypass)

The Dynamic Bypass parameter specifies whether dynamic bypass tunnels are enabled. The default is enabled.

Egress Label

(egressLabel)

The Egress Label parameter specifies the static hop egress label. The range is 0, and 16 to 1 048 575. The default is 0, which means that the parameter is not configured.

Egress Label

(egressLabelProtectSwap)

The Egress Label parameter specifies the static hop egress label when protection is in effect. The valid range is 0, and 16 to 1023. The default is 0. This parameter is configurable only when the “[Label Action](#)” parameter value is Swap/Protect- Swap.

Enable Auto-Bind

(enableAutoBinding)

The Enable Auto-Bind parameter specifies whether auto-binding is enabled on the LSP. This only applies to Dynamic LSPs. The options are:

- Enabled (default)
- Disabled

Enable CSPF

(cspfEnabled)

The Enable CSPF parameter specifies the CSPF routing algorithm to find a path that satisfies the constraints for the LSP. The constraints associated with the LSP can be related to bandwidth, class of service, or the number of path hops. The options are:

- false (default)
- true

CSPF also calculates detour routes when you set the [Fast Reroute](#) parameter to true. CSPF is not implemented if you define each hop in the LSP.

Enable SRLG

(enableSrlg)

The Enable SRLG parameter specifies whether the use of SRLG constraints is enabled for the computation of a secondary path for an LSP at the head-end LER. When the parameter is selected, the use of SRLG constraints in the computation is enabled.

- enabled
- disabled (default)



Note — The parameter applies only to standby and secondary paths.

Enable TE Metric

(enableTeMetric)

The Enable TE Metric parameter specifies whether the TE metric is used for the LSP path computation by CSPF. The options are:

- true
- false (default)

Fast Reroute

(fastRerouteEnabled)

The Fast Reroute parameter specifies a pre-computed detour LSP from each node in the path of the LSP. In case of failure of a link or LSP between two nodes, traffic is immediately rerouted on the pre-computed detour LSP. The immediate reroute of the traffic avoids packet-loss. The options are:

- false
- true (default)

Fast reroute is available only for the primary path. The LSP transit hops do not require configuration. The ingress router signals intermediate routers using RSVP to set up the detour routes. You must set the Enable CSPF parameter to true when you set the Fast Reroute parameter to true.

Groups Excluded (bitmap)

(adminGroupExclude)

The Groups Excluded parameter specifies the MPLS administrative groups for an LSP that are created using the tunnel template. The parameter value is an integer that represents a bit mask that is created using the Value (value) parameter setting of each excluded group. The range is 0 to 31. The default is 0.

As an example, Table 19-4 lists some MPLS administrative groups and the Groups Excluded parameter value that represents the groups.

Table 19-3 Groups Included parameter configuration example

MPLS administrative group name	Value parameter setting	Bit mask value	Groups Excluded parameter value (integer)
Group 1	1	00001	7, which represents the resulting bit mask of 00111
Group 2	2	00010	
Group 3	4	00100	

Groups Included

(all)(bitmap)(adminGroupIncludeAll)

The Groups Included (all) (bitmap) parameter specifies that all MPLS administrative groups for an LSP is created using the tunnel template.

Groups Included

(bitmap)(adminGroupInclude)

The Groups Included parameter specifies the MPLS administrative groups for an LSP that are created using the tunnel template. The parameter value is an integer that represents a bit mask created using the Value (value) parameter setting of each required group. The range is 0 to 31. The default is 0.

As an example, Table 19-4 lists some MPLS administrative groups and the Groups Included parameter value that represents the groups.

Table 19-4 Groups Included parameter configuration example

MPLS administrative group name	Value parameter setting	Bit mask value	Groups Included parameter value (integer)
Group 1	1	00001	7, which represents the resulting bit mask of 00111
Group 2	2	00010	
Group 3	4	00100	

Guarded Destination

(guardingDestinationAddress)

The Guarded Destination parameter specifies the IP address of the destination NE that is being protected by the guarding LSP. All LSPs passing through a node with this address as the last hop IP address is protected by the guarding LSP. Configure a valid IP address for this parameter.

Guarding Lsp

(guardingLsp)

The Guarding Lsp parameter is used to enable an LSP to be used as a guarding LSP. A guarding LSP protects a configurable guarding destination and is used as a bypass LSP by LSPs that have Fast Reroute enabled. The options are:

- Enabled
- Disabled (default)

Hold Priority

(holdPriority)

The priority of the session with respect to holding resources. The value 0 is the highest priority. Holding Priority is used in deciding whether this session can be preempted by another session. The range is 0 to 7. The default is 0.

Hop Index

(index)

The Hop Index parameter specifies the position of the hop in the ordered hop list. The range is 1 to 1024. There is no default. The value is incremented for each new hop.

Hop Limit

Table 19-5 lists where to find information about the hop limit parameter.

Table 19-5 Hop Limit parameter

Parameter	See
hop limit for LSP path	Hop Limit parameter in this section
hop limit for fast reroute lsp path	Hop Limit parameter in this section

Hop Limit

(fastRerouteHopLimit)

The Hop Limit parameter specifies the maximum number of hops for a fast reroute LSP path before the LSP path merges with the main LSP path. This parameter controls the number of loose hops associated with MPLS paths. The range is 0 to 255. The default is 16.

Hop Limit

(hopLimit)

The Hop Limit parameter specifies the maximum number of hops for the LSP path. An LSP is not set up if the hop limit is exceeded. This parameter controls the number of loose hops associated with MPLS paths. If there is an associated Inherit Value parameter, then the Hop Limit parameter is configurable only when you set the Inherit Value parameter to Disabled. The range is 2 to 255. The default is 255.

ID

See the [ID](#) parameter in section 36.1.

ID

(instanceId)

The ID parameter specifies the unique identifier for the MPLS path. The range is 1 to 65535. The default is 0.

Include ADSPEC in RSVP

(addSpec)

The Include ADSPEC in RSVP parameter specifies the inclusion of advertising data (ADSPEC) objects in the RSVP messages associated with LSPs. The options are:

- false (default)
- true

IGP Shortcut Enabled

(igpShortcut)

The IGP Shortcut Enabled parameter specifies whether to exclude or include an RSVP LSP from being used as a shortcut while resolving IGP routes. When this parameter is enabled, the RSVP LSP is used as a shortcut while resolving such routes. The parameter is only applicable to Dynamic LSPs.

By default, all RSVP LSPs originating on a node that has [RSVP Shortcut Enabled](#) enabled, are included by OSPF and IS-IS as direct links, as long as the destination address of the LSP corresponds to the router-id of a remote node. RSVP LSPs with a destination address corresponding to an interface address of a remote node are automatically not considered by IS-IS or OSPF. You can however, exclude a specific RSVP LSP from being used as a shortcut for resolving IGP routes by disabling this parameter. The options are:

- enabled (default)
- disabled

Ingress Label

(ingressLabel)

The Ingress Label parameter specifies the value of the static hop ingress label. The range is 0, and 32 to 1023. The default is 0, which means that the parameter is not configured.

Inherit Value

(propertyInheritance)

The Inherit Value parameter specifies if you want the LSP path to inherit the value of the property associated with this parameter. If you enable this, then the associated parameter takes its value from the parent LSP. If you disable it, then the associated parameter can be configured on the LSP path. The options are:

- Enabled (default)
- Disabled

Interface Name

(interfaceName)

The Interface Name parameter specifies the interface of this hop site. Choose an address by clicking on the Select button. There is no default.

IP Address

(ipAddress)

The IP Address parameter specifies the IP address of the ingress router for the LSP. Specify an IPv4 address.

Label Action

(labelAction)

The Label Action parameter specifies how the static hop treats a received label. Table 19-6 describes the parameter options:

Table 19-6 Path Destination Matching parameter

Option	Description
unspecified (displayed default)	This option is displayed only until the Site ID parameter is configured. The option is not selectable.
Pop (functional default)	The site specified by the Site ID parameter is the last hop; the NE removes the label. The Ingress Label value must match the Egress Label value of the previous hop.
Swap	The site specified by the Site ID parameter is an intermediate hop. The Ingress Label value must match the Egress Label value of the previous hop. The Egress Label value must match the Ingress Label value of the next hop.
Swap/Protect-Swap	The FRR support defines an alternate static swap label-map to use if the next-hop segment goes down. The Site ID is used to specify the node on which the LSP will be created. The Interface name specifies the MPLS interface to use to forward the MPLS packets. The Egress label under the Egress group specifies the value with which the ingress label is replaced and the packet is forwarded to the destination specified by the next-hop. Similarly the Egress label under the Egress Protect-Swap group specifies an alternate value with which the ingress label is replaced and the packet is forwarded to the destination specified by next-hop if the primary route (defined under Egress Group) fails.

LDP over RSVP include

(ldpOverRsvp)

The LDP over RSVP include parameter specifies whether this LSP is available for LDP-over-RSVP usage. The options are:

- enabled (default)
- not enabled

Least-Fill Path Selection

(enableLeastFill)

The Least-Fill Path Selection parameter specifies whether the use of the least-fill path selection method for the computation of the path of this LSP is enabled. A least-fill path is the path with the largest available bandwidth. The options are:

- not enabled (default)
- enabled

Main Class Type Retry Limit

(mainCTRetryLimit)

The Main Class Type Retry Limit parameter specifies the number of attempts that are made before switching to the [Diff-Serv Backup Class Type](#).

When an unmapped LSP primary path goes into retry, it attempts to use the main Class Type until the number of retries reaches the value you configure. If the primary path still does not come up, it starts using the backup Class Type.

This parameter only applies to Dynamic LSPs, and has no effect on an LSP primary path which retries due to a failure event. If you enter a value of the Main Class Type Retry Limit that is greater than the value of the LSP's [Retry Limit](#) parameter, the number of retries stops when the LSP primary path reaches the value of the LSP's Retry Limit. The LSP's Retry Limit represents the upper limit on the number of retries. This applies to both CSPF and non-CSPF LSPs.

The range is 0 to 10 000. The default is 0, which means the LSP primary path retries indefinitely.

Make before Break

(adaptive)

The Make before Break parameter specifies the traffic rerouting method when you move traffic between primary and secondary LSP paths. The the make-before-break functionality ensures that the transition to the new path does not cause any traffic disruption.

For example, when the parameters of an already-established LSP are changed due to a user configuration modification, when the parameter is set to true the resources of the existing LSP are not released until a new path with the same LSP ID is established and passing the traffic seamlessly handed over from the old LSP.

When enabled for the LSP, the make-before-break functionality is implemented for the primary path and all the secondary paths of the LSP. The options are:

- false
- true (default)

Maximum Bandwidth (mbps)

(autoBWMaxBw)

The Maximum Bandwidth (mbps) parameter specifies the maximum that an auto-bandwidth allocation is allowed to request for an LSP. The range is 0 to 100 000. The default is 100 000.

Maximum Transmitted Frame Size

(negotiatedMtu)

The Maximum Transmitted Frame Size parameter specifies the maximum frame size allowed over an LSP path. The default is 0.

Metric

(metric)

The Metric parameter specifies a value for the LSP that the 5620 SAM uses to select from a set of LSPs that lead to the same egress NE. The 5620 SAM uses the LSP with the lowest metric value. The range is 1 to 65 535. The default is 1.

Minimum Bandwidth (mbps)

(autoBWMinBw)

The Minimum Bandwidth (mbps) parameter specifies the minimum that an auto-bandwidth allocation is allowed to request for an LSP. The range is 0 to 100 000. The default is 0.

Monitor Bandwidth

(autoBWMonitorBw)

The Monitor Bandwidth parameter specifies whether the collection and display of auto-bandwidth measurements is enabled for the LSP. The options are:

- true
- false (default)

Name

See the [Name](#) parameter in section 36.1.

Next Hop

(nextHopAddr)

The Next Hop parameter specifies the IP address of the next hop in dotted-decimal format. There is no default.

Next Hop

(nextHopAddrProtectSwap)

The Next Hop parameter specifies the IP address of the next hop in dotted-decimal format, when protection is in effect. The default is 0.0.0.0. This parameter is configurable only when the “[Label Action](#)” parameter value is Swap/Protect-Swap.

Node Protect

(nodeProtect)

The Node Protect parameter specifies node and link protection on the LSP. Node protection ensures that traffic from an LSP that traverses a neighboring router reaches the required destination. The parameter is configurable when the [Fast Reroute](#) parameter is set to true. The options are:

- false
- true (default)

Overflow Limit

(autoBWOverFlow)

The Overflow Limit parameter specifies the number of overflow samples that initiates an overflow auto-bandwidth adjustment attempt. The range is 0 to 10. The default is 0.

Overflow Limit Bandwidth (mbps)

(autoBWOverFlwBw)

The Overflow Limit Bandwidth (mbps) parameter specifies the minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as an absolute bandwidth, to count an overflow sample. The range is 0 to 100 000. The default is 0.

Overflow Limit Threshold (percent)

(autoBWOverFlwThreshold)

The Overflow Limit Threshold (percent) parameter specifies the minimum difference between the current bandwidth of the LSP and the sampled data rate, expressed as a percentage of the current bandwidth, to count an overflow sample. The range is 0 to 100. The default is 0.

Overridden Properties

(propertyInheritance)

The Overridden Properties parameter allows the operator to specify which attributes can be overridden when a tunnel template is applied to an existing LSP path.

P2MPId

(p2mpId)

The P2MPId parameter specifies an optional identifier for the P2MP LSP. The range is 0 to 65 535. The default is 0.

Pacing Interval (seconds)

(pacingInterval)

The Pacing Interval (seconds) parameter specifies the length of time for resync between each re-signal for an execution policy. The range is 0 to 300. The default is 5.

Path Preference

(preference)

The Path Precedence parameter specifies the path's priority precedence among configured standby paths on an LSP. This value is defined to give priority to a specific standby path over other lower priority standby or non-standby secondary paths. The range from lowest to highest priority is 1 to 255. The default is 255.

Peak Rate

(peakRate)

The Peak Rate parameter specifies the maximum traffic rate supported by the LSP. The peak rate is expressed in multiples of 1 Kb/s. The range is 1 to 1,000,000. The default is 100.

Permit Merge

(permitMerge)

The Permit Merge parameter specifies if transit routers can merge this session with other RSVP sessions for the purpose of reducing resource overhead on downstream transit routers. The options are:

- Disabled (default)
- Enabled

Persistent

(persistent)

The Persistent parameter specifies whether a LSP should be restored automatically after a failure occurs. The options are:

- Disabled (default)
- Enabled

Preference

(**preference**)

The Preference parameter specifies the route preference for the LSP. When multiple routes are available to a destination, the LSP uses the route with the lowest preference. The range is 1 to 255. The default is 7.

The parameter is used for load balancing between multiple LSPs that may exist between the ingress and egress managed devices. By default, load balancing is equal between all LSPs. To favor one LSP, lower the parameter value. The LSP with the lowest setting is used first.

Rebuild Timer

(**rebuildTimer**)

The Rebuild Timer specifies the number of seconds to rebuild routing tables when an LSP is rerouted. The range is 0 to 86 400. The default is 1800.

Record Actual Path

(**record**)

The Record Actual Path parameter specifies whether the labels at each NE are recorded and displayed for the LSP path, to indicate the hops in the LSP path. The options are:

- Disabled (default)
- Enabled

Record Actual Path

(**record**)

The Record Actual Path parameter specifies if the labels at each NE are recorded and displayed for the LSP path, to indicate the hops in the LSP path. The options are:

- record (default)
- No Record

Record Actual Route

(**recordRoute**)

The Record Actual Route parameter specifies if the LSP path is recorded at each NE after it has been signaled. The options are:

- Enabled
- Disabled (default)

Record Label

(recordLabel)

The Record Label parameter enables the recording of the LSP labels at each device that an LSP path traverses. The options are:

- Enabled
- Disabled (default)

Record Label

(recordLabel)

The Record Label parameter enables the recording of all LSP labels at each device that an LSP path traverses. The options are:

- record
- No Record (default)

Reserved Bandwidth

(bandwidth)

The Reserved Bandwidth parameter specifies the minimum amount of the MPLS path bandwidth to reserve for the LSP. The parameter is configurable when the Auto Select Hop-less Path parameter is enabled. The range is 0 to 100 00. A value of 0 indicates that the parameter is not configured.

Reserved Bandwidth (Mbps)

(fastRerouteBandwidth)

The Reserved Bandwidth (Mbps) parameter specifies the minimum amount of the MPLS path bandwidth to reserve for the LSP. The range is 0 to 100 00. A value of 0 indicates that the parameter is not configured.

Resignal

(resignal)

The Resignal parameter specifies whether to resignal information about the LSP when make-before-break functionality is enabled. The options are:

- Do Action
- N/A (default)

Retry Limit

(retryLimit)

The Retry Limit parameter specifies how many attempts are made to re-establish the LSP after an LSP failure. The range is 1 to 10 000. The default is 0, indicating an infinite number of retries.

Retry Timer (seconds)

(retryTimer)

The Retry Timer (seconds) parameter specifies the time before LSP re-establishment attempts after an LSP failure. The range is 1 to 600. The default is 30.

RSVP Reserve Style

(rsvpStyle)

The RSVP Reserve Style parameter specifies the RSVP reservation style. A reservation style is a set of control options that specify a number of supported parameters. The style information is part of the LSP configuration. Table 19-7 describes the parameter options.

Table 19-7 RSVP Reserve Style parameter

Option	Option description	Dependencies
Shared-Explicit (default)	This option specifies a shared reservation environment with an explicit reservation scope. A single reservation is created on a link that is shared by an explicit list of senders. Because each sender is explicitly listed in the RESV message, different labels can be assigned to different sender receiver pairs, thereby creating separate LSPs.	—
Fixed-Filter	Specifies a single reservation with an explicit scope. This reservation style specifies an explicit list of senders and a distinct reservation for each. A specific reservation request is created for data packets from a specific sender. The reservation scope is determined by an explicit list of senders.	

Sample Multiplier

(autoBWSampleMul)

The Sample Multiplier parameter specifies the multiplier for collection intervals in a sample interval. The range is 1 to 511. The default is 1.

Scheduled Task Description

(description)

The Scheduled Task Description parameter specifies the description of this association of a schedule and a scheduled task. The range is 0 to 254 characters.

Scheduled Task Name

(displayName)

The Scheduled Task Name parameter specifies the name of this association of a schedule and a scheduled task. You must configure the parameter. The range is 1 to 32 characters.

Sequencing Order

(sequencingOrder)

The Sequencing Order parameter identifies the order of re-signaling. The options are:

- Ascending (default)
- Descending

Sequencing Target

(sequencingTarget)

The Sequencing Target parameter identifies how LSP path candidates are identified for re-signaling. The options are:

- None (default)
- Source Address
- Operational Bandwidth
- Metric

Setup Priority

(setupPriority)

The priority of the session with respect to taking resources. The value 0 is the highest priority. The Setup Priority is used in deciding whether this session can preempt another session. The range is 0 to 7. The default is 0.

Show created object

The Show created object parameter specifies whether to open the properties form for the object that you are creating from the template. The options are:

- Enabled (default)
- Disabled

Site ID

(nodeId)

The Site ID specifies the IP address of this hop site. Choose an address by clicking on the Select button. There is no default.

Source IP Address

(sourceIpAddress)

The Source IP Address parameter specifies the IP address of the source L3 interface on the source NE. The LSP exits the source device from the system interface if you do not specify an L3 interface. You can manually enter a source IP address for the interface or choose an address by clicking on the Select button.

Source Site ID

(sourceNodeId)

The Source Site ID parameter specifies the IP address of the LSP source site. Click on the Select button to choose a site.

System ID (Loopback IP Address)

(systemAddress)

The System ID (Loopback IP Address) parameter specifies the IP address of the network element. Specify an IPv4 address.

Termination Validation

(tunnelDestinationMatching)

The Termination Validation parameter specifies whether the LSP path terminates on the destination NE. Table 19-8 describes the parameter options.

Table 19-8 Path Destination Matching parameter

Option	Description
Destination Site (default)	Specifies that the path terminates on the LSP destination.
Any	Specifies that the path is loose or hopless and can terminate on any NE

Type

(type)

The Type parameter specifies an LSP path type. An LSP path is an LSP which is associated with an MPLS path. Table 19-9 describes the parameter options.

Table 19-9 Type parameter

Option	Option description	Dependencies
primary	Specifies that the path is the preferred route through the network. Each LSP can have only one primary path.	This is the only type of path that can be configured when the LSP originates from a 7250 SAS-ES 2.0 NE.
standby	Specifies that the LSP can switch to this path if the primary path is unavailable. Standby paths are signaled when they are created and remain in a standby state until needed.	Not supported on the 7250 SAS-ES or 7250 SAS-ESA.
secondary	Specifies that the LSP can switch to this path if the primary path is unavailable. Secondary path are usually not signaled until the primary path fails.	On the 7250 SAS-ES or 7250 SAS-ESA, a primary path must already exist before you can create a secondary path.

View the newly created Bypass Only Lsp

The View the newly created Bypass Only Lsp parameter specifies whether you want to view the configuration information about the newly created LSP. The Bypass Only LSP child form displays the service tunnel configuration information. The options are:

- Enabled
- Disabled (default)

View the newly created Dynamic LSP

The View the newly created Dynamic LSP parameter specifies whether you want to view the configuration information about the newly created LSP. The Dynamic LSP child form displays the service tunnel configuration information. The options are:

- Enabled
- Disabled (default)

20 – MPLS Paths parameters

20.1 MPLS Paths parameters 20-2

20.1 MPLS Paths parameters

This chapter describes the parameters on the Create MPLS Path form and child forms.

Administrative

See the [Administrative State](#) parameter in section 36.1.

Description

See the [Description](#) parameter in section 36.1.

Hop Type

(type)

The Hop Type parameter specifies the method used to select the routing path between devices. Table 20-1 describes the parameter options.

Table 20-1 Hop Type parameter

Option	Option description	Dependencies
loose	Specifies that the LSP can traverse unspecified devices between configured hop devices in the provisioned MPLS path.	—
strict	Specifies that the LSP must take a direct path between configured hop devices in the provisioned MPLS path.	

Insert Hop

Click the Insert Hop button to insert a hop in the MPLS provisioned path. A hop can be an interface on an Alcatel-Lucent-managed NE or a third-party device.

IP Address

(destinationIpAddress)

The IP Address parameter specifies the IP address for the L3 interface that is associated with the destination site for the MPLS path. The parameter is configurable when you set the Specify Site parameter to By Selection. You can manually enter an IP address for the L3 interface or list and choose an address. You can list and choose an address by clicking the Select button beside the IP Address parameter. The Select button is only enabled after you select a managed device using the Network Element parameter.

IP Address

(ipAddress)

The IP Address parameter specifies the IP address of MPLS path hop. The parameter is configurable when the [Specify Site](#) parameter is set to Manually.

IP Address

(interfacePointer)

The IP Address parameter specifies the IP address of a hop in the MPLS path. The parameter is configurable when the [Specify Site](#) parameter is set to By Selection.

Name

See the [Name](#) parameter in section 36.1.

Specify Site

The Specify Site parameter specifies the method for configuring the destination site of the MPLS path. Table 20-2 describes the parameter options.

Table 20-2 Specify Site parameter

Option	Option description	Dependencies
Manually	Specifies that you must select the destination site for the MPLS path by manually entering the IP address.	—
By Selection	Specifies that you must select the destination site for the MPLS path by: <ul style="list-style-type: none"> listing and choosing the network element site ID or IP address using the Select buttons manually entering the IP address 	

Starting Network Element

Click the Select button to specify the starting network element for the MPLS path.

21 – Service Tunnels parameters

21.1 Service Tunnels parameters 21-2

21.1 Service Tunnels parameters

This chapter describes the parameters on the Manage Service Tunnels forms and child forms.

Access Adapt QoS

(accessAdaptQos)

The Access Adapt QoS parameter specifies how the Ethernet Tunnel Group SAP queue and virtual scheduler buffering and rate parameters are adapted over multiple active MDAs. This parameter is only available when the [Protection Type](#) parameter is set to Load Sharing. The options are:

- Link
- Distribute (default)

Administrative

See the [Administrative State](#) parameter in section [36.1](#).

Administrative MTU

(pathMtu)

The Administrative MTU parameter specifies the maximum packet size that is supported by the network interface. The range is 0 or 576 to 9194. The default is 4462. A value of zero indicates that the MTU should be computed dynamically from the corresponding MTU of the tunnel.

Administrative State

(classForwardingAdminState)

The Administrative State parameter specifies the administration state of the SDP. The options are:

- up
- down (default)

Advertised MTU Override

(advertisedMtuOverride)

The Advertised MTU Override parameter specifies whether you override the advertised VC-type MTU. The options are:

- false (default)
- true

APS Command

(apsCommand)

The APS Command parameter allows you to perform protection switch actions. Table 21-1 describes the options.

Table 21-1 APS Command parameters

Option	Option Description
No Command (default)	Indicates that no command has been written to the Ethernet tunnel endpoint. The property cannot be set to this value by the user after it has been previously set to another value.
Clear	Clears all the switch commands (other than “No Command”) for the Ethernet tunnel Path Endpoint. In addition, if the Revert Time (seconds) parameter on the Ethernet tunnel endpoint is a non-zero value (revertive mode), the active WTR (Wait To Restore) state is also cleared.
Lockout of Secondary	Prevents the primary (working) member from switching to the secondary (protection) member. This property can only be set to this value if the Precedence of the Ethernet tunnel Path Endpoint is set to “secondary”.
Force Switch Primary to Secondary	Switches the primary member to the secondary member. This property can only be set to this value if the Precedence of the Ethernet tunnel Path Endpoint is set to “primary”.
Manual Switch Primary to Secondary	Switches the primary member to the secondary member. This property can only be set to this value if the Precedence of the Ethernet tunnel Path Endpoint is set to “primary”.
Exercise	Exercises the protocol for a protection switch of the Ethernet tunnel Path Endpoint by issuing an Exercise request for that member and checking the response on the APS member.

The associated “Perform APS Command” button is used to perform the selected command on the path endpoint.

The APS Command is not available on creation and is only applicable if the [Protection Type](#) parameter is set to G8031 1:1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 36.1.

BW (Mbps)

(defaultLspBw)

The BW (Mbps) parameter specifies the minimum amount of the MPLS path bandwidth to reserve for the LSP. The parameter is not configurable for a mesh topology rule. It is configurable for other topology rule types only when the [Tunnel Type](#) parameter value or the [Underlying Transport](#) parameter value is RSVP-LSP. The range is 0 to 100 000. A value of 0 means that the parameter is not configured.

CCM Hold Time Down (deciseconds)

(holdDownTime)

The CCM Hold Time Down (deciseconds) parameter specifies the delay, in deciseconds, used for the hold timer of the associated Continuity Check (CC) session down event dampening. This guards against reporting excessive path operational state transitions. It is implemented by not advertising subsequent transitions of the CC state to the Ethernet Ring Element until the configured timer has expired. A value of 0 specifies that a down transition is reported immediately. The range is 0 to 5000. The default is 0.

CCM Hold Time Up (deciseconds)

(holdUpTime)

The CCM Hold Time Down (deciseconds) parameter specifies the delay, in deciseconds, used for the hold timer of the associated Continuity Check (CC) session up event dampening. This guards against reporting excessive path operational state transitions. It is implemented by not advertising subsequent transitions of the CC state to the Ethernet Ring Element until the configured timer has expired. A value of 0 specifies that an up transition is reported immediately. The range is 0 to 5000. The default is 20.

CFM Test

(ccTestPointer)

The CFM Test parameter specifies a pointer to an existing CC Test. This is the CC Test under which MEPs for the Ethernet tunnel path endpoints under the Ethernet tunnel path are created.

Class Forwarding Capability

(classForwardingEnabled)

The Class Forwarding Capability parameter specifies whether forwarding a service packet over the SDP, based on the class of service of the packet is enabled. The options are:

- On
- Off (default)

Compatible Version

(compatibleVersion)

The Compatible Version parameter specifies the backward compatibility logic for an ethernet ring. Table [21-2](#) describes the options.

Table 21-2 Compatible Version parameter

Option	Option Description
Version 1	The Force Switch and Manual Switch tool commands are not supported and the Revert Time (seconds) parameter must be set to a non-zero value. Use this option if there is a node in the ethernet ring that follows version 1 of the ITU-T G.8032 standard.
Version 2 (default)	The restrictions listed for the Version 1 option do not apply.

Collect Accounting Statistics

(accountingOn)

The Collect Accounting Statistics parameter specifies whether the collection of accounting statistics on the SDP is enabled. The options are:

- Enabled (default)
- Disabled

Configured MAC Address

(macAddress)

The Configured Mac Address parameter assigns a specific MAC address to an Ethernet tunnel endpoint. If this parameter is left at its default value, a default MAC address is assigned by the system from the chassis MAC address pool.

Control Tag (Inner Encapsulation Value)

(endpointAInnerControlTag)

The Control Tag (Inner Encapsulation Value) parameter specifies the inner encapsulation value for the control tag property of Path Endpoint A. The parameter is configurable only on Release 8.0 and later NEs, and only when the Ethernet tunnel endpoint [Encap Type](#) value is Q in Q. The range is 0 to 4095. The default is 0.

The parameter cannot be modified after it is set. To replace an existing control tag, you must delete and recreate the parent path, and then specify a new control tag.

Control Tag (Inner Encapsulation Value)

(endpointBInnerControlTag)

The Control Tag (Inner Encapsulation Value) parameter specifies the inner encapsulation value for the control tag property of Path Endpoint B. The parameter is configurable only on Release 8.0 and later NEs, and only when the Ethernet tunnel endpoint [Encap Type](#) value is Q in Q. The range is 0 to 4095. The default is 0.

The parameter cannot be modified after it is set. To replace an existing control tag, you must delete and recreate the parent path, and then specify a new control tag.

Control Tag (Outer Encapsulation Value)

(endpointAControlTag)

The Control Tag (Outer Encapsulation Value) parameter specifies the outer encapsulation value for the control tag property of Path Endpoint A. The parameter is configurable only on Release 8.0 and later NEs, and only when the Ethernet tunnel endpoint [Encap Type](#) value is Q in Q. The range is -1 to 4095. The default is -1.

The parameter specifies the VLAN ID for Ethernet CFM and G.8031 control plane exchanges, and cannot be modified after it is set. To replace an existing control tag, you must delete and recreate the parent path, and then specify a new control tag.

Control Tag (Outer Encapsulation Value)

(endpointBControlTag)

The Control Tag (Outer Encapsulation Value) parameter specifies the outer encapsulation value for the control tag property of Path Endpoint B. The parameter is configurable only on Release 8.0 and later NEs, and only when the Ethernet tunnel endpoint [Encap Type](#) value is Q in Q. The range is -1 to 4095. The default is -1.

The parameter cannot be modified after it is set. To replace an existing control tag, you must delete and recreate the parent path, and then specify a new control tag.

Control Tag (Outer Encapsulation Value)

(controlTag)

The Control Tag (Outer Encapsulation Value) parameter specifies the VLAN-ID to be used for Ethernet CFM and G.8031 control plane exchanges. This parameter cannot be edited after it is set. To replace an existing control tag, the parent path needs to be deleted and recreated before a new control tag can be specified. The range is -1 to 4094, and 8191. The value 8191 specifies that the SAP is a Control SAP, and it can only be set when the tunnel's [Protection Type](#) parameter is set to "Load Sharing". The default value is -1.

Description

See the [Description](#) parameter in section [36.1](#).

Destination Site ID

(destinationNodeId)

Click on the Select button to list and choose the destination router for the service tunnel.

Element ID

(elementId)

The Element ID parameter specifies a unique identifier for the ethernet ring. The range is 1 to 128. The default is 0, which means that the ID is automatically assigned.

Enable BGP-Tunnel

(**bgpTunnelEnabled**)

The Enable BGP-Tunnel parameter specifies whether the transport tunnel uses BGP, as opposed to LDP or RSVP-signaled LSPs. This parameter cannot be set to true if either the [Enable LDP](#) or [Mixed Lsp Mode](#) parameters are set to true, or if there is at least one RSVP or static LSP provisioned.



Note — You can have an operational BGP tunnel only when the source and destination NEs belong to different AS.

The parameter is configurable only on MPLS SDPs that use BGP route tunnels to extend inter-AS support for the following services on a Release 8.0 or later 7450 ESS, 7710 SR, or 7750 SR in chassis mode C:

- Layer 2 services (all VPLS and VLL types)
- VPRN services (supported at the site level only, not the interface level)

The parameter options are:

- true
- false (default)

If the Enable BGP-Tunnel parameter is set to false, then [Keep-Alive Enabled](#) and [Mixed Lsp Mode](#) are set to true, and the [Revert Time \(seconds\)](#) parameter is displayed.

Enable LDP

(**ldpEnabled**)

The Enable LDP parameter specifies whether LDP is enabled on the routing instance. The options are:

- false (default)
- true

Enable Per Forwarding Path Ingress Queue

(**perFpIngQueuing**)

The Enable Per Forwarding Path Ingress Queue parameter specifies whether or not a more efficient method of queue allocation for Ethernet Tunnel Group SAPs should be utilized. This parameter is only available when the [Protection Type](#) parameter is set to Load Sharing. The options are:

- enabled
- disabled (default)

Encap Type

(encapType)

The Encap Type parameter specifies the encapsulation type of the ports that can be used as the member ports for the Path Endpoints of an Ethernet tunnel endpoint. Table 21-3 lists the parameter options and dependencies.

Table 21-3 Encap Type parameter

Option	Dependencies
Dot1 Q (default)	—
Q in Q	Release 8.0 or later NEs only

Enforce Diff-Serv Lsp-Fc Map

(enforceDiffServLspFcMap)

The Enforce Diff-Serv Lsp-Fc Map parameter specifies whether the FC to LSP mapping must conform to the Diff-Serv FC to Class Type mapping.

When this parameter is enabled, 5620 SAM queries RSVP to determine if the FC is supported by the LSP. RSVP checks if the FC maps to the CT of the LSP. If the FC is already configured on the LSP and the FC does not map to the CT of the LSP, then the 5620 SAM blocks the enabling of the Enforce Diff-Serv Lsp-Fc Map option.

The SDP continues to enforce the mapping of a single LSP per FC. However, when the Enforce Diff-Serv Lsp-Fc Map parameter is enabled, RSVP also enforces the use of a single CT per FC, as per the user-configured mapping in RSVP.

The options are:

- On
- Off (default)

Ethernet Ring ID

(subRingInterconnectId)

The Ethernet Ring ID parameter specifies the ethernet ring ID to which a sub-ring is interconnected. The parameter is configurable when the [Type](#) parameter is set to Virtual Link or Non Virtual Link. In the case of Non Virtual Link, the Ethernet Ring ID parameter must be set to a value of 4294967295, which indicates that the sub-ring is interconnected to a VPLS.

The parameter range is 0 to 4294967295. The default is 0.

Ethernet Tunnel Endpoint Control SAP

(ethTunnelControlSap)

The Ethernet Tunnel Endpoint Control SAP parameter indicates if this is a Control SAP. It is only available for SAPs that have an Ethernet Tunnel Endpoint as the Terminating Port. If the parameter is enabled, then the value of the [Outer Encapsulation Value](#) parameter is automatically set to 8191. The options are:

- enabled
- disabled (default)

FRR

(defaultLspFrr)

The FRR parameter specifies whether fast reroute is enabled for the service tunnel. The parameter is configurable when the [Tunnel Type](#) parameter value or the [Underlying Transport](#) parameter value is RSVP-LSP.

- Enabled (default)
- Disabled

Group Name

See the [Name](#) parameter in section 36.1.

Guard Time (deciseconds)

(guardTime)

The Guard Time (deciseconds) parameter specifies the guard time, in deciseconds, of an Ethernet Ring Element. It is used to prevent the ring element from acting upon outdated R-APS messages and prevent the possibility of forming a closed loop. While the guard timer is running, any received R-APS Request/State and Status information is blocked and not forwarded to the priority logic. When the guard timer is not running, the R-APS Request/State and Status information is forwarded unchanged. The range is 1 to 20. The default is 5.

Guard Time (centiseconds)

(guardTime)

For OmniSwitch configuration, the Guard Time (centiseconds) parameter specifies the guard time, in centiseconds, of an Ethernet Ring Element. The range is 1 to 200. The default is 50. See [Guard Time \(deciseconds\)](#) for more information.

Hello Message Length

(helloMessageLength)

The Hello Message Length parameter specifies the length of SDP echo request messages that are transmitted on the SDP. The range is 0, or 40 to 9198. The default is 0. The default value of 0 indicates that the message length should be equal to the MTU, as specified by the [Administrative MTU](#) parameter.

Hello Request Timeout

(helloRequestTimeout)

The Hello Request Timeout parameter specifies how long, in seconds, to wait for an acknowledgement of the SDP echo request message before a neighbor is declared down. The range is 1 to 10. The default is 5.

Hello Time

(helloTime)

The Hello Time parameter specifies how long, in seconds, the SDP echo request messages are transmitted on the SDP. The range is 1 to 3600. The default is 10.

Hold Down Time

(holdDownTime)

The Hold Down Time parameter specifies how long, in seconds, the SDP remains in the operationally down state in response to SDP keep-alive monitoring. The range is 1 to 3600. The default is 10.

Hold Time Down

(holdTimeDown)

Table 21-4 describes the Hold Time Down parameter options.

Table 21-4 Hold Time Down parameter

Object type	Parameter description
Ethernet tunnel	Hold Time Down (centiseconds) The Hold Time Down (centiseconds) parameter specifies the delay, in centiseconds, between detecting that the member path is down and reporting it to the G.8031 protection module. This parameter applies only to member path CCM and not to the member port link state. The parameter refers to both the global tunnel and the tunnel endpoint. The default is 0. The range is 0 to 1000.
Ethernet Ring	Hold Time Down (deciseconds) The Hold Time Down (deciseconds) parameter specifies the delay, in deciseconds, between detecting that the member path is down and reporting it to the G.8032 protection module. This parameter applies only to member path CCM and not to the member port link state. The parameter refers to both the global ring and the ring endpoint. The default is 0. The range is 0 to 5000.

Hold Time Up (deciseconds)

(holdTimeUp)

The Hold Time Up parameter specifies the delay, in deciseconds, used for the hold-timer for associated CC Session up event dampening. The parameter refers to both the global tunnel/ring and the tunnel/ring endpoint. The default is 20. The range is 0 to 5000.

ID

(id)

The ID parameter specifies a unique identifier for the Ethernet Ring Element. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 128 for other than OmniSwitch NEs. The default is 0. For OmniSwitch NEs the range is 1 to 2147483647.

ID

(id)

The ID parameter specifies a unique ID for the global Ethernet path. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 16. The default is 0.

ID

(pathId)

The ID parameter specifies a unique ID for the service tunnel. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 17 407. The default is 0.

Interconnected Ethernet Ring Element

(elementAInterconnectId or elementBInterconnectId)

The Interconnected Ethernet Ring Element parameter specifies a unique identifier for an Ethernet Ring Element. The default is 0. The range is 1 to 2147483647. When the [Type](#) parameter is set to Non Virtual Link, the Interconnected Ethernet Ring Element parameter must be set to a value of 4294967295, which indicates that the ring is interconnected to a VPLS.

Keep-Alive Enabled

(keepAliveOn)

The Keep-Alive Enabled protocol specifies whether SDP echo request and reply messages are used to monitor service tunnel (SDP) connectivity. The operating state of the SDP is affected by the keep-alive state on the SDP ID. SDP echo request messages are only sent when the SDP ID is configured and administratively up. When the SDP ID is administratively down, keep-alive messages for that SDP ID are disabled. The options are:

- Enabled
- Disabled (default)

Max Drop Count

(maxDropCount)

The Max Drop Count parameter specifies the number of failed responses to an SDP echo request before the SDP changes to a down state. The range is 1 to 5. The default is 3.

Member Port

(ctpPointer)

The Member Port parameter associates a port with an Ethernet Tunnel or Ethernet Ring Path Endpoint. After the parameter is set, the member port cannot be modified.

Member Port

(endpointACtpPointer)

The Member Port parameter associates a port with Ethernet Tunnel Path Endpoint A. After the parameter is set, the member port cannot be modified.

Member Port

(endpointBCtpPointer)

The Member Port parameter associates a port with Ethernet Tunnel Path Endpoint B. After the parameter is set, the member port cannot be modified.

Metric

(metric)

The Metric parameter specifies a value used by a tunnel table manager to determine a route. The parameter value helps identify the preferred route when multiple SDPs with the same destination exist. The preferred route is the route with the lowest parameter value. The range is 1 to 65 535. The default is 0.

Mgr ID

(ID)

The Mgr ID parameter specifies a unique identifier for the ethernet ring. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 1000000999999. The default is 0, with the associated Auto-Assign ID parameter enabled.

Mixed Lsp Mode

(mixedLspMode)

The Mixed Lsp Mode parameter specifies whether RSVP and LDP LSPs can co-exist in the SDP. The parameter is configurable on a Release 8.0 or later 7450 ESS, 7710 SR, or 7750 SR. When both RSVP and LDP are enabled on an SDP, the SDP can switch from using RSVP LSPs to LDP LSPs in the event that all RSVP LSP paths fail. The options are:

- true (default)
- false

When the Mixed Lsp Mode parameter is set to true, the [Revert Time \(seconds\)](#) parameter is configurable.

If you try to set the Mixed Lsp Mode parameter to false while there is at least one RSVP LSP associated with this SDP, 5620 SAM will reject your update and an error message will be issued.



Note — LDP has an associated timer parameter named [Tunnel Down Damp Time \(seconds\)](#) which is set to 3 seconds by default. This parameter specifies how long an LDP waits before sending a tunnel down event to the route table manager. When the LDP fails, the SDP will revert to the RSVP LSP only after the expiry of this timer. For an immediate switchover, this timer must be set to 0 seconds.

Name

See the [Name](#) parameter in section [36.1](#).

Naming Format

(namingFormat)

The Naming Format parameter specifies the naming format for the generated tunnel elements. System generated naming format configuration is similar to other naming formats within 5620 SAM. The user specified naming format allows the operator to attach a prefix to the tunnel ID to identify the tunnel. For example, add LSP to all LSP tunnels to distinguish them from SDP tunnels. The options are:

- System Generated (default)
- User Specified

No VLAN VC Ethertype

The No VLAN VC Ethertype parameter specifies whether a [VLAN VC Ethertype](#) parameter can be specified. When the No VLAN VC Ethertype parameter is enabled the [VLAN VC Ethertype](#) parameter cannot be set. The options are:

- enabled (default)
- disabled

Operational Path Endpoint Threshold

(pathThreshold)

The Operational Path Endpoint Threshold parameter specifies how many paths must be operationally up for the ethernet tunnel to be operationally up. When the number of operationally up paths is less than or equal to this threshold, the tunnel will become operationally down. This parameter is only available when the [Protection Type](#) parameter is set to Load Sharing. The range is 0 to 15. The default is 0.

Order

The Order parameter specifies whether the group is ordered or unordered. The options are:

- unordered (default)
- ordered

Path Endpoint

(pathEndpointAPointer)

The Path Endpoint parameter specifies a pointer to an existing Ethernet tunnel path endpoint. This parameter should be set if you add an existing Ethernet tunnel path endpoint to an Ethernet tunnel path.

Path Endpoint

(pathEndpointBPointer)

The Path Endpoint parameter specifies a pointer to an existing Ethernet tunnel path endpoint. This parameter should be set if you add an existing Ethernet tunnel path endpoint to an Ethernet tunnel path.

Path Endpoint Type

(pathEndpointRplType)

The Path Endpoint Type parameter specifies if the ethernet ring path endpoint acts as an RPL End or is in the normal state. This parameter is only configurable if the [Ring Protection Link Type](#) parameter is set to Owner or Neighbor. The options are:

- Normal (default)
- Ring Protection Link End

Path ID

(pathId)

The Path ID parameter specifies a unique ID for the Ethernet endpoint. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 16. The default is 0.

Path ID

(endpointAPathId)

The Path ID parameter specifies a unique ID for the primary Ethernet endpoint. The range is 1 to 16. The default is 0.

Path ID

(endpointBPathId)

The Path ID parameter specifies a unique ID for the secondary Ethernet endpoint. The range is 1 to 16. The default is 0.

PBB Ethernet Type

(pbbEtype)

The PBB Ethernet Type parameter specifies the addressing space available in the Ethernet frame. The range is 1536 to 65 535. The default is 35 047.

Precedence

(precedence)

The Precedence parameter specifies the precedence of the Ethernet endpoint path. The options are:

- primary
- secondary (default)

Precedence

(endpointAPrecedence)

The Precedence parameter specifies the precedence of the first Ethernet endpoint path.

Precedence

(endpointBPrecedence)

The Precedence parameter specifies the precedence of the second Ethernet endpoint path.

Propagate Topology Change

(subRingPropTopChange)

The Propagate Topology Change parameter specifies whether propagation of topology changes from the interconnected ring to the ethernet sub-ring is enabled. The default is False.

Protection Type

(protectionType)

The Protection Type parameter specifies the protection mode for the global tunnel and the tunnel endpoints. The options are:

- G8031 1:1 (default)
- Load Sharing

R-APS Tag (Inner Encapsulation Value)

(endpointAInnerEncapValue)

The R-APS Tag (Inner Encapsulation Value) parameter specifies the inner encapsulation value for the R-APS tag property of Path Endpoint A. The range is 0 to 4094. The default value is 0.

R-APS Tag (Outer Encapsulation Value)

(endpointAOuterEncapValue)

The R-APS Tag (Outer Encapsulation Value) parameter specifies the outer encapsulation value for the R-APS tag property of Path Endpoint A. The range is 0, and 1 to 4094. The default value is 0.

Revert Time (seconds)

(revertTime)

Table [21-5](#) describes the Revert Time (seconds) parameter options.

Table 21-5 Revert Time (seconds) parameter

Object type	Parameter description
IP/MPLS tunnel	The Revert Time (seconds) parameter specifies the amount of time to wait before reverting back from LDP to an associated LSP, when it becomes available. This only applicable while the Mixed Lsp Mode parameter is set to true. The range is -1 to 600 seconds, and the default value is 0. Setting the parameter to -1 will cause the system to never revert.
Ethernet tunnel	The Revert Time (seconds) parameter specifies the time in seconds to wait before trying to revert to the primary path defined on the service endpoint, after having failed over to a secondary path. An attempt to revert to the primary path is only made if the primary path has been restored to the Ethernet Tunnel. The range is 0 to 720. The default is 0, which indicates a non-revertive operation. The local revert time is inherited from the global revert time, but can be configured.
Ethernet Ring	Specifies the Wait-To-Restore (WTR) timer, in seconds. The WTR timer is used to prevent frequent operation of the protection switching due to intermittent signal failure defects. The range is 60 to 720 seconds. A value of 0 puts the Ethernet Ring Element into a non-revertive mode.

Revert Time (minutes)

([revertTime](#))

For OmniSwitch configuration, the Revert Time (minutes) parameter specifies the revert time, in minutes, of an Ethernet Ring Element. The range is 0 to 12. The default is 5. See [Revert Time \(seconds\)](#) for more information.

Ring Node ID

([ringNodeId](#))

The Ring Node ID parameter specifies the MAC address of the Ethernet Ring Element. The default value is 00:00:00:00:00:00, which resets the parameter to the system's MAC address.

Ring Protection Link Type

([rplType](#))

The Ring Protection Link Type parameter specifies the Ring Protection Link (RPL) type of the Ethernet Ring Element. The options are:

- None: the Ethernet Ring Element is not designated as either an RPL Owner or Neighbor.
- Owner: the Ethernet Ring Element is adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions. It is the responsibility of the RPL Owner for activating reversion behavior from protected or MS/FS conditions.
- Neighbor: the Ethernet Ring Element is adjacent to the RPL that is responsible for blocking its end of the RPL under normal conditions, in addition to the block by the RPL Owner node. The Ethernet Ring Element is not responsible for activating the reversion behavior.

The default is None.



Note — For OmniSwitch NEs, the Neighbor option is not applicable.

SDP Bandwidth Booking Factor (%)

(bookingFactor)

The SDP Bandwidth Booking Factor (%) parameter is used to calculate the maximum SDP available bandwidth, specified as the percentage of the SDP maximum available bandwidth for VLL call admission. When the value of the SDP Bandwidth Booking Factor is set to zero, no new VLL spoke SDP bindings with non-zero bandwidth are permitted with this SDP. Overbooking in excess of 100% is allowed. The range is 0 to 1000. The default is 100.

Show created object

The Show created object parameter specifies whether to open the properties form for the object that you are creating from the template. The options are:

- Enabled (default)
- Disabled

Signaling

(signallingType)

The Signaling parameter specifies the signaling protocol that is used to obtain the ingress and egress labels in frames transmitted and received on the service tunnel. When the parameter is set none (manual), the labels must be configured when the service tunnel is bound to a service. The signaling value can only be changed when the administrative status of the SDP is down. Table [21-6](#) describes the parameter options.

Table 21-6 Signaling Type parameter

Option	Option description	Dependencies
TLDP (default)	Specifies that the ingress and egress signaling auto labelling is enabled.	—
BGP	Specifies that the ingress and egress pseudowire signaling uses BGP to obtain the ingress/egress PW labels in frames transmitted and received on an SDP. This is the default value when a BGP VPLS automatically instantiates the SDP.	—
None (manual)	Specifies that the ingress and egress signal auto-labeling is not enabled. Each service that uses the specified SDP must use configured VPN labels.	—

Site ID

(endPointSiteId)

The Site ID parameter specifies the IP address for site on which the endpoint is located. Specify an IPv4 address in dotted-decimal format. There is no default.

Source Site ID

(siteId)

Click on the Select button to list and choose the source router for the service tunnel.

Template Versions

(templateVersionsPreference)

The Template Versions parameter specifies which version of the template is to be used for the rule. This option is necessary since a template can be updated after it has been applied to a rule. Rule configuration provides two options, it is recommended that you use the version initially assigned to the rule. If you choose the latest version, ensure that the version and the rule are compatible. The options are:

- Apply Versions Initially Assigned (default)
- Apply Latest Versions

Transport Destination Address

(transportDestAddr)

The Transport Destination Address parameter specifies the IP address of the remote end of the transport tunnel for the SDP. The value can only be changed when the administrative status of the SDP is down. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0 (or the same IPv4 address as the Destination Site ID).

Tunnel Creation Pacing Interval (seconds)

(**pacingInterval**)

The Tunnel Creation Pacing Interval (seconds) parameter specifies the time delay between tunnel creations. A delay allows the network time to converge. The range is 0 to 300 seconds. When the value is set to 0, no delay is set.

Tunnel Endpoint ID

(**tunnelEndpointId**)

The Tunnel Endpoint ID parameter specifies an identifier for the tunnel endpoint. The range is 1 to 1024. The number is inherited from the Tunnel ID but it can be changed.

Tunnel ID

(**tunnelId**)

The Tunnel ID parameter specifies an identifier for the tunnel. The range is 1 to 1024.

Tunnel Type

(**tunnelType**)

The Tunnel Type parameter specifies the type of service tunnel to create. The options are:

- SDP (default)
- RSVP-LSP

Type

(**EthRingSubRingType**)

The Type parameter specifies whether an ethernet ring is a sub-ring. Table [21-7](#) describes the parameter options.

Table 21-7 Type parameter

Option	Option description	Dependencies
None	Specifies that the ethernet ring is not a sub-ring.	—
Virtual Link	Specifies that the ethernet ring is a sub-ring with an R-APS virtual channel.	—
Non Virtual Link	Specifies that the ethernet ring is a sub-ring without an R-APS virtual channel.	—

Underlying Transport

(underlyingTransport)

The Underlying Transport parameter specifies the underlying transport protocol for the service tunnel. Table 21-8 describes the parameter options.

Table 21-8 Underlying Transport parameter

Option	Option description	Dependencies
GRE	Specifies a service tunnel that uses GRE encapsulation	—
MPLS:LDP	Specifies a service tunnel that uses MPLS:LDP encapsulation	
MPLS:BGP	Specifies a service tunnel that uses MPLS:BGP encapsulation	
RSVP-LSP	Specifies a service tunnel that uses RSVP-LSP encapsulation	
Mixed LSP Mode	Specifies a service tunnel that uses either RSVP-LSP or MPLS-LDP encapsulation.	
IPv4	Specifies a service tunnel that uses IPv4 encapsulation	

See the [Transport Type](#) parameter for more information on the MPLS:BGP and Mixed LSP Mode options.

User Specified Naming Prefix

(userSpecifiedNamingPrefix)

The User Specified Naming Prefix parameter specifies the naming prefix when the [Naming Format](#) parameter is set to User Specified. The range is 0 to 20 characters.

Value

(value)

The Value parameter specifies a unique value assigned to this Steering Parameter. The range is 0 to 31. There is no default value.

VC Type

(vcType)

The VC Type parameter specifies the default VC type signaled for the circuit-to-service-tunnel binding to the far end of a service tunnel. The actual signaling of the VC type depends on the signaling parameter defined for the service tunnel. The options are:

- Ethernet (default)
- VPLS
- VLAN

View the newly created tunnel

The View the newly created Dynamic LSP parameter specifies whether you want to view the configuration information about the newly created LSP. The Dynamic LSP child form displays the service tunnel configuration information. The options are:

- Enabled
- Disabled (default)

VLAN VC Ethertype

(vlanVcEtherType)

The VLAN VC Ethertype parameter specifies the Ethertype used in frames sent out when the VC type is VLAN. The range is 1536 to 65 535. The default is 33 024.

VLAN VC Tag

(vlanVcTag)

The VLAN VC Tag parameter specifies a dot1q value for encapsulation to the far end of the service tunnel. The range is 0 to 4095. The default is None.

VPLS

The VPLS parameter specifies whether ethernet ring element interconnection is enabled through VPLS. The VPLS parameter is configurable when the [Type](#) parameter is set to Non Virtual Link. When the VPLS parameter is set to True, the [Ethernet Ring ID](#) parameter is set to 4294967295. The default is False.

22 – IPsec VPN parameters

22.1 IPsec VPN parameters 22-2

22.1 IPsec VPN parameters

This chapter describes the parameters on the IPsec VPN management form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Authentication Key

Table 22-3 lists where to find more information about the Authentication Key parameter.

Table 22-1 Authentication Key parameter

Parameter	See
Authentication key in IPsec transform policy	Authentication Key parameter in this section
Inbound Authentication key in the IPsec VPN	Authentication Key parameter in this section
Outbound Authentication key in the IPsec VPN	Authentication Key parameter in this section

Authentication Key

(**authenticationKey**)

The Authentication Key parameter specifies the key that is used for the authentication algorithm defined by the transform algorithm in the IPsec transform policy. The range is 0 to 32 characters. There is no default.

Authentication Key

(**authenticationKeyInbound**)

The Authentication Key parameter specifies the key that is used for the inbound authentication algorithm defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters. There is no default.

Authentication Key

(**authenticationKeyOutbound**)

The Authentication Key parameter specifies the key that is used for the outbound authentication algorithm defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters. There is no default.

Auto Establish

(autoEstablish)

The Auto Establish parameter specifies whether there is an automatic attempt to establish a phase 1 exchange. The options are:

- Enabled
- Disabled (default)

Backup Remote Address

(backupRemIpAddress)

The Backup Remote Address parameter specifies the IP address of the backup remote endpoint of a GRE tunnel. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Description

See the [Description](#) parameter in section 14.1.

Designated

(bfdDesignate)

The Designated (bfdDesignate) parameter specifies whether the IPsec tunnel is the designated BFD tunnel. The options are:

- Enabled
- Disabled (default)

Destination Address

(bfdDstAddr)

The Destination Address parameters specifies the IP address for the BFD session. The default is 0.0.0.0.

Destination Address

(destIpAddress)

The Destination Address parameters specifies the IP address of the interface on the remote node of a GRE tunnel. Specify an IPv4 address in dotted-decimal format. There is no default.

Direction

(direction)

The Direction parameter specifies the direction on the IPsec tunnel to which the SA entry is applied. The options are:

- Inbound (default)
- Outbound

Direction

(staticSADirection)

The Direction parameter specifies the direction to which the IPsec static security association is applied. The options are:

- Bidirectional (default)
- Inbound
- Outbound

Displayed Name

See the [Displayed Name](#) parameter in section 14.1.

Enabled

(bfdEnable)

The Enabled (bfdEnable) parameter specifies whether to create a BFD object for the IPsec tunnel. The options are:

- Enabled
- Disabled (default)

Encryption Key

Table 22-2 lists where to find more information about the Encryption Key parameter.

Table 22-2 Encryption Key parameter

Parameter	See
Encryption key in IPsec transform policy	Encryption Key parameter in this section
Inbound encryption key in the IPsec VPN	Encryption Key parameter in this section
Outbound encryption key in the IPsec VPN	Encryption Key parameter in this section

Encryption Key

(encryptionKey)

The Encryption Key parameter specifies the key that is used for the encryption algorithm defined by the transform algorithm in the IPsec transform policy. The range is 0 to 32 characters. There is no default.

Encryption Key

(**encryptionKeyInbound**)

The Encryption Key parameter specifies the key that is used for the inbound encryption algorithm that is defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters. There is no default.

Encryption Key

(**encryptionKeyOutbound**)

The Encryption Key parameter specifies the key that is used for the outbound encryption algorithm that is defined by the algorithm in the IPsec VPN. The range is 0 to 32 characters. There is no default.

ID

See the [ID](#) parameter in section [14.1](#).

IKE Policy

(**ikePolicyPointer**)

The IKE Policy parameter specifies the IKE policy that is associated with the IPsec tunnel. Click on the Select button to choose an IKE policy.

IP Address

Table [22-3](#) lists where to find more information about the IP Address parameter.

Table 22-3 IP Address parameter

Parameter	See
Local IP Address for IPsec security policy	IP Address in this section
Remote IP Address for IPsec security policy	IP Address in this section

IP Address

(**localAddress**)

The IP Address parameter specifies the IP address of the local aggregate route in the IPsec security policy entry. Specify an IP address in dotted-decimal format for IPv4, or in colon-hexadecimal format for IPv6, or a DNS address. There is no default.

IP Address

(remoteAddress)

The IP Address parameter specifies the IP address of the remote aggregate route in the IPsec security policy entry. Specify an IP address in dotted-decimal format for IPv4, or in colon-hexadecimal format for IPv6, or a DNS address. There is no default.

Keying

(keying)

The Keying parameter specifies the keying type that the IPsec tunnel uses. The Keying parameter specifies whether the SA entry is created manually by the user or dynamically by the IPsec sub-system. The options are:

- None (default)
- Manual
- Dynamic

Link Corporate and Secured Service

(createCompositeService)

The Link Corporate and Secured Service parameter specifies whether corporate and secure services are associated with each other in the IPsec VPN. The options are:

- Enabled
- Disabled (default)

Local Address Option

(localAddressOption)

The Local Address Option specifies the local IP prefix for the IPsec security policy entry. The 5620 SAM considers the local IP as the source IP when traffic is examined in the direction of the VPRN to the tunnel, and as the destination IP when traffic flows from the tunnel to the VPRN. The options are:

- None (default)
- Any Address
- IP Address

Local Endpoint Address

(lclIpAddress)

The Local Endpoint Address parameter specifies the IP address of the local endpoint of a GRE tunnel. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Local Gateway Address

(gwIpAddress)

The Local Gateway Address parameter specifies the address of the interface on the local NE of the IPsec tunnel. Specify an IP address in dotted-decimal format or a DNS address.

Name

Table 22-4 lists where to find more information about the Name parameter.

Table 22-4 Name parameter

Parameter	See
Name for the object. The range depends on the type of object being configured.	Name parameter in section 14.1.
Name for an IPsec security policy entry	Name in this section.

Name

(ipsecPolicyEntryId)

The Name parameter specifies a name for the IPsec security policy entry. The range is 1 to 16. The default is 0.

Prefix Length

(localPrefixLength)

When combined with an IP address value, the Prefix Length parameter specifies a local IP prefix. The range is 1 to 32 for an IPv4 address. A value of 32 is typically reserved for an IPv4 system address. The IPv4 default is 24.

Prefix Length

(remotePrefixLength)

When combined with an IP address value, the Prefix Length parameter specifies a remote IP prefix. The range is 1 to 32 for an IPv4 address. A value of 32 is typically reserved for an IPv4 system address. The IPv4 default is 24.

Pre Shared Key

(preSharedKey)

The Pre Shared Key parameter specifies the secret key that is shared by the two peers that form the IPsec tunnel. Table 22-5 lists the parameter ranges for different device types. There is no default.

Table 22-5 Pre Shared Key parameter

Device type	Range (characters)
7750 SR and 7450 ESS, Release 8.0 and earlier	0 to 32
7750 SR and 7450 ESS, Release 9.0 and later	0 to 64

Remote Address

(remoteIpAddress)

The Remote Address parameter specifies the IP address of the remote endpoint of a GRE tunnel. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Remote Address Option

(remoteAddressOption)

The Remote Address Option specifies the remote IP prefix for the Ipsec security policy entry. The 5620 SAM considers the remote IP as the source IP when traffic flows from the tunnel to the VPRN when traffic flows from the VPRN to the tunnel. The options are:

- None (default)
- Any Address
- IP Address

Remote Gateway Address

(remoteAddressType)

The Remote Gateway Address parameter specifies the address of the interface on the remote NE of the IPsec tunnel. Specify an IPv4 address in dotted-decimal format, an IPv6 address in colon-hexadecimal format, or a DNS address.

Replay Window

(replayWindow)

The Replay Window parameter specifies the size of the anti-replay window for the IPsec tunnel. The anti-replay window protocol secures IP against an entity that can inject messages in a message stream from a source to a destination computer on the Internet. If the value is set to 0, anti-replay is disabled. The options are:

- 0 (default)
- 32
- 64
- 128
- 256
- 512

Security Policy ID

The Security Policy ID parameter specifies an ID for the IPsec security policy on the VPRN site. The range is 1 to 8192. The default is 0.

SPI

(spi)

The SPI parameter specifies the Security Parameter Index that is used to select the security association to verify and decrypt the incoming IPsec. The Security Parameter Index is an identification tag that is added to the header. The range is 256 to 16 383. The default is 0.

Transform ID 1

(dynamicKeyTransformId1Pointer)

The Transform ID 1 parameter specifies the IPsec transform policy that is associated with the IPsec tunnel. Click on the Select button to choose an IPsec transform policy.

Transform ID 2

(dynamicKeyTransformId2Pointer)

See the [Transform ID 1](#) in this section.

Transform ID 3

(dynamicKeyTransformId3Pointer)

See the [Transform ID 1](#) in this section.

Transform ID 4

(dynamicKeyTransformId4Pointer)

See the [Transform ID 1](#) in this section.

Tunnel Type

The Tunnel Type parameter specifies the tunnel type for the IPsec group. The options are:

- Dynamic (Site-to-Site)
- Dynamic (Soft Client)
- Static

23 – VLAN group and path parameters

23.1 VLAN group and path parameters 23-2

23.1 VLAN group and path parameters

This chapter describes the parameters on the Manage VLAN Groups and Manage VLAN Paths forms and child forms.

Description

See the [Description](#) parameter in section 36.1.

Description

(groupDescription)

The Description parameter specifies a description for the VLAN group. The range is 0 to 255 characters. There is no default.

Group Name

(groupName)

The Group Name parameter specifies a name for the VLAN group. The range is 1 to 32 characters. There is no default.

Head Ends

(headEnds)

The Head Ends parameter allows you to specify the NEs that act as ingress or egress NEs to an OmniSwitch VLAN group. The 5620 SAM supports 7750 SR, 7710 SR, and 7450 ESS NEs as head ends. The options are:

- Disabled (default)
- Enabled

Minimum Bandwidth (kbps)

The Minimum Bandwidth (kbps) parameter specifies the guaranteed bandwidth that is available across all network ports that have to be selected during creation of a VLAN path. This parameter is optional.

Name

See the [Name](#) parameter in section 36.1.

Node Type

(nodeType)

The Node Type parameter specifies the type of NEs that can be members of the VLAN group. The options are:

- OMNI (default)
- 9500

Technology

(groupMode)

The Technology parameter specifies the type of service supported by the group members. Currently only one option, VLAN, is supported.

Topology

(topology)

The Topology parameter specifies the topology of the VLAN group. Table 23-1 describes the options.

Table 23-1 Topology parameter

Options	Description	Dependencies
Ring	The nodes in the VLAN group are connected in a ring topology.	Available only when the Node Type parameter is set to OMNI
Mesh	The nodes in the VLAN group are connected in a mesh topology.	Available only when the Node Type parameter is set to 9500
Tree	The nodes in the VLAN group are connected in a tree topology.	The default value when the Node Type parameter is set to 9500

VLAN Space Management by SAM

(vlanIdManagement)

The VLAN Space Management by SAM parameter specifies whether the 5620 SAM manages the VLAN IDs that are used by a 9500 MPR service. When the check box is not selected, VLAN IDs must be managed by the user. The default value depends on the value of the [Topology](#) parameter. Table 23-2 describes the default value dependencies.

Table 23-2 VLAN Space Management by SAM parameter

Topology parameter value	Default value
Tree	Enabled
Mesh	Disabled

24 – Node Redundancy parameters

24.1 Node Redundancy parameters 24-2

24.1 Node Redundancy parameters

This chapter describes the parameters on the child forms of the Manage Node Redundancy form.

Administrative State

Table 24-1 lists where to find more information about the Administrative State parameter.

Table 24-1 Administrative State parameter

Parameter	See
Administrative State for object other than MC peer	Administrative State parameter in this section
Administrative State for first MC peer group or endpoint group	Administrative State parameter in this section
Administrative State for second MC peer group or endpoint group	Administrative State parameter in this section

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled. The options are:

- Up
- Down (default)

Administrative State

(firstSiteAdministrativeState)

The Administrative State parameter specifies whether MC peering is administratively enabled for the first site in the MC peer group or endpoint group. The options are:

- Up (default)
- Down

Administrative State

(secondSiteAdministrativeState)

The Administrative State parameter specifies whether MC peering is administratively enabled for the second site in the MC peer group or endpoint group. The options are:

- Up (default)
- Down

Authentication Key

Table 24-2 lists where to find more information about the Authentication Key parameter.

Table 24-2 Authentication Key parameter

Parameter	See
Authentication Key for MC peer in current context	Authentication Key parameter in this section
Authentication Key for first MC peer group member	Authentication Key parameter in this section
Authentication Key for second MC peer group member	Authentication Key parameter in this section

Authentication Key

(authenticationKey)

The Authentication Key parameter specifies the authentication key used between two MC peer group members. If the member is the first member of the MC peer group, the parameter value is automatically set to the [Authentication Key](#) value. Otherwise, the parameter value is automatically set to the [Authentication Key](#) value.

Authentication Key

(firstSiteAuthenticationKey)

The Authentication Key parameter specifies the authentication key for the first site in the MC peer group. Specify a string of printable, 7-bit ASCII characters. If the string contains special characters or spaces, you must enclose the string in double quotation marks. The range is 1 to 20 characters. There is no default.

Authentication Key

(secondSiteAuthenticationKey)

The Authentication Key parameter specifies the authentication key for the second site in the MC peer group. Specify a string of printable, 7-bit ASCII characters. If the string contains special characters or spaces, you must enclose the string in double quotation marks. The range is 1 to 20 characters. There is no default.

Auto-Assign ID

See the “[Auto-Assign ID](#)” parameter in section [182.1](#).

BFD Enabled

Table [24-4](#) lists where to find more information about the BFD Enabled parameter.

Table 24-3 BFD Enabled parameter

Parameter	See
BFD Enabled for the MC endpoint group on the first site	BFD Enabled parameter in this section
BFD Enabled for the MC endpoint group on the second site	BFD Enabled parameter in this section

BFD Enabled

(firstSiteBfdEnabled)

The BFD Enabled parameter specifies whether BFD is enabled for the first MC endpoint. The options are:

- Enabled
- Disabled (default)

BFD Enabled

(secondSiteBfdEnabled)

The BFD Enabled parameter specifies whether BFD is enabled for the second MC endpoint. The options are:

- Enabled
- Disabled (default)

Boot Timer

Table [24-4](#) lists where to find more information about the Boot Timer parameter.

Table 24-4 Boot Timer parameter

Parameter	See
Boot Timer for the MC endpoint group on the first site	Boot Timer parameter in this section
Boot Timer for the MC endpoint group on the second site	Boot Timer parameter in this section

Boot Timer

(firstSiteBootTimer)

The Boot Timer parameter specifies the maximum amount of time that the protocol for the first MC endpoint can try to establish a connection with the remote peer. The range is 1 to 600 s. The default is 300 s.

Boot Timer

(secondSiteBootTimer)

The Boot Timer parameter specifies the maximum amount of time that the protocol for the second MC endpoint can try to establish a connection with the remote peer. The range is 1 to 600 s. The default is 300 s.

Description

Table 24-5 lists where to find more information about the Description parameter.

Table 24-5 Description parameter

Parameter	See
Description for object other than an MC peer group	Description parameter in this section
Description for the first MC peer group member	Description parameter in this section
Description for the second MC peer group member	Description parameter in this section

Description

(description)

The Description parameter specifies a description for the object. The range is 0 to 80 characters. There is no default.

Description

(firstSiteDescription)

The Description parameter specifies a description for the first site in the MC peer group. The range is 0 to 80 characters. There is no default.

Description

(secondSiteDescription)

The Description parameter specifies a description for the second site in the MC peer group. The range is 0 to 80 characters. There is no default.

Destination IP Address

Table 24-6 lists where to find more information about the Destination IP Address parameter.

Table 24-6 Destination IP Address parameter

Parameter	See
Destination IP Address for IB-RCC messages	Destination IP Address parameter in this section
Destination IP Address for RNCV messages	Destination IP Address parameter in this section

Destination IP Address

(ibrccDestinationIpAddr)

The Destination IP Address parameter specifies the destination for IB-RCC messages. The MC ring cannot operate unless the parameter is set using the IP address of the BFD interface on the peer site. The default is 0.0.0.0, which means that the parameter is not configured.

Destination IP Address

(rncvDestinationIpAddr)

The Destination IP Address parameter specifies the destination for RNCV messages. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Encap Type

(type)

The Encap Type parameter specifies the encapsulation type of the port in the definition of a VLAN range. The parameter value is automatically set to the encapsulation type of the ports or LAGs specified using the [Port/LAG Name](#) parameter.

End VLAN Value

(endVlan)

The End VLAN Value parameter specifies the upper limit of the VLAN range. The range is 0 to 4095. The default is 0, which means that the parameter is not configured.

Hold On Neighbor Failure

Table 24-4 lists where to find more information about the Hold On Neighbor Failure parameter.

Table 24-7 Hold On Neighbor Failure parameter

Parameter	See
Hold On Neighbor Failure for the MC endpoint group on the first site	Hold On Neighbor Failure parameter in this section
Hold On Neighbor Failure for the MC endpoint group on the second site	Hold On Neighbor Failure parameter in this section

Hold On Neighbor Failure

(firstSiteHoldOnNeighborFailure)

The Hold On Neighbor Failure parameter specifies the number of keep-alive intervals that the local device waits for packets from the first MC endpoint peer. The range is 2 to 25 s. The default is 3 s.

Hold On Neighbor Failure

(secondSiteHoldOnNeighborFailure)

The Hold On Neighbor Failure parameter specifies the number of keep-alive intervals that the local device waits for packets from the second MC endpoint peer. The range is 2 to 25 s. The default is 3 s.

IGMP

(igmp)

The IGMP parameter specifies whether IGMP state information is synchronized with the MC peer. IGMP states on SAPs in the configured range of encapsulation values are synchronized with the MC peer. The options are:

- Enabled
- Disabled (default)

IGMP Snooping

(igmpSnooping)

The IGMP Snooping parameter specifies whether IGMP snooping state information is synchronized with the MC peer. IGMP snooping states on VPLS SAPs in the configured range of encapsulation values are synchronized with the MC peer. The options are:

- Enabled
- Disabled (default)

Interface Name

(ibrccInterfaceName)

The Interface Name parameter specifies the name of the interface to use for IB-RCC in the MC ring. The MC ring cannot operate unless the parameter is set using the name of an IES or VPRN interface that has BFD enabled. Specify an interface name of up to 32 characters, or click on the Select button to choose an interface. The default is N/A, which means that the parameter is not configured.

Interval (minutes)

(rncvInterval)

The Interval (minutes) parameter specifies, in minutes, the RNCV polling interval. The range is 1 to 6000. The default is 5.

Keep-Alive Interval (deciseconds)

Table 24-8 lists where to find more information about the Keep-Alive Interval (deciseconds) parameter.

Table 24-8 Keep-Alive Interval (deciseconds) parameter

Parameter	See
Keep-Alive Interval (deciseconds) for the first site MC endpoint group	Keep-Alive Interval (deciseconds) parameter in this section
Keep-Alive Interval (deciseconds) for the second site MC endpoint group	Keep-Alive Interval (deciseconds) parameter in this section
Keep-Alive Interval (deciseconds) for the MC LAG member	Keep-Alive Interval (deciseconds) parameter in this section

Keep-Alive Interval (deciseconds)

(firstSiteKeepAliveInterval)

The Keep-Alive Interval parameter specifies the number of deciseconds that the keep-alive messages are exchanged between the two systems in the first MC endpoint. The range is 5 to 500. The default is 10.

Keep-Alive Interval (deciseconds)

(secondSiteKeepAliveInterval)

The Keep-Alive Interval parameter specifies the interval that the keep-alive messages are exchanged between the two systems in the second MC endpoint. The range is 5 to 500. The default is 10.

Keep-Alive Interval (deciseconds)

(keepAliveInterval)

The Keep-Alive Interval (deciseconds) parameter specifies how often the MC LAG member sends keep-alive messages to the peer member to indicate that the member is operationally up. The range is 5 to 500. The default is 10.

LACP Key

(lacpKey)

The LACP Key parameter specifies a unique 16-bit key that must be identical on each member of the MC LAG. The range is 1 to 65 535. The default is 0, which means that the parameter is not configured.

LAG ID

Table 24-9 lists where to find more information about the LAG ID parameter.

Table 24-9 LAG ID parameter

Parameter	See
LAG ID for first MC LAG group member	LAG ID parameter in this section
LAG ID for second MC LAG group member	LAG ID parameter in this section

LAG ID

(firstLagId)

The LAG ID parameter specifies a unique identifier for the LAG on the first peer site of the MC LAG. The range is 1 to 200 for the 7450 ESS and 7750 SR. The range is 1 to 64 for the 7450 ESS-1, 7750 SR-1, and the 7710 SR. Click on the Select button to list and choose a LAG.

LAG ID

(secondLagId)

The LAG ID parameter specifies a unique identifier for the LAG on the second peer site of the MC LAG. The range is 1 to 200 for the 7450 ESS and 7750 SR. The range is 1 to 64 for the 7450 ESS-1, 7750 SR-1, and the 7710 SR. Click on the Select button to list and choose a LAG.

Lost Connection Wait Interval

(holdOnNeighborFailure)

The Lost Connection Wait Interval parameter specifies how long a standby MC LAG member waits for packets from the active member before it assumes that the active member is failing. When the parameter value is reached, the active and standby members reverse roles. The range is 2 to 25. The default is 3.

MAC LSB (hex)

(srcBMacLSB)

The MAC LSB (hex) parameter specifies the last 16 bits of the MAC address to be used for the traffic that ingresses the MC LAG link. The default is 00-00. The parameter is only configurable in chassis mode D when both peers are PBB-capable. The range is 00-00 to FF-FF.

Maximum Inner Encap Value

(maxInnerEncapValue)

The Maximum Inner Encap Value specifies the maximum inner encapsulation value for the VLAN range on the port. The range is 0 to 4095. The default is 0.

Maximum Outer Encap Value

(maxOuterEncapValue)

The Maximum Outer Encap Value specifies the maximum outer encapsulation value for the VLAN range on the port. The range is 1 to 4094. The default is 0, which means that the parameter is not configured.

MC Ring

(mcRing)

The MC Ring parameter specifies whether MC ring information is synchronized with the MC peer. The synchronized information includes the IB-RCC source IP address, destination IP address, encapsulation value of the BFD connection, and the VLAN ranges configured for the MC ring path B and exclusion paths. The options are:

- Enabled
- Disabled (default)

Minimum Inner Encap Value

(minInnerEncapValue)

The Minimum Inner Encap Value specifies the minimum inner encapsulation value for the VLAN range on the port. The range is 0 to 4095. The default is 0.

Minimum Outer Encap Value

(minOuterEncapValue)

The Minimum Outer Encap Value specifies the minimum outer encapsulation value for the VLAN range on the port. The range is 1 to 4094. The default is 0, which means that the parameter is not configured.

MLD Snooping

(mldSnooping)

The MLD Snooping parameter specifies whether MLD snooping state information is synchronized with the MC peer. When the parameter is enabled, MLD snooping states that are created on VPLS SAPs in the configured range of encapsulation values are synchronized. The options are:

- Enabled
- Disabled (default)

Name

(ringName)

The Name parameter specifies the name of the MC ring group. The range is 1 to 32 characters. There is no default.

Passive Mode Enabled

Table 24-10 lists where to find more information about the Passive Mode Enabled parameter.

Table 24-10 Passive Mode Enabled parameter

Parameter	See
Passive mode enabled for the MC endpoint group on the first site	Passive Mode Enabled parameter in this section
Passive mode enabled for the MC endpoint group on the second site	Passive Mode Enabled parameter in this section

Passive Mode Enabled

(firstSitePassiveMode)

The Passive Mode Enabled parameter specifies whether the device is in a standby state for the first site. The options are:

- Enabled
- Disabled (default)

When you choose Enabled for the first or second site, the Passive Mode Operational State parameter is enabled for the other site.

Passive Mode Enabled

(secondSitePassiveMode)

The Passive Mode Enabled parameter specifies whether the device is in a standby state for the second MC endpoint. The options are:

- Enabled
- Disabled (default)

When you choose Enabled for the second or first site, the Passive Mode Operational State parameter is enabled for the other site.

Peer Address

(peerIpAddress)

The Peer Address parameter specifies the IP address of the MC peer group member. If the member is the first member of the MC peer group, the parameter value is automatically set to the [Source Address](#) value. Otherwise, the parameter value is automatically set to the [Source Address](#) value.

Peer Name

Table [24-11](#) lists where to find more information about the Peer Name parameter.

Table 24-11 Peer Name parameter

Parameter	See
Peer Name for the first MC peer group member	Peer Name parameter in this section
Peer Name for the second MC peer group member	Peer Name parameter in this section

Peer Name

(firstSitePeerName)

The Peer Name parameter specifies the name of the remote peer for the first site. The range is 0 to 32 characters and the name is case-sensitive.

Peer Name

(secondSitePeerName)

The Peer Name parameter specifies the name of the remote peer for the second site. The range is 0 to 32 characters and the parameter is case-sensitive.

Port/LAG Name

(portName)

The Port/LAG Name parameter specifies the port or LAG that is synchronized with the port or LAG on the MC peer that has the same [Synchronization Tag](#) value. Click on the Select button to list and choose a port or LAG.

Ring Node Name

(ringNodeName)

The Ring Node Name parameter specifies a name for the access node that is to be a ring node in the MC ring group. The range is 1 to 32 characters. There is no default.

SAP Inner Encapsulation Value

(rncvInnerEncapValue)

The SAP Inner Encapsulation Value parameter specifies the inner encapsulation value of the SAP used for RNCV. The range is 0 to 4095, or *. The default is 0, which means that the SAP used for RNCV uses null encapsulation.

SAP Outer Encapsulation Value

(rncvOuterEncapValue)

The SAP Outer Encapsulation Value parameter specifies the outer encapsulation value of the SAP used for RNCV. The range is 0 to 4095, or *. The default is 0, which means that the SAP used for RNCV uses null encapsulation.

SAP Service ID

(rncvServiceId)

The SAP Service ID parameter specifies the identifier of the service that contains the SAP to be used for RNCV. The range is 0 to 2 147 483 647. The default is 0, which means that the parameter is not configured.

Service ID

(ibrccServiceId)

The Service ID parameter specifies the identifier of the IES or VPRN service that contains the interface used for IB-RCC in the MC ring. The range is 0 to 2 147 483 647. The default is 0, which means that the parameter is not configured.

Site ID

Table [24-12](#) lists where to find more information about the Site ID parameter.

Table 24-12 Site ID parameter

Parameter	See
Site ID for first MC ring group member	Site ID parameter in this section
Site ID for second MC ring group member	Site ID parameter in this section
Site ID for first MC APS group member	Site Id parameter in this section
Site ID for second MC APS group member	Site Id parameter in this section

Site ID

(firstSiteId)

The Site ID parameter specifies the IP address of the first site in the MC ring group. The parameter is automatically assigned the [Source Address](#) value from the parent MC peer group.

Site Id

(nodeIdHigh)

The Site Id parameter specifies the system IP address of the second MC APS group member. Click on the Select button to list and choose an NE.

Site Id

(nodeIdLow)

The Site Id parameter specifies the system IP address of the first MC APS group member. Click on the Select button to list and choose an NE.

Site ID

(secondSiteId)

The Site ID parameter specifies the IP address of the second site in the MC ring group. The parameter is automatically assigned the [Source Address](#) value from the parent MC peer group.

Source Address

Table [24-13](#) lists where to find more information about the Source Address parameter.

Table 24-13 Source Address parameter

For	See
Source Address for MC peer group member in current context	Source Address parameter in this section
Source Address for first MC peer group or MC endpoint member	Source Address parameter in this section
Source Address for second MC peer group or MC endpoint group member	Source Address parameter in this section

Source Address

(firstSiteSourceIpAddress)

The Source Address parameter specifies the source IP address of the first NE in the MC peer group or endpoint group. Specify an IPv4 address in dotted-decimal format. The default is the NE system IP address.

Source Address

(secondSiteSourceIpAddress)

The Source Address parameter specifies the source IP address of the second NE in the MC peer group or endpoint group. Specify an IPv4 address in dotted-decimal format. The default is the NE system IP address.

Source Address

(sourceIpAddress)

The Source Address parameter specifies the IP address of the MC peer group member. If the member is the first member of the MC peer group, the parameter value is automatically set to the [Source Address](#) value. Otherwise, the parameter value is automatically set to the [Source Address](#) value.

Source IP Address

(rncvSourceIpAddr)

The Source IP Address parameter specifies the RNCV source IP address. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Source MAC Address

(rncvSourceMacAddr)

The Source MAC Address parameter specifies the RNCV source MAC address. The default is 00-00-00-00-00-00, which means that the parameter is not configured.

SRRP

(srrp)

The SRRP parameter specifies whether SRRP state information is synchronized with the MC peer. The options are:

- Enabled
- Disabled (default)

Start VLAN Value

(startVlan)

The Start VLAN Value parameter specifies the lower limit of the VLAN range. The range is 0 to 4095. The default is 0, which means that the parameter is not configured.

Subscriber Host Tracking

(subscriberHostTracking)

The Subscriber Host Tracking parameter specifies whether subscriber host tracking information is synchronized with the MC peer. When the parameter is enabled, the peers synchronize the subscriber host tracking information on each VPLS SAP, IES group interface, and VPRN group interface that has an encapsulation value in the specified range. The options are:

- Enabled
- Disabled (default)

Subscriber Management

(subscriberManagement)

The Subscriber Management parameter specifies whether subscriber management state information is synchronized with the MC peer. When the parameter is enabled, the peers synchronize the subscriber management state information on each VPLS SAP, IES group interface, and VPRN group interface that has an encapsulation value in the specified range. The options are:

- Enabled
- Disabled (default)

Sync Administrative State

(commonSyncAdminState)

The Sync Administrative State parameter specifies whether MC protocol synchronization is administratively enabled for the MC peer group. The options are:

- Up
- Down (default)

Synchronization Tag

(tag)

The Synchronization Tag parameter is an ASCII string that specifies the synchronization tag of the MC synchronization group. State information is synchronized between two NEs that have the same synchronization tag. The range is 1 to 32 characters. There is no default.

Synchronize IGMP

(igmp)

The Synchronize IGMP parameter specifies whether IGMP state information is synchronized with the MC peer. IGMP states on SAPs in the configured range of encapsulation values are synchronized with the MC peer. The options are:

- Enabled
- Disabled (default)

Synchronize IGMP-Snooping

(igmpSnooping)

The Synchronize parameter specifies whether IGMP snooping state information is synchronized with the MC peer. IGMP snooping states on VPLS SAPs in the configured range of encapsulation values are synchronized with the MC peer. The options are:

- Enabled
- Disabled (default)

Synchronize MC Ring

(mcRing)

The Synchronize MC Ring parameter specifies whether MC ring information is synchronized with the MC peer. The synchronized information includes the IB-RCC source IP address, destination IP address, encapsulation value of the BFD connection, and the VLAN ranges configured for the MC ring path B and exclusion paths. The options are:

- Enabled
- Disabled (default)

Synchronize MLD Snooping

(mldSnooping)

The Synchronize MLD Snooping parameter specifies whether MLD snooping state information is synchronized with the MC peer. When the parameter is enabled, MLD snooping states that are created on VPLS SAPs in the configured range of encapsulation values are synchronized. The options are:

- Enabled
- Disabled (default)

Synchronize SRRP

(srrp)

The Synchronize SRRP parameter specifies whether SRRP state information is synchronized with the MC peer. The options are:

- Enabled
- Disabled (default)

Synchronize Subscriber Host Tracking

(subscriberHostTracking)

The Synchronize Subscriber Host Tracking parameter specifies whether subscriber host tracking information is synchronized with the MC peer. When the parameter is enabled, the peers synchronize the subscriber host tracking information on each VPLS SAP, IES group interface, and VPRN group interface that has an encapsulation value in the specified range. The options are:

- Enabled
- Disabled (default)

Synchronize Subscriber Management

(subscriberManagement)

The Synchronize Subscriber Management parameter specifies whether subscriber management state information is synchronized with the MC peer. When the parameter is enabled, the peers synchronize the subscriber management state information on each VPLS SAP, IES group interface, and VPRN group interface that has an encapsulation value in the specified range. The options are:

- Enabled
- Disabled (default)

Sync Tag Config Level

Table [24-14](#) lists where to find more information about the Sync Tag Config Level parameter.

Table 24-14 Sync Tag Config Level parameter

Parameter	See
Sync Tag Config Level for first MC sync group member	Sync Tag Config Level parameter in this section
Sync Tag Config Level for second MC sync group member	Sync Tag Config Level in this section

Sync Tag Config Level

(firstSiteSyncTagConfigLevel)

The Sync Tag Config Level specifies the synchronization tag context for the first site in a MC sync group. The options are:

- Port/LAG Level (default)
- VLAN Range Level

Sync Tag Config Level

(secondSiteSyncTagConfigLevel)

The Sync Tag Config Level specifies the synchronization tag context for the second site in a MC sync group. The parameter value is automatically set to the [Sync Tag Config Level](#) value.

System ID

(systemId)

The System ID parameter specifies a unique identifier for the MC LAG. Specify a unicast MAC Address. The default is 00-00-00-00-00-00, which means that the parameter is not configured.

System Priority

Table 24-15 lists where to find more information about the System Priority parameter.

Table 24-15 System Priority parameter

Parameter	See
System Priority for the first MC endpoint group member	System Priority parameter in this section
System Priority for the second MC endpoint group member	System Priority parameter in this section
System Priority for the MC LAG	System Priority parameter in this section

System Priority

(firstSiteSystemPriority)

The System Priority parameter specifies the system priority for the first MC endpoint. The peer with the lowest value is the active peer. The range is 0 to 255. The default is 0, which is the highest priority.

System Priority

(secondSiteSystemPriority)

The System Priority parameter specifies the system priority for the second MC endpoint. The peer with the highest value is the active peer. The range is 0 to 255. The default is 0, which is the highest priority.

System Priority

(systemPriority)

The System Priority parameter specifies the priority level of the MC LAG. The lowest value represents the highest priority level. The range is 0 to 65 535. The default is 0, which means that the parameter is not configured.

Use LACP Key

(srcBMacLsbUseLacpKey)

The Use LACP Key parameter specifies whether the LACP key is used as source BMAC LSB. The default is false which means that the LACP Key is not used. The parameter is only configurable in chassis mode D and when both peers are PBB-capable.

25 – Routing Instances parameters

25.1 Routing Instances parameters 25-2

25.1 Routing Instances parameters

This chapter describes the parameters on the Manage Routing Instances form and child forms, and the forms opened using the right-click contextual menu options for routing instances.

Action

See the [Action](#) parameter in section 14.1.

Allow Directed Broadcasts

See the [Allow Directed Broadcasts](#) parameter in section 203.1.

Autonomous System

(autonomousSystemNumber)

The Autonomous System parameter specifies the AS number for the device. A device can only belong to one AS. An AS number is a globally unique number with an AS. This number is used to exchange exterior routing information with neighboring ASs and as an identifier of the AS itself. The range is 0 to 65 535. The default is 1.

BGP Enabled

(bgpEnabled)

The BGP Enabled parameter specifies whether BGP is enabled for the device. Table 25-1 describes the parameter options.

Table 25-1 BGP Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that BGP routing is enabled on the device	The Autonomous System parameter must be set from the Routing tab button on the Routing Instance form.
Disabled (default)	Specifies that BGP routing is disabled on the device	—

Broadcast

See the [Broadcast](#) parameter in section 203.1.

Broadcast Address Format

See the [Broadcast Address Format](#) parameter in section 203.1.

Cflowd Type

See the [Cflowd Type](#) parameter in section 203.1.

Circuit ID

See the [Circuit ID](#) parameter in section 14.1.

Class

See the [Class](#) parameter in section 203.1.

Confederation Autonomous System

(confederationAutonomousSystemNumber)

The Confederation Autonomous System parameter specifies a confederation ID to reduce the IBGP mesh inside an AS. The range is 0 to 65 535. The default is 0.

An AS can be logically divided into smaller groupings called subconfederations. To create this division, you can use the parameter to assign the confederation ID. Each subconfederation has fully meshed IBGP and connections to other ASs outside of the confederation.

Description

See the [Description](#) parameter in section 203.1.

Egress Filter ID

See the [Egress Filter ID](#) parameter in section 203.1.

Enable DHCP Relay

(administrativeState)

The Enable DHCP Relay parameter specifies the administrative state for DHCP relay. DHCP discover messages are broadcast packets that typically do not leave the IP subnet. DHCP relay agents are used to intercept the requests and forward them as unicast messages to a DHCP server.

Exclusive

(isExclusive)

The Exclusive parameter specifies whether to allow the creation of an IP address range reserved for IESs or VPLSs. This provides a mechanism to reserve one or more address ranges for services. When this parameter is enabled, the configured IP addresses and subnet masks are exclusively used for services and cannot be assigned to network ports. The options are:

- Enabled
- Disabled (default)

IGMP Enabled

(igmpEnabled)

The IGMP Enabled parameter specifies whether IGMP is enabled for the device. Table 25-2 describes the parameter options.

Table 25-2 IGMP Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that IGMP is enabled on the device	—
Disabled (default)	Specifies that IGMP is disabled on the device	—

IGP Inhibit

See the [IGP Inhibit](#) parameter in section 203.1.

Ingress Filter ID

See the [Ingress Filter ID](#) parameter in section 203.1.

Interface ID

(interfaceId)

The Interface ID parameter specifies a unique ID for the interface. This parameter is not configurable when the Auto-Assign ID parameter is enabled. The range is 1 to 5119. The default is 0.

IP Address

See the [IP Address](#) parameter in section 203.1.

IS-IS Enabled

(isisEnabled)

The IS-IS Enabled parameter specifies whether IS-IS is configured for the device. The options are:

- Enabled
- Disabled (default)

When this parameter is enabled, IS-IS routing is enabled on the device.

LDP Enabled

(ldpEnabled)

The LDP Enabled parameter specifies whether LDP is enabled for the device. Table 25-3 describes the parameter options.

Table 25-3 LDP Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that LDP is enabled on the device	The Enable MPLS parameter must be set to Enabled.
Disabled (default)	Specifies that LDP is disabled on the device	—

Loopback Enabled

(loopbackEnabled)

The Loopback Enabled parameter specifies whether any ports are associated with the interface. If the Loopback Enabled parameter is selected, no ports are associated with the interface and the interface is in a loopback state. The options are:

- Enabled
- Disabled (default)

MAC Address

See the [MAC Address](#) parameter in section 203.1.

Mask Reply

See the [Mask Reply](#) parameter in section 203.1.

Maximum Number of Equal Cost Routes

The Maximum Number of Equal Cost Routes parameter specifies the number of routes for path sharing. Table 25-4 describes the parameter options.

Table 25-4 Maximum Number of Equal Cost Routes parameter

Option	Option description	Dependencies
1 (default)	The maximum number of equal cost routes allowed on this routing table instance, expressed as a number. The default 1 means equal cost routing is not implemented. For example, setting the parameter to 2 means two equal cost routes are used for cost sharing.	Can only be used for routes learned with the same preference and protocol.
0 to 16		

Member AS

(memberAS)

The Member AS parameter specifies the AS number of the BGP confederation member. The range is 1 to 65 535. There is no default.

You must configure the parameter to create a BGP confederation.

MPLS Enabled

(mplsEnabled)

The MPLS Enabled parameter specifies whether MPLS is enabled for the device. The options are:

- Enabled
- Disabled (default)

Name

See the [Name](#) parameter in section 203.1.

Network Policy ID

See the [Network Policy ID](#) parameter in section 203.1.

Number of Redirects

See the [Number of Redirects](#) parameter in section 203.1.

Number of TTL Expired

See the [Number of TTL Expired](#) parameter in section 203.1.

Number of Unreachables

See the [Number of Unreachables](#) parameter in section 203.1.

OSPFv2 Enabled

(ospfEnabled)

The OSPFv2 Enabled parameter specifies whether OSPFv2 is enabled on the device. The options are:

- Enabled
- Disabled (default)

OSPFv3 Enabled

(ospfv3Enabled)

The OSPFv3 Enabled parameter specifies whether OSPFv3 is enabled on the device. The options are:

- Enabled
- Disabled (default)

PIM Enabled

(pimEnabled)

The PIM Enabled parameter specifies whether PIM is enabled for the device. Table 25-5 describes the parameter options.

Table 25-5 PIM Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that PIM is enabled on the device	—
Disabled (default)	Specifies that PIM is disabled on the device	—

Physical Address

See the [Physical Address](#) parameter in section 203.1.

Prefix Length

(prefixLength)

The Prefix Length parameter is the short form of the subnet mask for an IP address. An IP address and a prefix create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the device.

The range is 0 to 128. The default is 24. Subnet mask 32 is reserved for system IP addresses. You can configure subnet mask 31 for interfaces that are used by routing protocols.

Primary

See the [Primary](#) parameter in section 203.1.

Redirects

See the [Redirects](#) parameter in section 203.1.

Redirects Time

See the [Redirects Time \(seconds\)](#) parameter in section 203.1.

Remote ID

See the [Remote ID](#) parameter in section 14.1.

RIP Enabled

(ripEnabled)

The RIP Enabled parameter specifies whether RIP is enabled on the device. The options are:

- Enabled
- Disabled (default)

Router ID

See the [Router ID](#) parameter in section 203.1.

Server 1

(server1)

The Server 1 parameter specifies a DHCP server for the interface. The DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format for the Server 1 parameter.

Server 2

(server2)

See the [Server 1](#) in this section for more information.

Server 3

(server3)

See the [Server 1](#) in this section for more information.

Server 4

(server4)

See the [Server 1](#) in this section for more information.

Server 5

(server5)

See the [Server 1](#) in this section for more information.

Server 6

(server6)

See the [Server 1](#) in this section for more information.

Server 7

(server7)

See the [Server 1](#) in this section for more information.

Server 8

(server8)

See the [Server 1](#) in this section for more information.

Shortcut Local TTL Propagate

(localTtlPropagate)

The Shortcut Local TTL Propagate parameter enables or disables TTL propagation of locally-generated IP packets. This provides the ability to specify whether an LSP shortcut should operate in Uniform or Pipe mode, which in effect, allows you to hide or reveal the hops of a customer MPLS network when their packets are carried over an LSP shortcut. This capability is required on a point-to-point LDP/RSVP LSP shortcut used in static, BGP, or IGP route resolution.

You can configure the behavior independently for local and transit IP packets for both LDP and MPLS LSP shortcuts. Enabling the Shortcut Local TTL Propagate parameter propagates the TTL from the header of locally-generated IP packets into the label stack of the resulting MPLS packets forwarded over the LSP shortcut. This is referred to as Uniform mode. When the parameter is disabled, a TTL of 255 is programmed onto the pushed label stack. This is referred to as Pipe mode.

The options are:

- enabled (default)
- disabled

Shortcut Transit TTL Propagate

(transitTtlPropagate)

The Shortcut Transit TTL Propagate parameter enables or disables TTL propagation of transit-generated IP packets. This provides the ability to specify whether an LSP shortcut should operate in Uniform or Pipe mode, which in effect, allows you to hide or reveal the hops of a customer MPLS network when their packets are carried over an LSP shortcut. This capability is required on a point-to-point LDP/RSVP LSP shortcut used in static, BGP, or IGP route resolution.

You can configure the behavior independently for local and transit IP packets for both LDP and MPLS LSP shortcuts. Enabling the Shortcut Transit TTL Propagate parameter propagates the TTL from the header of transit-generated IP packets into the label stack of the resulting MPLS packets forwarded over the LSP shortcut. This is referred to as Uniform mode. When the parameter is disabled, a TTL of 255 is programmed onto the pushed label stack. This is referred to as Pipe mode.

The options are:

- enabled (default)
- disabled

Snooping

(snooping)

The Snooping parameter specifies whether DHCP snooping is enabled for DHCP messages. The default depends on the type of managed device. The options are:

- Enabled
- Disabled

Source Address Termination

(ipOrInterfaceIndex)

The Source Address Termination parameter specifies whether the source address used by the IP application to send unsolicited packets to a managed node is a user-specified IP address or the primary address of the L3 access interface (referred to on the Source Address form as Interface Index).

The options are:

- IP Address
- Interface Index

Source IP Address

(sourceIpAddr)

The Source IP Address parameter specifies the IP address used by the IP application to send unsolicited packets to a node, in dotted-decimal format for IPv4, or colon-hexadecimal format for IPv6. The parameter is configurable when the Source Address Termination parameter is set to IP Address. The default is 0.0.0.0.

Source IP Application

(sourceIpApplication)

The Source IP Application parameter specifies the application for which the source IP or interface index is specified. The options are:

- Telnet
- FTP
- SSH
- RADIUS
- TACACS+
- SNMP Traps
- Syslog
- ICMP Ping
- Trace Route
- DNS
- SNTP
- NTP
- CFLOWD
- Telnet IPv6
- FTP IPv6
- RADIUS IPv6
- TACACS+ IPv6
- SNMP Traps IPv6
- Syslog IPv6
- ICMP Ping IPv6

You must select an IPv6 [“Source IP Address”](#) to select an IPv6 [“Source IP Application”](#).

Subnet Mask

See the [Subnet Mask](#) parameter in section [203.1](#).

Timeout

See the [Timeout \(seconds\)](#) parameter in section [203.1](#).

TTL Expired

See the [TTL Expired](#) parameter in section [203.1](#).

TTL Expired Time (seconds)

See the [TTL Expired Time \(seconds\)](#) parameter in section [203.1](#).

Unreachables

See the [Unreachables](#) parameter in section [203.1](#).

Unreachables Time (seconds)

See the [Unreachables Time \(seconds\)](#) parameter in section [203.1](#).

26 – VRRP Virtual Routers parameters

26.1 VRRP Virtual Routers parameters 26-2

26.1 VRRP Virtual Routers parameters

This chapter describes the parameters on the Virtual Router form and child forms, and the forms opened using the right-click contextual menu options for VRRP.

Administrative State

See the [Administrative State](#) parameter in section 36.1.

Backup Address

(backUpAddress)

The Backup Address parameter specifies the IP address on which the backup routers forward traffic if a master router fails in a virtual router. Specify an IPv4 address in dotted-decimal format, or an IPv6 address in colon-hexadecimal format. The default is 0.0.0.0, which indicates that the parameter is not configured.

Base Priority

(priority)

The Base Priority parameter specifies the ranking for backup router failover, so that the backup router configured with the highest priority becomes the master virtual router. The parameter is only configurable for non-owner VRRP instances.

The priority value affects the interaction between this VRID and the same VRID of other virtual routers participating in the same LAN. A higher priority value defines a greater priority in becoming the master virtual router for the VRID. The priority value can only be configured when the defined IP address on the IP interface is different from the virtual router IP address (non-owner mode).

The parameter value for an owner VRRP instance is 255 and is not configurable. The range for a non-owner VRRP instance is 1 to 254. The default for a non-owner VRRP instance is 100.

Description

See the [Description](#) parameter in section 36.1.

Destination Address

(bfdDstAddr)

The Destination Address parameters specifies the IP address for the BFD session. Specify an address in either IPv4 or IPv6 format.

Enable BFD Interface

(bfdEnable)

The Enable BFD Interface parameter specifies whether a BFD interface is enabled on a VRRP instance. The options are:

- false (default)
- true

Init Delay (seconds)

(initDelay)

The Init Delay (seconds) parameter specifies the delay, in seconds, before a VRRP router takes over as the master router for a specific VRRP network. This delay allows the router time to converge other IGPs and EGPs before assuming the virtual IP address ownership. The range is 0 to 65 535. The default is 0.

Key

(authenticationKey)

The Key parameter specifies a simple text password for authentication. The range is 0 to 8 characters. The default is an empty string. See the [Type](#) parameter in this section for information about configuring the type of authentication used.

MAC Address

(macAddress)

The MAC Address parameter specifies the MAC address of the IP interface on which the virtual router sends packets to the LAN. The default value is derived from the VRID.

The MAC address can be used instead of an IP address in ARP responses when the VRRP instance is the master. The MAC address configuration must be the same for all participating virtual routers. Otherwise, connectivity with the attached IP hosts may be affected.

All VRRP advertisements are transmitted with ieee-mac-addr as the source MAC address.

The parameter can be configured in both non-owner and owner modes of VRRP instances.

Master Inherit Interval

(masterIntervalInherit)

The Master Inherit Interval parameter specifies that, in non-owner VRRP instances, the current master advertisement interval setting overrides the locally configured advertisement interval setting.

If the current master changes, the new master setting is used. If the local virtual router becomes master, the locally configured advertisement interval is enforced. The options are:

- false (default)
- true

The parameter must be set to false when the [Message Interval \(milliseconds\)](#) parameter is set to a value other than 0.

Message Interval (seconds)

(messageInterval)

The Message Interval (seconds) parameter specifies the time, in full seconds, that the VRRP instance combines with the [Message Interval \(milliseconds\)](#) value to specify the administrative advertisement timer value. The master VRRP instance uses the combined value as a timer for sending VRRP advertisements; the backup VRRP instance uses it to derive the master down timer value for the VR instance. The value set for the parameter must be the same for every virtual router on the VRID. The range is 1 to 255. The default is 1.

Message Interval (milliseconds)

(messageIntervalMilSec)

The Message Interval (milliseconds) parameter specifies the time, in milliseconds, that the VRRP instance adds to the [Message Interval \(milliseconds\)](#) value to specify the administrative advertisement timer value. The master VRRP instance uses the combined value as a timer for sending VRRP advertisements; the backup VRRP instance uses it to derive the master down timer value for the VR instance. The value set for the parameter must be the same for every virtual router in the VRID. The range is 0 to 900, in increments of 100. The default is 0.

Name

See the [Name](#) parameter in section 36.1.

Owner

(owner)

The Owner parameter specifies the name of the router whose IP address (IPv4 or IPv6) is the same as the IP address of the virtual router. In owner mode, the backup IP address must be identical to one of the interface IP addresses. The backup address defines which IP addresses are in the VRRP advertisement IP address list. The options are:

- false (default)
- true

Ping Reply

(pingReply)

The Ping Reply specifies whether, on non-owner VRRP instances, ICMP echo request messages are prevented from being discarded at the IP interface of the instance when it is in master mode. ICMP echo request messages are always discarded in backup mode.

When the non-owner access ping reply is disabled, ICMP echo request messages destined to the non-owner virtual router instance IP addresses are silently discarded in both the master and backup modes. The options are:

- false (default)
- true

Preempt Mode

(preempt)

The Preempt Mode parameter specifies whether a VRRP instance overrides a non-owner master VRRP instance of a lower priority. The preempt command is only available for non-owner VRRP instances. The owner may not be preempted because the non-owner priority can never be higher than the owner priority.

When the Preempt Mode parameter is set to true, the priority of the incoming VRRP advertisement from the current master is compared to the priority configured on the local VRRP non-owner instance. If the local priority is higher, the received VRRP advertisement is discarded, resulting in the eventual expiration of the master down timer. A transition to the master state on the local VRRP non-owner instance therefore occurs.

When Preempt Mode parameter is set to false, the backup VRRP instance only becomes master if the master down timer expires before a VRRP advertisement is received from the master VRRP instance. The options are:

- false
- true (default)

SSH Reply

(sshReply)

The SSH Reply parameter specifies whether the non-owner master replies to SSH requests directed at the IP addresses of VRRP instances. When the SSH Reply parameter is not enabled, SSH requests to non-owner master virtual IP addresses are silently discarded. Non-owner backup virtual routers never respond to SSH requests, regardless of the SSH Reply parameter setting.

SSH must not have been disabled at the management security level (either on the IP interface or based on the SSH source host address). The options are:

- false (default)
- true

Standby Forwarding

(standByFwding)

The Standby Forwarding parameter specifies whether the router, when acting as a standby VRRP router, forwards traffic sent to the VRRP router MAC address. The parameter setting does not affect traffic sent to the physical router MAC address. The options are:

- false (default)
- true

The parameter can be configured only in VRRP instance non-owner mode.

Subnet Mask

(subnetMask)

The Subnet Mask parameter specifies the subnetwork mask of the backup IP address, in dotted-decimal format. The backup IP addresses must be on the same subnet. The range is 0 to 32. The default is 24.

Telnet Reply

(telnetReply)

The Telnet Reply parameter specifies whether the non-owner master replies to TCP port 23 Telnet requests directed at the IP addresses of VRRP instances. When the Telnet Reply parameter is disabled, the Telnet requests that are sent to non-owner master virtual IP addresses are silently discarded. Non-owner backup virtual routers do not respond to Telnet requests, regardless of the Telnet Reply parameter setting. The options are:

- false (default)
- true

Traceroute Reply

(traceRouteReply)

The Traceroute Reply parameter specifies whether a non-owner master replies to traceroute requests directed to the IP address of a VRRP instance.

A non-owner backup virtual router never responds to such traceroute requests regardless of the Traceroute Reply status. The options are:

- false (default)
- true

Type

(authenticationType)

The Type parameter specifies the type of authentication used to generate master VRRP advertisements and to validate VRRP advertisements. Table 26-1 describes the parameter options.

Table 26-1 Type parameter

Option	Option description
none (default)	No authentication is used.
password	A plain text password is used for authentication.

For more information, see “Key” in this section.

Virtual Router ID

(vrId)

The Virtual Router ID specifies the VRID. The parameter must have the same value on each virtual router associated with the redundant IP address. The VRID is included in all VRRP advertisements. The range is 1 to 255. The default is 0, which indicates that the parameter is not set.

VRRP Type

(vrrpType)

The VRRP Type parameter specifies the context of the VRRP instance. The options are:

- Network (default)
- IES
- VPRN

27 – Virtual Anycast RP parameters

27.1 Virtual Anycast RP parameters 27-2

27.1 Virtual Anycast RP parameters

This chapter describes the parameters on the Virtual Anycast RP form and child forms.

Anycast RP Type

(anyCastRPType)

The Anycast RP Type parameter specifies the type of Anycast RP. Table 27-1 describes the parameter options.

Table 27-1 Anycast RP Type parameter

Option	Option description	Dependencies
Network (default)	Defines a network-based Anycast RP type for base routing instances.	—
VPRN	Defines a VPRN-based anycast RP type for VRFs of the same VPRN service. The 5620 SAM uses the first discovered type if the anycast RP uses mixed routing instances. You can only mix routing instances in the same anycast RP using the CLI. The 5620 SAM raises an alarm if you add VRFs from different VPRNs to the same anycast RP set.	

Anycast RP Address

(anycastRpIPAddress)

The Anycast RP Address parameter specifies the IP address of a PIM anycast protocol instance for the RP. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP. The default is 0.0.0.0, which means that the parameter is not configured.

Auto Created Interface Name

(interfaceName)

The Auto Created Interface Name parameter specifies the default value used to name the loopback interface. The parameter value appears in the Enter Interface Name dialog in the 5620 SAM GUI. The range is 0 to 32 characters. There is no default.

Description

See the [Description](#) parameter in section 36.1.

Name

See the [Name](#) parameter in section 36.1.

Static Group IP Address

(staticGroupIPAddress)

The Static Group IP Address parameter combines with the Static Group Mask parameter to specify the range of multicast group addresses to which the router advertises the static RP address. The value of the Static Group IP Address parameter is sent as the RP address. The range is an IP address from 224.0.0.0 to 239.255.255.255.

Static Group Mask

(staticGroupMask)

The Static Group Mask parameter specifies the mask that, combined with the Static Group IP Address parameter value, provides the range of multicast group addresses to which the router advertises to become the static candidate RP. The range is 4 to 32. The default is 24.

28 – FIB Entries parameters

28.1 FIB Entries parameters 28-2

28.1 FIB Entries parameters

This chapter describes the parameters on the Manage FIB Entries form and child forms.

Auto Complete

The Auto Complete parameter specifies that the MAC address entered for a manually created FIB entry should be automatically created.

MAC Address

See the [MAC Address](#) parameter in section [36.1](#).

29 – Snapshot Instances parameters

29.1 Snapshot Instances parameters 29-2

29.1 Snapshot Instances parameters

This chapter describes the parameters on the Snapshot Instances form and child forms.

Description

(description)

The Description parameter specifies a description for the snapshot. The range is 0 to 252. The default is blank.

Gzip Exported File

(gzipExportedFile)

The Gzip Exported File parameter specifies whether Gzip file compression is applied to the exported snapshot file. The options are:

- Disabled (default)
- Enabled

Include Additional Information Attributes

(includeAdditionalInformation)

The Include Additional Information Attributes parameter specifies whether exported objects will include additional information attributes. The options are:

- Disabled (default)
- Enabled

Include Attributes with Read-Only Access

(includeReadOnlyAttributes)

The Include Attributes with Read-Only Access parameter specifies whether exported objects will include attributes with read-only access rights. The options are:

- Disabled (default)
- Enabled

Include Components and Attributes with Manufacturer Visibility

(includeManufacturerVisibility)

The Include Components and Attributes with Manufacturer Visibility parameter specifies whether exported objects will include components and attributes with manufacturer visibility. The options are:

- Disabled (default)
- Enabled

Include in the snapshot

(filtersOrNeEntities)

The Include in the snapshot parameter specifies which elements will be included in the snapshot. Table 29-1 describes the parameter options.

Table 29-1 Snapshot inclusion filter options

Option	Description
NE Entities Only (default)	The snapshot will only include objects for a specified set of NE entities.
Inclusion Filters Only	The snapshot will include all objects which match NEs which pass through specified search filters.
All Entities in the Network	The snapshot will include all applicable entities in the network.

Include States and Statuses

(includeStatesAndStatuses)

The Include States and Statuses parameter specifies whether exported objects will include administrative states and statuses. The options are:

- Disabled (default)
- Enabled

Snapshot Name

(displayName)

The Snapshot Name parameter specifies the snapshot name used to identify a snapshot object and associated export files. The character range is 1 to 64.

30 – Activation parameters

30.1 Activation parameters 30-2

30.1 Activation parameters

This chapter describes the parameters on the Activation form.

Name

(sessionName)

The Name parameter specifies the user assigned name for the session object. The range is 0 to 80.

Description

(description)

The Description parameter specifies the description for the activation session. The range is 0 to 252.

31 – Gateway configuration parameters

31.1 Gateway configuration parameters 31-2

31.1 Gateway configuration parameters

This chapter describes the parameters on the IPsec VPN form and child forms.

Accounting Interim Interval (s)

(acctIntmInterval)

The Accounting Interim Interval (s) parameter specifies the accounting interval, in s, for sending interim accounting information to the CDF. The range is 1 to 86 400. The default is 1800.

Accounting Level

(acctLevel)

The Accounting Level parameter specifies whether PDN-level accounting or QCI-level accounting is in effect. When PDN-level accounting is specified, diameter charging sessions to the CDF are set up on a per-PDN-connection basis. When QCI-level accounting is specified, diameter charging sessions to the CDF are set up on a per-bearer basis. The options are:

- QCI Level (default)
- PDN Level

Administrative State

(administrativeState)

The Administrative State parameter specifies whether the object is administratively enabled. The options are:

- Down (default)
- Up

Aggregated Downlink Rate (kbps)

(aggregatedDownlinkRate)

The Aggregated Downlink Rate (kbps) parameter specifies the maximum aggregate downlink bit rate per PDN for all non-GBR bearers for a UE. The range is 0 to 100 000. The default is 0.

Aggregated Uplink Rate (kbps)

(aggregatedUplinkRate)

The Aggregated Uplink Rate (kbps) parameter specifies the maximum aggregate uplink bit rate per PDN for all non-GBR bearers for a UE. The range is 0 to 100 000. The default is 0.

Allocation Type

(allocationType)

The Allocation Type parameter specifies whether a UE gets an IP address using RAN signaling or DHCP client functionality after the default bearer is established. The options are:

- ranSignaling (default)
- ietf

Application Transaction Timer (s)

(applTxTimer)

The Application Transaction Timer parameter specifies, in s, the application transaction timer for ACRs and ACAs. The range is 1 to 30. The default is 5.

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

Bearer Timeout (seconds)

(bearerTimeout)

The Bearer Timeout (seconds) parameter specifies the time, in s, that a bearer must be idle before the bearer is released. The default bearer cannot be released when the dedicated bearer has not reached the timeout value. The range is 300 to 3600. The default is 1800. A parameter value of 0 means that the parameter is disabled.

Configuration File Limit (Mbps)

(ocCf1Limit)

The Configuration File Limit (Mbps) specifies, in Mbytes, the maximum space that can be used to store ACR files on compact flash Cf1. When the limit is reached, the system can no longer support accurate charging. The range is 0 to 4 294 967 295. The default is 0.

Configuration File Limit (Mbps)

(ocCf2Limit)

The Configuration File Limit (Mbps) specifies the maximum space, in Mbytes, that can be used to store ACR files on compact flash Cf2. When the limit is reached, the system can no longer support accurate charging. The range is 0 to 4 294 967 295. The default is 0.

Description

(description)

The Description parameter specifies the APN associated with a UE. The range is 1 to 80 characters. The default is blank.

Duration before File Closure (hours)

(ocFileClsLifeTime)

The Duration before File Closure (hours) parameter specifies, in h, how long a file can remain open. The file is closed after the specified time. The range is 1 to 24. The default is 1.

Duration before File Deletion (days)

(ocFileObsoleteTime)

The Duration before File Deletion parameter specifies, in days, the time that a file is stored before deletion. The range is 1 to 31. The default is 7.

Dynamic PCC

(pccDynamicState)

The Dynamic PCC parameter specifies whether the gateway uses PCC rules sent from the PCRF during the creation of dedicated bearers. The options are.

- Disabled (default)
- Enabled

File Extension

(ocFileExtension)

The File Extension parameter specifies a file extension character string that is used in the file name. The range is 0 to 8 characters. There is no default.

Home Subscriber Server Assigned

(isIPAllocationHssStatic)

The Home Subscriber Server Assigned parameter specifies whether the UE IP address is the static IP address that is assigned by the HSS for the MME and sent to the PGW during the creation of the session. The options are:

- disabled (default)
- enabled

Ignore All

(chargingIgnoreAny)

The Ignore All parameter specifies whether the gateway ignores the HSS- or MME-supplied charging characteristics for all subscribers. Table 31-1 describes the parameter options.

Table 31-1 Ignore All parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default profiles.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profiles.

Ignore All

(chrgCcIgnoreAnyAdministrativeState)

The Ignore All parameter specifies how the APN processes HSS- or MME- supplied charging characteristics for all subscribers. Table 31-2 describes the parameter options.

Table 31-2 Ignore All parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default profiles.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profiles.
Inherit	Use the profiles inherited from the PGW configuration.

Ignore Home

(chargingIgnoreHome)

The Ignore Home parameter specifies whether the gateway ignores the charging characteristics supplied by the HSS or MME for all home subscribers. Table 31-3 describes the parameter options.

Table 31-3 Ignore Home parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default charging profile.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profile.

Ignore Home

(chrgCcIgnoreHomeAdministrativeState)

The Ignore Home parameter specifies how the APN processes charging characteristics supplied by the HSS or MME for home subscribers. Table 31-4 describes the parameter options.

Table 31-4 Ignore Home parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default profile.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profile.
Inherit	Use the profile inherited from the PGW configuration.

Ignore Roaming

(chargingIgnoreRoaming)

The Ignore Roaming parameter specifies whether the gateway ignores the charging characteristics supplied by the HSS or MME for roaming subscribers. Table 31-5 describes the parameter options.

Table 31-5 Ignore Roaming parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default profile.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profile.

Ignore Roaming

(chrgCcIgnoreRoamingAdministrativeState)

The Roaming Subscribers parameter specifies how the APN processes charging characteristics supplied by the HSS or MME for roaming subscribers. Table 31-6 describes the parameter options.

Table 31-6 Ignore Roaming parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default profile.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profile.
Inherit	Use the charging profile inherited from the PGW configuration.

Ignore Visiting

(chargingIgnoreVisiting)

The Ignore Visiting parameter specifies whether the gateway ignores the charging characteristics supplied by the HSS or MME for visiting subscribers. Table 31-7 describes the parameter options.

Table 31-7 Ignore Visiting parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default profile.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profile.

Ignore Visiting

(chrgCcIgnoreVisitAdministrativeState)

The Ignore Visiting parameter specifies how the APN processes the charging characteristics supplied by the HSS or MME for visiting subscribers. Table 31-8 describes the parameter options.

Table 31-8 Ignore Visiting parameter

Option	Description
Disabled (default)	Use the charging characteristics supplied by the MME or HSS. If a matching profile cannot be found, use the default profile.
Enabled	Ignore the charging characteristics supplied by the MME or HSS and use the default profile.
Inherit	Use the charging characteristics inherited from the PGW configuration.

Inherit Home Profile From Gateway

(chrgProfileHomeInherit)

The Inherit Home Profile From Gateway parameter specifies whether the APN uses the same home charging profile as the PGW or one specified by the user. The parameter must be configured on the PGW NE using the CLI. See the appropriate PGW NE documentation for information about configuring the parameter.

Inherit Roaming Profile From Gateway

(chrgProfileRoamingInherit)

The Inherit Roaming Profile From Gateway parameter specifies whether the APN uses the same roaming charging profile as the PGW or one specified by the user. The parameter must be configured on the PGW NE using the CLI. See the appropriate PGW NE documentation for information on configuring the parameter.

Inherit Visiting Profile From Gateway

(chrgProfileVisitingInherit)

The Inherit Visiting Profile From Gateway parameter specifies whether the APN uses the same visiting charging profile as the PGW or one specified by the user. The parameter must be configured on the PGW NE using the CLI. See the appropriate PGW NE documentation for information on configuring the parameter.

Inclusion of Charging-Group-ID AVP in ACR

(chargingGroupIDEnabled)

The Inclusion of Charging-Group-ID AVP in ACR parameter specifies whether the charging-group-ID AVP is included in an ACR message. The options are:

- enabled (default)
- disabled

IP Pool Address Hold Timer (minutes)

(addressHoldTimer)

The IP Pool Address Hold Timer (minutes) parameter specifies the time, in m, that a pool holds a newly released IP address before the address is available for reassignment. The range is 0 to 10. The default is 3.

IP Pool ID

(poolId)

The IP Pool ID parameter specifies the unique numeric identifier of an IP address pool. The range is 0 to 255. The default is 0.

IP Pool Name

(poolName)

The IP Pool Name parameter specifies the name of an IP address pool. The range is 1 to 32 characters. There is no default.

IP v4/v6

(typeIpv4v6Supported)

The IPv4/v6 parameter specifies whether an APN supports IP v4/v6 PDN sessions. The options are:

- disabled (default)
- enabled

IPv4

(typeIpv4Supported)

The IPv4 parameter specifies whether an APN supports IPv4 PDN sessions. The options are:

- disabled (default)
- enabled

IPV4 Primary Address

(pcoDnsV4PriAddr)

The IPV4 Primary Address parameter specifies an IPv4 address for the primary PCO DNS server. You must enable the check box beside the parameter before you can configure the IPv4 address in dotted decimal format. The check box is disabled by default.

IPV4 Primary Address

(pcoNbnsV4PriAddr)

The IPV4 Primary Address parameter specifies an IPv4 address for the primary PCO NetBIOS server. You must enable the check box beside the parameter before you can configure the IPv4 address in dotted decimal format. The check box is disabled by default.

IPV4 Primary Address

(pcoPcscfV4PriAddr)

The IPV4 Primary Address parameter specifies an IPv4 address for the primary PCO PCSCF server. You must enable the check box beside the parameter before you can configure the IPv4 address in dotted decimal format. The check box is disabled by default.

IPv4 Secondary Address

(pcoDnsV4SecAddr)

The IPv4 Secondary Address parameter specifies an IPv4 address for the secondary PCO DNS server. You must enable the check box beside the parameter before you can configure the IPv4 address in dotted decimal format. The check box is disabled by default.

IPv4 Secondary Address

(pcoNbnsV4SecAddr)

The IPv4 Secondary Address parameter specifies an IPv4 address for the secondary PCO NetBIOS server. You must enable the check box beside the parameter before you can configure the IPv4 address in dotted decimal format. The check box is disabled by default.

IPv6

(typeIpv6Supported)

The IPv6 parameter specifies whether an APN supports IPv6 PDN sessions. The options are:

- disabled (default)
- enabled

IPv6 Primary Address

(pcoDnsV6PriAddr)

The IPv6 Primary Address parameter specifies an IPv6 address for the primary PCO DNS server. You must enable the check box beside the parameter before you can configure the IPv6 address in colon-hexadecimal format. The check box is disabled by default.

IPv6 Primary Address

(pcoPcscfV6PriAddr)

The IPv6 Primary Address parameter specifies an IPv6 address for the primary PCO PCSCF server. You must enable the check box beside the parameter before you can configure the IPv6 address in colon-hexadecimal format. The check box is disabled by default.

IPv6 Secondary Address

(pcoDnsV6SecAddr)

The IPv6 Secondary Address parameter specifies an IPv6 address for the secondary PCO DNS server. You must enable the check box beside the parameter before you can configure the IPv6 address in colon-hexadecimal format. The check box is disabled by default.

Is Exclusive

(isExclusive)

The Is Exclusive parameter specifies whether an APN uses an IP address pool exclusively. The options are:

- disabled (default)
- enabled

Limit for the number of ACRs

(ocFileClsMaxAcrs)

The Limit for the number of ACRs parameter specifies the number of ACRs that are stored in a file. The file is closed after the specified limit is reached. The range is 100 to 5000. The default is 1000.

Local Pool

(ipAllocLocalPool)

The Local Pool parameter specifies whether the IP address of a UE can be assigned from the configured local IP address pools. The options are:

- enabled (default)
- disabled

Mobile Station APN Selection Mode

(selectMsProvided)

The Mobile Station APN Selection Mode parameter specifies whether the APN selection mode provided by a mobile station is allowed. APN selection mode verification is used to allow a mobile station subscription to use the APN. The parameter value must match the corresponding value on the MME. If the values do not match, the PGW rejects the session.

- disabled (default)
- enabled

Multiple PDNs allowed

(allowMultiplePdns)

The Multiple PDNs allowed parameter specifies whether multiple PDN types are allowed on an APN. Select the check box to allow multiple PDN types on the APN.

Name

(apnName)

The Name parameter specifies the APN associated with a UE. The range is 1 to 80 characters. The default is blank.

Network APN Selection Mode

(selectNwProvided)

The Network APN Selection Mode parameter specifies whether the network-provided APN selection mode is allowed. Selection mode verification is used to allow a mobile station subscription to use the APN. The value of the parameter must match the corresponding value on the MME. If the two values do not match, the PGW rejects the session. Select the check box to enable the network-provided APN selection mode.

Node ID

(nodeId)

The Node ID parameter specifies the string assigned to a node. The range is 0 to 20 characters. There is no default.

Operator-string AVP of an ACR Message

(operatorString)

The Operator-string AVP of an ACR Message parameter specifies an operator-specific string to be included in the operator-string AVP (non-standard) of an ACR message. The range is 0 to 80 characters. There is no default.

Origin Host

(diameterOriginHost)

The Origin Host parameter specifies the originating host name of a diameter node. The originating host information is sent to a diameter peer in request messages. The range is 0 to 80 characters. The default is N/A, which means that the parameter is not configured.

Origin Realm

(diameterOriginRealm)

The Origin Realm parameter specifies the originating realm or domain name of a diameter node. The originating realm is included in messages that are exchanged with a diameter peer. The range is 0 to 80 characters. The default is N/A, which means that the parameter is not configured.

PCRF Selection Dynamic PCC

(pcrfDynamicPccAdminState)

The PCRF Selection Dynamic PCC parameter specifies whether interaction with the PCRF is enabled for bearer creation. When interaction is enabled, the PCRF sends the PCC rules for dedicated bearer creation. When the parameter is set to inherit, the value is inherited from the dynamic PCC state of the PGW.

Pool Address Block

(isPoolAddrBlock)

The Pool Address Block parameter specifies whether the reassignment of a released IP address is allowed. The options are:

- disabled (default)
- enabled

Pool Address Type

(poolAddressType)

The Pool Address Type parameter specifies the type of IP address pool entry. The options are:

- IPv4 (default)
- IPv6

Pool IP Address

(poolIpAddress)

The Pool IP Address parameter specifies the IP pool address. You can specify an IPv4 or IPv6 address. There is no default.

Prefix Length

(prefixLength)

The Prefix Length parameter specifies the length of the IP prefix for the IP pool address. The range is 0 to 128. The default is 0.

Primary Compact Flash

(ocPrimaryCf)

The Primary Compact Flash parameter specifies which compact flash is the primary storage location for ACR files. If you try to set cf1 and cf1 is not available, cf2 is set as the primary storage location. If you try to set cf2 and cf2 is not available, cf1 is set as the primary storage location. The options are:

- cf1 (default)
- cf2

Private Info

(ocFilePrivateInfo)

The Private Info parameter specifies a private information field that is used in the file name.

Reject Charging

(chargingCcReject)

The Reject Charging parameter specifies whether subscriber charging takes place when the charging characteristics supplied by the HSS or MME do not contain a matching gateway profile. This parameter applies to only those subscribers that are not ignoring charging characteristics supplied by the HSS or MME. Table 31-9 describes the parameter options.

Table 31-9 Reject Charging parameter

Option	Description
Disabled (default)	Use the charging characteristics specified by the parameter settings on the gateway. See the Ignore All , Ignore Home , Ignore Roaming , and Ignore Visiting parameters in this section for more information.
Enabled	Charging only takes place when a matching profile is found on the gateway.

Reject Charging

(chargingReject)

The Reject Charging parameter specifies whether subscriber charging takes place when the charging characteristics supplied by the HSS or MME do not contain a matching APN profile. This parameter applies to only those subscribers that are not ignoring charging characteristics supplied by the HSS or MME. Table 31-10 describes the parameter options.

Table 31-10 Reject Charging parameter

Option	Description
Disabled (default)	Use the charging characteristics specified by the parameter settings on the APN. See the Ignore All , Ignore Home , Ignore Roaming , and Ignore Visiting parameters in this section for more information.
Enabled	Charging takes place only when a matching profile is found on the APN.
Inherit	Charging takes place only when a matching profile, inherited from the PGW, is found.

Reject Foreign Subscribers

(rejectForeignSubscribers)

The Reject Foreign Subscribers parameter specifies whether only subscribers from the home PLMN are allowed. The options are:

- enabled (default)
- disabled

Restriction Type

(restrictionType)

The Restriction Type parameter specifies the restriction level applied to EPS bearer contexts that are created to the APN. The value of the parameter determines whether a UE is allowed to establish EPS bearers to other APNs. The options are:

- any (default)
- public1
- public2
- private1
- private2

Retry Count

(diameterRetryCount)

The Retry Count parameter specifies the number of times that the 5620 SAM tries to retransmit a message before it declares the attempt to be failed. The range is 1 to 8. The default is 3.

Retry Count for ACR Messages (s)

(retryCount)

The Retry Count for ACR Messages parameter specifies the number of times that the same message is resent before the message is declared a failure. The range is 1 to 8. The default is 3.

Session Timeout (seconds)

The Session Timeout (seconds) parameter specifies, in s, the timeout value of a session. When a session times out, each bearer associated with the PDN session is deleted. The range is 0 or 1800 to 86 400. The default is 86 400. A value of 0 means that the parameter is disabled.

Size Limit Before File Closure (Mbps)

(ocFileClosureSize)

The Size Limit Before File Closure parameter specifies the maximum size, in Mbytes, that an ACR file can be before it is closed. The range is 1 to 100. The default is 5.

Span

The Span parameter specifies whether span of control filtering is enabled. Table 31-11 describes the parameter options.

Table 31-11 Span parameter

Option	Description
Span Off (default, if span filtering is disabled on the User Preferences form)	Span of control filtering is disabled; objects in the View Access and Edit Access spans of the current user are displayed.
Span On (default, if span filtering is enabled on the User Preferences form)	Span of control filtering is enabled; only objects in the Edit Access spans of the current user are displayed.
User Preference	Span of control filtering is enabled or disabled, as configured on the User Preferences form.

Subscribed APN Selection Mode

(selectSubscribed)

The Subscribed APN Selection Mode parameter specifies whether the subscribed APN selection mode is allowed. Selection mode verification allows an MS to use the APN. The parameter value must match the corresponding value on the MME. If the values do not match, the PGW rejects the MS session. The options are:

- enabled (default)
- disabled

Transaction Timer (s)

(diameterTransactionTimer)

The Transaction Timer (s) parameter specifies the maximum amount of time, in s, that the node waits for a diameter peer to respond before it tries another peer. The range is 1 to 180. The default is 5.

Type

(type)

The Type parameter specifies the type of APN. A virtual APN reduces the amount of APN provisioning by consolidating access to all real APNs through a single virtual APN at the PGW. The options are:

- Real (default)
- Virtual

32 – Mobile Regions parameters

32.1 Mobile Regions parameters 32-2

32.1 Mobile Regions parameters

This chapter describes the parameters on the Mobile Regions forms and the child forms.

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the mobile region. The options are:

- Enabled (default)
- Disabled

Mobile Country Code

(mcc)

The Mobile Country Code parameter specifies the unique three-digit identifier that represents the country of the mobile subscriber. Choose a value from the drop-down menu. The default is unspecified.

Mobile Network Code

(mnc)

The Mobile Network Code parameter specifies the unique two- or three-digit identifier that is used with the MCC and represents the mobile network operator or carrier. The range is 2 to 3 characters. The default is 00.

Region ID

(id)

The Region ID parameter specifies the identification number assigned to a region. The Region ID parameter is not available when the Auto-Assign ID parameter is enabled. The range is 1 to 1024 characters. The default is 0.

Region Name

(regionString)

The Region Name parameter specifies a name for the LTE region. The range is 1 to 10 characters. The default is Default.

33 – LTE User Stats parameters

33.1 LTE User Stats parameters 33-2

33.1 LTE User Stats parameters

This chapter describes the parameters on the LTE User Stats forms and the child forms.

APN Name

(apnName)

The APN Name parameter specifies the name of an APN to use as a query match criterion. The parameter is configurable when the [Include All APNs](#) parameter is disabled. The range is 1 to 80 characters. There is no default.

Bearer Context

(includeBearerContext)

The Bearer Context parameter specifies whether the query is to return bearer context statistics. The options are:

- enabled (default)
- disabled

Bearer ID

(bearerId)

The Bearer Id parameter specifies a bearer identification string to use as a query match criterion. The parameter is configurable when the [Include All Bearers](#) parameter is disabled. The range is 1 to 15 characters. The default is 0, which means that the parameter is not configured.

Description

(description)

The Description parameter specifies a description for the query. The range is 0 to 256 characters. There is no default.

IMSI

(ueImsi)

The IMSI parameter specifies the IMSI of the user that is the target of the query. Specify a 6- to 15-digit IMSI. There is no default.

Include All APNs

(apnNameAll)

The Include All APNs parameter specifies whether the query is to return statistics for all APNs associated with the user. The options are:

- enabled (default)
- disabled

Include All Bearers

(bearerIdAll)

The Include All Bearers parameter specifies whether the query is to return statistics for all bearers associated with the user. The options are:

- enabled (default)
- disabled

Include All Directions

(sdfFilterDirectionAll)

The Include All Directions parameter specifies whether the query is to return statistics for all directions of user traffic. The options are:

- enabled (default)
- disabled

Include All IDs

(sdfFilterIdAll)

The Include All IDs parameter specifies whether the query is to return statistics for all SDF filters associated with the user. The options are:

- enabled (default)
- disabled

Include All Precedences

(sdfPrecedenceAll)

The Include All Precedences parameter specifies whether the query is to return statistics for all precedences. The options are:

- enabled (default)
- disabled

PDN Context

(includePdnContext)

The PDN Context parameter specifies whether the query is to return PDN context statistics. The options are:

- enabled (default)
- disabled

SDF

(includeSdf)

The SDF parameter specifies whether the query is to return SDF statistics. The options are:

- enabled (default)
- disabled

SDF Direction

(sdfFilterDirection)

The SDF Direction parameter specifies an SDF direction to use as a query match criterion. The parameter is configurable when the [Include All Directions](#) parameter is disabled. The options are:

- undefined
- preRel7
- downLink
- upLink
- biDir

SDF Filter

(includeSdfFilter)

The SDF Filter parameter specifies whether the query is to return SDF filter statistics. The options are:

- enabled (default)
- disabled

SDF Filter ID

(sdfFilterId)

The SDF Filter ID parameter specifies an SDF filter identifier to use as a query match criterion. The parameter is configurable when the [Include All IDs](#) parameter is disabled. The range is 0 to 16. The default is 0.

SDF Precedence

(sdfPrecedence)

The SDF Precedence parameter specifies an SDF preference to use as a query match criterion. The parameter is configurable when the [Include All Precedences](#) parameter is disabled. The range is 0 to 65 535.

34 — LTE EPS Path Drill Down Hints parameters

34.1 LTE EPS Paths Drill Down Hints parameters 34-2

34.1 LTE EPS Paths Drill Down Hints parameters

This chapter describes the parameters on the LTE EPS Paths Drill Down Hints forms, the child forms, and the forms opened from other contextual menus.

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the path drill-down hint. The options are:

- Enabled (default)
- Disabled

Connection Type

(connectionType)

The Connection Type parameter specifies the type of transport segment connection that the 5620 SAM supports for each EPS path type. The connection type depends on the [Segment Type](#) parameter. The options are:

- Managed L2 Transport
- Managed Spoke Connector
- Physical Link
- Unmanaged L2 Transport
- unspecified

Description

(description)

The Description parameter specifies a description for the path drill-down hint. The range is 0 to 30. The default is blank.

Encapsulation Type

(encapType)

The Encapsulation Type parameter specifies the type of encapsulation to be configured on the Epipe SAP of a L2 VPN. The options are:

- Null
- Dot1 Q
- Q in Q

High Priority

(selectedForDrillDown)

The High Priority parameter specifies whether the EPS path drill-down hint is selected as a high-priority hint. A high-priority hint is a hint that the 5620 SAM uses during the automatic correlation of the transport layer with a new EPS path. The default is selected.

ID

(id)

The ID parameter specifies a unique ID for the path drill-down hint. The range is 1 to 30. The default is 0.

Inner Encapsulation Value

(innerEncapValue)

The Inner Encapsulation Value parameter specifies the inner encapsulation value for the port. This parameter is configurable when the [Encapsulation Type](#) parameter for the port is Q in Q. The range is 0 to 4094, or 4095 to indicate *. The default is 0. A value of 4095 is equivalent to * using the CLI, which indicates that all tags are accepted, regardless of the value. A value of 0 indicates that the port does not have a tag.

Order

(order)

The Order parameter specifies the position of a segment in an EPS path drill-down hint. The range is 1 to 30. The default is 0.

Outer Encapsulation Value

(outerEncapValue)

The Outer Encapsulation Value parameter specifies the outer encapsulation value for the port. This parameter is configurable when the [Encapsulation Type](#) for the port is set to Dot1 Q, or Q in Q. The range is 0 to 4095. The default is 0.

Segment Type

(segmentType)

The Segment Type parameter specifies a portion of the transport topology that underlies an EPS path. The segment types depend on the EPS path type that is specified by the [Type](#) parameter. The options are:

- eNodeB-NE
- NE-NE
- NE-SGW
- SGW-MME
- SGW-PGW
- PGW-PCRF
- unspecified

Type

(type)

The Type parameter specifies the type of EPS path for which the drill-down hint is configured. The options are:

- Gx
- S1-u (default)
- S11
- S5

35 – Call Trace parameters

35.1 Call Trace parameters 35-2

35.1 Call Trace parameters

This chapter describes the parameters on the Manage Call Trace Sessions form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 36.1.

Call Trace Session Name

(callTraceSessionName)

The Call Trace Session Name parameter specifies the name of a call-trace session. The range is 0 to 32 characters. There is no default.

Call Trace UDP Port

(callTraceUdpPort)

The Call Trace UDP Port parameter specifies the 5620 SAM auxiliary-server UDP port number for call-trace data collection. The range is 49 152 to 65 535. The default is 57 074.

Description

See the [Description](#) parameter in section 36.1.

Disk Usage Alarm Severity

(diskUsageAlarmSeverity)

The Disk Usage Alarm Severity parameter specifies the severity of the alarm that is raised when the 5620 SAM detects call-trace disk usage above the threshold specified by the [Disk Usage Alarm Threshold](#) parameter. The options are:

- cleared
- indeterminate
- info
- condition
- warning
- minor (default)
- major
- critical

Disk Usage Alarm Threshold

(diskUsageThreshold)

The Disk Usage Alarm Threshold parameter specifies the percentage of consumed call-trace disk space above which the 5620 SAM raises an alarm. The range is 1 to 95. The default is 80.

File Retention Time (hrs)**(fileRetentionTime)**

The File Retention Time (hrs) parameter specifies, in h, the length of time to keep each call-trace data file on the 5620 SAM auxiliary server. The range is 1 to 336. The default is 168.

File Rollover Time (min)**(rolloverTime)**

The File Rollover Time (min) parameter specifies, in m, the length of time during which the 5620 SAM auxiliary server writes call-trace data to each file. After the specified time elapses, the auxiliary server closes the current file and opens a new file for data collection. The range is 1 to 60. The default is 15.

IRAT Handover Threshold**(iratHThreshold)**

The IRAT Handover Threshold parameter specifies the number of outgoing IRAT handover attempts that trigger an event-based call trace session. The range is 0 to 300 000. The default is 0.

isPCMDEnabled**(isPCMDEnabled)**

The PCMD Collection Enabled parameter specifies whether PCMD collection is enabled for all cells on the eNodeB. The options are:

- disabled (default)
- enabled

isSignBasedCTEnabled**(isSignBasedCTEnabled)**

The Signaling Based Call Trace Enabled parameter specifies whether signaling-based call trace is enabled for all cells on the eNodeB. The options are:

- disabled
- enabled (default)

RRC Re-establishment Threshold**(rrcReestablishmentThreshold)**

The RRC Re-establishment Threshold parameter specifies the number of RRC connection re-establishment attempts that trigger an event-based call trace session. The range is 0 to 300 000. The default is 0.

Trace ID

(traceId)

The Trace ID parameter specifies the unique identifier of a call-trace session. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 32 767. The default is 0, which means that the parameter is not configured.

Trace Interface RRC (Uu)

(isRRCTraced)

The Trace Interface RRC (Uu) parameter specifies whether the RRC interface is to be traced. The options are:

- disabled
- enabled (default)

Trace Interface S1-MME

(isS1MMETraced)

The Trace Interface S1-MME parameter specifies whether the S1-MME interface is to be traced. The options are:

- disabled
- enabled (default)

Trace Interface X2

(isX2Traced)

The Trace Interface X2 parameter specifies whether the X2 interface is to be traced. The options are:

- disabled
- enabled (default)

Traffic Threshold (Connected UE) (%)

(trafficThreshold)

The Traffic Threshold (Connected UE) (%) parameter specifies the percentage of connected UE traffic that triggers an event-based call trace session. The range is 0 to 100. The default is 0, which means that the parameter is not configured.

36 — Common Manage menu parameters

36.1 Common Manage menu parameters 36-2

36.1 Common Manage menu parameters

This chapter describes the parameters that are common to the 5620 SAM Manage menus forms.



Note — This chapter also describes parameters common to the Service Template form and child forms. Service templates are intended for use in the 5620 SAM GUI. Alcatel-Lucent does not recommend using the 5620 SAM-O XML classes and methods associated with service templates.

Address ID

(index)

The Address ID parameter specifies a numeric identifier for the IP address. The range is 1 to 16. The default is 0, which means that the parameter is not configured.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled. The options are:

- Up (default)
- Down

Aggregate Rate Limit (kbps)

(egressAggRateLimit)

The Aggregate Rate Limit (kbps) parameter specifies, in kb/s, the maximum transmission rate of all egress queues for the access interface. You must select Assign Aggregate Rate Limit before you can configure the parameter. The range is -1, which means unlimited, or 1 to 40 000 000. When the parameter value is greater than zero, you cannot specify an egress scheduler.

Allow Binding Of Templates Not Associated With Any Subscriber

The Allow Binding Of Templates Not Associated With Any Subscriber parameter specifies whether you can bind templates even when they do not have a subscriber association. The options are:

- enabled (default)
- disabled

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

Configured IP MTU (Octets)

(ipMtu)

The Configured IP MTU (Octets) parameter specifies the maximum IP MTU size, in bytes, that the interface transmits. The range is 0, or 512 to 9000. A value of zero specifies that the value is set to the interface default, which is calculated by subtracting the DLC header size from the physical MTU size of the interface.

The Operational IP MTU value for the interface is displayed on the interface configuration form after interface creation. This value indicates the size of the largest IP MTU that the interface transmits. It is the lesser of the parameter value and the operational MTU value of the physical port to which the interface is bound.

Description

(description)

The Description parameter specifies a description for the created object. The range is 0 to 80 characters for most objects. Table 36-1 lists the exceptions.

Table 36-1 Description parameter

Object	Range
Bypass-only LSP	0 to 500
Call-trace session	0 to 255
Dynamic LSP	0 to 500
MPLS path	0 to 500
Template	0 to 500

Disable Fix Window

(ignoreFix)

The Disable Fix Window parameter specifies whether the solution recommended by the 5620 SAM can be applied to the problem. The options are:

- Enabled
- Disabled (default)

When you set the Disable Fix Window parameter to Enabled, you cannot choose the Fix Problem option to apply the 5620 SAM-recommended solution.

Frame Base Accounting

(egressFrameBaseAccounting)

The Frame Base Accounting parameter specifies whether to use Frame Base Accounting or packet-based accounting. Frame Base Accounting uses inter-frame gap and instructions to calculate overhead. The options are:

- Enabled
- Disabled (default)

Gateway MAC Address

(macAddress)

The Gateway MAC address parameter specifies the MAC address used by an SRRP instance. Unless specified, the system uses the same base MAC address for all SRRP instances. The same SRRP gateway MAC address should be in use by both the local and remote routers participating in the same SRRP context. The SRRP gateway MAC address can only be changed or removed when the SRRP instance is shutdown. Any MAC address except broadcast or multicast addresses can be used, expressed in normal Ethernet MAC address format. The default is 00-00-00-00-00-00.

ID

(id)

The ID parameter specifies a unique ID for the created object. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 65 535. The default is 0.

Inner Encapsulation Value

(innerEncapValue)

The Inner Encapsulation Value parameter specifies the inner encapsulation value for the port. This parameter is configurable when the Encap Type parameter value for the port is Q in Q. The range is 0 to 4094, or 4095 to indicate *. The default is 0. A value of 4095 is equivalent to * using CLI, which indicates that all tags are accepted, regardless of value. You can also use an asterisk (*). A value of 0 indicates that the port has no tag.

Interface ID

(id)

The Interface ID parameter specifies a unique ID for the interface. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 5119. The default is 0.

IP Address

(ipAddress)

The IP Address parameter specifies the IP address for an IES or VPRN neighbor, or for a numbered L3 interface. Specify an IP address in dotted-decimal format for IPv4, or in colon-hexadecimal format for IPv6. There is no default.

Keep Alive Interval

(interval)

The Keep Alive Interval parameter specifies the interval between SRRP advertisement messages sent when operating in the master state. The interval is also the basis for setting the master down timer used to determine when the master is no longer sending. The range is 1 to 100, and the value is in hundreds of milliseconds. The default is 1.

MAC Address

(macAddress)

The MAC Address parameter specifies the unicast MAC address. The default is 00-00-00-00-00-00.

Name

(displayName)

The Name parameter specifies the name of an object. The range is 1 to 32 characters for most objects; Table 36-2 lists the exceptions. There is no default.

Table 36-2 Name parameter

Object	Range (characters)
Virtual Anycast RP	1 to 80
VR	0 to 32
VPRN IPsec interface	0 to 32

Next Hop

See the [Next Hop](#) parameter in section 192.1.

Outer Encapsulation Value

(outerEncapValue)

The Outer Encapsulation Value parameter specifies the outer encapsulation value for the port. This parameter is configurable when the port encapsulation is dot1q, QinQ, BCP dot 1q, or frame relay. Table 36-3 lists the ranges for different encapsulation types. The default is 0.

Table 36-3 Outer Encapsulation Value parameter

Encapsulation type	Range	Range description
dot1q	0 to 4094, 8191	8191 indicates an Ethernet Tunnel Endpoint Control SAP
QinQ	0 to 4094	—
BCP dot1q	0 to 4094	—
FR	16 to 1022	—
Default SAP	4095 or *	<ul style="list-style-type: none">• Ethernet ports only• Dot1Q ports• VPLS and Epipe VLL• Null encapsulated port cannot exist on the same port as a default SAP

Prefix Length

(prefixLength)

When combined with an IP address value, the Prefix Length parameter specifies a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. The prefix must not overlap with other existing IP prefixes that are defined as local subnets on other IP interfaces in the same routing context within the device or service. The range is 1 to 32 for an IPv4 address, and 1 to 128 for an IPv6 address. A value of 32 is typically reserved for an IPv4 system address, but is available for general use in IPv6. The IPv4 default is 24; the IPv6 default is 64.

Priority

(priority)

The Priority parameter specifies the SRRP instance priority advertised by the SRRP instance to its neighboring NE. The SRRP instance priority is compared to the priority received from the neighboring NE. The NE with the best (highest) priority enters the master state while the other NE enters the backup state. If the priority of each NE is the same, the NE with the lowest source IP address in the SRRP advertisement message assumes the master state. The range is 1 to 254. The default is 100.

Remote IP Address

(remoteIpAddress)

The Remote IP Address parameter specifies a remote IP address for the interface. The default is 0.0.0.0.

SAP Administrative State

The SAP Administrative State parameter specifies whether the SAP is administratively enabled. The options are:

- Up (default)
- Down

SAP Description

The SAP Description parameter specifies a description for the SAP. The range is 0 to 80 characters.

Service Description

The Service Description parameter specifies a description for the created service. The range is 0 to 80 characters.

SRRP ID

(**srrpId**)

The SRRP ID parameter specifies a 32-bit instance ID that must be unique to the system. The instance ID must also match the instance ID used by the remote router that is participating in the same SRRP context. The range is 1 to 4 294 967 295. The default is 0.

Subscriber ID

(**subscriberId**)

The Subscriber ID parameter specifies a unique ID for the subscriber (customer). The range is 1 to 2 147 483 647. The default is 1.

Trusted

Table 36-4 lists where to find more information about the Trusted parameter.

Table 36-4 Trusted parameter

Parameter	See
Trusted for L3 interface	Trusted parameter in section 14.1
Trusted for DHCP	Trusted parameter in section 14.1

Use Multipoint Shared Queue

(**usesMultipointShared**)

The Use Multipoint Shared Queue parameter specifies whether the access interface uses a multipoint shared queue on the device. The options are:

- false (default)
- true

The 5620 SAM automatically enables the Use Shared Queue parameter when the Use Multipoint Shared Queue parameter is set to true.

Use Shared Queue

(sharedQueueOn)

The Use Shared Queue parameter specifies whether the access interface uses the shared queue on the device. The options are:

- enabled
- disabled (default)

The 5620 SAM automatically enables the Use Shared Queue parameter when the Use Multipoint Shared Queue parameter is set to true.

VC ID

(vcId)

The VC ID parameter specifies the value used by each end of a service tunnel to identify the VC. The range is 0 to 4 294 967 295. The default is 0.

VC Type

See the [VC Type](#) parameter in section 21.1.

VLAN VC Tag

(vlanVcTag)

The VLAN VC Tag parameter specifies a dot1q value for encapsulation to the far end of the service tunnel. The range is 0 to 4095. The default is None.

Policies menu parameters

- 37 – Access Ingress parameters
- 38 – 7210 Access Ingress parameters
- 39 – Access Egress parameters
- 40 – 7210 Access Egress parameters
- 41 – ATM QoS parameters
- 42 – MLPPP Ingress QoS Profile parameters
- 43 – MLPPP Egress QoS Profile parameters
- 44 – MCFR Ingress QoS Profile parameters
- 45 – MCFR Egress QoS Profile parameters
- 46 – Network parameters
- 47 – 7210 Network parameters
- 48 – Network Queue parameters
- 49 – 7210 Network Queue parameters
- 50 – Shared Queue parameters
- 51 – WRED Slope parameters
- 52 – 7210 Slope parameters

- 53 – HSMDA WRED Slope parameters
- 54 – Scheduler parameters
- 55 – Port Scheduler parameters
- 56 – HSMDA Scheduler parameters
- 57 – HSMDA WRR policy parameters
- 58 – 7210 Port Scheduler parameters
- 59 – Policer Control parameters
- 60 – HSMDA Pool parameters
- 61 – Named Buffer Pool parameters
- 62 – Ingress Queue Group Template parameters
- 63 – Egress Queue Group Template parameters
- 64 – 7705 SAR Fabric parameters
- 65 – 7250 SAS and Telco QoS parameters
- 66 – AOS QoS Policies parameters
- 67 – 9500 ATM QoS parameters
- 68 – ACL MAC Filter parameters
- 69 – ACL IP Filter parameters
- 70 – ACL IPv6 Filter parameters
- 71 – 7250 SAS and Telco ACL Standard IP Filter parameters
- 72 – 7250 SAS and Telco ACL Extended IP Filter parameters
- 73 – 7250 SAS and Telco ACL IGMP Filter parameters
- 74 – 7250 SAS and Telco ACL MAC Filter parameters
- 75 – Multicast Package parameters
- 76 – Egress Multicast Group parameters
- 77 – Multicast CAC parameters
- 78 – Ingress Multicast Path Management parameters
- 79 – Time of Day parameters

- 80 – Routing parameters
- 81 – VRRP parameters
- 82 – MPLS parameters
- 83 – Auto Tunnels parameters
- 84 – RADIUS Based Accounting parameters
- 85 – ISA-IPsec Transform parameters
- 86 – IPsec Static Security Association parameters
- 87 – ISA-IPsec Tunnel Template parameters
- 88 – IKE Policy parameters
- 89 – NAT Policy parameters
- 90 – Application Assurance parameters
- 91 – 802_1x parameters
- 92 – PBB MRP parameters
- 93 – AOS Ethernet Service parameters
- 94 – Connection profile parameters
- 95 – Service PW Template parameters
- 96 – Residential Subscriber parameters
- 97 – Network and Service Audits policy parameters
- 98 – Diameter Peer Profile parameters
- 99 – Diameter Profile parameters
- 100 – GTP Prime Server Group Profile parameters
- 101 – GTP Profile parameters
- 102 – PGW Charging Profile parameters
- 103 – PLMN List Group parameters
- 104 – QCI Policy parameters
- 105 – SGW Charging Profile parameters
- 106 – ANR Profile parameters

- 107 – eNodeB IPsec Profile parameters
- 108 – CPE Test-Head Profile parameters
- 109 – Remote Network Monitoring (RMON) parameters
- 110 – Size Constraint parameters
- 111 – Format and Range Policies parameters
- 112 – Common Policies menu parameters
- 113 – LTE LI delivery function peer parameters
- 114 – LTE LI interception target parameters
- 115 – Trusted Peer List parameters

37 – Access Ingress parameters

37.1 Access Ingress parameters 37-2

37.1 Access Ingress parameters

This chapter describes the parameters on the Access Ingress Policy form and child forms.

ATM VCI

See the [ATM VCI](#) parameter in section [68.1](#).

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [112.1](#).

Broadcast Policer ID

(broadcastPolicerId)

The Broadcast Policer ID parameter specifies a policer to be mapped to a forwarding class for broadcast traffic. The range is 0 to 32. The default is 0.

You can click on the Select button to list and choose a policer. The policer must be preexisting on the access ingress policy.

Broadcast Queue ID

(broadcastQueueId)

The Broadcast Queue ID parameter specifies a broadcast queue to be mapped to a forwarding class. Click on the Select button to list and choose a queue.

The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping you specify overrides the default forwarding-class-to-queue mapping for broadcast traffic.

Cir

(kbps)

See the [CIR \(kbps\)](#) parameter in section [112.1](#).

Cir Adaptation

See the [CIR Adaptation](#) parameter in section [112.1](#).

Committed Burst Size

(KB)

See the [Committed Burst Size \(kb\)](#) parameter in section [112.1](#).

Default FC

See the [Default FC](#) parameter in section 112.1.

Default FC HSMDA Counter Override

(defaultFCHsmdaCntrOvr)

The Default FC HSMDA Counter Override parameter specifies the counter override for the default forwarding class. The range is 0 to 8. The default is 0.

Description

See the [Description](#) parameter in section 112.1.

Destination IP

See the [Destination IP](#) parameter in section 112.1.

Destination MAC

(destinationMacAddress)

The Destination MAC parameter specifies the destination MAC address to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied. Specify a MAC address for the Destination MAC parameter in the format *xx-xx-xx-xx-xx-xx*.

When a packet contains the destination MAC address specified by the Destination MAC parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

Destination Port

See the [Destination Port](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Dot1p

Table 37-1 lists where to find information about the Dot1p parameter.

Table 37-1 Dot1p parameter

Parameter	See
Dot1p for forwarding class mapping	Dot1p parameter in this section
Dot1p for MAC match/forwarding class mapping	Dot1p parameter in this section

Dot1p

(dot1p)

The Dot1p parameter specifies the IEEE 802.1p value to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied. The range is 0 to 7. The default is 0.

When a packet is marked with the value specified by the Dot1p parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

Dot1p

(dot1pValue)

The Dot1p parameter specifies the IEEE 802.1p value to be used as the MAC match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied. The range is 0 to 7. The default is default.

When a packet is marked with the value specified by the Dot1p parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

DSCP

See the [DSCP](#) parameter in section [112.1](#).

Dst Mask

See the [Dst Mask](#) parameter in section [112.1](#).

Ether Type

(ethernetType)

See the [Ether Type](#) parameter in section [112.1](#).

Expedite

See the [Expedite](#) parameter in section [112.1](#).

Forwarding Class

See the [Forwarding Class](#) parameter in section [112.1](#).

Fragment

See the [Fragment](#) parameter in section [112.1](#).

Frame Type

See the [Frame Type](#) parameter in section [68.1](#).

High Priority Reserved

See the [High Priority Reserved](#) parameter in section [112.1](#).

HSMDA Broadcast Queue ID

(hsmdaBroadcastQueueId)

The HSMDA Queue ID parameter specifies the broadcast queue to use for packets in the forwarding class. This mapping is used when the SAP is on a HSMDA. The range is 0 to 8. The default is 0. A value of 0 means that the default queues should be used.

HSMDA Multicast Queue ID

(hsmdaMulticastQueueId)

The HSMDA Queue ID parameter specifies the multicast queue to use for packets in the forwarding class. This mapping is used when the SAP is on a HSMDA. The range is 0 to 8. The default is 0. A value of 0 means that the default queues should be used.

HSMDA Queue ID

(hsmdaQueueId)

The HSMDA Queue ID parameter specifies the HSMDA queue to use for packets in the forwarding class. This mapping is used when the SAP is on a HSMDA. The range is 0 to 8. The default is 0. A value of 0 means that the default queues should be used.

ID

Table [37-2](#) lists where to find more information about the ID parameter.

Table 37-2 ID parameter

Parameter	See
ID for access ingress policy	ID parameter in this section
ID for IP match criteria	
ID for MAC match criteria	
ID for queue	ID parameter in this section

ID

(id)

The ID parameter specifies a unique ID for an object. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 131 072. The default is 0. Table 37-3 describes the parameter.

Table 37-3 ID parameter

For	Description
Access ingress policy	Access ingress policy ID 1 is reserved for the default policy. The default access ingress policy is automatically applied to all access interfaces which do not have another access ingress policy assigned. The default policy is not configurable. All access ingress policies have a default queue for unicast traffic, which is identified by queue ID 1, and a default queue for multicast traffic, which is identified by queue ID 11.
IP match criteria MAC match criteria	—

ID

(queueId)

The ID parameter specifies a unique identifier for queues. All access ingress policies have a default queue for unicast traffic, which is identified by queue ID 1, and a default queue for multicast traffic, which is identified by queue ID 11.

Table 37-4 lists the parameter ranges for different queue types. The default is 0.

Table 37-4 ID parameter

Object	Range
HSMDA queues	1 to 8
Queues (except for HSMDA queues)	1 to 32

In DSCP

(inDscp)

The In DSCP parameter specifies the packet DSCP value to be set at egress when the In Remark parameter is set to dscp. See the Table 112-11 for the DSCP values. The default is default, which indicates that the DSCP value at egress is not to be modified.

In Precedence

(inPrecedence)

The In Precedence parameter specifies the packet precedence value to be set at ingress when the In Remark parameter is set to precedence. The range is 0 to 7. The default is default, which indicates that the precedence value at ingress is not to be modified.

In Remark

(inRemark)

The In Remark parameter specifies the type of remarking to be performed on ingress packets. Table 37-5 describes the parameter options.

Table 37-5 In Remark parameter

Option	Option description
none (default)	Specifies that no remarking is to be performed
dscp	Specifies that DSCP remarking is to be performed
precedence	Specifies that IP Precedence remarking is to be performed

LspExp

(lspExp)

The LspExp parameter specifies the unique MPLS LSP EXP value that matches an LspExp rule with the EXP value in ingress packets. This is a required parameter for an LspExp rule. The range is 0 to 7.

MAC Criteria Type

(macCritType)

The MAC Criteria Type parameter specifies which type of MAC Match Criteria entries this QoS policy can contain. The options are:

- Normal (default)
- VID

Mark DE bit1 as Out of Profile

(de1OutOfProfile)

The Mark DE bit 1 as Out Of Profile parameter specifies whether to mark traffic with discard eligibility. When the value is set to false, traffic is routed based on the existing configuration. When the value is set to true, the traffic is marked as out of profile.

The options are:

- false (default)
- true

Mask

Table 37-6 lists where to find information about the Mask parameter.

Table 37-6 Mask parameter

Parameter	See
Mask for Dot1p	Mask parameter in this section
Mask for source MAC address	Mask parameter in this section
Mask for destination MAC address	Mask parameter in this section

Mask

(destinationMacAddressMask)

The Mask parameter specifies the mask that is associated with a destination MAC address. The destination MAC address and the associated mask are used to specify a range of MAC addresses as the MAC match criteria for mapping packets to a forwarding class and enqueueing priority. Specify a mask for the Mask parameter in the format *xx-xx-xx-xx-xx-xx*.

Mask

(dot1pMask)

The Mask parameter specifies the 3-bit mask that is associated with a Dot1p value. The Dot1p value and the associated mask are used to specify a range of Dot1p values as the MAC match criterion for mapping packets to a forwarding class and enqueueing priority. For example, to specify a range from 4 up to 7 for the Dot1p value, set the Dot1p parameter to 4 and set the Mask parameter to 4. The range for the Mask parameter is 0 to 7. The default is 0.

Mask

(sourceMacAddressMask)

The Mask parameter specifies the mask that is associated with a source MAC address. The source MAC address and the associated mask are used to specify a range of MAC addresses as the MAC match criterion for mapping packets to a forwarding class and enqueueing priority. Specify a mask for the Mask parameter in the format *xx-xx-xx-xx-xx-xx*.

Maximum Burst Size

(bytes)

See the [Maximum Burst Size \(bytes\)](#) parameter in section 112.1.

Mode

See the [Mode](#) parameter in section 112.1.

Multipoint

(multicast)

See the [Multipoint](#) parameter in section 112.1.

Multipoint Policer ID

(multicastPolicerId)

The Multipoint Policer ID parameter specifies a policer to be mapped to a forwarding class for multicast traffic. The range is 0 to 32. The default is 0.

You can click on the Select button to list and choose a policer. The policer must be preexisting on the access ingress policy.

Multipoint Queue ID

(multicastQueueId)

The Multipoint Queue ID parameter specifies a multipoint queue to be mapped to a forwarding class. Click on the Select button to list and choose a queue.

The queue is mapped to a specific forwarding class specified by the Forwarding Class parameter. The mapping you specify overrides the default forwarding-class-to-queue mapping for multicast traffic.

Out DSCP

(outDscp)

The Out DSCP parameter specifies the packet DSCP value to be set at egress when the Out Remark parameter is set to dscp. See the Table 112-11 for the DSCP values. The default is default, which indicates that the DSCP value at egress is not to be modified.

Out Precedence

(outPrecedence)

The Out Precedence parameter specifies the packet precedence value to be set at egress when the Out Remark parameter is set to precedence. The range is 0 to 7. The default is default, which indicates that the egress precedence value is not to be modified.

Out Remark

(outRemark)

The Out Remark parameter specifies the type of remarking to be performed on egress packets. Table 37-7 describes the parameter options.

Table 37-7 Out Remark parameter

Option	Option description
none (default)	Specifies that no remarking is to be performed
dscp	Specifies that DSCP remarking is to be performed
precedence	Specifies that IP Precedence remarking is to be performed

Packet Byte Offset (bytes)

(hsmdaPerPacketOffset)

The Packet Byte Offset (bytes) parameter specifies the packet byte offset. The range is -32 to 31. The default is 0.

Packet Byte Offset

(pktOffset)

See the [Packet Byte Offset](#) parameter in section 112.1 for the parameter description.

Parent Arbiter

See the [Parent Arbiter](#) parameter in section 112.1.

Pir

(kbps)

See the [PIR \(kbps\)](#) parameter in section 112.1.

Pir Adaptation

See the [PIR Adaptation](#) parameter in section 112.1.

Policed

(policed)

See the [Policed](#) parameter in section 112.1.

Policer ID

(policerId)

See the [Policer ID](#) parameter in section 112.1.

Precedence

See the [Precedence](#) parameter in section 112.1.

Priority

Table 37-8 lists where to find information about the Priority parameter.

Table 37-8 Priority parameter

Parameter	See
Priority for policy	Priority parameter in this section
Priority for Dot1p, DSCP, EXP, Precedence, IP, and MAC mapping	Priority parameter in this section

Priority

(defaultFcPriority)

The Priority parameter specifies the default enqueueing priority for all packets received on an ingress access interface which uses the policy. Ingress enqueueing priority only affects ingress queuing on the access interface. The Priority parameter is not used after the packet is placed in a buffer on an ingress queue. Table 37-9 describes the parameter options.

Table 37-9 Priority parameter

Option	Option description	Dependencies
low (default)	Specifies that the probability of enqueueing a packet decreases when the ingress queue is congested	—
high	Specifies that the probability of enqueueing a packet increases when the ingress queue is congested	

Priority

(priority)

See the [Priority](#) parameter in section 112.1.

Profile

(profile)

See the [Profile](#) parameter in section 112.1.

Protocol

See the [Protocol](#) parameter in section 112.1.

Queue ID

See the [Queue ID](#) parameter in section 112.1.

Scheduler

See the [Scheduler button](#) parameter in section 112.1.

SNAP OUI

(snapOui)

The SNAP OUI parameter specifies an IEEE 802.3 LLC SNAP Ethernet frame OUI value as a match criterion. When enabled, the options are:

- off (default)
- zero
- Non Zero

The SNAP OUI and SNAP PID parameters appear only when the Frame Type parameter value is e802dot2SNAP.

SNAP PID

(snapPid)

The SNAP PID parameter specifies an IEEE 802.3 LLC SNAP Ethernet frame PID value as a match criterion. The SNAP OUI and SNAP PID parameters appear only when the Frame Type parameter value is e802dot2SNAP. The parameter is configurable when the SNAP OUI parameter is enabled. The range is -1 to 65 535. The default is -1, indicating that filtering on this parameter is disabled.

Source IP

See the [Source IP](#) parameter in section 112.1.

Source MAC

(sourceMacAddress)

The Source MAC parameter specifies the source MAC address to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied. Specify a MAC address for the Source MAC parameter in the format *xx-xx-xx-xx-xx-xx*.

When a packet contains the source MAC address specified by the Source MAC parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

Source Port

See the [Source Port](#) parameter in section 112.1.

Src Mask

See the [Src Mask](#) parameter in section 112.1.

Stats Mode

(statsMode)

See the [Stats Mode](#) parameter in section 112.1.

Unknown Policer ID

(unknownPolicerId)

The Unknown Policer ID parameter specifies a policer to be mapped to a forwarding class for unknown traffic types. The range is 0 to 32. The default is 0.

You can click on the Select button to list and choose a policer. The policer must be preexisting on the access ingress policy.

Unknown Queue ID

(unknownQueueId)

The Unknown Queue ID parameter specifies a unicast queue to be mapped to unknown forwarding classes. Click on the Select button to list and choose a queue.

The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping that you specify overrides the default forwarding-class-to-queue mapping for unknown traffic.

Use Policer

The Use Policer parameter specifies whether a policer is used in the forwarding class. You can assign a policer to a forwarding class for the following traffic types:

- Unicast
- Multicast
- Broadcast
- Unknown

When you assign a policer for one or more of the traffic types, you must select a policer ID for each traffic type in the Policers panel.

Use Queue Group

The Use Queue Group parameter specifies whether a queue from an ingress queue group template is used in the forwarding class, and if so, the type of queue. The options are:

- Unicast Queue
- Multicast Queue

- Broadcast Queue
- Unknown Queue

When you enable one or more of the options, you must select a ingress queue from the specified queue group template policy in the Queues panel. If you do not enable the parameter options, the ingress queues that are listed for each queue type are queues that are configured locally within the policy.

38 – 7210 Access Ingress parameters

38.1 7210 Access Ingress parameters 38-2

38.1 7210 Access Ingress parameters

This chapter describes the parameters on the 7210 Access Ingress Policy form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→7210 Access Ingress.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Broadcast Meter ID

(broadcastMeterId)

The Broadcast Meter ID parameter specifies a multipoint meter to be mapped to broadcast forwarding classes. By default, broadcast traffic is mapped to multipoint queue 11. Click on the Select button to list and choose a queue.

The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping that you specify overrides the default forwarding class-to-queue mapping for unicast traffic.

CIR (kbps)

See the [CIR \(kbps\)](#) parameter in section 112.1.

CIR Adaptation

See the [CIR Adaptation](#) parameter in section 112.1.

Committed Burst Size (kbps)

See the [Committed Burst Size \(kbps\)](#) parameter in section 112.1.

Default FC

(defaultFc)

The Default FC parameter specifies the default forwarding class for packets that enter an access ingress SAP. Packets with undefined DSCP bits are mapped to the specified forwarding class. Table 38-1 describes the parameter options.

Table 38-1 Default FC parameter

Option	Option description	Dependencies
be (default)	Specifies that packets in the class are treated, at best, as out-of-profile assured service packets. There are no delivery guarantees. The best-effort and low-2 forwarding class options are intended for best-effort traffic.	—
l2		
af	Specifies that packets in the class are forwarded or discarded based on the availability of bandwidth on NEs. The assured and low-1 forwarding class options are intended for assured traffic. Packets transmitted that are at or below the CIR are marked in-profile. Packets transmitted that are above the CIR are marked out-of-profile.	
l1		
h2	Specifies that packets in the class are always serviced at congestion points over other forwarding classes. The options are intended for high-priority traffic. <ul style="list-style-type: none">The h2 and ef forwarding class options are intended for delay/jitter sensitive traffic.The h1 forwarding class option is intended for secondary network control traffic or delay/jitter sensitive traffic.The nc forwarding class option is intended for network control traffic.	
ef		
h1		
nc		

Description

See the [Description](#) parameter in section 112.1.

Destination MAC

(destinationMacAddress)

The Destination MAC parameter specifies the destination MAC address to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied. Specify a MAC address for the Destination MAC parameter in the format *xx-xx-xx-xx-xx-xx*.

When a packet contains the destination MAC address specified by the Destination MAC parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

You must enable the check box beside the Destination MAC and Mask parameters before you can configure the parameter.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Dot1p

(dot1pValue)

The Dot1p parameter specifies the IEEE 802.1p value to be used as the MAC match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied. The range is 0 to 7. The default is -1, which means that the parameter is not set.

When a packet is marked with the value specified by the Dot1p parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

You must enable the check box beside the Dot1p and Mask parameters before you can configure the parameter.

DSCP

See the [DSCP](#) parameter in section 112.1.

Ether Type

See the [Ether Type](#) parameter in section 112.1.

Forwarding Class

See the [Forwarding Class](#) parameter in section 112.1.

Frame Type

(frameType)

The Frame Type parameter specifies an Ethernet frame type that is used as a match criterion. Table 38-2 describes the parameter options.

Table 38-2 Frame Type parameter

Option	Option description
e802dot3 (default)	The frame type is Ethernet IEEE 802.3.
Ethernet II	The frame type is Ethernet Type II.

ID

(id)

See the [ID](#) parameter in section 112.1.

Mask

Table 38-3 lists where to find information about the Mask parameter.

Table 38-3 Mask parameter

Parameter	See
Mask for Dot1p	Mask parameter in this section
Mask for source MAC address	Mask parameter in this section
Mask for destination MAC address	Mask parameter in this section

Mask

(destinationMacAddressMask)

The Mask parameter specifies the mask that is associated with a destination MAC address. The destination MAC address and the associated mask are used to specify a range of MAC addresses as the MAC match criteria for mapping packets to a forwarding class and enqueueing priority. Specify a mask for the Mask parameter in the format *xx-xx-xx-xx-xx-xx*.

You must enable the check box beside the Destination MAC and Mask parameters before you can configure the parameter.

Mask

(dot1pMask)

The Mask parameter specifies the 3-bit mask that is associated with a Dot1p value. The Dot1p value and the associated mask are used to specify a range of Dot1p values as the MAC match criterion for mapping packets to a forwarding class and enqueueing priority. For example, to specify a range from 4 up to 7 for the Dot1p value, set the Dot1p parameter to 4 and set the Mask parameter to 4. The range for the Mask parameter is 0 to 7. The default is 0.

You must enable the check box beside the Dot1p and Mask parameters before you can configure the parameter.

Mask

(sourceMacAddressMask)

The Mask parameter specifies the mask that is associated with a source MAC address. The source MAC address and the associated mask are used to specify a range of MAC addresses as the MAC match criterion for mapping packets to a forwarding class and enqueueing priority. Specify a mask for the Mask parameter in the format *xx-xx-xx-xx-xx-xx*.

You must enable the check box beside the Source MAC and Mask parameters before you can configure the parameter.

Maximum Burst Size (kbps)

See the [Maximum Burst Size \(kbps\)](#) parameter in section 112.1.

Meter ID

(meterId)

The Meter ID parameter specifies a unicast queue to be mapped to a forwarding class. By default, unicast traffic is mapped to queue 1. Click on the Select button to list and choose a queue.

The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping that you specify overrides the default forwarding class-to-queue mapping for unicast traffic.

Mode

(mode)

The mode parameter specifies whether the queue supports color-aware profiling or priority forwarding and real-time rate-limiting functions. Table 38-4 describes the parameter options.

Table 38-4 Mode parameter

Option	Option description
priority (default)	Specifies that the queue is to support the access-ingress priority state for each packet. Packets may be classified by the SAP ingress QoS policy classification commands as either high- or low-priority. High-priority packets receive preferential buffering during queue congestion. Forwarding classes and subclasses configured as in-profile or out-of-profile are not allowed to map to queues configured as priority-mode. Setting the mode parameter to priority is only allowed during queue creation. Real-time rate limiting is supported when the queue is operating in priority mode.
profile	Specifies that the queue is to support color -aware profiling of the forwarding class and sub-classes mapped to the queue. Color-aware operational behavior is as follows: <ul style="list-style-type: none">• Classes defined as in-profile are handled as high priority and are never marked out-of-profile. In-profile packets consume queue CIR bandwidth.• Classes defined as out-of-profile are handled as low priority and are never marked in-profile. Out-of-profile packets do not consume queue CIR bandwidth.• Classes not set to in-profile or out-of-profile are marked according to the dynamic rate as they are scheduled from the queue. Packets scheduled from the queue when the queue is below or equal to CIR are marked in-profile, and packets scheduled from the queue when the queue is above CIR are marked out-of-profile. Non-profiled packets consume queue CIR bandwidth.• Real-time rate limiting is not allowed on a queue operating in profile mode.

MultiPoint

See the [MultiPoint](#) parameter in section [112.1](#).

Multicast Meter ID

(multicastMeterId)

The Multicast Meter ID parameter specifies a multipoint meter to be mapped to multicast forwarding classes. By default, multicast traffic is mapped to multipoint queue 11. Click on the Select button to list and choose a queue.

The queue is mapped to a specific forwarding class specified by the Forwarding Class parameter. The mapping you specify overrides the default forwarding-class-to-queue mapping for multicast traffic.

Number of Qos Classifiers

(NumQosClassifiers)

The Number of Qos Classifiers parameter specifies the number of QoS classifiers used per SAP, to improve SAP scaling. The number of QoS classifiers must be greater than or equal to the number of match entries and meters that are specified in the SAP ingress policy. To reduce the number of QoS classifiers, you must first delete the match criteria and meters that are not required.

For the 7210 SAS-M and 7210 SAS-D-6F-4T (ETR), the options are 4 (default), 8, 16, 32, 64, 128, and 256. For the 7210 SAS-E, the options are 16 (default), 36, and 72.

PIR (kbps)

See the [PIR \(kbps\)](#) parameter in section [112.1](#).

PIR Adaptation

See the [PIR Adaptation](#) parameter in section [112.1](#).

Rate Mode

(rateMode)

The Rate Mode parameter specifies the mode of the meter. The options are:

- trTCM (default)
- srTCM
- trTCM (RFC 2698)
- trTCM (RFC 4115)

Scope

See the [Scope](#) parameter in section [112.1](#).

Source MAC

(sourceMacAddress)

The Source MAC parameter specifies the source MAC address to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied. Specify a MAC address for the Source MAC parameter in the format *xx-xx-xx-xx-xx-xx*.

When a packet contains the source MAC address specified by the Source MAC parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

You must enable the check box beside the Source MAC and Mask parameters before you can configure the parameter.

Unknown Meter ID

(unknownMeterId)

The Unknown Meter ID parameter specifies a multipoint meter to be mapped to unknown forwarding classes. By default, unknown traffic is mapped to multipoint queue 11. Click on the Select button to list and choose a queue.

The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping that you specify overrides the default forwarding-class-to-queue mapping for unknown traffic.

39 – Access Egress parameters

39.1 Access Egress parameters 39-2

39.1 Access Egress parameters

This chapter describes the parameters on the Access Egress Policy form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

CIR (kbps)

See the [CIR \(kbps\)](#) parameter in section 112.1.

CIR Level

See the [CIR Level](#) parameter in section 112.1.

CIR Level

See the [CIR Level](#) parameter in section 112.1.

CIR Weight

See the [CIR Weight](#) parameter in section 112.1.

CIR Weight

See the [CIR Weight](#) parameter in section 112.1.

CIR Adaptation

See the [CIR Adaptation](#) parameter in section 112.1.

Committed Burst Size (kb)

See the [Committed Burst Size \(kb\)](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Destination IP

See the [Destination IP](#) parameter in section 112.1.

Destination Port

See the [Destination Port](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

dot1p

(dot1p)

The dot1p parameter specifies the forwarding class-to-IEEE 802.1p mapping for 802.1Q or 802.1P encapsulated packets that egress the access interface which uses the access egress policy. When a packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the IEEE 802.1p value specified by the Dot1p parameter. The range is 0 to 7, or default. The default is default. Specifying 0 is equivalent to removing the explicit marking.

DSCP

See the [DSCP](#) parameter in section 112.1.

Dst Mask

See the [Dst Mask](#) parameter in section 112.1.

Expedite

See the [Expedite](#) parameter in section 112.1.

Force DE value

(forceDeValue)

The Force DE Value parameter specifies whether the [Mark DE bit](#) parameter value is forced. By default the discard eligible (DE) bit setting depends on whether the packet is in or out of profile. The options are:

- default (default)
- 0
- 1

Forwarding Class

See the [Forwarding Class](#) parameter in section 112.1.

Fragment

See the [Fragment](#) parameter in section 112.1.

High Priority Reserved

See the [High Priority Reserved](#) parameter in section 112.1.

HSMDA Egress Profiling

See the [HSMDA Egress Profiling](#) parameter in section [112.1](#).

HSMDA Packet Byte Offset (bytes)

(hsmdaPerPacketOffset)

The HSMDA Packet Byte Offset (bytes) parameter specifies the packet byte offset. The range is -32 to 31. The default is 0.

HSMDA Queue ID

(hsmdaQueueId)

The HSMDA Queue ID parameter specifies the HSMDA queue to use for packets in the forwarding class. This mapping is used when the SAP is on a HSMDA. The range is 0 to 8. The default is 0. A value of 0 means that the default queues should be used.

ID

Table [39-1](#) lists where to find information about the ID parameter.

Table 39-1 ID parameter

Parameter	See
ID for access egress policy	ID parameter in this section
ID for queue	ID parameter in this section

ID

(id)

See the [High Priority Reserved](#) parameter in section [112.1](#).

ID

(queueId)

The ID parameter specifies a unique identifier for a queue. The range is 1 to 8. The default is 0.

All access egress policies have a default queue, which is identified by queue ID 1.

In DSCP

(inDscp)

The In DSCP parameter specifies the packet DSCP value to be set at egress when the In Remark parameter is set to dscp. The default is default, which indicates that the DSCP value at egress is not to be modified.

In Precedence

(inPrecedence)

The In Precedence parameter specifies the packet precedence value to be set at egress when the In Remark parameter is set to precedence. The range is 0 to 7. The default is default, which indicates that the ingress precedence value is not to be modified.

In Profile

(inDot1p)

The In Profile parameter specifies which Dot1p should be configured and depends on whether traffic is in or out of profile. The range is 0 to 7, or default. The default is default. Specifying 0 is equivalent to removing the explicit marking.

Level

See the [Level](#) parameter in section 112.1.

Level

See the [Level](#) parameter in section 112.1.

Low Burst Max Class

(hsmdaLowBurstMaxClass)

The Low Burst Max Class parameter specifies which class should use the low priority burst threshold. All classes starting from 1, up to and including the class configured for this property use the low priority burst threshold. All classes greater than the value configured for this property, up to and including class 8, use the high priority burst threshold. The range is 1 to 8. The default is 8.

Mark DE bit

(deMark)

The Mark DE parameter specifies whether the Ethernet frame is marked eligible to be dropped when the network traffic is in excess of the committed rate. The values are:

- True
- False (default)

Maximum Burst Size (bytes)

See the [Maximum Burst Size \(bytes\)](#) parameter in section 112.1.

Out DSCP

(outDscp)

The Out DSCP parameter specifies the packet DSCP value to be set at egress when the Out Remark parameter is set to dscp. The default is default, which indicates that the DSCP value at egress is not to be modified.

Out Profile

(outDot1p)

The Out Profile parameter specifies which Dot1p should be configured and depends on whether traffic is in or out of profile. The range is 0 to 7, or default. The default is default. Specifying 0 is equivalent to removing the explicit marking.

Out Precedence

(outPrecedence)

The Out Precedence parameter specifies the packet precedence value to be set at egress when the Out Remark parameter is set to precedence. The range is 0 to 7. The default is default, which indicates that the egress precedence value is not to be modified.

Packet Byte Offset

See the [Packet Byte Offset](#) parameter in section [112.1](#).

Packet Byte Offset

(hsmdaPerPacketOffset)

The Packet Byte Offset parameter specifies the packet byte offset to use for the HSMDA queue accounting. A positive number adds bytes. A negative number removes bytes. The range is -32 to +31. The default is 0.

Packet Byte Offset

(IOM3-XP specific)

See the [Packet Byte Offset](#) parameter in section [175.1](#).

Parent Arbiter

See the [Parent Arbiter](#) parameter in section [112.1](#).

PIR (kbps)

See the [PIR \(kbps\)](#) parameter in section [112.1](#).

PIR Adaptation

See the [PIR Adaptation](#) parameter in section 112.1.

Policer ID

([policerId](#))

See the [Policer ID](#) parameter in section 112.1.

Priority

([priority](#))

See the [Priority](#) parameter in section 112.1.

Port Average Overhead (%)

See the [Port Average Overhead \(%\)](#) parameter in section 112.1.

Port Parent

See the [Port Parent](#) parameter in section 112.1.

Precedence

See the [Precedence](#) parameter in section 112.1.

Profile

([profile](#))

See the [Profile](#) parameter in section 112.1 for the parameter description.

Protocol

See the [Protocol](#) parameter in section 112.1.

Queue ID

See the [Queue ID](#) parameter in section 112.1.

Scheduler

See the [Scheduler button](#) parameter in section 112.1.

Source IP

See the [Source IP](#) parameter in section 112.1.

Source Port

See the [Source Port](#) parameter in section 112.1.

Src Mask

See the [Src Mask](#) parameter in section 112.1.

Stats Mode

See the [Stats Mode](#) parameter in section 112.1.

Traffic Control

The Traffic Control parameter specifies the type of object used in the forwarding class. The options are:

- Use Policer
- Use Queue Group
- Use Queue (default)

The Use Policer option specifies whether a policer is used in the forwarding class. You can assign a policer to a forwarding class for Unicast traffic. When you assign a policer, you must select a Policer ID in the Policers panel.

The Use Queue Group option specifies whether a queue from an egress queue group template is used in the forwarding class. You must select an egress queue from the specified queue group template policy in the Queue panel.

The Use Queue option specifies whether a queue configured locally within the policy is used in the forwarding class. You must select a Queue ID in the Queue panel.

Use As Multiclass MLPPP Policy For 7705 SAR

(isMulticlassMlpppSubtype)

The Use As Multiclass MLPPP Policy For 7705 SAR parameter specifies whether the access egress policy is an MC MLPPP access egress policy on the 7705 SAR, Release 2.1 or later. Table 39-2 describes the parameter options.

Table 39-2 Use As Multiclass MLPPP Policy For 7705 SAR parameter

Option	Description	Dependencies
True	When the port of a 7705 SAR L2 access interface is an MC MLPPP bundle, the parameter must be set to True on the access egress policy binding for the L2 access interface.	You cannot modify the parameter for a 7705 SAR local policy when the 7705 SAR has one or more L2 access interfaces that are bound to the policy.

(1 of 2)

Option	Description	Dependencies
False (default)	When the port of a 7705 SAR L2 access interface is not an MC MLPPP bundle or an MLPPP bundle, the Use As Multiclass MLPPP Policy For 7705 SAR parameter must be set to False on the access egress policy binding for the L2 access interface.	You cannot modify the parameter for a 7705 SAR local policy when the 7705 SAR has one or more L2 access interfaces that are bound to the policy.

(2 of 2)

Use WRED Queue

See the [Use WRED Queue](#) parameter in section [112.1](#).

Weight

See the [Weight](#) parameter in section [112.1](#).

Weight

See the [Weight](#) parameter in section [112.1](#).

40 – 7210 Access Egress parameters

40.1 7210 Access Egress parameters 40-2

40.1 7210 Access Egress parameters

This chapter describes the parameters on the 7210 Port Access Egress Policy form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

CIR Adaptation

See the [CIR Adaptation](#) parameter in section 112.1.

CIR (kbps)

See the [CIR \(kbps\)](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Forwarding Class

See the [Forwarding Class](#) parameter in section 112.1.

ID

(id)

See the [ID](#) parameter in section 112.1.

ID

(queueId)

The ID parameter specifies a unique identifier for a queue. The range is 1 to 8. The default is 0.

All access egress policies have a default queue, which is identified by queue ID 1.

In Profile

(inDot1p)

See the [In Profile](#) parameter in section 112.1.

Out Profile

(outDot1p)

See the [Out Profile](#) parameter in section 112.1.

PIR (kbps)

See the [PIR \(kbps\)](#) parameter in section 112.1.

PIR Adaptation

See the [PIR Adaptation](#) parameter in section 112.1.

Scope

See the [Scope](#) parameter in section 112.1.

41 – ATM QoS parameters

41.1 ATM QoS parameters 41-2

41.1 ATM QoS parameters

This chapter describes the parameters on the ATM QoS Policy form and the 9500 ATM QoS Policy form, and their child forms. The 5620 SAM menu path is Policies→QoS→ATM QoS. For 9500 MPR, the 5620 SAM menu path is Policies→QoS→9500 MPR QoS→9500 ATM QoS.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

CDVT

(cdvt)

The CDVT parameter specifies the cell delay variation tolerance. The parameter appears when the Service Category parameter is set to CBR, rt-VBR or nrt-VBR. The range is 0 to 4 294 967 295 ms. The default is 250 ms. For 9500 MPR, the default is 1000 ms, and the range is 0 to 40 000 ms.

CLP Tagging

(clpTagging)

The CLP Tagging parameter specifies whether to enable CLP tagging for ATM cells in a VPRN and IES service. When the value is enabled, cells which exceed the allowed limit are discarded if congestion occurs on the network. The value can be set to enabled on ATM MDAs and ASAP MDAs. The options are:

- Enabled
- Disabled (default)

Description

See the [Description](#) parameter in section 112.1.

Descriptor Type

(descriptorType)

The Descriptor Type parameter specifies the type of ATM traffic descriptor profile, based on ATM Forum Traffic Management Specification Version 4.1. The options are:

- clp0And1pcrPlusClp0And1scr
- clp0And1pcrPlusClp0scr
- clp0And1pcrPlusClp0And1scr

The descriptor type defines interpretation of traffic parameters that are specified for this profile. Table 41-1 describes the relationship between the parameter and the [Service Category](#) parameter in section 112.1.

Table 41-1 Descriptor Type and Service Category parameters relationship

Descriptor Type	Rates interpretation	Application service categories
clp0And1pcrPlusClp0And1scr	PIR applies to CLP=0 and CLP=1 cell flows	CBR, UBR, and UBR with MIR
clp0And1pcrPlusClp0And1scr	PIR applies to CLP=0 and CLP=1 cell flows SCR applies to CLP=0 and CLP=1 cell flows	rt-VBR and nrt-VBR
clp0And1pcrPlusClp0scr	PIR applies to CLP=0 and CLP=1 cell flows SCR applies to CLP=0 and CLP=0 cell flows	

Displayed Name(displayedName)

See the [Displayed Name](#) parameter in section 112.1.

Domain Name

(domainName)

The Domain Name parameter allows the user to select between ATM and PWE3 for 9500 MPR QoS Policy creation. The default is ATM.

MBS (cells)

(mbs)

The MBS (cells) parameter specifies the maximum number of ATM cells in a burst that can be transmitted at the peak rate. The parameter appears when the Service Category parameter is set to rt-VBR or nrt-VBR. The range is 0 to 4 294 967 295 cells. The default is 32.

When the Service Category parameter is set to rt-VBR and nrt-VBR, ensure that MBS is between 3 to 256 000 cells.

MIR (kbps)

(mdcr)

The MIR (kbps) parameter specifies the minimum data transfer rate for a path. The parameter appears when the Service Category parameter is set to UBR. The range is 0 to 4 294 967 295. The default is 0.

MDCR

(mdcr)

The MDCR parameter specifies the minimum desired cell rate in cells per second. For the 9500 MPR, the range is 0 to 1. The default is 0.

PCR

(pcr)

The PCR parameter specifies the peak cell rate, in cells per second, which the endpoint may never exceed. For the 9500 MPR, the range is 1 to 71 480. The default is 1.

PIR (kbps)

(pcr)

The PIR (kbps) parameter specifies the cell rate, in kilobits per second, that the endpoint cannot exceed. The range is 0 to 4 294 967 295. The default is 0.

Shaping

(shaping)

The Shaping parameter specifies the shaping for egress direction traffic that uses the CBR, nrt-VBR, rt-VBR, and UBR service categories. When the Service Category parameter is set to CBR or rt-VBR the parameter is set to enabled and cannot be changed. When the Service Category parameter is set to UBR, the parameter is set to disabled and cannot be changed. When the Service Category parameter is set to nrt-VBR, the options are enable and disabled.

For egress traffic, if the parameter is enabled, the sum of the traffic descriptor rate (PIR for CBR, SIR for rt-VBR or nrt-VBR, MIR for UBR) and the consumed shaped bandwidth on the ATM interface cannot exceed the physical speed of the ATM interface. For the 9500 MPR, shaping does not apply.

SIR (kbps)

(sir)

The SIR (kbps) parameter specifies the average cell rate of a traffic source in cells per second. SIR is an upper bound on the conforming average rate of an ATM connection over time scales which are long, relative to those for which the PCR is defined. The parameter appears when the Service Category parameter is set to rt-VBR or nrt-VBR. The range is 0 to 4 294 967 295. The default is 0.

42 — MLPPP Ingress QoS Profile parameters

42.1 MLPPP Ingress QoS Profile parameters 42-2

42.1 MLPPP Ingress QoS Profile parameters

This chapter describes the parameters on the Manage MLPPP Ingress QoS Profile form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→MLPPP Ingress QoS Profile.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Profile ID

(id)

See the [Profile ID](#) parameter in section 112.1.

Reassembly Timeout (msec)

(reassemblyTimeout)

See the [Reassembly Timeout \(msec\)](#) parameter in section 112.1.

43 — MLPPP Egress QoS Profile parameters

43.1 MLPPP Egress QoS Profile parameters 43-2

43.1 MLPPP Egress QoS Profile parameters

This chapter describes the parameters on the Manage MLPPP Egress QoS Profile form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→MLPPP Egress QoS Profile.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Maximum Queue Size (msec)

(maxQueueSize)

See the [Maximum Queue Size \(msec\)](#) parameter in section 112.1.

MIR (%)

(mir)

See the [MIR \(%\)](#) parameter in section 112.1.

MLPPP Class

(mlpppClass)

The MLPPP Class parameter specifies the MLPPP class assigned to a forwarding class. The range is 0 to 3. Table 43-1 lists the default MC MLPPP class for each forwarding class.

Table 43-1 MLPPP Class parameter

Forwarding class	Forwarding class name	MLPPP class
0	BE	3
1	L2	2
2	AF	2
3	L1	2
4	H2	2
5	EF	1
6	H1	0
7	NC	0

Profile ID

(id)

See the [Profile ID](#) parameter in section 112.1.

Weight (%)

(weight)

See the [Weight \(%\)](#) parameter in section 112.1.

44 — MCFR Ingress QoS Profile parameters

44.1 MCFR Ingress QoS Profile parameters 44-2

44.1 MCFR Ingress QoS Profile parameters

This chapter describes the parameters on the Manage MCFR Ingress QoS Profile form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→MCFR Ingress QoS Profile.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [112.1](#).

Description

See the [Description](#) parameter in section [112.1](#).

Profile ID

(id)

See the [Profile ID](#) parameter in section [112.1](#).

Reassembly Timeout (msec)

(reassemblyTimeout)

See the [Reassembly Timeout \(msec\)](#) parameter in section [112.1](#).

45 — MCFR Egress QoS Profile parameters

45.1 MCFR Egress QoS Profile parameters 45-2

45.1 MCFR Egress QoS Profile parameters

This chapter describes the parameters on the Manage MCFR Egress QoS Profile form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→MCFR Egress QoS Profile.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Maximum Queue Size (msec)

(maxQueueSize)

See the [Maximum Queue Size \(msec\)](#) parameter in section 112.1.

MIR (%)

(mir)

See the [MIR \(%\)](#) parameter in section 112.1.

Profile ID

(id)

See the [Profile ID](#) parameter in section 112.1.

Weight (%)

(weight)

See the [Weight \(%\)](#) parameter in section 112.1.

46 — Network parameters

46.1 Network parameters 46-2

46.1 Network parameters

This chapter describes the parameters on the Network Policy form and its child forms. The 5620 SAM menu path is Policies→QoS→Network.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Default FC

See the [Default FC](#) parameter in section 112.1.

Default FC Profile

(defaultProfile)

The Default FC Profile parameter specifies whether packets that ingress a network interface which uses the network policy are by default considered in-profile or out-of-profile. All packets with undefined DSCP or LSP EXP bits are mapped to the specified default profile and associated forwarding class. The default forwarding class is specified by the Default FC parameter. Table 46-1 describes the parameter options.

Table 46-1 Default FC Profile parameter

Option	Option description	Dependencies
out (default)	Specifies that packets are by default out-of-profile. In-profile packets are preferentially queued over out-of-profile packets.	—
in	Specifies that packets are by default in-profile. In-profile packets are preferentially queued over out-of-profile packets.	

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Dot1p

See the [Dot1p](#) parameter in section 112.1.

Dot1p In Profile

See the [Dot1p In Profile](#) parameter in section 112.1.

Dot1p Out Profile

See the [Dot1p Out Profile](#) parameter in section 112.1.

DSCP

(dscp)

The DSCP parameter specifies the DSCP value to forwarding class and profile mapping for LSP packets that ingress the network interface which uses the network policy. When a packet is marked with the value specified by the DSCP parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the profile specified by the Profile parameter. Table 46-2 lists the parameter options.

Table 46-2 DSCP parameter

Options			
be (default)	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43

DSCP In Profile

(dscpInProfile)

The DSCP In Profile parameter specifies the forwarding-class-to-DSCP mapping for in-profile packets that egress the network interface which uses the network policy. When an in-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the DSCP value specified by the DSCP In Profile parameter. The default for the DSCP In Profile parameter depends on the forwarding class. For example, for the ef forwarding class, the default is ef. Table 46-3 lists the parameter options.

Table 46-3 DSCP In Profile parameter

Options			
default	ef	nc1	nc2
be	cp2	cp3	cp4
cp1	cp6	cp7	cp9
cp5	cp13	cp15	cp17
cp11	cp21	cp23	cp25
cp19	cp29	cp31	cp33
cp27	cp37	cp39	cp41
cp35	cp43	cp44	cp45
cp42	cp49	cp50	cp51
cp47	cp53	cp54	cp55
cp52	cp58	cp59	cp60
cp57	cp62	cp63	cs1
cp61	cs3	cs4	cs5
cs2	af12	af13	af21
af11	af23	af31	af32
af22	af41	af42	af43
af33	—	—	—

DSCP Out Profile

(dscpOutProfile)

The DSCP Out Profile parameter specifies the forwarding class to DSCP mapping for in-profile packets that egress the network interface which uses the network policy. When an out-of-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the DSCP value specified by the DSCP Out Profile parameter. The default for the DSCP Out Profile parameter depends on the forwarding class. For example, for the ef forwarding class, the default is ef. Table 46-3 lists the parameter options.

Force DE value

(forceDeValue)

The Force DE Value parameter specifies whether the [Mark DE bit](#) parameter value is forced. By default the value is set to the same value as the node; and the value is not forced. The options are:

- default (default)
- 0
- 1

Force DSCP Remark

(forceRemark)

The Force DSCP Remark parameter specifies whether to allow remarking of both the MPLS EXP and inner IP DSCP bits. Due to a difference in the marking and handling of different classes of services at AS Border Router boundaries between IP-VPN domains, there is a need to remark traffic egressing one AS and entering another. A VPRN model “B” boundary interface configured as a network port enables this remarking of DSCP and/or LSP EXP bits.

If the Force DSCP Remark parameter is set to true, it forces the remarking of all header markings based on the Forwarding Class mappings defined under the egress node of the network QoS policy. If the associated QoS Policy has enabled Force Remark and the policy includes mapping for both EXP and DSCP, then the traffic egressing that network interface has both fields remarked. If no DSCP mapping is configured, the DSCP bits are not changed. If only the DSCP mapping is configured, then only the DSCP bits are remarked. The options are:

- false (default)
- true

Forwarding Class

See the [Forwarding Class](#) parameter in section 112.1.

ID

(id)

See the [ID](#) parameter in section 112.1.

LER Use DSCP

(lerUseDscp)

The LER Use DSCP parameter specifies whether the LER in an LSP uses DSCP. The options are:

- false (default)
- true

LSP Exp

(lspExp)

The LSP Exp parameter specifies the LSP EXP value to forwarding class and profile mapping of LSP packets that ingress the network interface which uses the network policy. When a packet is marked with the value specified by the LSP Exp parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the profile specified by the Profile parameter. The range is 0 to 7. The default is 0.

LSP Exp In Profile

(lspExpInProfile)

The LSP EXP In Profile parameter specifies the forwarding class to LSP EXP mapping of in-profile LSP packets that egress the network interface which uses the network policy. When an in-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the LSP EXP value specified by the LSP EXP In Profile parameter. The default for the LSP EXP In Profile parameter depends on the forwarding class. The range is 0 to 7, or default.

LSP Exp Out Profile

(lspExpOutProfile)

The LSP EXP Out Profile parameter specifies the forwarding class to LSP experimental bit mapping of out-of-profile LSP packets that egress the network interface which uses the network policy. When an out-of-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the LSP experimental bit value specified by the LSP EXP Out Profile parameter. The default for the LSP EXP Out Profile parameter depends on the forwarding class. The range is 0 to 7, or default.

Mark DE bit

(deMark)

The Mark DE parameter specifies whether the Ethernet frame is marked eligible to be dropped when the network traffic is in excess of the committed rate. The values are:

- True
- False (default)

Profile

(profile)

See the [Profile](#) parameter in section 112.1.

Queue ID

See the [Queue ID](#) parameter in section 112.1.

Remark

(egressRemark)

The Remark parameter specifies whether packets that egress the network interface are remarked based on the forwarding class to DSCP and LSP EXP bit mapping defined by the network policy. The options are:

- false (default)
- true

Use Queue Group

The Use Queue Group parameter specifies whether a queue from an egress queue group template is used in the egress forwarding class of a network policy. The options are:

- Enabled
- Disabled (default)

When you set the Use Queue Group to Enabled, you must enter the egress queue ID specified in the queue group template policy in the Queue panel when applied to an IP interface.

47 – 7210 Network parameters

47.1 7210 Network parameters 47-2

47.1 7210 Network parameters

This chapter describes the parameters on the 7210 Network Policy form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→7210 Network.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

CIR Adaptation

See the [CIR Adaptation](#) parameter in section 112.1.

CIR (kbps)

See the [CIR \(kbps\)](#) parameter in section 112.1.

Committed Burst Size (kbps)

(cbs)

See the [Committed Burst Size \(kbps\)](#) parameter in section 112.1.

Default FC

See the [Default FC](#) parameter in section 112.1.

Default FC Profile

(defaultProfile)

The Default FC Profile parameter specifies whether packets that ingress a network interface which uses the network policy are by default considered in-profile or out-of-profile. All packets with undefined DSCP bits are mapped to the specified default profile and associated forwarding class. The default forwarding class is specified by the Default FC parameter. Table 47-1 describes the parameter options.

Table 47-1 Default FC Profile parameter

Option	Option description	Dependencies
out (default)	Specifies that packets are by default out-of-profile. In-profile packets are preferentially queued over out-of-profile packets.	—
in	Specifies that packets are by default in-profile. In-profile packets are preferentially queued over out-of-profile packets.	

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Dot1p

See the [Dot1p](#) parameter in section 112.1.

Dot1p In Profile

See the [Dot1p In Profile](#) parameter in section 112.1.

Dot1p Out Profile

See the [Dot1p Out Profile](#) parameter in section 112.1.

DSCP

See the [DSCP](#) parameter in section 112.1.

DSCP In Profile

(dscpInProfile)

The DSCP In Profile parameter specifies the forwarding-class-to-DCSP mapping for in-profile packets that egress the network interface which uses the network policy. When an in-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the DSCP value specified by the DSCP In Profile parameter. The default for the DSCP In Profile parameter depends on the forwarding class. For example, for the ef forwarding class, the default is ef. Table 47-2 lists the parameter options.

Table 47-2 DSCP In Profile parameter

Options			
default	ef	nc1	nc2
be	cp2	cp3	cp4
cp1	cp6	cp7	cp9
cp5	cp13	cp15	cp17
cp11	cp21	cp23	cp25
cp19	cp29	cp31	cp33
cp27	cp37	cp39	cp41
cp35	cp43	cp44	cp45
cp42	cp49	cp50	cp51
cp47	cp53	cp54	cp55
cp52	cp58	cp59	cp60
cp57	cp62	cp63	cs1

(1 of 2)

Options			
cp61	cs3	cs4	cs5
cs2	af12	af13	af21
af11	af23	af31	af32
af22	af41	af42	af43
af33	—	—	—

(2 of 2)

DSCP Out Profile

(dscpOutProfile)

The DSCP Out Profile parameter specifies the forwarding class to DSCP mapping for in-profile packets that egress the network interface which uses the network policy. When an out-of-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the DSCP value specified by the DSCP Out Profile parameter. The default for the DSCP Out Profile parameter depends on the forwarding class. For example, for the ef forwarding class, the default is ef. Table 47-2 lists the parameter options.

Forwarding Class

See the [Forwarding Class](#) parameter in section 112.1.

ID

See the [ID](#) parameter in section 112.1.

LSP Exp

(lspExp)

The LSP Exp parameter specifies the LSP-Exp value to forwarding class and profile mapping of LSP packets that ingress the network interface which uses the network policy. When a packet is marked with the value specified by the LSP-Exp parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the profile specified by the Profile parameter. The range is 0 to 7. The default is 0.

LSP Exp In Profile

(lspExpInProfile)

The LSP Exp In Profile parameter specifies the forwarding class to LSP-Exp mapping of in-profile LSP packets that egress the network interface which uses the network policy. When an in-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the LSP-Exp value specified by the LSP Exp In Profile parameter. The default for the LSP Exp In Profile parameter depends on the forwarding class. The range is 0 to 7, or default.

LSP Exp Out Profile

(lspExpOutProfile)

The LSP EXP Out Profile parameter specifies the forwarding class to LSP experimental bit mapping of out-of-profile LSP packets that egress the network interface which uses the network policy. When an out-of-profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the LSP experimental bit value specified by the LSP EXP Out Profile parameter. The default for the LSP EXP Out Profile parameter depends on the forwarding class. The range is 0 to 7, or default.

Maximum Burst Size (kbps)

See the [Maximum Burst Size \(kbps\)](#) parameter in section 112.1.

Meter

(meter)

The Meter parameter overrides the default unicast forwarding type meter mapping. When the forwarding class mapping is executed, the unicast traffic on a port using this policy is forwarded using this parameter value. The range is 1 to 12. The default is N/A, which means that all unicast traffic uses the default meter mapping for the forwarding class.



Note — The 7210 SAS-M node supports only one default meter with ID: 1. The 7210 SAS-M Uplink node supports two default meters with IDs: 1 and 9.

Mode

(mode)

The Mode parameter specifies the mode of the meter. Table 47-3 describes the parameter options.

Table 47-3 Mode parameter options

Options	Description
trTCM	Specifies the maximum burst size that can be transmitted by the source at the PIR while complying with the PIR. If the transmitted burst is lower than the MBS value, the packets are marked as out-profile by the meter to indicate that the traffic is not complying with the CIR, but is complying with the PIR. If the packet burst is higher than MBS, packets that are marked as red are dropped by the meter.
srTCM	Specifies the maximum burst size that can be transmitted by the source while not complying with the CIR. If the transmitted burst is less than the MBS value, the packets are marked as out-profile by the meter to indicate that the traffic is not complying with the CIR. If the packet burst is greater than MBS, the packets that are marked as red are dropped by the meter.

(1 of 2)

Options	Description
trTCM (RFC 2698)	Specifies the maximum burst size that can be transmitted by the source at the PIR while complying with the PIR. If the transmitted burst is less than the MBS value, the packets are marked as out-profile by the meter to indicate that the traffic is not complying with the CIR, but is complying with the PIR. If the packet burst is greater than MBS, packets that are marked as red are dropped by the meter. This option, or trTCN (RFC 4115) must be selected in order to distribute ingress meters on a 7210 network policy on SAS-X or SAS-M switches of version 2.0 R4 or higher.
trTCM (RFC 4115)	Specifies the maximum burst size that can be transmitted by the source at the PIR while complying with the PIR. If the transmitted burst is less than the MBS value, the packets are marked as out-profile by the meter to indicate that the traffic is not complying with the CIR, but is complying with the PIR. If the packet burst is greater than MBS, packets that are marked as red are dropped by the meter. This option, or trTCN (RFC 2698) must be selected in order to distribute ingress meters on a 7210 network policy on SAS-X or SAS-M switches of version 2.0 R4 or higher.

(2 of 2)

MultiCast-Meter

(mCastMeter)

The MultiCast-Meter parameter overrides the default multicast forwarding type meter mapping for multicast traffic. When the forwarding class mapping is executed, all multicast traffic on a port using this policy is forwarded using this parameter value. The range is 1 to 12. The default is N/A, meaning that all multicast traffic uses the default meter mapping for the forwarding class.

MultiPoint

(mCast)

See the [MultiPoint](#) parameter in section 112.1.

Nw Mgr ID

(id)

The Nw Mgr ID parameter specifies a unique Id for the policy. You can configure the parameter for policies when the [Auto-Assign ID](#) parameter is set to disabled. The options are 1 to 12. You cannot create or delete meter ID 1 (unicast default) or 9 (multipoint default).

PIR Adaptation

See the [PIR Adaptation](#) parameter in section 112.1.

PIR (kbps)

See the [PIR \(kbps\)](#) parameter in section 112.1.

Policy Id

(nwPolicyId)

The Policy Id parameter specifies a unique Id for the policy. You can configure the parameter for policies when the [Auto-Assign ID](#) parameter is set to disabled. The options are 1 to 12. Each policy must have a unique combination of Policy Id and [Type](#) parameter settings.

Profile

See the [Profile](#) parameter in section [112.1](#).

Remark

(egressRemark)

The Remark parameter specifies whether packets that egress the network interface are remarked based on the forwarding class to DSCP and LSP EXP bit mapping defined by the network policy. The options are:

- false (default)
- true

Scope

See the [Scope](#) parameter in section [112.1](#).

Type

(nwPolicyType)

The Type parameter specifies the type of object to which the policy applies. The options are:

- Port
- Network Interface

Each policy must have a unique combination of the [Policy Id](#) and Type parameter settings.

48 – Network Queue parameters

48.1 Network Queue parameters 48-2

48.1 Network Queue parameters

This chapter describes the parameters on the Network Queue Policy form and its child forms. The 5620 SAM menu path is Policies→QoS→Network Queue.

Burst Limit (bytes)

(burstLimit)

The Burst Limit (bytes) parameter specifies the explicit shaping burst size of a queue. The range is -1 and 1 to 1 000 000. The default is -1.

CIR (%)

(cir)

The CIR (%) (kb/s) parameter specifies the committed information rate, as a percentage of available bandwidth, for a queue on a network port or daughter card. The range is 0 to 100. The default is 100.

The CIR defines the rate at which the device prioritizes the queue over other queues that are competing for the same bandwidth. On network ingress interfaces, the CIR also defines the rate that packets are considered in-profile by the system.

CIR Adaptation

(cirAdaptation)

The CIR Adaptation parameter specifies the constraint enforced when adapting the committed information rate defined by the [CIR \(%\)](#) parameter. Table 48-1 describes the parameter options.

Table 48-1 CIR Adaptation parameter options

Option	Option description
Closest (default)	Operational CIR for the queue is the rate closest to the rate specified using the CIR (%) parameter.
Min	Operational CIR for the queue is equal to or greater than the administrative rate specified using the CIR (%) parameter.
Max	Operational CIR for the queue is equal to or less than the administrative rate specified using the CIR (%) parameter.

CIR Level

See the [CIR Level](#) parameter in section [112.1](#).

CIR Weight

See the [CIR Weight](#) parameter in section [112.1](#).

Committed Burst Size (%)

(cbs)

The Committed Burst Size (%) parameter specifies the relative amount of reserved buffer pool space for an ingress network daughter card queue or an egress network port queue. The range is 0 to 100. The default depends on the forwarding class mapping to the queue.

The CBS for a queue determines whether it has exhausted its reserved buffer pool space while enqueueing packets. When the queue has exceeds the amount of buffer pool space considered in reserve for the queue, it must contend with other queues for the available shared buffer space in the buffer pool. Access to this shared pool space is controlled by the RED slope, as specified using the Slope Policy Manager.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Egress HSMDA Queue ID

(fcEgrHsmdaQueue)

The Egress HSMDA Queue ID parameter specifies an egress HSMDA queue to be mapped to a forwarding class. The range is 1 to 8.

The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping that you specify overrides the default forwarding class-to-queue mapping for egress HSMDA traffic.

Forwarding Class

See the [Forwarding Class](#) parameter in section 37.1.

High Priority Reserved (%)

(highPriority)

The High Priority Reserved (%) parameter specifies the relative amount of queue buffer pool space that is reserved for high priority traffic on an ingress network daughter card queue or an egress network port queue. The range is 0 to 100. The default depends on the forwarding class mapping to the queue.

The difference between the MBS for the queue and the high-priority reserve defines the threshold at which low priority traffic is discarded. The result is used on the queue to define a threshold where low priority packets are discarded, leaving the rest of the default MBS size for high priority packets only.

For example, if the current MBS for the queue is 10 Mb, a value of 5% for high priority traffic results in a high priority reserve on the queue of 500 kb. A value of 0 specifies that none of the MBS of the queue is reserved for high-priority traffic. This setting does not affect the RED slope operation for packets attempting to be queued.

Level

See the [Level](#) parameter in section 112.1.

Maximum Burst Size (bytes)

(mbsBytes)

The Maximum Burst Size (bytes) parameter specifies the maximum burst pool size for a queue and overrides the default reserved burst pool for the queue. The range is 0 to 2 668 000. Default specifies that the device calculates committed burst pool size based on the the PIR. The default is Default enabled.

Maximum Burst Size (%)

(mbs)

The Maximum Burst Size (%) parameter specifies the relative amount of reserved buffer pool space for the maximum buffer for an ingress network daughter card or an egress network port queue. The range is 0 to 100. The default depends on the forwarding class mapping to the queue.

The MBS for a queue is used to determine whether the queue has exhausted its total allowed buffer space while enqueueing packets. After the queue has exceeded its maximum amount of buffer space, all packets are discarded until the queue transmits a packet.

Even when a queue has not exceeded its MBS size, buffer pool space is not guaranteed. The RED slope may also force the discard of the packet. You must set proper CBS parameter values and control CBS oversubscription to avoid to queue starvation (when a queue does not receive its fair share of buffer space). You must also properly set the RED slope parameters for the needs of the network queues using the Slope Policy Manager.

Multicast

See the [Multipoint](#) parameter in section 37.1.

Multipoint Queue ID

(multicastQueueId)

The Multipoint Queue ID parameter specifies a multicast queue to be mapped to a forwarding class.

The queue is mapped to a specific forwarding class specified by the Forwarding Class parameter. The mapping you specify overrides the default forwarding-class-to-queue mapping for multicast traffic.

PIR (%)

(pir)

The PIR (%) parameter specifies the peak information rate, as a percentage of available bandwidth, for an ingress network MDA queue or an egress network port queue. The range is 0 to 100. The default is 100.

On ingress, the PIR defines the maximum rate that the queue can transmit packets through the switch fabric. On egress, the PIR defines the maximum rate that the queue can transmit packets out an egress interface.

The specified PIR (%) value does not guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

Queue ID

(queueId)

The Queue ID parameter specifies a unicast queue to be mapped to a forwarding class. The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping that you specify overrides the default forwarding class-to-queue mapping for unicast traffic.

PIR Adaptation

(cirAdaptation)

The PIR Adaptation parameter specifies the constraint enforced when adapting the peak information rate defined by the [PIR \(%\)](#) parameter. Table 48-2 describes the parameter options.

Table 48-2 PIR Adaptation parameter options

Option	Option description
Closest (default)	Operational PIR for the queue is the rate closest to the rate specified using the PIR (%) parameter.
Min	Operational PIR for the queue is equal to or greater than the administrative rate specified using the PIR (%) parameter.
Max	Operational PIR for the queue is equal to or less than the administrative rate specified using the PIR (%) parameter.

Port Average Overhead (%)

See the [Port Average Overhead \(%\)](#) parameter in section 112.1.

Port Parent

See the [Port Parent](#) parameter in section 112.1.

Weight

See the [Weight](#) parameter in section 112.1.

49 – 7210 Network Queue parameters

49.1 7210 Network Queue parameters 49-2

49.1 7210 Network Queue parameters

This chapter describes the parameters on the 7210 Network Queue policy form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→7210 Network Queue.

CIR (%)

(cir)

See the [CIR \(%\)](#) parameter in section 112.1.

CIR Adaptation

See the [CIR Adaptation](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

PIR (%)

(pir)

See the [PIR \(%\)](#) parameter in section 112.1.

PIR Adaptation

See the [PIR Adaptation](#) parameter in section 112.1.

50 – Shared Queue parameters

50.1 Shared Queue parameters 50-2

50.1 Shared Queue parameters

This chapter describes the parameters on the QoS→Shared Queue form and its child forms.

CIR (%)

(cir)

The CIR (%) parameter specifies the committed information rate, as a percentage of the maximum rate for the queue, for an ingress or egress daughter card queue to transmit packets through the switch fabric or out an egress interface. The range is 0 to 100%. The default depends on the queue ID.

For SAP ingress on daughter cards, the CIR defines the rate that packets are considered in-profile by the system. In-profile packets are preferentially queued by the system at egress and at subsequent next-hop devices on which the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

Committed Burst Size (%)

(cbs)

The Committed Burst Size (%) parameter specifies the relative percentage of reserved buffer pool space allotted for a daughter card queue. The range is 0 to 100%. The default depends on the forwarding class mapping to the queue.

The committed burst size for a queue determines whether the queue has exhausted its reserved buffer pool space while queuing packets. When the queue has exceeded the amount of buffer pool space considered in reserve for the queue, it must contend with other queues for the available shared buffer space in the buffer pool. Access to this shared pool space is controlled by the RED slope.

Two RED slopes are maintained in each buffer pool. A high-priority slope is used by in-profile packets. A low-priority slope is used by out-of-profile packets. All nc forwarding class packets are considered in-profile. Assured packets are handled by their in-profile and out-of-profile markings. All be packets are considered out-of-profile.

Premium queues should be configured such that the committed burst size is sufficient to prevent shared buffering of packets. This is handled by the CIR scheduling of premium queues and the overall small amount of traffic on the class. Premium queues in a properly designed system drain before all others, limiting their buffer utilization. The RED slopes detect congestion conditions and work to discard packets and slow down random TCP session flows through the queue.

The resultant committed burst size can be larger than the maximum burst size. This results in a portion of the committed burst size for the queue unused and should be avoided.

Description

See the [Description](#) parameter in section 112.1.

High Priority Reserved (%)

(highPriority)

The High Priority Reserved (%) parameter specifies the relative percentage of queue buffer pool space that is reserved for high-priority traffic in an ingress network daughter card queue or an egress network port queue. The range is 0 to 100%. The default is 10%.

The difference between the maximum burst size for the queue and the high-priority reserve defines the threshold at which low-priority traffic is discarded. The result is used on the queue to define a threshold at which low-priority packets are discarded, leaving the rest of the default maximum burst size for high-priority packets only.

For example, if the current maximum burst size for the queue is 10 Mb, a value of 5% for high-priority traffic results in a high priority reserve on the queue of 500 kb. A value of 0% specifies that none of the maximum burst size of the queue is reserved for high-priority traffic. This setting does not affect RED slope operation for packets attempting to be queued.

Maximum Burst Size (%)

(mbs)

The Maximum Burst Size (%) parameter specifies the relative percentage of reserved buffer pool space for the maximum buffer allotted for a daughter card queue. The range is 0 to 100%. The default depends on the forwarding class mapping to the queue.

The maximum burst size for a queue is used to determine whether the queue has exhausted its total allowed buffer space while queuing packets. When the queue has exceeded its maximum amount of buffer space, all packets are discarded until the queue transmits a packet.

Even when a queue has not exceeded its maximum burst size, buffer pool space is not guaranteed. The RED slope may also force the discard of the packet. You must set proper committed burst size parameter values and control committed burst size oversubscription to avoid queue starvation (when a queue does not receive its fair share of buffer space). You must also properly set the RED slope parameters for the needs of the network queues using the Slope Policy Manager.

The MBS size can sometimes be smaller than the CBS. This results in a portion of the CBS for the queue to be unused and should be avoided.

PIR (%)

(pir)

The PIR (%) parameter specifies the peak information rate, as a percentage of the maximum rate for the queue, for an ingress or egress daughter card queue to transmit packets through the switch fabric or out an egress interface. The range is 0 to 100%. The default is 100%.

On ingress, the PIR defines the maximum rate at which the queue can transmit packets through the switch fabric. On egress, the PIR defines the maximum rate at which the queue can transmit packets out an egress interface.

The specified PIR value does not guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or the available bandwidth.

51 — WRED Slope parameters

51.1 WRED Slope parameters 51-2

51.1 WRED Slope parameters

This chapter describes the parameters on the Slope Policy form and child forms.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

High Slope

The High Slope parameter specifies how the high-priority packets, also known as in-profile packets, access the shared portion of the buffer pool. The probability of the buffer pools discarding packets is determined by the RED slope. The RED slope is indicated on the client GUI using a graph.

The Start Avg., Max Avg., and Max Prob. parameters specify the values of the RED slope.

In general, packets that are in-profile fall within the configured CIR and PIR ranges. This means the packets are more likely to gain access to the shared buffer pool, and not be discarded because of a buffer overflow.

Low Slope

The Low Slope parameter specifies how the low-priority packets, also known as out-of-profile packets, access the shared portion of the buffer pool. The probability of the buffer pools discarding packets is determined by the RED slope. The RED slope is indicated on the client GUI using a graph.

The Start Avg., Max Avg., and Max Prob. parameters specify the values of the RED slope.

In general, packets that are out-of-profile fall outside configured CIR and PIR ranges. This means the packets should not be allowed to cause a buffer overflow in the shared buffer pool, and should be more likely to be discarded because of a buffer overflow.

Max Avg.

(maxAverage)

The Max Avg. parameter specifies the maximum average of the RED slope position. The parameter indicates that the packet discard probability has increased to 1, and packets are discarded. The range is 0 to 100%. The default is 75% buffer pool utilization before the packet discard probability is 100% for the low slope and 90% for the high slope. The parameter must be greater than or equal to the Start Avg. parameter.

For example, when out-of-profile packets arrive on an interface configured with a low slope policy that has the parameter set to 75% and the Start Avg. parameter set to 50%, out-of-profile packets may start to be discarded by the buffer when it reaches 50% full, and all packets are dropped when the buffer reaches 75% full. The probability of the packets being discarded before the Max Avg. parameter is reached is determined by the Max Prob. parameter.

Max Prob.

(maxProbability)

The Max Prob. parameter specifies the maximum probability that a packet is dropped by the buffer pool. The range is 0 to 100%. The default is 80%. The parameter specifies that an in-profile or out-of-profile packet is, by default, 80% likely to be dropped by the buffer pool after the shared buffer size reaches the percentage full conditions, as specified by the Start Avg. and Max Avg. parameters.

For example, when out-of-profile packets arrive on an interface configured with a low slope policy that has the Start Avg. parameter set to 50% and the Max. Avg. parameter set to 75%, out-of-profile packets may start to be discarded by the buffer when it reaches 50% full, and all packets are dropped when the buffer reaches 75% full. The probability of the packets being discarded before the Max Avg. parameter is reached is determined by the Max Prob. parameter.

Start Average

(startAverage)

The Start Avg. parameter specifies the starting average of the RED slope position. The parameter indicates that the packet discard probability has increased above 0 to the percentage specified of the shared buffer size. The range is 0 to 100%. The default is 50% for the low slope and 70% for the high slope.

For example, when out-of-profile packets arrive on an interface configured with a low slope policy that has the parameter set to 50%, out-of-profile packets may be discarded by the buffer when it reaches 50% full. When the buffer reaches the Max Avg. parameter, all packets above that percentage value are dropped. The probability of the packets being discarded is determined by the Max Prob. parameter.

Time Average Factor (weight)

(timeAverageFactor)

The Time Average Factor (Weight) parameter specifies a weight factor between the previous shared buffer average utilization and current shared buffer instantaneous utilization when a new shared buffer average utilization is calculated. The range is 0 to 15. The default is 7, which indicates an instantaneous shared buffer utilization of 0.8%.

The Time Average Factor (Weight) parameter must be set to 3 on the 7705 SAR.

Weighting occurs when the buffer pool uses a portion of the previous shared buffer average and adds the factor to the instantaneous shared buffer utilization. A low value, such as 3, weights the new shared buffer average utilization more towards the shared buffer instantaneous utilization. A high value, such as 11, weights the new shared buffer average utilization more towards the previous shared buffer average utilization value, rather than the shared buffer instantaneous utilization.

52 – 7210 Slope parameters

52.1 7210 Slope parameters 52-2

52.1 7210 Slope parameters

This chapter describes the parameters on the 7210 Slope Policy form and child forms.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether the low slope or high slope parameters are enabled. The options are:

- Disabled (default)
- Enabled

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Queue1 Drop Rate

(queue1DropRate)

The Queue 1 Drop Rate parameter specifies the RED slope drop rate for the shared buffer per queue. This parameter is expressed as a percentage of the packets dropped in congested conditions. A value of 100% means that after the shared buffer utilization reaches the value specified by the “[Start Threshold](#)” parameter, the packets egressing out from a specific queue are dropped at a 100% rate. The high slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. You can configure this parameter for the low slope and high slope shared buffer. The options are:

- | | |
|-----------------------------|-------------|
| • 100 (low slope default) | • .78125 |
| • 6.25 (high slope default) | • .390625 |
| • 3.125 | • .1953125 |
| • 1.5625 | • .09765625 |

Queue2 Drop Rate

(queue2DropRate)

See the [Queue1 Drop Rate](#) in this section for more information.

Queue3 Drop Rate

(queue3DropRate)

See the [Queue1 Drop Rate](#) is this section for more information.

Queue4 Drop Rate

(queue4DropRate)

See the [Queue1 Drop Rate](#) is this section for more information.

Queue5 Drop Rate

(queue5DropRate)

See the [Queue1 Drop Rate](#) is this section for more information.

Queue6 Drop Rate

(queue6DropRate)

See the [Queue1 Drop Rate](#) is this section for more information.

Queue7 Drop Rate

(queue7DropRate)

See the [Queue1 Drop Rate](#) is this section for more information.

Queue8 Drop Rate

(queue8DropRate)

See the [Queue1 Drop Rate](#) is this section for more information.

Start Threshold

(startThreshold)

The Start Threshold parameter specifies the low slope or high slope RED position for the shared buffer instantaneous utilization value when the packet discard probability comes into affect. The parameter value is expressed as a percentage of the shared buffer size. The range is 0 to 100. The low slope default is 50 and the high slope default is 75.

53 — HSMDA WRED Slope parameters

53.1 HSMDA WRED Slope parameters 53-2

53.1 HSMDA WRED Slope parameters

This chapter describes the parameters on the HSMDA Slope Policy form and child forms.

Administrative State

See the [Administrative State](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

HSMDA High Slope

The High Slope parameter specifies how the high-priority packets, also known as in-profile packets, access the shared portion of the buffer pool. The probability of the buffer pools discarding packets is determined by the RED slope. The RED slope is indicated on the client GUI in a graph.

The Start Depth, Max Depth, and Max Prob. parameters specify the values of the RED slope.

In general, packets that are in-profile fall within the configured CIR and PIR ranges. This means that the packets are more likely to gain access to the shared buffer pool, and not be discarded because of a buffer overflow.

HSMDA Low Slope

The Low Slope parameter specifies how the low-priority packets, also known as out-of-profile packets, access the shared portion of the buffer pool. The probability of the buffer pools discarding packets is determined by the RED slope. The RED slope is indicated on the client GUI in a graph.

The Start Depth, Max Depth, and Max Prob. parameters specify the values of the RED slope.

In general, packets that are out-of-profile fall outside configured CIR and PIR ranges. This means that the packets should not be allowed to cause a buffer overflow in the shared buffer pool, and are more likely to be discarded because of a buffer overflow.

Max Depth

(maxDepth)

The Max Depth parameter specifies where (based on MBS utilized) the discard probability rises to 100%. The range is .01 to 100%. The default for the HSMDB low slope is 90%. The default for the HSMDB high slope is 100%.

Max Probability

(maxProbability)

The Max Probability parameter specifies where the discard probability deviates from the slope and rises to 100%. The range is .01 to 100 percent. The default for the HSMDB low and high slopes is 100 percent.

Queue MBS (bytes)

(queueMbs)

The Queue MBS (bytes) parameter specifies the queue MBS. The range is 0 to 500 000. The default is 16 800.

Start Depth

(startDepth)

The Start Depth parameter specifies where the discard probability for the slope starts to rise above 0%. The range is .01 to 100%. The default for the HSMDB low slope is 90%. The default for the HSMDB high slope is 100%.

54 – Scheduler parameters

54.1 Scheduler parameters 54-2

54.1 Scheduler parameters

This chapter describes the parameters on the Scheduler Policy form and its child forms.

CIR (kbps)

(cir)

The CIR (kbps) parameter specifies the committed information rate of the scheduler. Table 54-1 describes the parameter options.

Table 54-1 CIR (kbps) parameter

Option	Option description	Dependencies
MAX (default)	The CIR is set to infinity, and is only dependent on the forwarding class of the service access interface.	Configurable when the Summed CIR parameter is set to false
-1, 0 to 100 000 000	The CIR, in kb/s, for the scheduler. This is shown as MAX on the client GUI.	Configurable when the Summed CIR parameter is set to false and the MAX parameter is disabled

The CIR and PIR ranges that are configured for schedulers are used to define its profile marking level and the bandwidth the scheduler receives when schedulers are contending for bandwidth on a congested service interface.

The MAX option specifies whether the CIR (kbps) parameter is set to infinity or can be configured. The options are:

- disabled (default)
- enabled

When MAX is enabled, you cannot configure the CIR parameter.

CIR Level

See the [CIR Level](#) parameter in section 112.1.

CIR Weight

See the [CIR Weight](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Frame Based Accounting

(schedulerPolicyFrameBasedAcct)

The Frame Based Accounting parameter specifies whether to use Frame Base Accounting or packet based accounting. Frame Based Accounting uses inter-frame gap and instructions to calculate overhead.

Level

See the [Level](#) parameter in section 112.1.

Parent Scheduler

(nextSchedulerName)

The Parent Scheduler specifies the higher-tier scheduler that is the parent scheduler for a tier 2 or tier 3 scheduler. The parameter is configurable when the Tier parameter is set to the 2 or 3 option.

Enter the same name as the Displayed Name parameter, or click on the Select button and choose a parent scheduler from the Select a Parent Scheduler list.

PIR (kbps)

(pir)

The PIR parameter specifies the peak information rate of the scheduler. Table 54-2 describes the parameter options.

Table 54-2 PIR (kbps) parameter

Option	Option description	Dependencies
MAX (default)	The PIR is set to infinity, and forwards packets at the maximum rate.	—
-1, 1 to 100 000 000	The PIR, in kb/s, for the scheduler. This is the maximum rate at which the scheduler can forward packets as a peak rate. This is shown as MAX on the client GUI.	Configurable when the MAX parameter is disabled.

The CIR and PIR ranges that are configured for schedulers are used to define the profile marking level and the bandwidth the scheduler receives when schedulers are contending for bandwidth on a congested service interface.

The MAX option specifies whether the PIR (kbps) parameter is set to infinity or can be configured. The options are:

- disabled (default)
- enabled

When MAX is enabled, you cannot configure the PIR parameter.

Port Parent

See the [Port Parent](#) parameter in section 112.1.

Summed CIR

(summedCir)

The Summed CIR parameter specifies whether to define the CIR at which the scheduler operates or to use the maximum CIR. Table 54-3 describes the parameter options.

Table 54-3 Summed CIR parameter

Option	Option description	Dependencies
true (default)	The CIR is set to infinity, and the rate is only dependent on the forwarding class for the service interface using the scheduler.	—
false	The CIR rate is defined for the scheduler.	Configure the CIR parameter and the MAX parameter to specify the CIR rate.

The CIR and PIR ranges that are configured for schedulers are used to define the profile marking level and the bandwidth the scheduler receives when schedulers are contending for bandwidth on a congested service interface.

Tier

(tier)

The Tier parameter specifies the hierarchical level that a group of schedulers are associated with. The range is 1 to 3. The default is 1, which represents the highest tier.

The parameter defines the hierarchy scheduler within the schedule policy tiers. 1 represents the highest tier, 2 the second highest tier, and 3 the lowest tier. For example, a tier 2 scheduler can be the child of a tier 1 parent. In this case, the child tier 2 scheduler can use bandwidth from the parent tier 1 scheduler. A tier 1 scheduler is considered root, and cannot be the child of another scheduler. However, you can create a tier 2 scheduler without creating a parent tier 1 scheduler and you can create a tier 3 scheduler without creating a tier 2 scheduler.

When multiple schedulers share the child status with the parent scheduler, the Weight and Level parameters are used to define how child schedulers contend for the parent scheduler's bandwidth.

Weight

See the [Weight](#) parameter in section 112.1.

55 — Port Scheduler parameters

55.1 Port Scheduler parameters 55-2

55.1 Port Scheduler parameters

This chapter describes the parameters on the Port Scheduler Policy form and its child forms. The 5620 SAM menu path is Policies→QoS→Port Scheduler.

CIR (kbps)

(lvl1Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 1 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR (kbps)

(lvl2Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 2 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR (kbps)

(lvl3Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 3 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR (kbps)

(lvl4Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 4 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR (kbps)

(lvl5Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 5 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR (kbps)

(lvl6Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 6 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR (kbps)

(lvl7Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 7 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR (kbps)

(lvl8Cir)

The CIR (kbps) parameter specifies the total committed information rate for priority level 8 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

CIR Level

(orphanCirLevel)

The CIR Level parameter specifies the CIR priority level of orphan port schedulers and queues in comparison to other orphan port schedulers and queues for within-CIR distribution. The range is Default, 1 to 8. The default is Default. The higher the number, the higher the CIR priority level of the orphan port scheduler within-CIR request from the parent.

When two orphan port schedulers or queues have the same CIR Level parameter value, the [CIR Weight](#) parameter determines which scheduler first receives the CIR bandwidth.

CIR Weight

(orphanCirWeight)

The CIR Weight parameter specifies the default relative importance of an orphan port scheduler in comparison to other schedulers at the same port priority level for within-CIR distribution. The range is 000 to 100. The default is 000. The higher the number, the higher the priority of the orphan port scheduler CIR bandwidth request.

A setting of 000 specifies that the orphan port schedulers and queues do not receive bandwidth from the within-CIR distribution. All bandwidth for the orphan port schedulers and queues is allocated from the above-CIR distribution.

Description

See the [Description](#) parameter in section [112.1](#).

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Level

(orphanLevel)

The Level parameter specifies the port priority level of orphan port schedulers and queues for traffic above the parent scheduler CIR. The range is 1 to 8. The default is 1. The higher the number, the higher the port priority level of the orphan port scheduler bandwidth request.

Orphan schedulers with the Level parameter set lower than other orphan schedulers do not receive bandwidth until all orphan schedulers with a higher level have reached their maximum bandwidth allocation, or have no packets to pass.

When two orphan port schedulers have the same Level parameter value, the Weight parameter determines which scheduler first receives bandwidth.

For example, there are three tier 2 schedulers with the same tier 1 parent scheduler:

- orphan port scheduler alpha has its Level parameter set to 3
- orphan port scheduler beta has its Level parameter set to 6
- orphan scheduler omega has its Level parameter set to 7

When the parent scheduler receives traffic above its CIR, bandwidth is allocated to the orphan schedulers. Orphan scheduler omega receives the bandwidth from the parent scheduler before beta and alpha. When omega reaches its maximum bandwidth requirements, and there is bandwidth remaining, scheduler beta receives the bandwidth before scheduler alpha.

Maximum Rate (kbps)

(maxRate)

The Maximum Rate (kbps) parameter specifies the maximum bandwidth for the port scheduler policy. When the port scheduler policy is associated with a port or channel, the bandwidth of the port or channel is limited to the lesser of the port or channel line rate and the value of the Maximum Rate (kbps) parameter. The range is 1 to 100 000 000, or 1. The default is MAX.

PIR (kbps)

(lvl1Pir)

The PIR (kbps) parameter specifies the total peak information rate for priority level 1 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

PIR (kbps)

(lvl2Pir)

The PIR (kbps) parameter specifies the total peak information rate for priority level 2 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

PIR (kbps)**(lvl3Pir)**

The PIR (kbps) parameter specifies the total peak information rate for priority level 3 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

PIR (kbps)**(lvl4Pir)**

The PIR (kbps) parameter specifies the total peak information rate for priority level 4 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

PIR (kbps)**(lvl5Pir)**

The PIR (kbps) parameter specifies the total peak information rate for priority level 5 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

PIR (kbps)**(lvl6Pir)**

The PIR (kbps) parameter specifies the total peak information rate for priority level 6 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

PIR (kbps)**(lvl7Pir)**

The PIR (kbps) parameter specifies the total peak information rate for priority level 7 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

PIR (kbps)**(lvl8Pir)**

The PIR (kbps) parameter specifies the total peak information rate for priority level 8 of the port scheduler. The range is 0 to 100 000 000, or –1. The default is MAX.

Weight**(orphanWeight)**

The Weight parameter specifies the relative importance of orphan port schedulers and queues in comparison to other orphan port schedulers and queues that have identical [Level](#) parameter settings for above-CIR distribution. The range is 000 to 100. The default is 000. The higher the number, the higher the priority of the orphan port scheduler bandwidth request.

Weight in group**(lvl1GroupWeight)**

The Weight in group parameter specifies the weight of priority level 1 within the associated scheduler group. The range is 1 to 100. The default is 1.

Weight in group**(lvl2GroupWeight)**

The Weight in group parameter specifies the weight of priority level 2 within the associated scheduler group. The range is 1 to 100. The default is 1.

Weight in group**(lvl3GroupWeight)**

The Weight in group parameter specifies the weight of priority level 3 within the associated scheduler group. The range is 1 to 100. The default is 1.

Weight in group**(lvl4GroupWeight)**

The Weight in group parameter specifies the weight of priority level 4 within the associated scheduler group. The range is 1 to 100. The default is 1.

Weight in group**(lvl5GroupWeight)**

The Weight in group parameter specifies the weight of priority level 5 within the associated scheduler group. The range is 1 to 100. The default is 1.

Weight in group**(lvl6GroupWeight)**

The Weight in group parameter specifies the weight of priority level 6 within the associated scheduler group. The range is 1 to 100. The default is 1.

Weight in group**(lvl7GroupWeight)**

The Weight in group parameter specifies the weight of priority level 7 within the associated scheduler group. The range is 1 to 100. The default is 1.

Weight in group**(lv18GroupWeight)**

The Weight in group parameter specifies the weight of priority level 8 within the associated scheduler group. The range is 1 to 100. The default is 1.

56 — HSMDA Scheduler parameters

56.1 HSMDA Scheduler parameters 56-2

56.1 HSMDA Scheduler parameters

This chapter describes the parameters on the HSMDA Scheduler Policy form and child forms.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Group

Table 56-1 lists where to find information about the Group parameter.

Table 56-1 Group parameter

Parameter	See
Group for class 1	Group parameter in this section
Group for class 2	Group parameter in this section
Group for class 3	Group parameter in this section
Group for class 4	Group parameter in this section
Group for class 5	Group parameter in this section
Group for class 6	Group parameter in this section
Group for class 7	Group parameter in this section
Group for class 8	Group parameter in this section

Group

(level1Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 1 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Group

(level2Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 2 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Group

(level3Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 3 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Group

(level4Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 4 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Group

(level5Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 5 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Group

(level6Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 6 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Group

(level7Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 7 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Group

(level8Group)

The Group parameter specifies the weighted scheduling of the group that the HSMDA scheduler policy class 8 belongs to. The options are:

- None (default)
- Group 1
- Group 2

Maximum Rate (Mbps)

(schedulerMaxRate)

The Maximum Rate parameter specifies the explicit maximum frame-based bandwidth for the HSMDA scheduler policy context. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that all instances of the scheduler policy on the egress ports are allowed at the available line rate.

Rate (Mbps)

Table 56-2 lists where to find information about the Rate (Mbps) parameter.

Table 56-2 Rate (Mbps) parameter

Parameter	See
Rate for group 1	Rate (Mbps) parameter in this section
Rate for group 2	Rate (Mbps) parameter in this section
Rate for class 1	Rate (Mbps) parameter in this section
Rate for class 2	Rate (Mbps) parameter in this section
Rate for class 3	Rate (Mbps) parameter in this section
Rate for class 4	Rate (Mbps) parameter in this section
Rate for class 5	Rate (Mbps) parameter in this section
Rate for class 6	Rate (Mbps) parameter in this section

(1 of 2)

Parameter	See
Rate for class 7	Rate (Mbps) parameter in this section
Rate for class 8	Rate (Mbps) parameter in this section

(2 of 2)

Rate (Mbps)

(group1Rate)

The Rate (Mbps) parameter specifies the maximum rate allowed for the scheduling classes mapped to group 1. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the bandwidth limitation is removed from group 1.

Rate (Mbps)

(group2Rate)

The Rate (Mbps) parameter specifies the maximum rate allowed for the scheduling classes mapped to group 2. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the bandwidth limitation is removed from group 2.

Rate (Mbps)

(level1Rate)

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 1. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Rate (Mbps)

(level2Rate)

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 2. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Rate (Mbps)

(level3Rate)

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 3. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Rate (Mbps)**(level4Rate)**

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 4. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Rate (Mbps)**(level5Rate)**

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 5. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Rate (Mbps)**(level6Rate)**

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 6. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Rate (Mbps)**(level7Rate)**

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 7. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Rate (Mbps)**(level8Rate)**

The Rate (Mbps) parameter specifies the maximum rate allowed for scheduling class 8. The parameter is configurable when the MAX check box is disabled. The range is 1 to 100 000. The default is MAX. MAX means that the limit is not enforced for the class.

Weight

Table [56-3](#) lists where to find information about the Weight parameter.

Table 56-3 Weight parameter

Parameter	See
Weight for class 1	Weight parameter in this section
Weight for class 2	Weight parameter in this section
Weight for class 3	Weight parameter in this section
Weight for class 4	Weight parameter in this section
Weight for class 5	Weight parameter in this section
Weight for class 6	Weight parameter in this section
Weight for class 7	Weight parameter in this section
Weight for class 8	Weight parameter in this section

Weight

(level1Weight)

The Weight parameter specifies the relative weight of class 1 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

Weight

(level2Weight)

The Weight parameter specifies the relative weight of class 2 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

Weight

(level3Weight)

The Weight parameter specifies the relative weight of class 3 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

Weight

(level4Weight)

The Weight parameter specifies the relative weight of class 4 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

Weight

(level5Weight)

The Weight parameter specifies the relative weight of class 5 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

Weight

(level6Weight)

The Weight parameter specifies the relative weight of class 6 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

Weight

(level7Weight)

The Weight parameter specifies the relative weight of class 7 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

Weight

(level8Weight)

The Weight parameter specifies the relative weight of class 8 to the other scheduling classes within the group. The parameter is configurable when the [Group](#) parameter is set to a value other than None. The range is 1 to 100. The default is 1.

57 — HSMDA WRR policy parameters

57.1 HSMDA WRR Policy parameters 57-2

57.1 HSMDA WRR Policy parameters

This chapter describes the parameters on the HSMDA WRR Policy form and child forms.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Class Aggregate Weight

(classAggWeight)

The Class Aggregate Weight parameter specifies the weight assigned to the group of queues specified by the [Include Queues](#) parameter within the HSMDA scheduler. The possible values are 1, 2, 4, or 8. The default is 1.

Include Queues

(includeQueues)

The Include Queues parameter specifies the queues that can be scheduled in the same class in a Weighted Round Robin (WRR) fashion within the HSMDA scheduler. The options are:

- 1-2 (default)
- 1-3

Packet Byte Offset (bytes)

(hsmdaEgrQosPackByteOffOvrd)

The Packet Byte Offset (bytes) parameter specifies the packet byte offset of an HSMDA egress policy. The range is -128 to +31. The value -128 means that there is no override.

Schedule Using Class

(scheduleUsingClass)

The Schedule Using Class parameter specifies which class to schedule the queues specified by the [Include Queues](#) parameter within the HSMDA scheduler. The range is 1 to 3. The default is 1.

58 — 7210 Port Scheduler parameters

58.1 7210 Port Scheduler parameters 58-2

58.1 7210 Port Scheduler parameters

This chapter describes the parameters on the 7210 Port Scheduler policy form and its child forms. The 5620 SAM menu path is Policies→QoS→SROS QoS→7210 Port Scheduler.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Mode

(mode)

The Mode parameter specifies a mode of scheduling for the policy. The options are:

- RoundRobin
- Strict (default)
- WeightedDeficitRoundRobin
- WeightedRoundRobin

Weight

(queue1Weight)

The weight parameter specifies the weight assigned to a port egress queue. You can only configure the queue weight when the port scheduling mode is set to WeightedRoundRobin or WeightedDeficitRoundRobin. The Strict checkbox associated with each queue must be disabled before you can configure the weight. The Strict checkbox is disabled by default. The range is 0 to 5. A weight of 0 means that the queue scheduling is treated as strict.

When the port scheduling mode is set to WeightedRoundRobin the queue weight corresponds to the number of packets that need to be sent out in a cycle for that specific queue.

When the port scheduling mode is set to WeightedDeficitRoundRobin the weight corresponds to the ratio of traffic that is sent out for that specific queue.

Weight

(queue2Weight)

See the [Weight](#) in this section for more information.

Weight**(queue3Weight)**

See the [Weight](#) in this section for more information.

Weight**(queue4Weight)**

See the [Weight](#) in this section for more information.

Weight**(queue5Weight)**

See the [Weight](#) in this section for more information.

Weight**(queue6Weight)**

See the [Weight](#) in this section for more information.

Weight**(queue7Weight)**

See the [Weight](#) in this section for more information.

Weight**(queue8Weight)**

See the [Weight](#) in this section for more information.

59 – Policer Control parameters

59.1 Policer Control parameters 59-2

59.1 Policer Control parameters

This chapter describes the parameters on the Policer Control Policy form and its child forms. The 5620 SAM menu path is Policies→QoS→Policer Control.

Arbiter Name

See the [Displayed Name](#) parameter in section 112.1.

Cumulative MBS Contribution

The Cumulative MBS Contribution parameter specifies the maximum amount of cumulative buffer space (in bytes) allowed for a specific priority level by a policer control policy. The range is 1 to 134217728. The default is the maximum value.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Fixed MBS contribution

The Fixed MBS Contribution parameter specifies if the cumulative buffer space is fixed for a specific priority level. When this parameter is set to True for a priority level, the system treats the defined Cumulative MBS Contribution value as an explicit MBS definition for the priority level.

Frame Based Bandwidth Rate

(maxframeBasedBW)

The Frame Based Bandwidth Rate parameter specifies the maximum bandwidth limit for an arbiter for a specific tier level.

Level

(level)

The Level parameter specifies a specific level of QoS policer control policy. The range is 1 to 8. The default is 1.

Maximum Frame Based Bandwidth

(maxframeBasedBW)

The Maximum Frame Based Bandwidth parameter specifies the total maximum bandwidth limit for a policer. This bandwidth limit is used by the root arbiter and its children.

Minimum Separation Buffer Space

(minAmntSepBufSpace)

The Minimum Separation Buffer Space parameter specifies the minimum separation between any discard thresholds when more than one child policer is associated with a parent policer priority level.

Parent Arbiter

(parentArbiter)

See the [Parent Arbiter](#) parameter in section 112.1.

Priority Level

(priorityLevel)

The Priority Level parameter specifies the priority level of a tier 1 or tier 2 child arbiter in comparison to other child arbiters with the same parent arbiter. The Priority Level parameter helps determine relative importance when child arbiters are contending for bandwidth. The range is 1 to 8. The default is 1. The higher the number, the higher the priority level of the child arbiter bandwidth request.

Child arbiters with the Priority Level parameter set lower than other child arbiters do not receive bandwidth until all child arbiters with a higher priority level have reached their maximum bandwidth allocation, or have no packets to pass.

When two child arbiters have the same Level parameter value, the Weight parameter determines which arbiter first receives bandwidth.

Tier

(tier)

The Tier parameter specifies the hierarchical level with which a group of arbiters are associated. The value can be 1 or 2. The default is 1.

The parameter defines the arbiter hierarchy within a policer control policy. A tier 2 arbiter can be the child of a tier 1 parent. In this case, the child tier 2 arbiter inherits bandwidth from the parent tier 1 arbiter. The root arbiter of the policer control policy acts as parent to all tier 1 and tier 2 arbiters, and inherits its bandwidth from the policy's maximum bandwidth rate. You can create a tier 2 arbiter without creating a parent tier 1 arbiter.

When multiple arbiters share child status under the same parent arbiter, the Weight and Level parameters are used to define how child arbiters contend for the parent arbiter's bandwidth.

Weight

(weight)

The Weight parameter specifies the relative importance of a child arbiter in comparison to other child arbiters that have identical Level parameter settings. The parameter is configurable when the Tier parameter is set to the 1 or 2 option. The range is 000 to 100. The default is 001.

A setting of 000 specifies that the child arbiter receives bandwidth from the parent only after all non-000 weighted child arbiters have received bandwidth.

60 — HSMDA Pool parameters

60.1 HSMDA pool parameters 60-2

60.1 HSMDA pool parameters

This chapter describes the parameters on the HSMDA Pool Policy form and child forms.

Allocation Percent

Table 60-1 lists where to find information about the Allocation Percent parameter.

Table 60-1 Allocation Percent parameter

Parameter	See
Allocation Percent for class 1	Allocation Percent in this section
Allocation Percent for class 2	Allocation Percent parameter in this section
Allocation Percent for class 3	Allocation Percent parameter in this section
Allocation Percent for class 4	Allocation Percent parameter in this section
Allocation Percent for class 5	Allocation Percent parameter in this section
Allocation Percent for class 6	Allocation Percent parameter in this section
Allocation Percent for class 7	Allocation Percent parameter in this section
Allocation Percent for class 8	Allocation Percent parameter in this section

Allocation Percent

(poolClass1AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by the [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 40.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Percent

(poolClass2AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 35.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Percent

(poolClass3AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by the [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 30.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Percent

(poolClass4AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by the [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 25.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Percent

(poolClass5AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by the [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 20.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Percent

(poolClass6AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by the [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 50.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Percent

(poolClass7AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by the [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 40.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Percent

(poolClass8AllocPercent)

The Allocation Percent parameter specifies, indirectly, the size of the first class pool. The value (in one hundredths of a percentage point) determines the percentage of the root pool with which the first class pool is associated, as specified by the [Root Parent](#) parameter, is available for this class. The range is 0.01 to 100. The default is 30.

When the Default check box is enabled you cannot configure the Allocation Percent parameter.

Allocation Weight

Table [60-2](#) lists where to find information about the Allocation Weight parameter.

Table 60-2 Allocation Weight parameter

Parameter	See
Allocation Weight for class 1	Allocation Weight parameter in this section
Allocation Weight for class 2	Allocation Weight parameter in this section
Allocation Weight for class 3	Allocation Weight parameter in this section
Allocation Weight for class 4	Allocation Weight parameter in this section
Allocation Weight for class 5	Allocation Weight parameter in this section
Allocation Weight for class 6	Allocation Weight parameter in this section
Allocation Weight for class 7	Allocation Weight parameter in this section
Allocation Weight for class 8	Allocation Weight parameter in this section

Allocation Weight

(poolRoot1AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the first root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 75.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Allocation Weight

(poolRoot2AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the second root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 25.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Allocation Weight

(poolRoot3AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the third root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 0.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Allocation Weight

(poolRoot4AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the fourth root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 0.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Allocation Weight

(poolRoot5AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the fifth root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 0.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Allocation Weight

(poolRoot6AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the sixth root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 0.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Allocation Weight

(poolRoot7AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the seventh root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 0.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Allocation Weight

(poolRoot8AllocWeight)

The Allocation Weight parameter specifies the weight that is applied to the eighth root pool. The weight is divided by the sum of all root pool weights to derive the buffer allocation factor of the pool. The range is 1 to 100. The default is 0.

When the Default check box is enabled you cannot configure the Allocation Weight parameter.

Default

See the [Default](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Root Parent

Table 60-3 lists where to find information about the Root Parent parameter.

Table 60-3 Root Parent parameter

Parameter	See
Root Parent for class 1	Root Parent parameter in this section
Root Parent for class 2	Root Parent parameter in this section
Root Parent for class 3	Root Parent parameter in this section
Root Parent for class 4	Root Parent parameter in this section
Root Parent for class 5	Root Parent parameter in this section
Root Parent for class 6	Root Parent parameter in this section
Root Parent for class 7	Root Parent parameter in this section

(1 of 2)

Parameter	See
Root Parent for class 8	Root Parent parameter in this section

(2 of 2)

Root Parent

(poolClass1Parent)

The Root Parent parameter specifies the root pool to which the first class pool is associated. The range is 1 to 8. The default is 1.

Root Parent

(poolClass2Parent)

The Root Parent parameter specifies the root pool to which the second class pool is associated. The range is 1 to 8. The default is 1.

Root Parent

(poolClass3Parent)

The Root Parent parameter specifies the root pool to which the third class pool is associated. The range is 1 to 8. The default is 1.

Root Parent

(poolClass4Parent)

The Root Parent parameter specifies the root pool to which the fourth class pool is associated. The range is 1 to 8. The default is 1.

Root Parent

(poolClass5Parent)

The Root Parent parameter specifies the root pool to which the fifth class pool is associated. The range is 1 to 8. The default is 1.

Root Parent

(poolClass6Parent)

The Root Parent parameter specifies the root pool to which the sixth class pool is associated. The range is 1 to 8. The default is 2.

Root Parent

(poolClass7Parent)

The Root Parent parameter specifies the root pool to which the seventh class pool is associated. The range is 1 to 8. The default is 2.

Root Parent

(poolClass8Parent)

The Root Parent parameter specifies the root pool to which the eighth class pool is associated. The range is 1 to 8. The default is 2.

System Reserve (%)

(poolSystemReserve)

The System Reserve (%) parameter specifies the percentage of HSMDA buffers that are reserved for the system root pools. The rest of the buffers are available to the provisioned root pools. The range is 1 to 30. The default is 10.

61 — Named Buffer Pool parameters

61.1 Named buffer pool parameters 61-2

61.1 Named buffer pool parameters

This chapter describes the parameters on the Named Buffer Pool Policy form and its child forms. The 5620 SAM menu path is Policies→QoS→Named Buffer Pool.

Access Weight

(accessAllocationWeight)

The Access Weight parameter is used to divide the access buffer space available to the pools between each named pool. The range is 0 to 100. The default is 50.

Default Reserved CBS

The Default Reserved CBS parameter specifies whether the default percent for reserved CBS is used. The options are:

- Enabled
- Disabled

Default Weight

(defaultWeight)

The Default Weight parameter specifies the weights used to divide the buffers managed by a port into three categories; default, MDA and port. The default category is assigned to the default named pools. The range is 0 to 100. The default is 50.

MDA Weight

(mdaWeight)

The MDA Weight parameter specifies the weights used to divide the buffers managed by a port into three categories; default, MDA and port. The MDA category is assigned to the MDA named pools. The range is 0 to 100. The default is 50.

Network Weight

(networkAllocationWeight)

The Network Weight parameter specifies how the network buffer space available to the pools is divided between each named pool. The range is 0 to 100. The default is 50.

Pool Name

(poolName)

The Pool Name parameter specifies the name of a named buffer pool. You can manually enter a name, or use the Select button to choose a pool from a list.

Port Weight

(portWeight)

The Port Weight parameter specifies the weights used to divide the buffers managed by a port into three categories; default, MDA and port. The port category is assigned to the local port named pools. The range is 0 to 100. The default is 50.

Reserved CBS (%)

(reservedCBS)

The Reserved CBS (%) parameter specifies the percent of buffer space within the pool that is not considered shared. The range is 0 to 100 percent. The default is 30 percent.

62 – Ingress Queue Group Template parameters

62.1 Ingress Queue Group Template parameters 62-2

62.1 Ingress Queue Group Template parameters

This chapter describes the parameters on the Ingress Queue Group Template Policy form and its child forms.

Cir (kbps)

See the [CIR \(kbps\)](#) parameter in section 112.1.

Cir Adaptation

See the [CIR Adaptation](#) parameter in section 112.1.

CIR Level

See the [CIR Level](#) parameter in section 112.1.

CIR Weight

See the [CIR Weight](#) parameter in section 112.1.

Committed Burst Size (kb)

See the [Committed Burst Size \(kb\)](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Expedite

See the [Expedite](#) parameter in section 112.1.

High Priority Reserved

See the [High Priority Reserved](#) parameter in section 112.1.

ID

(id)

The ID parameter specifies a unique ID for the queue. The range is 1 to 32. The default is 0.

Level

See the [Level](#) parameter in section 112.1.

Maximum Burst Size (bytes)

See the [Maximum Burst Size \(bytes\)](#) parameter in section 112.1.

Mode

See the [Mode](#) parameter in section 112.1.

Multicast

(multicast)

See the [Multipoint](#) parameter in section 112.1.

Named Buffer Pool

See the [Named Buffer Pool](#) parameter in section 112.1.

Pir (kbps)

See the [PIR \(kbps\)](#) parameter in section 112.1.

Pir Adaptation

See the [PIR Adaptation](#) parameter in section 112.1.

Policed

(policed)

See the [Policed](#) parameter in section 112.1.

Scheduler

See the [Scheduler button](#) parameter in section 112.1.

Weight

See the [Weight](#) parameter in section 112.1.

63 — Egress Queue Group Template parameters

63.1 Egress Queue Group Template parameters 63-2

63.1 Egress Queue Group Template parameters

This chapter describes the parameters on the Egress Queue Group Template Policy form and its child forms.

CIR

(kb/s)

See the [CIR \(kbps\)](#) parameter in section 112.1.

CIR (Percentage)

(cirPercent)

The CIR (cirPercent) parameter specifies the administrative committed information rate for a queue, in terms of a percentage of the port maximum rate. The parameter specifies the rate at which the system prioritizes the queue over other queues that are competing for the same bandwidth.

The range is 0 to 100 percent, dependant on the line rate of the object to which the policy is applied. The default is 0 percent.

CIR Level

See the [CIR Level](#) parameter in section 112.1.

CIR Weight

See the [CIR Weight](#) parameter in section 112.1.

CIR Adaptation

See the [CIR Adaptation](#) parameter in section 112.1.

Committed Burst Size

(kb)

See the [Committed Burst Size \(kb\)](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Expedite

See the [Expedite](#) parameter in section 112.1.

Forwarding Class

See the [Forwarding Class](#) parameter in section 112.1.

High Priority Reserved

See the [High Priority Reserved](#) parameter in section 112.1.

ID

(queueId)

The ID parameter specifies a unique identifier for the queue. The range is 1 to 8. The default is 0.

Level

See the [Level](#) parameter in section 112.1.

Maximum Burst Size

(bytes)

See the [Maximum Burst Size \(bytes\)](#) parameter in section 112.1.

Named Buffer Pool

See the [Named Buffer Pool](#) parameter in section 112.1.

PIR

(kb/s)

See the [PIR \(kbps\)](#) parameter in section 112.1.

PIR (Percentage)

(pirPercent)

The PIR (pirPercent) parameter specifies the administrative peak information rate for a queue, in terms of a percentage of the port maximum line rate. The parameter specifies the maximum rate that the queue can transmit packets through the switch fabric for access ingress, or out an egress interface for access egress queues. Specifying a value for the PIR parameter does not guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The range is 0 to 100 percent, dependant on the line rate of the object to which the policy is applied. The default is 100 percent.

PIR Adaptation

See the [PIR Adaptation](#) parameter in section 112.1.

Port Parent

See the [Port Parent](#) parameter in section 112.1.

Queue ID

See the [Queue ID](#) parameter in section 112.1.

Rate Type

(rateType)

The Rate Type parameter specifies the manner in which the CIR and PIR parameters are configured for the egress queue:

- When set to Percentage, the rate is specified in terms of a percentage of the maximum port rate).
- When set to Specific, the rate is specified in kb/s.

The default is Specific.

Scheduler

See the [Scheduler button](#) parameter in section 112.1.

Use WRED Queue

See the [Use WRED Queue](#) parameter in section 112.1.

Weight

See the [Weight](#) parameter in section 112.1.

64 – 7705 SAR Fabric parameters

64.1 7705 SAR Fabric parameters 64-2

64.1 7705 SAR Fabric parameters

This chapter describes the parameters on the 7705 SAR Fabric creation form and child forms.

Aggregate Rate

(aggregateRate)

The Aggregate Rate parameter specifies the maximum rate that is distributed to all the daughter card slots. That is, there is one rate that is applied to all the daughter card slots in the 7705 SAR. You can configure the rate in the range 1 to 1 000 000 kb/s and 200 000 kb/s is the default value.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

ID

See the [ID](#) parameter in section 112.1.

Mode

(mode)

The Mode parameter specifies how the rates are applied to the daughter card slots. There are two options, Aggregate and Destination.

In Aggregate mode, there is one rate that is applied evenly to all the daughter card slots in the 7705 SAR. You can configure the rate in the range 1 to 1 000 000 kb/s and 200 000 kb/s is the default value.

In Destination mode, you can configure the rates individually for each daughter card slot on the 7705 SAR. There is a rate for each slot identified by IOMslot/daughter card slot; for example, Rate to MDA 1/1, Rate to MDA 1/2, and so on. You can configure each of the rates in the range 1 to 1 000 000 kb/s and 200 000 kb/s is the default value.

MultiPoint Rate

(multipointRate)

The MultiPoint Rate parameter specifies the maximum rate, in kb/s, to all daughter card slots. That is, there is one rate that is applied evenly to all daughter card slots in the 7705 SAR. The range is 1 to 1 000 000 kb/s. The default is 200 000 kb/s.

Rate To MDA (destRateTo1<card#>

The Rate To MDA parameter specifies the rate, in kb/s, to each daughter card slot. You can configure the rates individually for each daughter card slot on the 7705 SAR. There is a rate for each slot identified by IOMslot/daughter card slot; for example, Rate to MDA 1/1, Rate to MDA 1/2, and so on. You can configure each of the rates in the range 1 to 1 000 000 kb/s and 200 000 kb/s is the default value.

65 – 7250 SAS and Telco QoS parameters

65.1 7250 SAS and Telco QoS parameters 65-2

65.1 7250 SAS and Telco QoS parameters

This chapter describes the parameters on the 7250 SAS and Telco QoS Node Level Policy form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Color

(conformanceLevelType)

The Color parameter specifies the type of color mark that is applied to packets in the traffic class specified by the Traffic Class parameter. The color mark indicates the packet discard priority in congestion conditions within queues. The options are:

- Conforming (green) (default)
- Non-Conforming (red)
- Partially Conforming (yellow)

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Drop Algorithm

(transmitXType)

The Drop Algorithm parameter specifies the type of congestion-avoidance mechanism that is used. Table 65-1 lists the parameter options.

Table 65-1 Drop Algorithm parameter

Option	Option Description
None (default)	Specifies that no congestion-avoidance mechanism is put into effect
Random Detect	Specifies that the WRED congestion-avoidance mechanism is used for the configured interface
Tail Drop	Specifies that the tail-drop congestion-avoidance mechanism is used for the configured interface

DSCP

(dscp)

The DSCP parameter specifies whether DSCP remarking is applied to packets in the traffic class specified by the Traffic Class parameter using the DSCP Value parameter. The options are:

- Enabled
- Disabled (default)

DSCP Value

(dscpValue)

The DSCP Value parameter specifies the DSCP value that is applied to packets in the traffic class specified by the Traffic Class parameter. The range is 0 to 63. The default is 0.

Filter ID

(id)

The Filter ID parameter specifies a unique identifier for the filter. The range is 1 to 1 000 000. The default is 0.

Priority

(priority)

The Priority parameter specifies the dot1p value applied to packets in the traffic class that is specified by the Traffic Class parameter. The range is and 0 to 7. The default is 0.

Queue Algorithm

(queueAlgorithmType)

The Queue Algorithm parameter specifies how queues are serviced. Table 65-2 describes the parameter options.

Table 65-2 Queue Algorithm parameter

Option	Option Description
Strict Priority (default)	Queues are serviced based on the traffic class only.
Hybrid 1	Queue 7 is serviced first, then the remaining queues are serviced according to the weight values specified by the Txq 0 through Txq 6 parameter values in the Hybrid 1 panel of the Scheduling Tx Queue tab.
Hybrid 2	Queues 7 and 6 are serviced in descending numerical order, then the remaining queues are serviced according to the weight values specified by the Txq 0 through Txq 5 parameter values in the Hybrid 2 panel of the Scheduling Tx Queue tab.

(1 of 2)

Option	Option Description
Hybrid 3	Queues 7, 6, and 5 are serviced in descending numerical order, then the remaining queues are serviced according to the weight values specified by the Txq 0 through Txq 4 parameter values in the Hybrid 3 panel of the Scheduling Tx Queue tab.
Hybrid 4	Queues 7, 6, 5, and 4 are serviced in descending numerical order, then the remaining queues are serviced according to the weight values specified by the Txq 0 through Txq 3 parameter values in the Hybrid 4 panel of the Scheduling Tx Queue tab.
Hybrid 5	Queues 7, 6, 5, 4, and 3 are serviced in descending numerical order, then the remaining queues are serviced according to the weight values specified by the Txq 0, Txq 1, and Txq 2 parameter values in the Hybrid 5 panel of the Scheduling Tx Queue tab.
Hybrid 6	Queues 7, 6, 5, 4, 3, and 2 are serviced in descending numerical order, then queues 1 and 0 are serviced according to the weight values specified by the Txq 0 and Txq 1 parameter values in the Hybrid 6 panel of the Scheduling Tx Queue tab.
Weighted Round-Robin	Queues are serviced based on the weight values assigned to them by the Txq 0 through Txq 7 parameter values in the Weighted Round-Rob panel of the Scheduling Tx Queue tab.

(2 of 2)

Shaper Rate

(shaperRate)

The Shaper Rate parameter specifies the rate for the transmit port or transmit port and queue. Traffic shaping is used to control the rate of outgoing traffic to ensure that the traffic conforms to the maximum rate of transmission available for it. Traffic that exceeds the shaping rate is queued and transmitted at the configured rate. If the burst of traffic exceeds the queue size, packets are dropped to maintain transmission at the configured shaping rate. The options are:

- None (default)
- Rate

Traffic Class

(trafficClass)

The Traffic Class parameter specifies the traffic class to which the DSCP, DSCP Value, Color, and Priority parameter entries apply. The range is 0 to 63. The default is 0.

Txq 0

(txq0)

The Txq 0 parameter specifies a weight value to be assigned to queue 0 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 0 parameter is configurable when the Queue Algorithm parameter value is not Strict Priority. The default is 0.

Txq 1

(txq1)

The Txq 1 parameter specifies a weight value to be assigned to queue 1 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 1 parameter is configurable when the Queue Algorithm parameter value is Hybrid 1, Hybrid 2, Hybrid 3, Hybrid 4, Hybrid 5, Hybrid 6, or Weighted Round-Robin. The default is 0.

Txq 2

(txq2)

The Txq 2 parameter specifies a weight value to be assigned to queue 2 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 2 parameter is configurable when the Queue Algorithm parameter value is Hybrid 1, Hybrid 2, Hybrid 3, Hybrid 4, Hybrid 5, or Weighted Round-Robin. The default is 0.

Txq 3

(txq3)

The Txq 3 parameter specifies a weight value to be assigned to queue 3 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 3 parameter is configurable when the Queue Algorithm parameter value is Hybrid 1, Hybrid 2, Hybrid 3, Hybrid 4, or Weighted Round-Robin. The default is 0.

Txq 4

(txq4)

The Txq 4 parameter specifies a weight value to be assigned to queue 4 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 4 parameter is configurable when the Queue Algorithm parameter value is Hybrid 1, Hybrid 2, Hybrid 3, or Weighted Round-Robin. The default is 0.

Txq 5

(txq5)

The Txq 5 parameter specifies a weight value to be assigned to queue 5 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 5 parameter is configurable when the Queue Algorithm parameter value is Hybrid 1, Hybrid 2, or Weighted Round-Robin. The default is 0.

Txq 6

(txq6)

The Txq 6 parameter specifies a weight value to be assigned to queue 6 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 6 parameter is configurable when the Queue Algorithm parameter value is Hybrid 1 or Weighted Round-Robin. The default is 0.

Txq 7

(txq7)

The Txq 7 parameter specifies a weight value to be assigned to queue 7 for servicing priority. The range is 0 to 100. The weight values assigned to this queue and the other queues must total 10 or 100. The Txq 6 parameter is configurable when the Queue Algorithm parameter value is Weighted Round-Robin. The default is 0.

66 – AOS QoS Policies parameters

66.1 AOS QoS Policies parameters 66-2

66.1 AOS QoS Policies parameters

This chapter describes the OmniSwitch QoS policies parameters on the Manage AOS QoS Policies form and its child forms. The 5620 SAM menu path is Policies→Qos→AOS QoS Policies.

Action

(actionDisposition)

The Action parameter specifies the action to be performed when traffic matches a condition that is defined in a QoS policy. Table 66-1 describes the parameter options.

Table 66-1 Action parameter

Option	Option description
Accept (default)	Specifies that the switch should accept the flow
Drop	Specifies that the switch should silently drop the flow
Deny	Specifies that the switch should drop the flow and issue an ICMP message that indicates the flow was dropped for administrative reasons. Currently provides the same result as the drop option.

Destination IP

(destinationIpAddress)

The Destination IP parameter specifies a destination IP address for a policy condition. You must select the check box beside the parameter before you can configure the parameter. The default is 0.0.0.0.

Destination IP Port (End)

(destinationIpPortEnd)

The Destination IP Port (End) parameter specifies the destination IP port range end value, which is used for traffic classification. You must select the check box beside the [Match Destination IP Port Range](#) parameter before you can configure the Destination IP Port (End) parameter. The range is 0 to 65 535. The default is 0.

Destination IP Port (Start)

(destinationIpPortStart)

The Destination IP Port (Start) parameter specifies the destination IP port range start value, which is used for traffic classification. You must select the check box beside the [Match Destination IP Port Range](#) parameter before you can configure the Destination IP Port (Start) parameter. The range is 0 to 65 535. The default is 0.

Destination LAG

(redirectAggStatus)

The Destination LAG parameter specifies whether redirection is enabled on the aggregate. You must select the check box to enable.

Destination MAC

(destinationMacAddress)

The Destination MAC parameter specifies a destination MAC address for a policy condition. You must select the check box beside the parameter before you can configure the parameter. The default is 00-00-00-00-00-00.

Destination Mask

(destinationIpAddressMask)

The Destination Mask parameter specifies a destination IP address mask for a policy condition. You must select the check box beside the [Destination IP](#) parameter before you can configure the Destination Mask parameter. The range is 0 to 32. The default is 32.

Destination Mask

(destinationMacAddressMask)

The Destination Mask parameter specifies a destination MAC address mask for a policy condition. You must select the check box beside the [Destination MAC](#) parameter before you can configure the Destination Mask parameter. The default is FF-FF-FF-FF-FF-FF.

Destination Net Mask

(destinationIpAddressFullMask)

The Destination Net Mask parameter specifies a destination full IP address mask for a policy condition. You must select the check box beside the [Destination IP](#) parameter before you can configure the Destination Net Mask parameter. The default is 255.255.255.255.

Destination Port

(destinationPort)

The Destination Port parameter specifies a destination port number for a policy condition. The destination port and slot conditions are only applied to bridged, not routed traffic. The parameter is configurable when the [Match Destination Port](#) parameter is selected. The range is 1 to 52. The default is 1.

Destination Port

(redirectSlotStatus)

The Destination Port parameter specifies whether redirection is enabled on the slot or port. You must select the check box to enable.

Destination Slot

(destinationSlot)

The Destination Slot parameter specifies a destination slot number for a policy condition. The destination port and slot conditions are only applied to bridged, not routed traffic. The parameter is configurable when the [Match Destination Port](#) parameter is selected. The range is 0 to 8. The default is 1.

Differentiated Services Code Point

(dscp)

The Differentiated Services Code Point parameter specifies the DSCP that a QoS policy condition uses to filter incoming traffic, or that a QoS policy action assigns to outgoing traffic that matches a QoS policy condition. You must select the check box beside the parameter before you can configure the parameter. The default is be. Table [66-2](#) lists the parameter options.

Table 66-2 Differentiated Services Code Point parameter

Options			
be	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43

Displayed Name

(**displayedName**)

See the [Displayed Name](#) parameter in section 112.1.

ICMP Code

(**icmpCode**)

The ICMP Code parameter specifies an ICMP code to classify traffic in a QoS policy condition. You must select the check box beside the parameter before you can configure the parameter. The range is 0 to 255. The default is 0.

ICMP Type

(**icmpType**)

The ICMP Type parameter specifies an ICMP type to classify traffic in a QoS policy condition. You must select the check box beside the [ICMP Code](#) parameter before you can configure the ICMP Type parameter. The range is 0 to 255. The default is 0.

IP Protocol

(**protocol**)

The IP Protocol parameter specifies an IP protocol for a policy condition. Table 66-3 lists the parameter options.

Table 66-3 IP Protocol parameter

Options			
HOPOPT	SEP	CPNX	SCPS
ICMP	3PC	CPHB	QNX
IGMP	IDPR	WSN	A/N Active Networks (107)
GGP	XTP	PVP	IPComp
IP	DDP	BR_SAT_MON	SNP
ST	IDPR_CMT	SUN_ND	Compaq_Peer
TCP	TP++	WB_MON	IPX_in_IP
CBT	IL	WB_EXPAK	VRRP
EGP	IPv6	ISO_IP	PGM
IGP	SDRP	VMTP	any 0-hop protocol (114)
BBN_RCC_MON	IDRP	SECURE_VMTP	L2TP
NVP_II	RSVP	VINES	DDX
PUP	GRE	TTP	IATP
ARGUS	MHRP	NSFNET_IGP	STP

(1 of 2)

Options			
EMCON	BNA	DGP	SRP
XNET	I_NLSP	TCF	UTI
CHAOS	SWIPE	EIGRP	SMP
UDP	NARP	OSPFIGP	SM
MUX	MOBILE	Sprite_RPC	PTP
DCN_MEAS	TLSP	LARP	ISIS
HMP	SKIP	MTP	FIRE
PRM	IPv6_ICMP	AX.25	CRTP
XNS_IDP	IPv6_No Nxt	IPIP	CRUDP
TRUNK_1	any host internal protocol (61)	MICP	SSCOMPCE
TRUNK_2	CFTP	SCC_SP	IPLT
LEAF_1	any local network (63)	ETHERIP	SPS
LEAF_2	SAT_EXPAK	ENCAP	PIPE
RDP	KRYPTOLAN	any private encryption scheme (99)	SCTP
IRTP	RVD	GMTP	FC
ISO_TP4	any distributed file system (68)	IFMP	RSVP_E2E_IGNORE
NETBLT	SAT_MON	PNNI	—
MFE_NSP	VISA	PIM	—
MERIT_INP	IPCV	ARIS	—

(2 of 2)

LAG Number

(redirectAgg)

The LAG Number parameter specifies the LAG to which all traffic (flooded, bridged, routed, and multicast) that matches a redirect policy is directed. You must enable the check box beside the parameter before you can configure the parameter. The range is 0 to 31. The default is 1.

List Type

(listType)

The List Type parameter is used to specify the type of AOS QoS list being configured. The options are:

- UNP
- VRF
- Ingress (default)

- Egress
- SLB

Mask

Table 66-4 lists where to find information about the Mask parameter.

Table 66-4 Mask parameter

Parameter	See
Mask for a DSCP in a policy condition	Mask parameter in this section
Mask for the ToS precedence bits in a policy condition	Mask parameter in this section

Mask

(dscpMask)

The Mask parameter specifies the mask for the DSCP in a policy condition. Table 66-2 describes the parameter options. You must select the check box beside the [Differentiated Services Code Point](#) parameter before you can configure the Mask parameter. The default is cp63.

Mask

(tosValueMask)

The Mask parameter specifies the mask for the ToS precedence bits in a policy condition. You must select the check box beside the [ToS Precedence](#) parameter before you can configure the Mask parameter. The range is 0 to 7. The default is 7.

Match Destination IP Port Range

(matchDestinationIpPort)

The Match Destination IP Port Range parameter specifies whether the destination IP port range must match. You must select the check box beside the parameter before you can configure the [Destination IP Port \(Start\)](#) and [Destination IP Port \(End\)](#) parameters.

Match Destination Port

(matchDestinationPort)

The Match Destination Port parameter specifies whether the destination physical slot and port must match. You must select the check box beside the parameter before you can configure the [Destination Slot](#) and [Destination Port](#) parameters.

Match Source IP Port Range

(matchSourceIpPort)

The Match Source IP Port Range parameter specifies whether the source IP port range must match. You must select the check box beside the parameter before you can configure the [Source IP Port \(Start\)](#) and [Source IP Port \(End\)](#) parameters.

Match Source Port

(matchSourcePort)

The Match Source Port parameter specifies whether the source physical slot and port must match. You must select the check box beside the parameter before you can configure the [Source Slot](#) and [Source Port](#) parameters.

Maximum Bandwidth (Kbps)

(maxBandwidth)

The Maximum Bandwidth parameter specifies the maximum bandwidth for a policy action. You must select the check box beside the parameter before you can configure the parameter. The range is 0 to 4 294 967 296. The default is 0.

Policy Status

(enabled)

The Policy Status parameter specifies whether a QoS policy is enabled. The options are:

- Enabled (default)
- Disabled

Port

(redirectPort)

The Port parameter specifies the port to which all traffic (flooded, bridged, routed, and multicast) that matches a redirect policy is directed. You must enable the check box beside the parameter before you can configure the parameter. The check box enables or disables the configuration of this parameter and the [Slot](#) parameter. The range is 1 to 52. The default is 1.

Precedence

(precedence)

The Precedence parameter specifies the precedence for a QoS policy. The OmniSwitch attempts to classify traffic according to policy precedence. The rule with the highest precedence is applied to the traffic. The range is 0 to 65 535. The default is 0.

Priority

(actionPriority)

The Priority parameter specifies the priority for queuing a flow to which the QoS action applies. This priority value is independent of 802.1Q, ToS, or DSCP values. You must select the check box beside the parameter before you can configure the parameter. The range is 0 to 7. The default is 0.

Priority

(dot1pValue)

The Priority parameter specifies the 802.1p that a QoS policy condition uses to filter incoming traffic, or that a QoS policy action assigns to outgoing traffic that matches a QoS policy condition. You must select the check box beside the parameter before you can configure the parameter. The range is 0 to 7. The default is 0.

Share Resources

(shared)

The Share Resources parameter specifies whether queues that are created by a specific action can be shared. If multiple rules have the same action, more than one traffic flow may be scheduled on the same queue when the queue is defined as shared; otherwise, a separate queue is created for each flow.

Each traffic flow must be sent over the same virtual port for the traffic flows to share a queue. For example, flows with the same 802.1q tag may share the same queue. You must select the check box beside the parameter before you can configure the parameter. The options are:

- No (default)
- Yes

Slot

(redirectSlot)

The Slot parameter specifies the slot of the port to which all traffic (flooded, bridged, routed, and multicast) that matches a redirect policy is directed. You must enable the check box beside the parameter before you can configure the parameter. The check box enables or disables the configuration of this parameter and the [Port](#) parameter. The range is 1 to 16. The default is 1.

Source IP

(sourceIpAddress)

The Source IP parameter specifies a source IP address for a policy condition. You must select the check box beside the parameter before you can configure the parameter. The default is 0.0.0.0.

Source IP Port (End)

(sourceIpPortEnd)

The Source IP Port (End) parameter specifies the source IP port range end value, which is used for traffic classification. You must select the check box beside the [Match Source IP Port Range](#) parameter before you can configure the Source IP Port (End) parameter. The range is 0 to 65 535. The default is 0.

Source IP Port (Start)

(sourceIpPortStart)

The Source IP Port (Start) parameter specifies the source IP port range start value, which is used for traffic classification. You must select the check box beside the [Match Source IP Port Range](#) parameter before you can configure the Source IP Port (Start) parameter. The range is 0 to 65 535. The default is 0.

Source MAC

(sourceMacAddress)

The Source MAC parameter specifies a source MAC address for a policy condition. You must select the check box beside the parameter before you can configure the parameter. The default is 00-00-00-00-00-00.

Source Mask

(sourceIpAddressMask)

The Source Mask parameter specifies a source IP address mask for a policy condition. You must select the check box beside the [Source IP](#) parameter before you can configure the Source Mask parameter. The range is 0 to 32. The default is 32.

Source Mask

(sourceMacAddressMask)

The Source Mask parameter specifies the mask for the source MAC address. You must select the check box beside the [Source MAC](#) parameter before you can configure the Source Mask parameter. The default is FF-FF-FF-FF-FF-FF.

Source Net Mask

(sourceIpAddressFullMask)

The Source Net Mask parameter specifies a source full IP address mask for a policy condition. You must select the check box beside the [Source IP](#) parameter before you can configure the Source Net Mask parameter. The default is 255.255.255.255.

Source Port

(sourcePort)

The Source Port parameter specifies a source port number for a policy condition. You must select the check box beside the [Match Source Port](#) parameter before you can configure the Source Port parameter. The range is 1 to 52. The default is 1.

Source Slot

(sourceSlot)

The Source Slot parameter specifies a source slot number for a policy condition. You must select the check box beside the [Match Source Port](#) parameter before you can configure the Source Slot parameter. The range is 0 to 8. The default is 1.

Source VLAN

(sourceVlan)

The Source VLAN parameter specifies a source VLAN for a policy condition. You must select the check box beside the parameter before you can configure the parameter. The range is 0 to 4095. The default is 0.

ToS Precedence

(tosValue)

The ToS Precedence parameter specifies a ToS value for a policy condition. You must select the check box beside the parameter before you can configure the parameter. The range is 0 to 7. The default is 0.

Type of Service

(tosValue)

The Type of Service parameter specifies the value of the ToS bits to be applied to packets in outgoing traffic flows to which the specified policy applies. You must select the check box beside the parameter before you can configure the parameter. The range is 0 to 7. The default is 0.

VRF Status

(vRfNameStatus)

The VRF Status parameter indicates the VRF instance status and is applicable to the OS 9700E and OS 9800E. The options are:

- Disabled (default)
- Enabled

VRF Name

(vRFName)

The VRF name parameter allows the user to describe the VRF instance on an OS 9700E or OS 9800E. The range is 0 to 31 characters. The “VRF Status” parameter must be enabled to display this parameter on the AOS QoS Condition, Global Policy (Create) form.

67 – 9500 ATM QoS parameters

67.1 ATM QoS parameters 67-2

67.1 ATM QoS parameters

This chapter describes the parameters on the Manage 9500 ATM QoS Policies form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

CDVT (microseconds)

(cdvt)

The CDVT parameter specifies the cell delay variation tolerance. The parameter appears when the Service Category parameter is set to CBR, rt-VBR or nrt-VBR. The range is 0 to 4 294 967 295 ms. The default is 250 ms. For 9500 MPR, the default is 1000 ms, and the range is 0 to 40 000 ms.

Displayed Name(displayedName)

See the [Displayed Name](#) parameter in section 112.1.

Domain Name

(domainName)

The Domain Name parameter allows the user to select between ATM and PWE3 for 9500 MPR QoS Policy creation. The default is ATM.

MDCR

(mdcr)

The MDCR parameter specifies the minimum desired cell rate in cells per second. For the 9500 MPR, the range is 0 to 1. The default is 0.

PCR (cells/second)

(pcr)

The PCR parameter specifies the peak cell rate, in cells per second, which the endpoint may never exceed. For the 9500 MPR, the range is 1 to 71 480. The default is 1.

68 – ACL MAC Filter parameters

68.1 ACL MAC Filter parameters 68-2

68.1 ACL MAC Filter parameters

This chapter describes the parameters on the ACL MAC Filter form and child forms.

Action

See the [Action](#) parameter in section 112.1.

Administrative State

See the [Administrative State](#) parameter in section 112.1.

ATM VCI

(atmvci)

The ATM VCI parameter specifies a VCI-based filter entry in a SAP access ingress QoS policy. The parameter is configurable as a Mac Match criterion for a VPI SAP of an atm-vpc Apipe service on a 7450 ESS, 7710 SR, or 7750 SR. The range is 1, 2, or 5 to 65 535. The default is 0.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Default Action

(action)

The Default Action parameter specifies the action that should be performed with the packet when no action is specified in the IP filter entries or when the packets do not match the specified criteria. The options are:

- drop (default)
- forward

Description

See the [Description](#) parameter in section 112.1.

Destination MAC

(destinationMacAddress)

The Destination MAC parameter specifies a unicast MAC address as a match criterion. When enabled, specify a MAC address. The default is 00-00-00-00-00-00.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Dot1p

(dot1pValue)

The Dot1p parameter specifies the IEEE 802.1p value to be used as the match criterion. The range is 0 to 7, or Not Set (-1). The default is Not Set (-1), indicating that filtering for this parameter is disabled.

Dot1p Mask

(dot1pMask)

The Dot1p Mask parameter specifies a mask value as match criterion when you filter on a dot1p value. The parameter is configurable when the Dot1p parameter is enabled. The range is 0 to 7, or Not Set (-1), indicating that filtering for this parameter is disabled. The default is 7.

Dst Mask

(destinationMacAddressMask)

The Dst Mask parameter specifies a mask value to the match criterion when you filter on a destination MAC address. The parameter is configurable when the Destination MAC parameter is enabled. The default is 00-00-00-00-00-00.

Entry ID

See the [Entry ID](#) parameter in section [112.1](#).

Ether Type

(ethernetType)

The Ether Type parameter specifies an Ethernet type II value as the match criterion. The range is 1536 to 65 535, or -1. The default is -1, indicating that filtering for this parameter is disabled. This parameter is configurable only when the Frame Type parameter is set to Ethernet II.

Filter ID

(id)

The Filter ID parameter specifies a unique identifier for the filter. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 65 535. The default is 0.

Frame Type

(frameType)

The Frame Type parameter specifies an Ethernet frame type used as match criterion. Table [68-1](#) describes the parameter options.

Table 68-1 Frame Type parameter

Option	Option description	Dependencies
e802dot3 (default)	The frame type is Ethernet IEEE 802.3.	—
e802dot2LLC	The frame type is Ethernet IEEE 802.2 LLC.	
e802dot2SNAP	The frame type is Ethernet IEEE 802.2 SNAP.	
Ethernet II	The frame type is Ethernet Type II.	
ATM	The frame type is ATM.	ATM is applicable to Mac Match criteria only.

Inner Encap Value

See the [Inner Encap Value](#) parameter in section [112.1](#).

MAC Filter Type

(macFilterType)

The MAC Filter Type parameter specifies which type of entries this MAC Filter policy can contain. This parameter can only be changed if the filter is not applied and if it has no entries. The options are:

- Normal (default)
- ISID
- VID

Selecting the Normal option means that all match criteria except [Low ISID](#) and [High ISID](#) are accepted.

Selecting the ISID option means that the only accepted match criteria for the filter entries are [Low ISID](#) and [High ISID](#).

The VID option allows ingress and egress MAC filtering using VLAN IDs. Filtering ranges are set using the related parameters Inner Tag Value, Inner Tag VID Mask, Outer Tag Value, and Outer Tag VID Mask.

The following restrictions apply to the VID option:

- Hardware: the VID option requires the use of IOM3- or IMM-based systems. It is only supported on 7450 ESS and 7750 SR NEs equipped with either of these cards.
- SAPs: L2 access interfaces can perform QoS and MAC filtering based on the VLAN ID field. This is supported for the following services: VPLS, MVPLS, I-VPLS, I-MVPLS, and VLL Epipes. L3 access interfaces are not supported.

Outer Encap Value

See the [Outer Encap Value](#) parameter in section [112.1](#).

Path ID

See the [Path ID](#) parameter in section 112.1.

Port Name

See the [Port Name](#) parameter in section 112.1.

SNAP OUI

(snapOui)

The SNAP OUI parameter specifies an IEEE 802.3 LLC SNAP Ethernet frame OUI value as a match criterion. This parameter is configurable only when the Frame Type parameter is set to e802dot2SNAP. When enabled, the options are:

- off (default)
- zero
- Non Zero

SNAP PID

(snapPid)

The SNAP PID parameter specifies an IEEE 802.3 LLC SNAP Ethernet frame PID value as a match criterion. The parameter is configurable when the SNAP OUI parameter is enabled. The range is -1 to 65 535. The default is -1, indicating that filtering on this parameter is disabled.

Source MAC

(sourceMacAddress)

The Source MAC parameter specifies a unicast MAC address as a match criterion. When enabled, specify a MAC address. The default is 00-00-00-00-00-00.

Src Mask

(sourceMacAddressMask)

The Src Mask parameter specifies a mask value to use as a match criterion when you filter on a source MAC address. The parameter is configurable when the Source MAC parameter is enabled. The default is 00-00-00-00-00-00.

VC ID

See the [VC ID](#) parameter in section 112.1.

69 – ACL IP Filter parameters

69.1 ACL IP Filter parameters 69-2

69.1 ACL IP Filter parameters

This chapter describes the parameters on the ACL IP Filter form and child forms.

Action

See the [Action](#) parameter in section 112.1.

Administrative State

See the [Administrative State](#) parameter in section 112.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Cflowd If Sample

(cflowdIfSample)

The Cflowd If Sample parameter specifies whether a packet is matched when the packet arrives at an interface that is configured for Cflowd analysis. Cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, and SLA measurement. When the Cflowd If Sample parameter is enabled, all packets forwarded by the interface are analyzed according to the Cflowd configuration. The options are:

- true (default)
- false

Cflowd Sample

(cflowdSample)

The Cflowd Sample parameter specifies whether a packet is matched when it is tagged for cflowd analysis. Cflowd is used for network planning and traffic engineering, capacity planning, security, application and user profiling, performance monitoring, usage-based billing, and SLA measurement. When the Cflowd Sample parameter is enabled, only tagged packets are analyzed. The options are:

- true
- false (default)

Credit Control Count

See the [Credit Control Count](#) parameter in section 112.1.

Credit Control Start Entry

See the [Credit Control Start Entry](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

DSCP

See the [DSCP](#) parameter in section 112.1.

Entry ID

See the [Entry ID](#) parameter in section 112.1.

Filter ID**(id)**

The parameter specifies a unique identifier for the filter. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 65 535. The default is 0.

Forward NH**(nextHop)**

The Forward NH parameter specifies the next hop IP address of the route destination as match criterion. The parameter is configurable when the Action parameter is forward. The default is 0.0.0.0.

Forward NH Interface**(nextHopInterfaceName)**

The Forward NH Interface parameter specifies the next hop address, by name, in case the next hop is over an unnumbered interface on this node, as match criterion for the filter. The parameter is configurable when the Action parameter is forward. The range is 0 to 32 characters.

Fragment

See the [Fragment](#) parameter in section 112.1.

High WaterMark (%)

See the [High WaterMark \(%\)](#) parameter in section 112.1.

ICMP Code

See the [ICMP Code](#) parameter in section 112.1.

ICMP Type

See the [ICMP Type](#) parameter in section 112.1.

Inner Encap Value

See the [Inner Encap Value](#) parameter in section 112.1.

IP Option

(ipOptionValue)

See the [IP Option](#) parameter in section 112.1

IP Opt Mask

(ipOptionMask)

See the [IP Opt Mask](#) parameter in section 112.1

Is Indirect

(nextHopIndirectlyReachable)

The Is Indirect parameter specifies whether to match on a packet where the destination node is not directly connected to a network configured on this device but can be reached using multiple paths. The parameter is configurable when the Action parameter is Forward. The options are:

- true
- false (default)

Low WaterMark (%)

See the [Low WaterMark \(%\)](#) parameter in section 112.1.

Multiple Option

(multipleOption)

See the [Multiple Option](#) parameter in section 112.1

Option Present

(optionPresent)

See the [Multiple Option](#) parameter in section 112.1.

Outer Encap Value

See the [Outer Encap Value](#) parameter in section 112.1.

Path ID

See the [Path ID](#) parameter in section 112.1.

Port Name

See the [Port Name](#) parameter in section 112.1.

Protocol

See the [Protocol](#) parameter in section 112.1.

RADIUS Count

See the [RADIUS Count](#) parameter in section 112.1.

RADIUS Start Entry

See the [RADIUS Start Entry](#) parameter in section 112.1.

Remark Dot1p**(remarkDot1p)**

The Remark Dot1p parameter specifies the remark Dot1p value as match criterion when remarking is applied. The parameter is configurable when the Action parameter is Forward. When enabled, the range is 0 to 7, or Not Set (-1). The default is Not Set (-1).

Remark DSCP**(remarkDscp)**

The Remark DSCP parameter specifies the remark DSCP value as match criteria when remarking is applied. The parameter is configurable when the Action parameter is Forward. When enabled, the range is 0 to 255, or Not Set. The default is Not Set.

Remark DSCP Mask**(remarkDscpMask)**

The Remark DSCP Mask parameter specifies the remark DSCP mask value as match criteria when remarking is applied. The parameter is configurable when the Action parameter is Forward. The range is 0 to 255, or Not Set. The default is 255.

Source IP

See the [Source IP](#) parameter in section 112.1.

Source Port

See the [Source Port](#) parameter in section 112.1.

Src Mask

See the [Src Mask](#) parameter in section 112.1.

TCP Ack

See the [TCP Ack](#) parameter in section 112.1.

TCP Syn

See the [TCP Syn](#) parameter in section 112.1.

VC ID

See the [VC ID](#) parameter in section 112.1.

70 – ACL IPv6 Filter parameters

70.1 ACL IP and ACL IPv6 Filter parameters 70-2

70.1 ACL IP and ACL IPv6 Filter parameters

This chapter describes the parameters on the ACL IPv6 Filter form and child forms.

Action

See the [Action](#) parameter in section 112.1.

Administrative State

See the [Administrative State](#) parameter in section 112.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Credit Control Count

See the [Credit Control Count](#) parameter in section 112.1.

Credit Control Start Entry

See the [Credit Control Start Entry](#) parameter in section 112.1.

Default Action

See the [Default Action](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Destination IP

See the [Destination IP](#) parameter in section 112.1.

Dest Port

See the [Dest Port](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

DSCP

See the [DSCP](#) parameter in section 112.1.

Dst Mask

See the [Dst Mask](#) parameter in section 112.1.

Entry ID

See the [Entry ID](#) parameter in section 112.1.

Filter ID

See the [Filter ID](#) parameter in section 112.1.

High WaterMark (%)

See the [High WaterMark \(%\)](#) parameter in section 112.1.

ICMP Code

See the [ICMP Code](#) parameter in section 112.1.

ICMP Type

See the [ICMP Type](#) parameter in section 112.1.

Log ID

See the [Log ID](#) parameter in section 112.1.

Low WaterMark (%)

See the [Low WaterMark \(%\)](#) parameter in section 112.1.

Protocol

See the [Protocol](#) parameter in section 112.1.

RADIUS Count

See the [RADIUS Count](#) parameter in section 112.1.

RADIUS Start Entry

See the [RADIUS Start Entry](#) parameter in section 112.1.

Source IP

See the [Source IP](#) parameter in section 112.1.

Source Port

See the [Source Port](#) parameter in section 112.1.

Src Mask

See the [Src Mask](#) parameter in section 112.1.

TCP Ack

See the [TCP Ack](#) parameter in section 112.1.

TCP Syn

See the [TCP Syn](#) parameter in section 112.1.

71 – 7250 SAS and Telco ACL Standard IP Filter parameters

71.1 7250 SAS and Telco ACL Standard IP Filter parameters 71-2

71.1 7250 SAS and Telco ACL Standard IP Filter parameters

This chapter describes the parameters on the 7250 SAS and Telco ACL Standard IP Filter form and its child forms. The 5620 SAM menu path is Policies→Filter→7250 SAS and Telco ACL Standard IP Filter.

Action

(defaultAction)

The Action parameter specifies the action that should be performed with a packet when the specified match criteria are met. Table 71-1 describes the parameter options.

Table 71-1 Action parameter

Option	Option description
Deny (default)	Discard the packet.
Permit	Forward the packet.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Filter ID

(id)

The Filter ID parameter specifies a unique identifier for the filter. The range is 1 to 99. The default is 0.

Loggable

See the [Loggable](#) parameter in section 112.1.

Source IP

(sourceIpAddress)

The Source IP parameter is combined with the Src Mask parameter to specify a source IP address range as a match criterion. The default is 0.0.0.0.

Src Mask

(sourceIpAddressMask)

The Src Mask parameter specifies the IP mask value to use as a match criterion along with the Source IP parameter value. The range is 0 to 32. The default is 32.

VLAN Priority Tag

See the [VLAN Priority Tag](#) parameter in section 112.1.

72 – 7250 SAS and Telco ACL Extended IP Filter parameters

72.1 7250 SAS and Telco ACL Extended IP Filter parameters 72-2

72.1 7250 SAS and Telco ACL Extended IP Filter parameters

This chapter describes the parameters on the 7250 SAS and Telco ACL Extended IP Filter form and its child forms. The 5620 SAM menu path is Policies→Filter→7250 SAS and Telco ACL Extended IP Filter.

Action

(defaultAction)

The Action parameter specifies the action that should be performed with a packet when the specified match criteria are met. Table 72-1 describes the parameter options.

Table 72-1 Action parameter

Option	Option description
Deny (default)	Discard the packet.
Permit	Forward the packet.

Description

See the [Description](#) parameter in section 112.1.

Dest Mask

(destinationIpAddressMask)

The Dest Mask parameter specifies the IP mask value to use as a match criterion along with the Destination IP parameter value. The range is 0 to 32. The default is 32.

Destination IP

(destinationIpAddress)

The Destination IP parameter is combined with the Dest Mask parameter to specify a destination IP address range as a match criterion. The default is 0.0.0.0.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Filter ID

(id)

The Filter ID parameter specifies a unique identifier for the filter. The range is 100 to 199. The default is 0.

Loggable

See the [Loggable](#) parameter in section [112.1](#).

Precedence

(precedence)

The Precedence parameter specifies the IP precedence value to be used as a match criterion for the filter. The parameter is configurable when the check box is selected. The options are:

- None (default)
- Routine
- Priority
- Immediate
- Flash
- Flash Override
- Critical
- Internet
- Network

Protocol

(protocol)

The Protocol parameter specifies an IP protocol as a match criterion for the filter. When you specify ICMP, TCP, or UDP, you must configure additional parameters. Table [72-2](#) lists the parameter options.

Table 72-2 Protocol parameter

Options			
ALL	SEP	IPPC	IFMP
HOPOPT	3PC	any distributed file system (68)	PNNI
ICMP	IDPR	SAT_MON	PIM
IGMP	XTP	VISA	ARIS
GGP	DDP	IPCV	SCPS
IP (default)	IDPR_CMTDP	CPNX	QNX
ST	TP++	CPHB	A/N Active Networks (107)
TCP	IL	WSN	IPComp
CBT	IPv6	PVP	SNP
EGP	SDRP	BR_SAT_MON	Compaq_Peer
IGP	IPv6Route	SUN_ND	IPX_in_IP
BBN_RCC_MON	IPv6Frag	WB_MON	VRRP
NVP_II	IDRP	WB_EXPAK	PGM
PUP	RSVP	ISO_IP	any 0-hop protocol (114)

(1 of 2)

Options			
ARGUS	GRE	VMTP	L2TP
EMCON	MHRP	SECURE_VMTP	DDX
XNET	BNA	VINES	IATP
CHAOS	ESP	TTP	STP
UDP	AH	NSFNET_IGP	SRP
MUX	I_NLSP	DGP	UTI
DCN_MEAS	SWIPE	TCF	SMP
HMP	NARP	EIGRP	SM
PRM	MOBILE	OSPFIGP	PTP
XNS_IDP	TLSP	Sprite_RPC	ISIS
TRUNK_1	SKIP	LARP	FIRE
TRUNK_2	IPv6_ICMP	MTP	CRTP
LEAF_1	IPv6_No_Nxt	AX.25	CRUDP
LEAF_2	IPv6_Opts	IPIP	SSCOPMCE
RDP	any host internal protocol (61)	MICP	IPLT
IRTP	CFTP	SCC_SP	SPS
ISO_TP4	any local network (63)	ETHERIP	PIPE
NETBLT	SAT_EXPAK	ENCAP	SCTP
MFE_NSP	KRYPTOLAN	any private encryption scheme (99)	FC
MERIT_INP	RVD	GMTP	RSVP_E2E_IGNORE

(2 of 2)

Source IP

(sourceIpAddress)

The Source IP parameter is combined with the Src Mask parameter to specify a source IP address range as a match criterion. The default is 0.0.0.0.

Src Mask

(sourceIpAddressMask)

The Src Mask parameter specifies the IP mask value to use as a match criterion along with the Source IP parameter value. The range is 0 to 32. The default is 32.

TOS

(tos)

The TOS parameter specifies the IP TOS value as a match criterion for the filter. The parameter is configurable when the check box is selected. The options are:

- None (default)
- Normal
- Minimum Monetary Cost
- Maximum Reliability
- TOS 3
- Maximum Throughput
- TOS 5
- TOS 6
- TOS 7
- Minimum Delay
- TOS 9
- TOS 10
- TOS 11
- TOS 12
- TOS 13
- TOS 14
- TOS 15

VLAN Priority Tag

(vpt)

See the [VLAN Priority Tag](#) parameter in section 112.1.

73 – 7250 SAS and Telco ACL IGMP Filter parameters

73.1 7250 SAS and Telco ACL IGMP Filter parameters 73-2

73.1 7250 SAS and Telco ACL IGMP Filter parameters

This chapter describes the parameters on the 7250 SAS and Telco ACL IGMP Filter form and its child forms. The 5620 SAM menu path is Policies→Filter→7250 SAS and Telco ACL IGMP Filter.

Action

(action)

The Action parameter specifies the action that should be performed with a packet when the criterion specified in the IGMP filter are met. Table 73-1 describes the parameter options.

Table 73-1 Action parameter

Option	Option description	Dependencies
Deny (default)	Do not allow any traffic that matches the filter criterion.	—
Permit	Allow traffic that matches the filter criterion.	

Auto-Assign ID

See the “[Auto-Assign ID](#)” parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Dest Mask

(destinationIpAddressMask)

The Dest Mask parameter specifies the IP mask value to use as a match criterion for the specified destination IP address in the IGMP filter. The range is 0 to 32. The default is 32.

Destination IP

(destinationIpAddress)

The Destination IP parameter, combined with the Dest Mask parameter, specifies a destination IP address range as match criterion for the IGMP filter. When used as a match criterion, specify an IP address and mask value. The default is 0.0.0.0.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Filter ID

(id)

The Filter ID parameter specifies a unique ID for the ACL IGMP Filter object. The range is 300 to 399. There is no default.

IGMP Option

(igmpOption)

The IGMP Option parameter specifies the type of IGMP filter to use to manage how subscribers access multicast broadcast TV streams. You can configure the parameter when the check box is enabled. The default is None. The options are:

- Membership Query (017)
- Membership Report (018)
- Membership Report v2 (022)
- Leave Group v2 (023)
- Membership Report v3 (034)

When you create a 7250 SAS and Telco IGMP ACL filter policy from a multicast package policy, the parameter is set to the same value as the parameter on the multicast package policy configuration form.

Loggable

(loggable)

The Loggable parameter specifies whether to generate logging information about IGMP filtering. The options are:

- None (default)
- Log
- Log Input

When you create a 7250 SAS and Telco ACL IGMP filter policy from a multicast package policy, the parameter is set to the same value as the parameter on the multicast package policy configuration form.

Name

(packagePolicyPointer)

The Name parameter specifies the name of an IGMP multicast package. Click on the Select button to choose a name from the list of multicast packages.

Source IP

(sourceIpAddress)

The Source IP parameter, combined with the Src Mask parameter, specifies a destination IP address range as match criterion for the IGMP filter. When used as a match criterion, specify an IP address and mask value. The default is 0.0.0.0.

Src Mask

(sourceIpAddressMask)

The Src Mask parameter specifies the IP mask value to use as a match criterion in combination with the Source IP parameter value. This parameter is configurable when the Source IP parameter is enabled. The range is 0 to 32. The default is 32.

74 – 7250 SAS and Telco ACL MAC Filter parameters

74.1 7250 SAS and Telco ACL MAC Filter parameters 74-2

74.1 7250 SAS and Telco ACL MAC Filter parameters

This chapter describes the parameters on the 7250 SAS and Telco ACL MAC Filter form and its child forms. The 5620 SAM menu path is Policies→Filter→7250 SAS and Telco ACL MAC Filter.

Action

(action)

The Action parameter specifies the action that should be performed with the packet when the specified match criteria are met. Table 74-1 describes the parameter options.

Table 74-1 Action parameter

Option	Option description
Deny (default)	Discard the packet.
Permit	Forward the packet.

Description

See the [Description](#) parameter in section 112.1.

Destination MAC

(destinationMacAddress)

The Destination MAC parameter specifies a hexadecimal MAC address value in the format *xx-xx-xx-xx-xx-xx* as a match criterion. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The default is 00-00-00-00-00-00.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Dst Mask

(destinationMacAddressMask)

The Dst Mask parameter specifies a hexadecimal MAC mask value in the format *xx-xx-xx-xx-xx-xx* as a match criterion when you filter on a destination MAC address. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The default is 00-00-00-00-00-00.

Filter ID

(id)

The Filter ID parameter specifies a unique identifier for the filter. The range is 400 to 499. The default is 0.

Loggable

See the [Loggable](#) parameter in section [112.1](#).

Pattern

(pattern)

The Pattern parameter specifies a hexadecimal MAC address value in the format *xx-xx-xx-xx-xx-xx* as a match criterion. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The parameter is configurable when the check box is selected.

Pattern Mask

(patternMask)

The Pattern Mask parameter specifies a hexadecimal MAC mask value in the format *xx-xx-xx-xx-xx-xx* as a match criterion. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The parameter is configurable when the check box is selected.

Source MAC

(sourceMacAddress)

The Source MAC parameter specifies a hexadecimal MAC address value in the format *xx-xx-xx-xx-xx-xx* as a match criterion. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The default is 00-00-00-00-00-00.

Src Mask

(sourceMacAddressMask)

The Src Mask parameter specifies a hexadecimal MAC mask value in the format *xx-xx-xx-xx-xx-xx* as a match criterion when you filter on a destination MAC address. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The default is 00-00-00-00-00-00.

75 – Multicast Package parameters

75.1 Multicast Package parameters 75-2

75.1 Multicast Package parameters

This chapter describes the parameters on the Multicast Package Policy form and its child forms.

Channel

(channel)

The Channel parameter specifies an association between a multicast IP address used to deliver broadcast TV and the channel the subscriber uses to view the content from that multicast IP address. The range is 0 to 10 characters.

Cost

(cost)

The Cost parameter specifies an price association between a multicast IP address used to deliver broadcast TV and the price that the subscriber must pay to view the content from that multicast IP address. The parameter is for information only. The range is 0 to 15 characters.

Description

See the [Description](#) parameter in section 112.1.

ID

(id)

The ID parameter specifies a unique ID for the object. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 99. The default is 0.

IGMP Option

(igmpOption)

The IGMP Option parameter specifies the type of IGMP filter to use to manage how subscribers access multicast broadcast TV streams. The options are:

- None (default)
- Membership Query (017)
- Membership Report (018)
- Membership Report v2 (022)
- Leave Group v2 (023)
- Membership Report v3 (034)

Is Root Catalogue

(mainChannelCatalogue)

The Is Root Catalogue parameter specifies that a multicast package policy is a master or root of all the multicast channels. The options are:

- enabled
- disabled (default)

When the parameter is enabled, you can associate the multicast package policy with a ring group with multicast VLAN registration enabled by distributing the policy to devices or ring groups.

When the parameter is enabled, you can also distribute the policy to all 7450 ESS devices in a multicast VPLS to assign a common set of multicast groups.

Loggable

See the [Loggable](#) parameter in section 112.1.

Multicast Address

(address)

The Multicast Address parameter specifies the IP address for the multicast stream. There is no default. The range is a valid multicast IP address in the range 224.0.0.0 to 239.255.255.255.



Note — Multicast addresses are distributed to ring groups when a Multicast Package is associated with the ring group. All 7250 SAS and Telco devices in the ring group receives the multicast broadcast TV streams. Use IGMP access control list policies to ensure that subscribers are limited to the broadcast channels paid for.

Name

See the [Name](#) parameter in section 112.1. Use the Name parameter to create an operations-friendly name to associated the Multicast Address parameter. For example, if a Multicast IP address is associated with a pay per view channel that distributes spy movies, you could set the Name parameter to pay per view spy movies.

76 – Egress Multicast Group parameters

76.1 Egress Multicast Group parameters 76-2

76.1 Egress Multicast Group parameters

This chapter describes the parameters on the Egress Multicast Group form and child forms.

Description

See the [Description](#) parameter in section 112.1.

Destination Chain Limit

(chainLimit)

The Destination Chain Limit parameter specifies the maximum number of destination SAPs that are permitted on an EMG. The range is 1 to 30. The optimal length is 10 to 16. The default is 16.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Dot1 Q Ethertype

(dot1qEtype)

The Dot1 Q Ethertype parameter specifies the Ethertype expected when the [Encapsulation Type](#) parameter is set to Dot1 Q. The range is 1536 to 65 535 (0x600 to 0xffff). The default is 33 024 (0x8100).

Encapsulation Type

(encapType)

The Encapsulation Type parameter specifies the type of encapsulation that is shared by all members of the Egress Multicast Group. The encapsulation type must be the same for all the members of the chain associated with a service. The options are:

- Null (default)
- Dot1 Q

QinQ Ethertype

(qInqEtype)

The QinQ Ethertype parameter specifies the Ethertype expected when the [Encapsulation Type](#) parameter is set to QinQ. The range is 1536 to 65 535 (0x600 to 0xffff). The default is 33 024 (0x8100).

QinQ Fixed Tag Value

(adminQinqFixedTagVal)

The QinQ Fixed Tag Value parameter specifies the fixed 802.1Q tag value of each QinQ-encapsulated SAPs in the Egress Multicast Group. The parameter is configurable when the [Encapsulation Type](#) parameter is set to QinQ. The range is 0 to 4094. The default is 0.

77 – Multicast CAC parameters

77.1 Multicast CAC parameters 77-2

77.1 Multicast CAC parameters

This chapter describes the parameters on the Multicast CAC form and its child forms. The 5620 SAM menu path is Policies→Multicast→Multicast CAC.

Administrative State

See the [Administrative State](#) parameter in section 112.1.

Bandwidth (kbps)

(bandwidth)

The Bandwidth (kbps) parameter specifies the bandwidth for the object. The range depends on the type of object being configured. Table 77-1 lists the Bandwidth parameter ranges for different policy object types.

Table 77-1 Bandwidth (kbps) parameter

Object	Range (characters)
Channel	10 to 20 000
Bundle Level	1 (default) to 4 294 967 295

Class

(channelClass)

The Class parameter specifies the multicast ingress throughput limitation. The options are:

- Low (default)
- High

Default Action

(defaultAction)

The Default Action parameter specifies the action to be applied to multicast streams (channels) when the streams do not match any of the multicast addresses defined in the multicast CAC policy. The options are:

- Accept
- Discard (default)

Description

See the [Description](#) parameter in section 112.1.

End Address

(endAddress)

The End Address parameter specifies the end address of a BTV channel range. Specify an IPv4 multicast address in dotted-decimal format. If only one channel is specified for the range, the address specified for the start address is also used for the end address.

Max Bandwidth (kbps)

(bandwidth)

The Max Bandwidth (kbps) parameter specifies the maximum bandwidth allowed for channels in a bundle. The range is 1 to 4 294 967 295 kbps. The default is 100 kbps.

Name

See the [Name](#) parameter in section 112.1.

Start Address

(startAddress)

The Start Address parameter specifies the start address of a BTV channel range. Specify an IPv4 multicast address in dotted-decimal format.

Type

(channelType)

The Type parameter specifies if the multicast channel is mandatory or optional. The options are:

- Not Mandatory (default)
- Mandatory

If the channel is configured as mandatory, the bandwidth is reserved in the bundle and on all potential interfaces to guarantee the channel request is accepted. If the channel is configured as Not Mandatory, the channel request are accepted only if the bandwidth of the bundle and the interface are available.

78 – Ingress Multicast Path Management parameters

78.1 Ingress Multicast Path Management parameters 78-2

78.1 Ingress Multicast Path Management parameters

This chapter describes the parameters on the Ingress Path Management Policies form and child forms.

Address

(address)

The Address parameter specifies the IP address of the video interface. Specify an IPv4 address. There is no default.

Admin BW Use Threshold (kbps)

(adminBwUseThreshold)

The Admin BW Use Threshold parameter specifies the bandwidth rate at which a multicast channel configured to use an administrative rate starts and stops using that rate as the in-use ingress bandwidth when managing ingress multicast paths. The range is from 1 to 40 000 000 kbps. The default is 10.

Admin State

(ingrPathMgmtAdminState)

The Admin State parameter specifies the administrative state of multicast path management on the MDA (IOM or IOM 2) or the forwarding plane of an IOM 3 or IMM. The options are:

- Down (default)
- Up

Administrative BW (kbps)

The Administrative BW parameter specifies the multicast channel's administrative bandwidth in kilo-bits per second. The range is from 0 to 40 000 000 kbps. The default is 0.

The XML property name for this parameter varies depending on where it is set, namely at the bundle, channel range, or channel override level. The variations are listed in Table 78-1.

Table 78-1 Administrative BW (kbps) parameter variations

Parameter configuration level	XML property name
Channel bundle	defaultAdminBw
Channel range	adminBw
Channel override	adminBw

Administrative State

(adminState)

The Administrative State parameter specifies the administrative state of the multicast reporting destination. The options are:

- Down (default)
- Up

Ancillary Path Limit (mbps)

(ancillaryPathLimit)

The Ancillary Path Limit parameter specifies the override for the ancillary path limit of the bandwidth policy for the MDA. Units are in megabits per second. The value zero, means unspecified. Maximum supported value is 5000 mbps. The default is 0.

Black Hole Rate (kbps)

The Black Hole Rate parameter specifies at which current rate a channel (including channels within a channel range or bundle) should be placed in the black-hole state (packets are dropped). This value can only be set when the [BW Decision](#) parameter is set to Dynamic. The range is 0 to 40 000 000. The default is 0, which means never.

The XML property name for this parameter varies depending on where it is set, namely at the bundle, channel range, or channel override level. The variations are listed in Table [78-2](#).

Table 78-2 Black Hole Rate (kbps) parameter variations

Parameter configuration level	XML property name
Channel bundle	defaultBlackHoleRate
Channel range	blackHoleRate
Channel override	blackHoleRate

Buffer Size

(rtBufferSize)

The Buffer Size parameter specifies the number of milliseconds worth of channel packets to store for the Retransmission (RT) server. The range is 300 to 8000. The default is 300.

BW Decision

The BW Decision parameter specifies how the multicast ingress path manager determines the amount of bandwidth required by a multicast channel, including channels within a channel range or bundle.

The XML property name and default value for this parameter varies depending on where it is set, namely at the bundle, channel range, or channel override level. The variations are listed in Table 78-3.

Table 78-3 BW Decision parameter variations

Parameter configuration level	XML property name	Default value
Channel bundle	defaultBwDecision	Dynamic
Channel range	bwDecision	unspecified
Channel override	bwDecision	unspecified

Channel Type

(channelType)

The Channel Type parameter specifies the video channel type. The options are:

- High Definition (HD) (default)
- Standard Definition (SD)
- Picture-in-Picture (PIP)

Committed Buffer Space (%)

(cbs)

The Committed Buffer Space parameter specifies the path CBS (queue length/depth) as a percentage of the total buffer pool. The range is 0 to 100. The default percentages for the primary, secondary and ancillary path are 5%, 30%, and 65% respectively.

This parameter is configurable for T1 and T2 paths. The T2 path values are used for nodes that use an IOM 3 or IMM. The T1 values are used for all other IOM types.

Congestion Priority Threshold

(congestPriorityThreshold)

The Congestion Priority Threshold parameter specifies the preference level at which a multicast record changes from low congestion priority to high congestion priority. Allowed escalating values are 0 to 7. The default is 4.

Continuity Counter Error

(ccError)

The Continuity Counter Error parameter specifies whether continuity counter errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

Description

See the [Description](#) parameter in section 112.1.

Description

(analyzerDesc)

The Description parameter specifies the description for the video analyzer settings configured in the VQM tab. The range is 0 to 80.

Destination Address

(destinationAddress)

The Destination Address parameter specifies the IP address of the multicast reporting destination. Specify an IPv4 address in dotted-decimal format. There is no default.

Destination UDP Port

(udpPort)

The Destination UDP Port parameter specifies the UDP port address of the multicast reporting destination. The range is 1 to 65 535. The default is 1037.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

ECMP Optimization Threshold

(ecmpOptimizationThreshold)

The ECMP Optimization Threshold parameter specifies the preference level at which the ECMP path manager is allowed to optimize channels. Channels with a preference level below the set threshold are considered for optimization. Allowed values are 0 to 7. The default is 7.

End Address

(endAddress)

The End Address parameter indicates the ending address (in IPv4, IPv6, or DNS format) of the multicast channel range. The ending address should always be greater than or equal to the [Start Address](#) parameter. The default is 0.0.0.0.

Explicit Path

The Explicit Path parameter specifies an explicit ingress switch fabric multicast path (Primary, Secondary, Ancillary) for the channels (including those in a range or a bundle). If the parameter is not set, the Multicast Path Manager dynamically places channels on the most optimal switch fabric paths. The default is “unspecified”.

The XML property name for this parameter varies depending on where it is set, namely at the bundle, channel range, or channel override level. The variations are listed in Table 78-4.

Table 78-4 Explicit Path parameter variations

Parameter configuration level	XML property name
Channel bundle	defaultExplicitPath
Channel range	explicitPath
Channel override	explicitPath

Falling Delay (seconds)

The Falling Delay parameter specifies the value the bandwidth manager uses as a threshold to hold on to the previous highest bandwidth until the delay time has expired, while operating in dynamic bandwidth mode. This allows the bandwidth manager to ignore momentary drops in channel bandwidth. This value can only be set if **BW Decision** is set to Dynamic. A value of 0 specifies that a non-zero value of the parent is applied.

The XML property name for this parameter varies depending on where it is set, namely at the bundle, channel range, or channel override level. The variations are listed in Table 78-5.

Table 78-5 Falling Delay (seconds) parameter variations

Parameter configuration level	XML property name	Default value	Range	Parent
Channel bundle	defaultFallingDelay	30	10 to 3600s	—
Channel range	fallingDelay	0	0 10 to 3600	Channel bundle
Channel override	fallingDelay	0	0 10 to 3600	Channel bundle Channel range

Falling Percent Reset (%)

(fallingPercentReset)

The Falling Percent Reset parameter specifies the percentage of bandwidth decrease that must occur to reset the dynamic bandwidth monitoring function for a multicast channel. The range is 1 to 100. The default is 100.

FCC Burst

(fccBurst)

The FCC Burst parameter specifies the percentage increase over the received rate at which the FCC server sends unicast data to the client to allow the client to catch up to the multicast stream. The value is only applicable if the [FCC Server Mode](#) parameter is set to Burst or Hybrid. When the value of the [Channel Type](#) parameter is HD, the maximum value of FCC Burst is 100. For example, a value of 30 indicates that FCC Burst rate is set to 30% over the received rate. The range is 0 to 600. The default is 25.

FCC MC Handover Rate

(fccMcHandover)

The FCC MC Handover Rate parameter specifies the percentage rate at which the FCC server sends unicast data to the client during the handover to the multicast stream. When the value of the [Channel Type](#) parameter is HD, the maximum value of FCC MC Handover Rate is 100. The range is 0 to 600. The default is 25.

FCC Server

(fccServerState)

The FCC Server parameter specifies whether the Fast Channel Change (FCC) server is enabled on the multicast information policy bundle. The options are:

- Enabled
- Disabled (default)

FCC Server Mode

(fccServerMode)

The FCC Server Mode parameter specifies the mode of the Fast Channel Change (FCC) server. It indicates how the FCC server sends a unicast stream to the client. When Burst is specified, the FCC server is enabled, and sends the channel at a nominally faster rate than the channel was received at, based on the [FCC Burst](#) parameter setting. When None is specified, the FCC server is disabled. The options are:

- Burst
- Dent
- Hybrid
- None (default)

High Bandwidth Alarm

(mCastAlarm)

The High Bandwidth Alarm parameter applies to an MDA or a forwarding plane (IOM3 and IMM). Table 78-6 describes the meaning of the parameter for each application. The options are:

- True (default)
- False

Table 78-6 High Bandwidth Alarm parameter

Parameter application	Description
MDA	Specifies whether an alarm is raised if there is more than one high bandwidth multicast traffic tap sharing a queue.
Forwarding plane	Specifies whether if an alarm is raised if there are more than one high bandwidth multicast traffic tap sharing a forwarding plane.

High Bandwidth Multicast Traffic Taps Group

(mCastGroup)

The High Bandwidth Multicast Traffic Taps Group parameter specifies the group of high bandwidth multicast traffic taps to which a tap belongs. This parameter is not valid unless the [High Bandwidth Source](#) parameter is enabled. A value of 0 specifies that this tap is not a member of any High Bandwidth Multicast Group. The range is 0 to 32. The default is 0.

High Bandwidth Source

(mCastSource)

The High Bandwidth Source parameter applies to an MDA or a forwarding plane (IOM3 or IMM). Table 78-7 describes the meaning of the parameter for each application. The options are:

- True
- False (default)

Table 78-7 High Bandwidth Source parameter

Parameter application	Description
MDA	Specifies if this MDA should attempt to use separate queues when allocating high bandwidth multicast traffic taps.
Forwarding plane	Specifies whether the forwarding plane should attempt to allocate separate fabric planes to high bandwidth multicast traffic taps.

High Priority Traffic (%)

(highPriority)

The High Priority Traffic parameter specifies a percentage of the queue depth reserved for high congestion priority traffic. The range is 0 to 100. The default percentages for the three paths is 10% each.

This parameter is configurable for T1 and T2 paths. The T2 path values are for nodes that use an IOM 3 or IMM. The T1 values are used for all other IOM types.

Ingress LER

(senderIpAddress)

The Ingress LER parameter specifies the IP address of the sender ingress LER node. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Local Server

(localRtState)

The Local Server parameter specifies whether a local retransmission (RT) server is enabled on this multicast information policy bundle. It also indicates whether to process the retransmission requests from the client. The options are:

- Enabled
- Disabled (default)

Max Delay (Deciseconds)

(maxDelay)

The Max Delay (Deciseconds) parameter specifies the maximum delay after which any cached reports are sent to the reporting destination. A value of 0 means the reports are not cached; when reports are not cached every report triggers an outgoing message. The range is 0 to 100. The default is 1.

Max IGMP Latency

(maxIgmpLatency)

The Max IGMP Latency parameter specifies the per-client maximum IGMP latency. The range is 10 to 1000. The default value is 100.

Max Number of Sessions

(maxSessions)

The Max Number of Sessions parameter specifies the per-client maximum number of sessions. The range is 1 to 65536. The default value is 256.

Maximum Buffer Space (%)

(mbs)

The Maximum Buffer Space parameter specifies the path's committed buffer size (queue length/depth) as a percentage of the total buffer pool. The default percentages for the primary, secondary and ancillary path are 5%, 30%, and 65% respectively.

This parameter is configurable for T1 and T2 paths. The T2 path values are used for nodes that use an IOM 3 or IMM. The T1 values are used for all other IOM types.

Min Duration (msec)

(fccMinDuration)

The Min Duration (msec) parameter specifies the minimum time duration, in milliseconds, of the Fast Channel Change (FCC) burst. This determines the starting point of the FCC burst. If the current Group of Pictures (GOP) has less than the minimum duration worth of data, the FCC burst starts from the previous GOP. The range is 300 to 8000. The default is 300.

Name

See the [Name](#) parameter in section 112.1.

Name

(ingrPathMgmtBwPolicyPointer)

The Name parameter specifies the name of the multicast bandwidth policy configured on the MDA. The range is 1 to 32 characters. There is no default.



Note — The multicast bandwidth policy named “default” cannot be modified or deleted.

Name

(ingrPathMgmtPolicyPointer)

The Name parameter specifies the name of the multicast information policy configured on the VPLS, VPRN site, or the default routing instance. The range is 1 to 32 characters. There is no default.



Note 1 — The multicast information policy named “default” cannot be modified or deleted.

Note 2 — You cannot use the colon symbol in the policy name. The 5620 SAM uses colons as separators for the object full name.

Non Video PID Absent Intv (msec)

(vidPidAbsent)

The Non Video PID Absent Intv (msec) parameter specifies the counting interval for counting the number of non-video PID absent errors for the video PID stream. A value of 0 means no error counting occurs. The range is 0 to 5000, and must be adjusted in increments of 100. The default value is 0.

Number of Secondary T2 Paths

(numberOfSecondaryT2Paths)

The Number of Secondary T2 Paths parameter specifies how many paths are configured as T2 secondary paths. Paths that are not configured as T2 secondary paths are configured as primary paths. The range is 1 to 15. The default is 1.

P2MP ID for LDP

(p2mpId)

The P2MP ID for LDP parameter specifies the identifier of a P2MP that is LSP associated with the tunnel interface. The range is 0 to 4 294 967 295. The default is 0.

P2MP LSP Name

(p2mpLspName)

The P2MP LSP Name parameter specifies the name of the RSVP P2MP LSP that is associated with the tunnel interface. The range is 0 to 32. There is no default.

PAT Repetition Error

(patRepError)

The PAT Repetition Error parameter specifies whether PAT repetition errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

PAT Syntax

(patSyntaxErr)

The PAT Syntax parameter specifies whether PAT syntax errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

Path Limit (mbps)

(pathLimit)

The Path Limit parameter overrides the default path limit for each of the three ingress multicast paths into the switch fabric. The minimum is 1. The maximum value for the primary and secondary paths is 2000, and for the ancillary path is 5000. The default value for the primary path is 2000, for the secondary path is 1500, and for the ancillary path is 5000.

PCR Repetition Error

(pcrRepError)

The PCR Repetition Error parameter specifies whether PCR repetition errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

Percentage of Total pool (%)

(mcastBufferPoolPercentage)

The Percentage of Total pool parameter specifies how much of the total ingress buffer pool space for the MDA is dedicated for multicast channels managed by the bandwidth policy. The range is 1 to 50. The default is 10.

PMT Repetition Error

(pmtRepError)

The PMT Repetition Error parameter specifies whether PMT repetition errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

PMT Syntax Error

(pmtSyntaxErr)

The PMT Syntax Error parameter specifies whether PMT syntax errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

Preference Level

The Preference Level parameter specifies the relative preference level for multicast channels. The preference of a channel (including those in a bundle or range) specifies its relative importance over other multicast channels. Eight levels of preference are supported: 0 through 7. Preference value 7 indicates the highest preference level.

The XML property name and default value for this parameter varies depending on where it is set, namely at the bundle, channel range, or channel override level. The variations are listed in Table 78-8.

Table 78-8 Preference Level parameter variations

Parameter configuration level	XML property name	Default value
Channel bundle	defaultPrefLevel	7
Channel range	prefLevel	0
Channel override	prefLevel	0

Primary Interface

(priIfName)

The Primary Interface parameter specifies the primary interface used for multicast traffic in stream selection.

Primary Path Limit (mbps)

(primaryPathLimit)

The Primary Path Limit parameter specifies the override for primary path limit of the bandwidth policy for the MDA. Units are in megabits per second. The value zero, means unspecified. Maximum supported value is 2000 mbps. The default is 0.

QoS (msec)

(qosPatRep)

The QoS (msec) parameter specifies the value of QoS in milliseconds for PAT repetition. The value of this parameter must be greater than the value of the [TNC \(msec\)](#) parameter. The value must be a multiple of 100. The range is 200 to 900. The default value is 200.

QoS (msec)

(qosPcrRep)

The QoS (msec) parameter specifies the value of QoS in milliseconds for PCR repetition. The value of this parameter must be greater than the value of the [TNC \(msec\)](#) parameter. The value must be a multiple of 100. The range is 200 to 900. The default value is 200.

QoS (msec)

(qosPmtRep)

The QoS (msec) parameter specifies the value of QoS in milliseconds for PMT repetition. The value of this parameter must be greater than the value of the [TNC \(msec\)](#) parameter. The value must be a multiple of 100. The range is 200 to 4900. The default value is 800.

Re-order Audio Interval (msec)

(reorderAudio)

The Re-order Audio Interval (msec) parameter specifies the amount of time, in milliseconds, by which the audio packets are reordered in the ad stream. If the value of this object is set to 0, then audio reordering is disabled. It can also be set to disabled by selecting the adjacent check box. The range is 0 to 1000. The default is 0.

Reserved CBS (%)

(mcastBufferPoolResvCbsPercentage)

The Reserved (CBS) parameter specifies the percentage of the pool to be reserved for multicast path queues within their Committed Buffer Size threshold. The range is 1 to 100. The default is 50.

RT Payload Type

(rtPayloadType)

The RT Payload Type parameter specifies the format to be used by the RT server to send retransmission packets. The range is 33 to 127. The default value is 99.

The default value of 99 indicates that the frames will be sent in the RFC 4588 format. A value between 96 and 127 indicates the dynamic payload type value (as per RFC 3551) to be used for RFC 4588 formatted retransmission packets. A value of 33 indicates an MPEG-TS payload.

RT Rate

(rtRate)

The RT Rate parameter specifies the percentage increase over the nominal bandwidth at which retransmission packets are sent to the client. For example, a value of 20 indicates that the retransmission rate is set to 20% over the nominal bandwidth. The range is 1 to 100. The default is 5.

(RT) Server

(rtServerState)

The (RT) Server parameter specifies whether a Retransmission (RT) Server is enabled on this multicast information policy bundle. The options are:

- Enabled
- Disabled (default)

SCTE35 Error

(scte35Error)

The SCTE35 Error parameter specifies whether SCTE35 errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

Secondary Interface

(secIfName)

The Secondary Interface parameter specifies the secondary interface used for multicast traffic in stream selection.

Secondary Path Limit (mbps)

(secondaryPathLimit)

The Secondary Path Limit parameter specifies the override for the secondary path limit of the bandwidth policy for the MDA. Units are in megabits per second. The value zero, means unspecified. Maximum supported value is 2000 mbps. The default is 0.

Source Address

(srcAddress)

The Source Address parameter indicates the address of an explicit multicast channel for which you want to specify overrides. The channel's IP address should fall within the containing range of the Channel Range and must be of the same IP address type (in IPv4, IPv6, or DNS format) as the range. The default is 0.0.0.0.

Source Address

(priAddr)

The Source Address parameter specifies the IPv4 address of the primary source for stream selection. A unicast address must be entered. The default is 0.0.0.0.

Start Address

(startAddress)

The Start Address parameter indicates the starting address (in IPv4, IPv6, or DNS format) of the multicast channel range. The start address should always be less than or equal to the [End Address](#) parameter. The default is 0.0.0.0.

TEI Error

(teiError)

The TEI Error parameter specifies whether TEI errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

TNC (msec)

(tncPatRep)

The TNC (msec) parameter specifies the value of TNC in milliseconds for PAT repetition. The value must be a multiple of 100. The range is 100 to 800. The default value is 100.

TNC (msec)

(tncPcrRep)

The TNC (msec) parameter specifies the value of TNC in milliseconds for PCR repetition. The value must be a multiple of 100. The range is 100 to 800. The default value is 100.

TNC (msec)

(tncPmtRep)

The TNC (msec) parameter specifies the value of TNC in milliseconds for PMT repetition. The value must be a multiple of 100. The range is 100 to 4800. The default value is 400.

TOA (msec)

(poaPcrRep)

The POA (msec) parameter specifies the value of POA in milliseconds for PCR repetition. The value of this parameter must be greater than the value of the [QoS \(msec\)](#) parameter. The value must be a multiple of 100. The range is 300 to 1000. The default value is 500.

TOA (msec)

(poaPmtRep)

The POA (msec) parameter specifies the value of POA in milliseconds for PMT repetition. The value of this parameter must be greater than the value of the [QoS \(msec\)](#) parameter. The value must be a multiple of 100. The range is 300 to 5000. The default value is 2000.

TOA (msec)

(toaPatRep)

The TOA (msec) parameter specifies the value of TOA in milliseconds for PAT repetition. The value of this parameter must be greater than the value of the [QoS \(msec\)](#) parameter. The value must be a multiple of 100. The range is 300 to 1000. The default value is 500.

TS Sync Loss Error

(tsSyncLossErr)

The TS Sync Loss Error parameter specifies whether TS sync loss errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

Unreferenced PID Error

(pidPmtUnref)

The Unreferenced PID Error parameter specifies whether unreferenced PID (PIDs not specified in the PMT) errors are enabled or disabled for the video stream. The options are:

- Enabled
- Disabled

Video Group ID

(videoGroupId)

The Video Group ID parameter specifies the video group information for the multicast information policy bundle. A value 0 indicates that no video group is assigned to the multicast information policy bundle. The range is 0 to 4. The default is 0.

Video PID Absent Interval (msec)

(vidPidAbsent)

The Video PID Absent Interval (msec) parameter specifies the counting interval for counting the number of video PID absent errors for the video PID stream. A value of 0 means no error counting occurs. The range is 0 to 5000, and must be adjusted in increments of 100. The default value is 0.

79 – Time of Day parameters

79.1 Time of Day parameters 79-2

79.1 Time of Day parameters

This chapter describes the parameters on the Time Range and Time of Day Suite forms and child forms.

End Run Day

(frequencySettingTo)

The End Run Day parameter specifies the end day of a time range when the [Frequency](#) parameter is set to Weekly. The default is Sunday.

The End Run Day parameter is configurable when the [Ongoing](#) parameter is enabled.

End Time

(endDate)

The End Time parameter specifies the end date and time of the time range entry. You can use the up and down arrows to change the year, month, day, hour, or minute, or use the calendar icon to set the date. The default value is the current system time of the 5620 SAM server.

When the [Ongoing](#) parameter is disabled, the format is YYYY/MM/dd HH:mm.
When the [Ongoing](#) parameter is enabled, the format is HH:mm.

Frequency

(frequency)

The Frequency parameter specifies how often the schedule operates. The options are:

- Daily (default)
- Weekdays
- Weekend
- Weekly

The Frequency parameter is configurable when the [Ongoing](#) parameter enabled.

Name

The Name parameter specifies a name for the created time range policy or time of day suite policy. The range is 1 to 32 characters.

Ongoing

(onGoing)

The Ongoing parameter specifies whether a schedule has an end time. When the parameter is enabled, the schedule operates indefinitely. The options are:

- Enabled
- Disabled (default)

Priority

The Priority parameter specifies the priority of the time of day suite entry. If there are overlapping time range entries within a time of day suite entry, the time range entry with the highest priority is run first. The range is 1 to 10, where 1 is the highest priority, and 10 is the lowest. The default is 5.

The Priority parameter value must be unique within a same policy type.

Start Run Day

(frequencySettingFrom)

The Start Run Day parameter specifies the start day of a time range when the [Frequency](#) parameter is set to Weekly. The default is Sunday.

The Start Run Day parameter is configurable when the [Ongoing](#) parameter is enabled.

Start Time

(startDate)

The Start Time parameter specifies the start date and time of the time range entry. You can use the up and down arrows to change the year, month, day, hour, or minute, or use the calendar icon to set the date. The default value is the current system time of the 5620 SAM server.

When the [Ongoing](#) parameter is disabled, the format is YYYY/MM/dd HH:mm.
When the [Ongoing](#) parameter is enabled, the format is HH:mm.

When the parameter value is greater than the current date and time, no tasks are run until the scheduled start time is reached.

80 – Routing parameters

80.1 Routing parameters 80-2

80.1 Routing parameters

This chapter describes the parameters on the Routing Policy Manager form and child forms.

Action

(action)

The Action parameter specifies what action, if any, should be taken for routes that match a specific routing policy statement entry. There can be one action for each routing policy statement. Table 80-1 describes the parameter options.

Table 80-1 Action parameter

Option	Option description	Dependencies
None (default)	No action is defined for the route. The Default Action parameter value is executed. If Default Action parameter is not configured, then the routing protocol default or the route configuration determines the action performed on the route, instead of the routing policy.	—
Accept	Routes that match the statement entry criteria are accepted and propagated based on the configurations set for the routing policy statement entry.	
Reject	Routes that match the statement entry criteria are rejected and not propagated based on the configurations set for the routing policy statement entry.	
Next Entry	Policy evaluation continues with the next policy entry within the same routing policy statement entry.	
Next Policy	Policy evaluation continues with the next routing policy statement following the current routing policy statement.	You must configure an additional routing policy for import or export of routes using the Prefix List 1 parameter and subsequent Prefix List parameters.

All Instances

(isAllInstances)

The All Instances parameter specifies that all OSPF route instances are announced neighboring nodes. The options are:

- Enabled
- Disabled (default)

You can configure the All Instances parameter when the [Protocol](#) parameter is set to OSPF.

BGP AS Path Name

(asPathName)

The AS Path Name parameter specifies the name that references an AS path regular expression statement that is used as a match criterion for a routing policy statement entry. The AS path name must already be created using the Path Name parameter. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR.

Begin Length

(beginLength)

The Begin Length parameter specifies the prefix list matching criteria for the mask value of the IP address. The parameter value is greater than or equal to the value for the Mask parameter. You can configure the parameter when the Type parameter is set to Range. The parameter is configurable on the 7450 ESS in mixed mode, or the 7750 SR. The range is the *Mask parameter value* to 32. The default is 0.

BGP AS Path Action

(pathAction)

The BGP AS Path Action parameter specifies what action to take for BGP AS path routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR. Table 80-2 describes the parameter options.

Table 80-2 BGP AS Path Action parameter

Option	Option description	Dependencies
None (default)	No action is defined for the route. The Default Action parameter value is used. If the Default Action parameter is not configured, the routing protocol defaults or the route configuration determines the action performed on the route, instead of the routing policy.	—
Add	Routes that match the routing policy statement entry have a new AS regular expression path list appended to the existing AS path list for the route.	The action specified is performed. You can configure the BGP AS Path Name parameter to specify the AS path name, as configured using the AS Path Name parameter. The AS Path Name references the AS regular expression list.
Remove	Routes that match the routing policy statement entry have their AS regular expression path list removed.	
Replace	Routes that match the routing policy statement entry have the new AS regular expression path list replace the existing AS path list for the route.	

BGP AS Prepend number

(prependAs)

The BGP AS Prepend number parameter specifies the AS number that is added to routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR and the Prepend Count parameter is set to 1 or higher. The range is 0 to 4294967295. The default is 0.

Use the BGP AS Prepend number and Prepend Count parameters to specify the AS number and the number of times that the AS numbers are added to the AS path attributes of routes.

BGP Local Preference

(localPreference)

The BGP Local Preference parameter specifies a metric value modifier that is applied to BGP routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR and the Local Preference Set parameter is set to true. The range is 0 to 4 294 967 295. The default is 0.

Check Dependencies

(enforceDependencies)

The Check Dependencies parameter specifies whether the 5620 SAM checks for dependencies between the policy and other policies such as damping policies, AS path policies, or community policies during policy distribution. If this parameter is enabled, the 5620 SAM compares the criteria configured in the dependencies before distributing the policy. The options are:

- True
- False (default)

Community Action 1

(communityAction1)

The Community Action 1 parameter specifies what action, if any, should be taken for BGP community describes for routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR. Table 80-3 describes the parameter options.

Table 80-3 Community Action 1 parameter

Option	Option description	Dependencies
None (default)	No action is defined for the BGP community list.	The community path setting for matching routes is not modified.

(1 of 2)

Option	Option description	Dependencies
Add	Routes that match the routing policy statement entry have the specified BGP community list added to any existing list for the route.	The action specified is performed. You can configure the Community Name 1 and Community Name 2 parameters to specify the BGP community list to be used. An existing community list must be configured using the Community List Name parameter.
Remove	Routes that match the routing policy statement entry have the specified BGP community list removed from any existing list for the route.	
Replace	Routes that match the routing policy statement entry have the specified BGP community list replace the existing list for the route.	

(2 of 2)

Community Action 2

(communityAction2)

See the [Community Action 1](#) in this section.

The Community Action 2 parameter is not configurable when the Community Action 1 parameter is set to None.

Community List Name

(communityName)

The Community List Name parameter specifies the community name used as a match criterion for the routing policy statement entry. The name must have been created using the Community Name parameter. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR.

Do not use a colon in the community name because the 5620 SAM uses colons as separators for the object full name.

Community Member

(member)

The Community Member parameter specifies the community ID of a community member. Regular-expression matching is supported for the Community and Extended Community values.

A valid Community Member (comm-id) is entered in the following format:

```
<2byte-asnumber:comm-val>|<reg-ex>|<ext-comm>|<well-known-comm>
```

Permitted values for each component of the comm-id string are shown in Table [80-4](#).

Table 80-4 Community Member parameter string attributes

Component	Permitted value
2byte-asnumber	0 to 65535
comm-val	0 to 65535
reg-ex	A maximum of 72 characters
ext-comm	<p><type>:{<ip-address:comm-val> <reg-ex1&reg-ex2> <ip-address&reg-ex2> <2byte-asnumber:ext-comm-val> <4byte-asnumber:comm-val>}</p> <p>where:</p> <p>type = target origin</p> <p>ip-address = IPv4 address, in the form of x.x.x.x</p> <p>comm-val = 0 to 65535</p> <p>reg-ex1 = 72 characters maximum</p> <p>reg-ex2 = 72 characters maximum</p> <p>2byte-asnumber = 0 to 65535</p> <p>ext-comm-val = 0 to 4294967295</p> <p>4byte-asnumber = 0 to 4294967295</p>
well-known-comm	null no-export no-export-subconfed no-advertise

Community Member

(member)

The Community Member parameter specifies the community ID of the community member. The parameter is configurable when the Default Action parameter is set to the Accept, Next Entry, or Next Policy option on the 7450 ESS in mixed mode, or the 7750 SR. The range is 1 to 256 characters. The characters must be 7-bit ASCII characters, excluding double quotation marks. Double quotation marks are used to delimit the start and end of a string that contains spaces.

Community Name

(communityName)

The Community Name parameter specifies the route policy community list to use in routing policy entries. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR. The range is 1 to 32 characters. The characters must be 7-bit ASCII characters, excluding double quotation marks. Double quotation marks are used to delimit the start and end of a string that contains spaces.

You must configure at least one community member using the Community Member parameter.

The parameter defines the name of a community list. Community lists are composed of a group of route destinations that share a common property. A community list allows you to perform actions on a community rather than on each member of the community.

Community Name 1

(communityName1)

The Community Name 1 parameter specifies the BGP community list to use for the action specified by the Community Action 1 parameter. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR and the Community Action 1 parameter is set to an option other than None. The name must have been created using the Community List Name parameter.

Community Name 2

(communityName2)

See the [Community Name 1](#) in this section.

The Community Name 2 parameter is not configurable when the Community Action 1 parameter is set to None and the Community Action 2 parameter is set to None.

Damping Name

(dampingName)

The Damping Name parameter specifies the damping name for the route damping profile. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR. The range is 1 to 32 characters long. The characters must be 7-bit ASCII characters, excluding double quotation marks. Double quotation marks are used to delimit the start and end of a string that contain spaces.

Route damping controls route flap. Route flapping occurs when an advertised route between devices alternates between two paths due to network problems.

Damping Profile Name

(damping)

The Damping Profile Name parameter specifies the damping profile to be assigned to routes that match a routing policy statement entry. The name must already be created using the Damping Name parameter. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR.

Default Action

(action)

The Default Action parameter specifies what action, if any, should be taken for routes that do not match a specific routing policy statement entry. Table [80-5](#) describes the parameter options.

Table 80-5 Default Action parameter

Option	Option description	Dependencies
None (default)	No action is defined for the route. The routing protocol defaults or route configuration settings are used to determine the action performed on the route, instead of the routing policy.	—
Accept	Routes that match are accepted and propagated.	
Reject	Routes that match are rejected and not propagated.	
Next Entry	Policy evaluation continues with the next policy statement entry within the same routing policy statement.	
Next Policy	Policy evaluation continues with the next routing policy following the current routing policy.	

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

(**displayedName**)

See the [Displayed Name](#) parameter in section 112.1.

Entry ID

(**entryId**)

The Entry ID parameter specifies the unique instance of a routing policy statement entry within a routing policy statement. Table 80-6 lists the ranges for different device types. There is no default.

Table 80-6 Entry ID parameter

Device	Range
7450 ESS, 7750 SR, and 7710 SR	1 to 4 294 967 295
Telco	1 to 65 535

Alcatel-Lucent recommends that you stagger the incremental value of the parameter, for example, set the parameter to 10 for the first routing policy entry, 20 for the second routing policy entry, and so on. This allows for the insertion of new routing policy entries without renumbering the entire set.

Routing policy entries are compared against incoming packets. When a match is found, the action specified using the Action parameter occurs. If no action is specified, the action specified using the Default Action parameter occurs. If no action is specified, the default action for the protocol or the route configuration occurs. For this reason, Alcatel-Lucent recommends that you sequence the routing policy entries to ensure the first entry is the most explicit and the last entry is the least explicit.

Half Life

(halfLife)

The Half Life parameter specifies the time required for a route to remain stable in order for the figure of merit value to be reduced by one half. The range is 0 to 45 min. The default is 0 min.

The figure of merit value is a value added to a route each time that the route flaps. For example, if the Half Life parameter is set to 6, and the route remains stable for 6 min. the new figure of merit value is 3 min. After another 3 min. pass and the route remains stable, the new figure of merit value is 1.5 min.

When the figure of merit value is less than the Reuse parameter value, the route is considered valid and can be reused or included in route advertisements.

IGMP Host Prefix List Name

(igmpHostPrefixList)

The IGMP Host Prefix List Name parameter specifies the name of the prefix list that is used as a match criterion for the IGMP host IP address. The value of the object is an empty string if it has not been set. The range is 0 to 32 characters.

Instance ID

(instanceIndex)

The Instance ID parameter specifies an OSPF route instance. The parameter can be used to identify routes installed by that instance and advertised to neighboring nodes. If you do not specify an instance ID, only routes installed by the base routing instance are advertised to neighboring nodes.

You can configure the Instance ID parameter when the [Protocol](#) parameter is set to OSPF. The range is 0 to 31. The default is 0.

Interface

(multicastRedirectionInterface)

The Interface parameter specifies the interface index of the interface to which IGMP multicast traffic is to be redirected. Click on the Select button to list and choose an existing local network interface, VPRN L3 access interface, or IES L3 access interface. The parameter is configurable only when creating a local routing policy statement.

Interface Name

(interfaceName)

The Interface Name parameter specifies the interface name for the route instance. The range is 0 to 31.

IS-IS External Route

(isisEnabled)

The IS-IS External Route parameter specifies whether IS-IS external routes are used as match criteria for a routing policy statement entry. Table 80-7 describes the parameter options.

Table 80-7 IS-IS External Route parameter

Option	Option description	Dependencies
true	IS-IS external routes are used as match criteria.	The external and internal routes as specified by the Level parameter are considered as match criteria.
false (default)	IS-IS external routes are not used as match criteria.	—

IS-IS external routes have a higher preference cost than IS-IS internal routes.

Level

(isisLevel)

The Level parameter specifies the IS-IS route level to use as a match criterion for the routing policy statement entry. Table 80-8 describes the parameter options.

Table 80-8 Level parameter

Option	Option description
0 (default)	IS-IS is not used as a match criterion.
1	IS-IS level 1 routes are used as a match criterion.
2	IS-IS level 2 routes are used as a match criterion.

Local Preference Set

(localPreferenceSet)

The Local Preference Set parameter specifies whether to allow the assignment of a BGP local preference value to routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to the Accept, Next Entry, or Next Policy option. The options are:

- true
- false (default)

You can configure the BGP Local Preference parameter when the parameter is set to the true option.

Mask

(mask)

The Mask parameter specifies the mask for the IP address in the prefix list entry. The range is 0 to 128. The default is 32.

Max Suppression

(maxSuppression)

The Max Suppression parameter specifies the maximum time that a route can remain suppressed after the figure of merit value for the route is exceeded. The range is 0 to 720 min. The default is 0 min, indicating suppression is disabled.

A route is considered valid or suppressed based on the Suppress and Reuse parameters.

Metric Action

(metricAction)

The Metric Action parameter specifies the metric action performed on routes that match the routing policy statement entry. The parameter is configurable when the Default Action parameter is set to the Accept, Next Entry, or Next Policy option. Table 80-9 describes the parameter options.

Table 80-9 Metric Action parameter

Option	Option description	Dependencies
None (default)	No metric action is performed on matching routes.	—
Add	Add the metric value defined in the Metric Value parameter to the route metric value.	
Subtract	Subtract the metric value defined in the Metric Value parameter from the route metric value.	
Set	Replace the existing metric value of the route with the metric value defined in the Metric Value parameter.	

Metric Value

(metricValue)

The Metric Value parameter specifies a metric value modifier that is added to, subtracted from, or replaces the metric value for routes that meet a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to the Accept, Next Entry, or Next Policy option and the Metric Action parameter is set to an option other than None. The range is 0 to 4 294 967 295. The default is 0.

Multicast Group Prefix List Name

(mcastGroupPrefixList)

The Multicast Group Prefix List Name parameter specifies the name of the prefix list that is used as a match criterion for the multicast group address. The range is 0 to 32 characters.

Multicast Source IP Address

(mcastSourceIpAddress)

The Multicast Source IP Address parameter specifies the IP address of the multicast source router. This parameter is used by multicast protocols such as PIM and IGMP. Specify an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format. The default is 0.0.0.0, which means that the IP address is unconfigured.

Neighbor IP Address

(neighborIpAddress)

The Neighbor IP Address parameter specifies the neighbor IP address that is used as a match criterion for a routing policy statement entry. Specify an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format. The default is 0.0.0.0, which means that the IP address is unconfigured.

Neighbor Prefix List Name

(neighborPrefixList)

The Neighbor Prefix List Name parameter specifies the neighbor prefix list name that is used as a match criterion for a routing policy statement entry. The name must already be created using the Prefix List Name parameter. Specify a name of up to 32 characters.

Next Hop

(nextHop)

The Next Hop parameter specifies the assignment of the IP address of the next hop for routes that match the routing policy statement entry. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR and the Use Next Hop parameter is enabled. The default is 0.0.0.0.

Next Hop Self

(nextHopSelf)

The Next Hop Self parameter specifies whether to advertise a next-hop IP address even if a third-party next hop is available to routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to Accept, Next Entry, or Next Policy on the 7450 ESS in mixed mode, or the 7750 SR. The options are:

- true
- false (default)

When the parameter is set to false, you can configure the Use Next Hop parameter. You cannot configure the parameter when the Use Next Hop parameter is enabled.

Next Hop Type

(nextHopType)

The Next Hop Type parameter specifies the type of next hop. The parameter is configurable when the Default Action parameter is set to Accept, Next Policy, or Next Entry. The options are:

- IPv4 (default)
- IPv6

No Route Tag

(noRouteTag)

The No Route Tag parameter specifies whether matches are allowed on untagged routes. The parameter is disabled by default, meaning that matches are not allowed on untagged routes.

This parameter is available on the on the 7705 SAR 4.0 R1 and later.

Origin

(origin)

The Origin parameter specifies the type of BGP route that is considered as a match criterion for a routing policy statement entry. The parameter is configurable on the 7450 ESS in mixed mode, or the 7750 SR. Table [80-10](#) describes the parameter options.

Table 80-10 Origin parameter

Option	Option description	Dependencies
None (default)	BGP routes are not used as a match criterion.	—
IGP	Only IGP BGP routes that originate within the AS are used as a match criterion.	—
EGP	Only EGP BGP routes that originate in another AS are used as a match criterion.	—
Incomplete	BGP routes that are not learned from IGP or EGP are used as a match criterion.	Use this option to allow match criteria for BGP routes learned using another protocol.
Any	Any BGP routes that originate in another AS are used as a match criterion.	—
AAA	Only subscriber host routes assigned via RADIUS can be exported to BGP.	You cannot specify these options on pre-9.0 nodes.
DHCP	Only subscriber host routes assigned via a DHCP server can be exported to BGP.	
LUDB	Only subscriber host routes assigned via a local user database can be exported to BGP.	

OSPF Area

(area)

The OSPF Area parameter specifies the IP address of an OSPF area that is used as a match criterion for a routing policy statement entry. The parameter is configurable when the OSPF Area Set parameter is set to true. The default is 0.0.0.0.

All OSPF internal and external routes that use the parameter are matched. Only export routing policies use the parameter.

OSPF Area Set

(areaSet)

The OSPF Area Set parameter specifies whether to use the OSPF Area parameter as a match criterion for a routing policy statement entry. The options are:

- true
- false (default)

OSPF, RIP, or ISIS Tag (Hex)

(tag)

The OSPF, RIP, or ISIS Tag (Hex) parameter specifies the hexadecimal tag that is added to OSPF, RIP, or ISIS routes that meet the match criterion specified in a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to Accept, Next Policy, or Next Entry. The range is a hexadecimal string from 0x0 to 0xFFFFFFFF.

For OSPF and ISIS routes, all four octets are used. For RIP routes, only the two most significant octets are used.

OSPF Route Type

(ospfRouteType)

The OSPF Route Type parameter specifies:

- the type of OSPF LSAs that are used as a match criterion for a routing policy statement entry
- assigns the type of OSPF LSAs to routes that match a routing policy statement entry

Table 80-11 describes the parameter options.

Table 80-11 OSPF Route Type parameter

Option	Option description	Dependencies
0 (default)	OSPF link state types are not used as a match criterion, or no link state types are assigned to OSPF routes that meet the match criterion.	You can specify the assignment of LSA types when the Default Action parameter is set to Accept, Next Entry, or Next Policy.
1	Specifies that: <ul style="list-style-type: none"> • type 1 OSPF link state advertisements are used as a match criteria. • type 1 OSPF link state advertisements are assigned to routes that meet the match criteria 	
2	Specifies that: <ul style="list-style-type: none"> • type 2 OSPF link state advertisements are used as a match criteria. • type 2 OSPF link state advertisements are assigned to routes that meet the match criteria 	

Path Name

(pathName)

The Path Name parameter specifies the path name for the route policy AS path regular expression. The range is 1 to 32 characters. The characters must be 7-bit ASCII characters, excluding double quotes. Double quotes are used to delimit the start and end of a string that contains spaces.

Policy Statement Name

(policyStatementName)

The Policy Statement Name parameter specifies the name of the routing action policy. The range is 1 to 32 characters.

Prefix

(prefix)

The Prefix parameter specifies the IP address for a prefix list entry. Specify an IPv4 address in dotted-decimal format, or an IPv6 address in colon-hexadecimal format.

Prefix List 1

(prefixList1)

The Prefix List 1 and Prefix List 2 to 5 parameters specify the prefix list used as a from criteria to match routing policy statement entries. The name must already be created using the Prefix List Name parameter.

Prefix List 2

(prefixList2)

See the [Prefix List 1](#) in this section.

Prefix List 3

(prefixList3)

See the [Prefix List 1](#) in this section.

Prefix List 4

(prefixList4)

See the [Prefix List 1](#) in this section.

Prefix List 5

(prefixList5)

See the [Prefix List 1](#) in this section.

Prefix List Name

(prefixListName)

The Prefix List Name parameter specifies the name of a prefix list to use in a routing policy statement entry. The range is 1 to 32 characters. The characters must be 7-bit ASCII characters, excluding double quotation marks. Double quotation marks delimit the start and end of a string that contains spaces.

Prefix List Flag

(prefixListFlag)

The Prefix List Flag parameter specifies whether to match any, all, or none of the entries in the prefix list. The options are:

- Any (default)
- All
- None

Prepend Count

(prependCount)

The Prepend Count parameter specifies the number of times that a BGP AS number is added to routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to the Accept, Next Entry, or Next Policy option. The range is 0 to 50. The default is 0, which means AS numbers are not added to route AS paths.

Use the BGP AS Prepend number and Prepend Count parameters to specify the AS number and how many times the AS numbers are added to the AS path attributes of routes.

Protocol

(protocol)

The Protocol parameter specifies the routing protocol to be used as a match criterion for a routing policy statement entry. Not all of the options are supported on every node type. The options for the From Criteria and the To Criteria are:

- | | |
|-------------|--------------|
| • None | • IGMP |
| • Direct | • PIM |
| • Static | • OSPFv3 |
| • BGP | • LDP |
| • IS-IS | • Subscriber |
| • OSPF | • MLD |
| • RIP | • VPN Leak |
| • Aggregate | • NAT |
| • BGP-VPN | |

Regular Expression

(regularExpression)

The Regular Expression parameter specifies the regular expression for the route policy AS path. The range is 1 to 255 characters. The characters must be 7-bit ASCII characters, excluding double quotes. Double quotes are used to delimit the start and end of a string that contains spaces.

Regular expressions are strings that are used to specify match criteria for:

- an AS path string, for example, “100 200 300”
- a community string, for example, “100:200”, where 100 is the AS number and 200 is the community value

Each regular expression is comprised of terms and operators. Table 80-12 describes the terms and operators.

Table 80-12 AS path regular expression terms and operators

Type of term or operator	Use	Example
Terms		
Elementary	An AS number	200
Range	Two elementary terms that are separated by a -	200-300
Wildcard	A dot (.) to match any elementary term	.
Regular	Expression in round brackets	(200)
Set of choices	Square brackets to specify a set of elementary or range terms	[100-300 400]
Operators		
	Pipe to match terms on alternate sides	—
*	Matches multiple occurrences of the term	
—	Underscore matches one or no occurrences of the term	
+	Matches one or more occurrences of the term	
{m,n}	Matches the least (m) and most (n) occurrences of the term	
^	Matches the beginning of the community string	
\$	Matches the end of the community string	

Reuse

(reuse)

The Reuse parameter specifies whether to consider a route valid, based on a comparison with the figure of merit value for the route. The parameter must be less than the Suppress parameter. The range is 1 to 20 000. The default is 0.

When the figure of merit value is less than the Reuse parameter value, the route is considered valid and is included in route advertisements.

Route Origin

(origin)

The Route Origin parameter specifies the assignment of a BGP route type to BGP routes that meet the match criterion specified in a routing policy statement entry. Table 80-13 describes the parameter options.

Table 80-13 Route Origin parameter

Option	Option description	Dependencies
None (default)	BGP route types are not assigned to BGP routes that match the route criterion specified in the routing policy statement entry.	You can specify the assignment of these BGP route types using the Route Origin parameter when the Default Action parameter is set to the Accept option.
IGP	Routes that match the route criterion are set as IGP BGP routes.	
EGP	Routes that match the route criterion are set as EGP BGP routes.	
Incomplete	—	—

Route Preference

(preference)

The Route Preference parameter specifies the route preference value assigned to a route that matches a routing policy statement entry. The parameter value is used by the routing table manager to assign preferences to the route, which override the routing preferences applied to the routes by the individual protocols. The range is 1 to 255. The default is 0, which indicates that no route preference is set for matching routes.

Static Route Tag

(staticRouteTag)

The Static Route Tag parameter specifies an identifier for the static route. The range is 0 to 4 294 967 295. The default is 0, which means that the identifier is unspecified.

Suppress

(suppress)

The Suppress parameter specifies whether a route is considered valid based on the number of times that the route has flapped. Route flapping occurs when an advertised route between devices alternates back and forth between two paths due to network problems. The range is 1 to 20 000. The default is 0.

The parameter must be greater than the Reuse parameter. When the figure of merit value is greater than the Suppress parameter value, the route is not considered valid and is removed from route advertisements.

Through Length

(throughLength)

The Through Length parameter specifies the prefix list matching criterion for the mask value of the IP address. The parameter value must be greater than or equal to the Mask parameter. The parameter is configurable when the Type parameter is set to the Through or Range options. The range is *Mask parameter value* to 32. The default is 0.

Triggered Re-evaluation of Route Policies

(manualPolicyTrigger)

The Triggered Re-evaluation of Route Policies parameter specifies whether to trigger a route policy re-evaluation. Table 80-14 describes the parameter options.

Table 80-14 Triggered Re-evaluation of Route Policies parameter

Option	Option description	Dependencies
true	When a triggered re-evaluation is enabled, any routing policy change or policy assignment change within the protocol does not take effect until the protocol is reset or a clear command is issued to re-evaluate the route policy.	You must reset the applicable protocol before any changes to the routing policy take effect.
false (default)	When changes to a routing policy are saved, the change is effective immediately. This should be used with caution, because changes that affect the routing across a network, for example, changes for all BGP peers, may cause routing update storms in the network. Routing storms may cause potential impacts on network performance when the routes are updated.	—

Type

(type)

The Type parameter specifies how the Prefix and Mask parameters are matched in the prefix entry list. Table 80-15 describes the parameter options.

Table 80-15 Type parameter

Option	Option description	Dependencies
Exact (default)	The prefix list entry only matches routes with the exact values specified in the Prefix and Mask parameters.	—
Longer	The prefix list entry only matches routes with the exact value specified in the Prefix parameter, and a mask greater than the Mask parameter value.	—

(1 of 2)

Option	Option description	Dependencies
Through	The prefix list entry only matches routes with the exact value specified in the Prefix parameter, and a mask in the range specified in the Through Length parameter.	You can configure the Through Length parameter to a value between the Mask parameter value and 32.
Range	The prefix list entry only matches routes with the exact value specified in the Prefix parameter, and a mask in the range specified in the Begin Length and Through Length parameters.	You can configure the Begin Length and Through Length parameters to a value between the Mask parameter value and 32.

(2 of 2)

Use Next Hop

(isNextHopEnabled)

The Use Next Hop parameter specifies whether to allow the assignment of an IP address as the next hop to routes that match a routing policy statement entry. The parameter is configurable when the Default Action parameter is set to the Accept, Next Entry, or Next Policy option. The options are:

- Enabled
- Disabled (default)

When the parameter is enabled and the Next Hop Self parameter is set to false, you can specify the IP address using the Next Hop parameter.

Value

(value)

The Value parameter specifies the group value associated with this SRLG group. It is a bit mask value that uniquely identifies the group, and this value is unique within a virtual router instance. The range is 0 to 4,294,967,295. There is no default value.

View the newly created Policy Statement

The View the newly created Policy Statement parameter specifies whether the properties form for the policy is displayed when the current configuration form is closed. The options are:

- Enabled
- Disabled (default)

81 — VRRP parameters

81.1 VRRP parameters 81-2

81.1 VRRP parameters

This chapter describes the parameters on the VRRP Policy form and child forms.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Delta in Use Limit

(deltaInUseLimit)

The Delta in Use Limit parameter specifies a value that is subtracted from the current in-use priority for all VRRP instances to which the policy is applied. Multiple delta priority events can apply simultaneously, creating a dynamic priority value. The base priority for the instance minus the sum of the delta values yields the actual priority value in use.

The range is 1 to 254. The default is 1, which prevents delta priority events from operationally disabling the VRRP instance.

Description

See the [Description](#) parameter in section 112.1.

Hold Clear (seconds)

(holdClear)

The Hold Clear (seconds) parameter specifies the amount of time by which the effect of a cleared event on the associated VRRP instance is delayed for a VRRP priority-control event.

The Hold Clear (seconds) time is used to prevent black hole conditions in the time gap between when a VRRP instance advertises itself as a master and other conditions associated with the cleared event have had a chance to enter a forwarding state. The range is 0 to 86400 s. The default is 0 s.

Hold Set (seconds)

(holdSet)

The Hold Set (seconds) parameter specifies the amount of time that must pass before the set state for a VRRP priority-control event can transition to the cleared state. The purpose of this parameter is to dampen flapping event, in which the event continually transitions between clear and set. The Hold Set (seconds) value is loaded into a hold set timer that prevents a set event from transitioning to the cleared state until it expires. The range is 0 to 86400 s. The default is 0 s.

Hop Address

(hopAddress)

The Hop Address parameter specifies an allowed next hop IPv4 or IPv6 address to match the IP route prefix for a route unknown priority-control event.

If the Hop Address does not match one of the defined IP addresses, the match is considered unsuccessful and the route unknown event transitions to the set state.

The Hop Address parameter is optional. If no Hop Address parameter is configured, the comparison between the RTM prefix return and the RouteIP route prefix is not included in the next hop information. The default is 0.0.0.0 for IPv4 hop addresses. There is no default for IPv6 hop addresses.

ID

See the [ID](#) parameter in section [112.1](#).

Interface Name

(interfaceName)

The Interface Name parameter specifies a name you can give to the interface you are monitoring, provided that the associated [IP Address](#) parameter is a Link Local Address. You can specify up to 32 characters. There is no default.

Interval for Echo Request (seconds)

(interval)

The Interval for Echo Request (seconds) parameter specifies the amount of time that expires before the next directed ICMP echo request message is sent to the host IP address. The range is 1 to 60 s. The default is 1 s.

IP Address

(ipAddress)

The IP Address parameter specifies the IPv4 or IPv6 address of the host at which connectivity is monitored. The host address receives a continuous ICMP echo request (ping) probe from the host unreachable priority event. If a ping fails, the event is considered to be set. If a ping is successful, the event is considered to be clear. The default is 0.0.0.0 for IPv4 host unreachable events. There is no default for IPv6 host unreachable events.

LAG ID

(lagId)

The LAG ID parameter specifies the unique identifier of the LAG. The range is 1 to 64. The default is 0, which means that the parameter is not configured.

Less Specific

(lessSpecific)

The Less Specific parameter specifies whether to shorten the search parameters for the IP route prefix specified in the route-unknown priority event. Specifying a less-specific allows a CIDR shortest match hit on a route prefix that contains the IP route prefix. The options are:

- false (default)
- true

Limit of Echo Request Failures

(dropCount)

The Limit of Echo Request Failures parameter specifies the number of consecutively sent ICMP echo request messages that must fail before the host unreachable priority-control event is set. The range is from 1 to 60 s. The default is 3.

Mask

(mask)

The Mask parameter specifies the IP address subnet mask in dotted-decimal format or as a 32-bit integer. The range is from 0 to 32. The default is 24.

Number of Ports Down

(numberOfPortsDown)

The Number of Ports Down parameter specifies the number of ports that must be in an operationally down state before the event can be set. When all ports enter into the operational up state, the event is considered to be clear. As ports enter the operational up state, any previous set threshold that represents more down ports is considered cleared, and the event is considered to be set. The range is 1 to 8. The default is 0.

Priority

(priority)

The Priority parameter specifies the effect that the set event has on the VRRP instance in-use priority. When the event is set, the priority level is determined by how you configure the Priority Type. The range is 0 to 254. The default is 0. See the [“Priority Type”](#).

Priority Type

(priorityType)

The Priority Type parameter specifies how the set event affects the in-use priority for the VRRP instance. Table [81-1](#) describes the parameter options.

Table 81-1 Priority Type parameter

Option	Option description
Delta (default)	Subtracts a value from the current in-use priority for all VRRP instances to which the policy is applied.
Explicit	Defines the in-use priority for the VRRP instance. The value is not affected by the delta in-use priority limit.

Protocol

(protocol)

The Protocol parameter specifies the source protocol from which the installed route must be populated in the route unknown policy for a VRRP instance. There is no default. The options are:

- BGP-VPN
- RIP
- OSPF
- Static
- IS-IS
- BGP

Timeout for Echo Request (seconds)

(timeout)

The Timeout for Echo Request parameter (seconds) specifies the amount of time that must expire before the far-end IP host is considered unresponsive to an outstanding ICMP echo request message. The range is from 1 to 60 s. The default is 1 s.

82 – MPLS parameters

82.1 MPLS parameters 82-2

82.1 MPLS parameters

This chapter describes the parameters on the Admin Group (MPLS) Policy, Shared Risk Link Group Policy, Static Configuration for SRLGs Policy, and LSP Template MVPN Policy creation forms and child forms.

Backup Type

(fastRerouteBackupType)

The Backup Type parameter specifies the type of backup route associated with a failed link or LSP. Table 82-1 describes the parameter options.

Table 82-1 Backup Type parameter

Option	Option description	Dependencies
One To One	Specifies a backup LSP that intersects the original LSP downstream of the point of link or node failure. A separate backup LSP is established for each LSP that is backed up.	The parameter is configurable when the Fast Reroute parameter is set to true.
Many To One	Specifies that a single backup LSP is used to backup multiple original LSPs. This type of LSP is often called a bypass tunnel.	

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Enable CSPF

(cspfEnabled)

The Enable CSPF parameter specifies the CSPF routing algorithm to find a path that satisfies the constraints for the LSP. The constraints associated with the LSP can be related to bandwidth, class of service, or the number of path hops. The options are:

- false (default)
- true

CSPF also calculates detour routes when you set the [Fast Reroute](#) parameter to true. CSPF is not implemented if you define each hop in the LSP.

Enable TE Metric

(enableTeMetric)

The Enable TE Metric parameter specifies whether the TE metric is used for the LSP path computation by CSPF. The options are:

- true
- false (default)

Fast Reroute

(fastRerouteEnabled)

The Fast Reroute parameter specifies a pre-computed detour LSP from each node in the path of the LSP. In case of failure of a link or LSP between two nodes, traffic is immediately rerouted on the pre-computed detour LSP. The immediate reroute of the traffic avoids packet-loss. The options are:

- false
- true (default)

Fast reroute is available only for the primary path. The LSP transit hops do not require configuration. The ingress router signals intermediate routers using RSVP to set up the detour routes. You must set the Enable CSPF parameter to true when you set the Fast Reroute parameter to true.

Hop Limit

(hopLimit)

The Hop Limit parameter specifies the maximum number of hops for the LSP path. An LSP is not set up if the hop limit is exceeded. This parameter controls the number of loose hops associated with MPLS paths. If there is an associated Inherit Value parameter, then the Hop Limit parameter is configurable only when you set the Inherit Value parameter to Disabled. The range is 2 to 255. The default is 255.

Make before Break

(adaptive)

The Make before Break parameter specifies the traffic rerouting method when you move traffic between primary and secondary LSP paths. The the make-before-break functionality ensures that the transition to the new path does not cause any traffic disruption.

For example, when the parameters of an already-established LSP are changed due to a user configuration modification, when the parameter is set to true the resources of the existing LSP are not released until a new path with the same LSP ID is established and passing the traffic seamlessly handed over from the old LSP.

When enabled for the LSP, the make-before-break functionality is implemented for the primary path and all the secondary paths of the LSP. The options are:

- false
- true (default)

Record Actual Path

(record)

The Record Actual Path parameter specifies if the labels at each node are recorded and displayed for the LSP path, to indicate the hops in the LSP path. The options are:

- Disabled (default)
- Enabled

Record Label

(recordLabel)

The Record Label parameter enables the recording of all LSP labels at each device that an LSP path traverses. The options are:

- Enabled
- Disabled (default)

Reserved Bandwidth

(bandwidth)

The Reserved Bandwidth parameter specifies the minimum amount of the MPLS path bandwidth to reserve for the LSP. The parameter is configurable when the Auto Select Hop-less Path parameter is enabled. The range is 0 to 100 00. A value of 0 indicates that the parameter is not configured.

Retry Limit

(retryLimit)

The Retry Limit parameter specifies how many attempts are made to re-establish the LSP after an LSP failure. The range is 1 to 10 000. The default is 0, indicating an infinite number of retries.

Retry Timer (seconds)

(retryTimer)

The Retry Timer (seconds) parameter specifies the time before LSP re-establishment attempts after an LSP failure. The range is 1 to 600. The default is 30.

Value

(value)

The Value parameter specifies a unique value to use for the created administrative group in 32 bit mask format. The value is used by MPLS interfaces to advertise administrative group associations using CSPF. The value must be identical across all routers within a single domain. The range is 0 to 31. The default is 0.

83 – Auto Tunnels parameters

83.1 Auto Tunnels parameters 83-2

83.1 Auto Tunnels parameters

This chapter describes the parameters on the Manage Auto Tunnel Rules and Manage Rule-Based Groups forms and child forms.

Administrative

See the [Administrative State](#) parameter in section 112.1.

Auto-Rule Execution

(adminState)

The Auto-Rule Execution parameter specifies whether a rule is automatically applied to an object that is added to the rule-based group. The options are:

- Enabled
- Disabled

Class Forwarding Capability

(classForwardingEnabled)

The Class Forwarding Capability parameter specifies whether forwarding a service packet over the SDP, based on the class of service of the packet is enabled. The options are:

- On
- Off (default)

Description

See the [Description](#) parameter in section 112.1.

Enable LDP-over-RSVP

(ldpOverRsvpEnabled)

The Enable LDP-over-RSVP parameter specifies whether LDP over RSVP is enabled on the routing instance. When the LDP over RSVP parameter is enabled, the 5620 SAM creates a T-LDP session between two tunnel endpoints and associates LSPs to the T-LDP. A maximum of 4 LSPs can be associated with a T-LDP. When a rule or a managed tunnel element is deleted, the rule-created LSPs are no longer associated with the T-LDP, but the T-LDP is not deleted. The options are:

- false (default)
- true

Group Name

See the [Name](#) parameter in section 112.1.

Name

See the [Name](#) parameter in section 112.1.

Naming Format

(namingFormat)

The Naming Format parameter specifies the naming format for the generated tunnel elements. System generated naming format configuration is similar to other naming formats within 5620 SAM. The user specified naming format allows the operator to attach a prefix to the tunnel ID to identify the tunnel. For example, add LSP to all LSP tunnels to distinguish them from SDP tunnels. The options are:

- System Generated (default)
- User Specified

Order

The Order parameter specifies whether the group is ordered or unordered. The options are:

- unordered (default)
- ordered

Template Versions

(templateVersionsPreference)

The Template Versions parameter specifies which version of the template is to be used for the rule. This option is necessary since a template can be updated after it has been applied to a rule. Rule configuration provides two options, it is recommended that you use the version initially assigned to the rule. If you choose an updated version, you need to ensure that the version and the rule are compatible. The options are:

- Apply Version Initially Assigned (default)
- Apply Latest Version

Tunnel Creation Pacing Interval (seconds)

(pacingInterval)

The Tunnel Creation Pacing Interval parameter specifies the time delay between tunnel creations. A delay allows the network time to converge. The range is 0 to 300 seconds. When the value is set to 0, no delay is set.

Tunnel Type

(tunnelType)

The Tunnel Type parameter specifies the type of service tunnel to create. The options are:

- SDP (default)
- RSVP-LSP

Underlying Transport

(underlyingTransport)

The Underlying Transport parameter specifies the underlying transport protocol for the service tunnel. Table 83-1 describes the parameter options.

Table 83-1 Underlying Transport parameter

Option	Option description	Dependencies
GRE	Specifies a service tunnel that uses GRE encapsulation	—
MPLS:LDP	Specifies a service tunnel that uses MPLS:LDP encapsulation	
MPLS:BGP	Specifies a service tunnel that uses MPLS:BGP encapsulation	
RSVP-LSP	Specifies a service tunnel that uses RSVP-LSP encapsulation	
Mixed LSP Mode	Specifies a service tunnel that uses either RSVP-LSP or MPLS-LDP encapsulation.	

See the [Transport Type](#) parameter for more information about the MPLS:BGP and Mixed LSP Mode selections.

User Specified Naming Prefix

(userSpecifiedNamingPrefix)

The User Specified Naming Prefix parameter specifies the naming prefix when the [Naming Format](#) parameter is set to User Specified. The range is 0 to 20 characters.

View the newly created tunnel

The View the newly created Dynamic LSP parameter specifies whether you want to view the configuration information for the newly created LSP. The Dynamic LSP child form displays the service tunnel configuration details. The options are:

- Enabled
- Disabled (default)

84 — RADIUS Based Accounting parameters

84.1 RADIUS Based Accounting parameters 84-2

84.1 RADIUS Based Accounting parameters

This chapter describes the parameters on the RADIUS Accounting Policy form and child forms.

Access Algorithm

(accessAlgorithm)

The Access Algorithm parameter specifies the algorithm that is used to select a RADIUS server from the list of configured servers. The options are:

- Direct (default)
- Round-robin

Calling Station ID Type

(callingStationIdType)

The Calling Station ID Type parameter specifies the string for the RADIUS Calling Station ID parameter when included in RADIUS accounting request messages. The Calling Station ID Type parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter. The options are:

- SAP String (default)
- MAC Address
- SAP ID
- Remote ID

Enable

The Enable parameter specifies whether the interval for updating subscriber host information is enabled. The options are:

- enabled
- disabled (default)

When the Enable parameter is set to disabled, the subscriber host information is not updated. When the parameter is set to enabled, you can configure the [Value \(minutes\)](#) parameter.

Host Accounting Message

(hostAccountingMessage)

The Host Accounting Message parameter specifies the kind of accounting information that is forwarded to a RADIUS server. Table [84-1](#) describes the parameter options.

Table 84-1 Host Accounting Message parameter

Option	Description
SLA Only (default)	Specifies that only per-SLA accounting information is sent; on Release 7.0 or 8.0 NEs, is equivalent to disabled host accounting
Host And SLA	Specifies that per-host and per-SLA accounting information is sent; on Release 7.0 or 8.0 NEs, is equivalent to enabled host accounting
Host Only	Specifies that only per-host accounting information is sent; this information includes interim updates Deployable only to a 7450 ESS in mixed mode, 7710 SR, or 7750 SR at Release 9.0 or later; deployment to NEs at earlier releases has no effect

Port

(port)

The Port parameter specifies the UDP port of the RADIUS server that is contacted. The range is 1 to 65 535. The default is 1813.

Port Binary Specification

(nasPortBitspec)

The Port Binary Specification parameter specifies the value of the RADIUS NAS Port parameter when included in RADIUS accounting request messages. The Port Binary Specification parameter is configurable when the NAS Port option is enabled for the RADIUS Attributes parameter. If fewer than 32 bits are specified, the least significant bits are used, and the omitted higher bits are set to zero. The range is 1 to 255 characters, or 1 to 32 bits. There is no default.

Port Prefix String

(nasPortPrefixString)

The Port Prefix String parameter specifies the string to be added as a prefix to the NAS Port ID option of the RADIUS Attributes parameter when included in RADIUS accounting requests. The range is 0 to 8. The prefix is configurable when the Port Prefix Type parameter is set to User String.

Port Prefix Type

(nasPortPrefixType)

The Port Prefix Type parameter specifies the prefix type to be added to the NAS Port ID option of the RADIUS Attributes parameter when included in RADIUS accounting requests. The options are:

- None (default)
- User String

Port Suffix Type

(nasPortSuffixType)

The Port Suffix Type parameter specifies the suffix type to be added to the NAS Port ID option of the RADIUS Attributes parameter when included in RADIUS accounting requests. The options are:

- None (default)
- Circuit Id
- Remote Id

Port Type

(nasPortTypeType)

The Port Type parameter specifies the value of the RADIUS NAS Port Type parameter when included in RADIUS accounting request messages. The parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter. The options are:

- Standard (default)
- Config

Port Type Value

(nasPortTypeValue)

The Port Type Value parameter specifies the value of the RADIUS NAS Port Type parameter when included in RADIUS accounting request messages. The parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the Port Type parameter is set to Config. The range is 0 to 255. The default is 0.

RADIUS Attributes

(radiusAttributes)

The RADIUS Attributes parameter specifies the RADIUS attributes that are included in RADIUS accounting requests. Table 84-2 describes the parameter options.

Table 84-2 RADIUS Attributes parameter

Option	Description
Subscriber Profile (subscrProfile)	The subscriber profile is included in the request.
NAS Port ID (nasPortID)	The NAS port ID is included in the request.
Circuit ID (circuitID)	The circuit ID is included in the request.
Framed IP Mask (framedIPMask)	The framed IP mask is included in the request.

(1 of 2)

Option	Description
SLA Profile (slaProfile)	The SLA profile is included in the request.
User Name (userName)	The username is included in the request.
Tunnel Server Attributes	The tunnel server attributes are included in the request.
NAS Port Type	The NAS port type is included in the request.
Accounting Authentication	The accounting authentication is included in the request.
NAS ID (nasID)	The NAS ID is included in the request.
Remote ID (remoteID)	The remote server ID is included in the request.
Subscriber ID (subscriberID)	The subscriber ID is included in the request.
Framed IP Address (framedIPAddr)	The framed IP address is included in the request.
Calling Station ID (callingStationID)	The calling station ID is included in the request.
Called Station ID	The called station ID is included in the request.
MAC Address	The MAC address is included in the request.
Accounting Delay Time	The accounting delay time is included in the request.
NAS Port	The NAS port is included in the request.
NAT Port Range	The NAT port range is included in the request.

(2 of 2)

Retry Attempts

(retryAttempts)

The Retry Attempts parameter specifies the number of times an attempt is made to send an accounting request to the same RADIUS server. The range is 1 to 10. The default is 3.

Router Instance

(routerType)

The Router Instance parameter specifies the type of virtual router for the RADIUS-based accounting policy. Table 84-3 describes the options.

Table 84-3 Router Instance parameter

Option	Description	Dependencies
Matched (default)	Base and Management router instances are the same.	—
VPRN	A VPRN service that is used as the routing instance for the RADIUS accounting policy.	This option is not available for the 7450 ESS in a local policy.

(1 of 2)

Option	Description	Dependencies
Base	The routing table configuration of the router is the routing instance for the RADIUS accounting policy.	—
Management	The bof configuration of the router is the routing instance for the RADIUS accounting policy.	—

(2 of 2)

Secret Name

(secret)

The Secret name parameter specifies the secret key associated with the RADIUS server. The range is 1 to 20 characters.

Server IP Address

(address)

The Server IP Address specifies the IP address of the RADIUS server. Each RADIUS server must have its own unique IP address. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Session ID Format

(sessionIDFormat)

The Session ID Format parameter specifies the format for the acct-session-id attribute used in RADIUS accounting requests. The options are:

- Description (default)
- Number

Source Address

(sourceAddress)

The Source Address parameter specifies the source IP address of a RADIUS packet for DHCP-RADIUS accounting. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Timeout (seconds)

(timeoutSeconds)

The Timeout (seconds) parameter specifies the time that elapses before an attempt is made to resend an accounting request to the same RADIUS server. The range is 1 to 90. The default is 5.

Use Standard Accounting Attribute

(useStdAcctAttrib)

The Use Standard Accounting Attribute parameter specifies whether standard accounting attributes or vendor-specific attributes are used. If the parameter is enabled, standard accounting attributes are used. When the parameter is disabled, vendor-specific accounting attributes are used. The options are:

- Enabled
- Disabled (default)

Value (minutes)

(updateInterval)

The Value (minutes) parameter specifies how often subscriber host accounting information is updated. The range is 10 to 1080. The default is 0, which means that no updates are sent.

The Value (minutes) parameter is configurable when the [Enable](#) parameter is set to enabled.

85 — ISA-IPsec Transform parameters

85.1 ISA_IPsec Transform parameters 85-2

85.1 ISA_IPsec Transform parameters

This chapter describes the parameters on the IPsec Transform creation form and child forms.

Authentication Algorithm

(authAlgorithm)

The Authentication Algorithm parameter specifies the hash algorithm that is used for the IKE authentication. Table 85-1 describes the parameter options.

Table 85-1 Authentication Algorithm (authAlgorithm) parameter

Option	Description	Dependencies
Null	No authentication algorithm is used.	—
MD5	The HMAC-MD5 algorithm is used.	—
SHA1 (default)	The HMAC-SHA1 algorithm is used.	—

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Description

See the [Description](#) parameter in section 14.1.

Encryption Algorithm

(encryptionAlgorithm)

The Encryption Algorithm parameter specifies the encryption algorithm that is used for the IPsec session. Table 85-2 describes the parameter options.

Table 85-2 Encryption Algorithm parameter

Option	Description	Dependencies
Null	No encryption algorithm is used	—
DES	Configures the 56-bit DES algorithm for encryption. Low level of security.	—
3DES	Configures the 3-DES algorithm for encryption. Uses multiple DES operations for a higher level of security.	—
AES128 (default)	Configures the AES algorithm with a block size of 128 bits. This is the mandatory implementation size for AES.	—
AES192	Configures the AES algorithm with a block size of 192 bits. This is a stronger version of AES.	—

(1 of 2)

Option	Description	Dependencies
AES256	This parameter configures the AES algorithm with a block size of 256 bits. This is the strongest version of AES.	—

(2 of 2)

Policy ID

The Policy ID parameter specifies a unique ID for the IPsec transform policy. The range is 1 to 2048. The default is 0.

86 — *IPsec Static Security Association parameters*

86.1 IPsec Static Security Association parameters 86-2

86.1 IPsec Static Security Association parameters

This chapter describes the parameters on the IPsec Static Security Association creation form and child forms.

Authentication Algorithm

(staticSAauthAlgorithm)

The Authentication Algorithm parameter specifies the authentication algorithm that is used for the IPsec static security association. The options are:

- md5
- sha1 (default)

Authentication Key

(staticSAAuthKey)

The Authentication Key parameter specifies the key used for the authentication defined by the [Authentication Algorithm](#) and [Authentication Key Type](#) parameters. The range is 0 to 40 characters.

Table 86-1 lists the value dependencies for the IPsec static security association authentication parameters.

Table 86-1 Authentication parameter dependencies for IPsec static security associations

Authentication Algorithm	Authentication Key Type	Authentication Key
md5	Ascii-key	16 characters
md5	Hex-key	32 characters
sha1	Ascii-key	20 characters
sha1	Hex-key	40 characters

Authentication Key Type

(staticSAAuthKeyType)

The Authentication Key Type parameter specifies the type of authentication key for the IPsec static security association. The options are:

- Hex-key (default)
- Ascii-key

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Direction

(staticSADirection)

The Direction parameter specifies the direction to which the IPsec static security association is applied. The options are:

- Bidirectional (default)
- Inbound
- Outbound

Protocol

(staticSAProtocol)

The Protocol parameter specifies the protocol used by the IPsec static security association. The options are:

- esp (default)
- ah

Security Parameter Index

(staticSASpi)

The Security Parameter Index parameter specifies the SPI that is used to select the security association to verify and decrypt the incoming IPsec. The SPI is an identification tag that is added to the header. The range is 256 to 16 383. The default is 0.

Static SA Description

(staticSADescription)

The Static SA Description parameter describes the IPsec static security association. The range is 0 to 32 characters.

Static SA Name

(staticSAName)

The Static SA Name parameter specifies the name of the IPsec static security association. The range is 1 to 32 characters.

87 — ISA-IPsec Tunnel Template parameters

87.1 ISA-IPsec Tunnel Template parameters 87-2

87.1 ISA-IPsec Tunnel Template parameters

This chapter describes the parameters on the IPsec Tunnel Template creation form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Description

See the [Description](#) parameter in section 14.1.

Policy ID

The Policy ID parameter specifies a unique ID for the IPsec transform policy. The range is 1 to 2048. The default is 0.

Replay Window

(replayWindow)

The Replay Window parameter specifies the size of the anti-replay window for the IPsec tunnel. The anti-replay window protocol secures IP against an entity that can inject messages in a message stream from a source to a destination computer on the Internet. If the value is set to 0, anti-replay is disabled. The options are:

- 0 (default)
- 32
- 64
- 128
- 256
- 512

Reverse Route

(reverseRoute)

The Reverse Route parameter specifies whether the NE that uses the template accepts framed routes sent by the RADIUS server, and installs them for the lifetime of the tunnel as managed routes. The options are:

- Use Security Policy (adds a route to every client-side protected subnet as signaled by the client)
- None (default)

88 — IKE Policy parameters

88.1 IKE Policy parameters 88-2

88.1 IKE Policy parameters

This chapter describes the parameters on the IKE Policy creation form and child forms.

Authentication Algorithm

(authAlgorithm)

The Authentication Algorithm parameter specifies the hash algorithm that is used for the IKE authentication. Table 88-1 describes the parameter options.

Table 88-1 Authentication Algorithm (authAlgorithm) parameter

Option	Description	Dependencies
Null	No authentication algorithm is used.	—
MD5	The HMAC-MD5 algorithm is used.	—
SHA1 (default)	The HMAC-SHA1 algorithm is used.	—

Authorization Method

(authMethod)

The Authorization Method parameter specifies the IKE standard authentication method that is used in the IPsec session to prevent ID spoofing. Table 88-2 describes the parameter options.

Table 88-2 Authentication Method parameter

Option	Description	Dependencies
Psk (default)	Uses the Pre-Shared Key mutual authentication method for site-to-site VPNs. The same secret value must be configured on both peers so that they can authenticate each other.	—
Plain-Psk-XAuth	Uses Extended Authentication asymmetric authentication method for remote access, to prompt remote users for a secondary login.	—

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 14.1.

Dead Peer Detection (DPD)

(policyDpd)

The Dead Peer Detection (DPD) parameter specifies whether DPD is enabled. The options are:

- Enabled
- Disabled
- Reply Only (reply to DPD keep alive requests only)

Description

See the [Description](#) parameter in section 14.1.

Diffie-Hellman (DH) Group

(dhgGroup)

The Diffie-Hellman (DH) Group parameter specifies the Diffie-Hellman group that is used to calculate session keys. The greater the number of bits, the higher the level of security. Table 88-3 describes the parameter options.

Table 88-3 Diffie-Hellman (DH) Group parameter

Option	Description	Dependencies
Group 1	768 bits	—
Group 2 (default)	1024 bits	—
Group 5	1536 bits	—

Encryption Algorithm

(encryptionAlgorithm)

The Encryption Algorithm parameter specifies the encryption algorithm that is used for the IPsec session. Table 88-4 describes the parameter options.

Table 88-4 Encryption Algorithm parameter

Option	Description	Dependencies
Null	No encryption algorithm is used	—
DES	Configures the 56-bit DES algorithm for encryption. Low level of security.	—
3DES	Configures the 3-DES algorithm for encryption. Uses multiple DES operations for a higher level of security.	—
AES128 (default)	Configures the AES algorithm with a block size of 128 bits. This is the mandatory implementation size for AES.	—
AES192	Configures the AES algorithm with a block size of 192 bits. This is a stronger version of AES.	—

(1 of 2)

Option	Description	Dependencies
AES256	This parameter configures the AES algorithm with a block size of 256 bits. This is the strongest version of AES.	—

(2 of 2)

Force Keep Alive

(natBehindNatOnly)

The Force Keep Alive parameter specifies whether the keepalive interval for NAT traversal is forced. The options are:

- Enabled
- Disabled

ID

See the [ID](#) parameter in section [14.1](#).

Internet Security Association and Key Management Life Time (seconds)

(isakmpLifeTime)

The Internet Security Association and Key Management Life Time (seconds) parameter specifies the lifetime of a phase 1 IKE key. The range is 1200 to 172 800. The default is 86 400.

Interval

(policyDpdInterval)

The Interval parameter specifies the interval at which connectivity is tested to the tunnel peer. The range is 10 to 300. The default is 30.

This parameter configurable only when the [Dead Peer Detection \(DPD\)](#) parameter is set to Enabled or Reply Only.

IPsec Life Time (seconds)

(ipsecLifeTime)

The IPsec Life Time (seconds) parameter specifies the lifetime of a phase 2 IKE key. The range is 1200 to 172 800. The default is 3600.

Keep Alive Interval

(natKeepAliveInterval)

The Keep Alive Interval parameter specifies the keep alive interval for NAT traversal. The range is 120 to 600. The default is 0.

Max Retries

(policyDpdMaxRetries)

The Max Retries parameter specifies the maximum number of times that connectivity to an IKE peer is tested before the tunnel is removed. The range is 2 to 5. The default is 3.

This parameter is configurable only when the [Dead Peer Detection \(DPD\)](#) parameter is set to Enabled or Reply Only.

Mode

(mode)

The Mode parameter specifies the negotiation mode to establish the IPsec session between peers. Table 88-5 describes the parameter options.

Table 88-5 Mode parameter

Option	Description	Dependencies
Main (default)	Specifies identity protection for the hosts initiating the IPsec session. This mode takes slightly longer to complete than the aggressive mode. More messages are exchanged.	—
Aggressive	Exposes the identity of the peers and is faster than the main mode. Fewer messages are exchanged.	—

NAT Traversal

(natTraversal)

The NAT Traversal parameter specifies whether NAT traversal is enabled. The options are:

- Disable (default)
- Enable
- Force

Perfect Forward Secrecy (PFS)

(pfs)

The Perfect Forward Secrecy (PFS) parameter specifies whether PFS is enabled. PFS provides for a new Diffie-Hellman key exchange each time the SA key is renegotiated. The options are:

- Enabled
- Disabled (default)

PFS DH Group

(pfsDhgGroup)

The PFS DH Group parameter specifies the Diffie-Hellman group that is used to calculate session keys when PFS is enabled. The greater the number of bits, the higher the level of security. This parameter is configurable when the [Perfect Forward Secrecy \(PFS\)](#) parameter is enabled. Table 88-6 describes the parameter options.

Table 88-6 PFS DH Group parameter

Option	Description	Dependencies
Group 1	768 bits	—
Group 2 (default)	1024 bits	—
Group 5	1536 bits	—

Version

(ikeVersion)

The Version parameter specifies the IKE version. The options are:

- 1 (default)
- 2

89 – NAT Policy parameters

89.1 NAT Policy parameters 89-2

89.1 NAT Policy parameters

This chapter describes the parameters on the NAT Policy form and child forms.

ALG Protocols

(algBitMask)

The ALG Protocols parameter specifies the set of protocols for which the NAT Application Level Gateway (ALG) is enabled. Multiple options can be enabled. The options are:

- SIP
- RTSP
- FTP

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Filtering

(filtering)

The Filtering parameter specifies the type of NAT filtering for the policy. Table 89-1 describes the parameter options.

Table 89-1 Filtering parameter

Option	Description
Address and Port Dependent	Specifies large-scale NAT filtering
Endpoint Independent (default)	Specifies L2-aware NAT filtering

High Watermark

(watermarkHigh)

The High Watermark parameter specifies, for each subscriber associated with the policy, the percentage of allocated NAT ports in use above which the 5620 SAM raises an alarm. The alarm clears when the port usage drops below the [Session Low Watermark](#) value. The parameter value must be higher than the [Session Low Watermark](#) value, unless both parameters are set to 0. The range is 0 to 100. The default is 0.

ICMP Query (sec)

(toIcmpQuery)

The to ICMP Query (sec) parameter specifies, in s, the length of time after which NAT closes an ICMP query session. The range is 60 to 240. The default is 60.

Low Watermark

(watermarkLow)

The Low Watermark parameter specifies, for each subscriber associated with the policy, the percentage of allocated NAT ports in use below which the 5620 SAM clears an alarm raised for port usage that exceeds the [Session High Watermark](#) value. The parameter value must be lower than the [Session High Watermark](#) value, unless both parameters are set to 0. The range is 0 to 99. The default is 0.

Port Reservation Count

(portReservationCount)

The Port Reservation Count parameter specifies, for each NAT subscriber associated with the policy, how many ports are reserved for traffic that matches one of the forwarding classes specified by the [Priority Session Forwarding Class Set](#). The parameter value must be less than the number of ports allocated to the subscriber. The range is 0 to 65 534. The default is 0.

Priority Session Forwarding Class Set

(prioritySessionFCSet)

The Priority Session Forwarding Class Set parameter specifies the traffic forwarding classes that are exempt from port and session usage limits, and are assigned ports in a reserved range. You can specify one or more of the following options:

- nc
- ef
- ll
- l2
- h1
- h2
- af
- be

Reservation Count

(sessionReservationCount)

The Reservation Count parameter specifies, for each NAT subscriber associated with the policy, how many sessions are reserved for traffic that matches one of the forwarding classes specified by the [Priority Session Forwarding Class Set](#). The parameter value must be less than the [Session Limit](#) value. The range is 0 to 65 534. The default is 0.

Session High Watermark

(sessionWatermarkHigh)

The High Watermark parameter specifies, for each subscriber associated with the policy, the percentage of active NAT sessions above which the 5620 SAM raises an alarm. The alarm clears when the session usage drops below the [Session Low Watermark](#) value. The parameter value must be higher than the [Session Low Watermark](#) value, unless both parameters are set to 0. The range is 0 to 100. The default is 0.

Session Limit

(sessionLimit)

The Session Limit parameter specifies the maximum number of NAT sessions for each NAT subscriber associated with the policy. The range is 1 to 65 535. The default is 65 535.

Session Low Watermark

(sessionWatermarkLow)

The Session Low Watermark parameter specifies, for each subscriber associated with the policy, the percentage of active NAT sessions below which the 5620 SAM clears an alarm raised for session usage that exceeds the [Session High Watermark](#) value. The parameter value must be lower than the [Session High Watermark](#) value, unless both parameters are set to 0. The range is 0 to 99. The default is 0.

SIP (sec)

(sipTimeout)

The SIP parameter specifies the sip inactive media timeout, which is the amount of time a temporary mapping will remain active without any media traffic. The range is 10 to 2550. The default is 120.

TCP Established (sec)

(toTcpEstab)

The TCP Established (sec) parameter specifies, in s, the length of time after which NAT closes an idle TCP session in the established state. The range is 7440 to 86 400. The default is 7440.

TCP Syn (sec)

(toTcpSyn)

The TCP Syn (sec) parameter specifies, in s, the length of time after which NAT closes a TCP session in the SYN state. The range is 6 to 86 400. The default is 15.

TCP Time Wait (sec)**(toTcpTimeWait)**

The TCP Time Wait (sec) parameter specifies, in s, the length of time after which NAT closes a TCP session in the TIME-WAIT state. The range is 0 to 240. The default is 0.

TCP Transitory (sec)**(toTcpTrans)**

The TCP Transitory (sec) parameter specifies, in s, the length of time after which NAT closes a TCP session in a transitory state. The range is 240 to 86 400. The default is 240.

UDP (sec)**(toUdp)**

The UDP (sec) parameter specifies, in s, the length of time after which NAT closes an idle UDP session. The range is 120 to 86 400. The default is 300.

UDP DNS (sec)**(toUdpDns)**

The UDP DNS (sec) parameter specifies, in s, the length of time after which NAT closes a UDP session with destination port 53. The range is 15 to 86 400. The default is 15.

UDP Inbound Refresh**(udpInbndRefresh)**

The UDP Inbound Refresh parameter specifies the NAT inbound refresh behavior. The parameter is disabled by default.

UDP Initial (sec)**(toUdpInitial)**

The UDP Initial (sec) parameter specifies, in s, the length of time after which NAT closes a new UDP session in which a single packet has been sent. The range is 10 to 300. The default is 15.

90 – Application Assurance parameters

90.1 Application Assurance parameters 90-2

90.1 Application Assurance parameters

This chapter describes the parameters on the Manage Application Assurance Policies child forms.

Action

(policerAction)

The Action parameter specifies the action to be performed by a single-bucket bandwidth policer when managing non-conforming traffic. Table 90-1 describes the parameter options.

Table 90-1 Action parameter

Option	Option description
Permit Deny (default)	Non-conforming traffic is dropped.
Priority Mask	Non-conforming traffic is marked out of profile. Conforming traffic is marked in profile. The markings overwrite any previous IOM QoS markings.

Address

(address)

The Address parameter specifies the address associated with the transit subscriber. Specify an IPv4 address, or a DNS address as a string. The default is 0.0.0.0.

Address

(dstAddr)

The Address parameter specifies the existing destination address that is matched against to resolve to an AQP action. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Address

(srcAddr)

The Address parameter specifies the existing source address to match against to resolve to an AQP action. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Address Length

(dstAddrLength)

The Address parameter specifies the number of relevant bits within the destination address. The range is 0 to 32. The default is 0.

Address Length

(srcAddrLength)

The Address parameter specifies the number of relevant bits within the source address. The range is 0 to 32. The default is 0.

Address Operator

(dstAddrOperator)

The Address Operator parameter specifies the operator to be used in conjunction with the [Address](#) and [Address Length](#) parameters. The options are:

- None (default)
- Equal
- Not Equal

Address Operator

(srcAddrOperator)

The Address Operator parameter specifies the operator to be used in conjunction with the [Address](#) and [Address](#) parameters. The options are:

- None (default)
- Equal
- Not Equal

Administrative State

(adminState)

The Administrative State parameter specifies the administrative state of an AA filter component or an AQP. The options are:

- In Service
- Out of Service (default)

Application Flag

(applicationFlag)

The Application Flag parameter specifies whether the AA application is based on TCP or UDP protocol. This parameter is used by the 5670 RAM for the purpose of protocol-class reporting. The options are:

- None (default)
- TCP
- UDP

Application Group Operator

(appGroupOperator)

The Application Group Operator parameter specifies the operator that is applied in conjunction with the [Displayed Name](#) parameter when matched against to resolve an AQP action. The options are:

- None (default)
- Equal
- Not Equal

Application Operator

(applicationOperator)

The Application Operator parameter specifies the operator that is applied in conjunction with the [Displayed Name](#) parameter when matched against to resolve an AQP action. The options are:

- None (default)
- Equal
- Not Equal

ASO Characteristic

(asoCharName)

The ASO Characteristic parameter specifies a string of up to 32 characters that uniquely identifies the ASO characteristic.

ASO Characteristic Default Value

(asoCharDefValue)

The ASO Characteristics Default Value parameter specifies an ASO characteristic value as a default value. When a default value is specified, application profile entries that do not explicitly include this characteristic inherit the default value and use it as part of the AQP match criteria based on that application profile. A default value is required for each characteristic.

ASO Characteristic Operator

(charOperator)

The ASO Characteristic Operator parameter specifies the ASO characteristic entry to match against to resolve to an AQP action. The options are:

- None (default)
- Equal

ASO Characteristic Value

(asoCharacteristicValue)

The ASO Characteristic Value parameter specifies a string of up to 32 characters that uniquely identifies the ASO characteristic value associated with an application profile.

ASO Characteristic Value

(asoCharValue)

The ASO Characteristic Value parameter specifies a string of up to 32 characters that uniquely identifies the ASO characteristic value associated with an application profile.

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

Bit Rate High Watermark

(bitRateHighMark)

The Bit Rate High Watermark parameter specifies the bit rate threshold on the ISA-AA when an ISA-AA group bit rate warning alarm will be raised by the 5620 SAM. Entering a value of -1 or selecting the MAX check box will set the parameter value to the maximum possible value and will prevent the NE from raising bit rate alarms. The range is 1 to 10000. The default is MAX.

Bit Rate Low Watermark

(bitRateLowMark)

The Bit Rate Low Watermark parameter specifies the bit rate threshold on the ISA-AA when an ISA-AA group bit rate warning alarm will be cleared by the 5620 SAM. The value of this parameter cannot be higher than the value of the [Bit Rate High Watermark](#) parameter. The range is 0 to 9999. The default is 0.

Capacity Cost

(capacityCost)

The Capacity Cost parameter specifies a cost to be assigned to diverted SAPs. The cost is used for load-balancing SAPs between ISAs and for a threshold that notifies the operator if capacity planning is exceeded.

The load balancing decision is made based on the AA capacity cost of AA subscriber SAPs and ESM subscribers. The capacity cost is configured in the application profile. When you assign a new diverted AA subscriber to an ISA, the ISA with the lowest cost (that also has sufficient resources) is chosen. This approach provides several different load-balancing approaches on a per-group basis:

- AA subscriber count balancing—Configure the capacity cost for each application profile to the same number (for example, 1). Because each AA subscriber has the same cost, AA subscriber count-based balancing results.
- AA subscriber statistics resource balancing—Configure the capacity cost to the number of statistics collected for AA subscribers using the application profile. If different partitions have significantly different statistics requirements, try to spread based on statistics usage.
- bandwidth balancing—Configure the capacity cost to the total bandwidth in both directions (in kb/s) that is expected for the AA subscriber. For different AA subscribers that have highly varying bandwidth needs, this provides bandwidth-based balancing.

The range is 1 to 65 535. The default is 1.

CBS (KB)

(policerCBS)

The CBS parameter specifies the committed burst size of dual-bucket bandwidth AA Policers. To be used in conjunction with the CIR parameters. The range is 0 to 131071. The default is 0.

CIR (Kbps)

(policerAdminCIR)

The CIR (Kbps) parameter specifies the administrative CIR of dual-packet bandwidth AA Policers. The range is -1 to 100 000 000. The default is 0. A value of -1 results in maximum rate.

CIR

(policerCIRAdaptation)

The CIR parameter specifies the adaptation rule to be used while computing the operational CIR value. The adaptation rule specifies the rules to compute the operational values while maintaining minimum offset. Table 90-2 describes the parameter options.

Table 90-2 CIR parameter

Option	Option description
Max	The operational CIR for the queue is equal to or less than the administrative rate specified using the rate command.

(1 of 2)

Option	Option description
Min	The operational CIR for the queue is equal to or greater than the administrative rate specified using the rate command.
Closest (default)	The operational CIR for the queue is the rate closest to the rate specified using the rate command.

(2 of 2)

Collect Accounting Statistics

(collectStats)

The Collect Accounting Statistics parameter specifies whether the collection of AA accounting statistics is enabled for an object. The options are:

- Disabled (default)
- Enabled

Custom Protocol Expression Direction

(custProcExprDirection)

The Custom Protocol Expression Direction parameter specifies the protocol direction to match against to resolve to a custom protocol. The options are:

- Client to Server Direction
- Server to Client Direction
- Any

Custom Protocol Expression Offset

(custProcExprOffset)

The Custom Protocol Expression Offset parameter specifies the offset (in octets) in the protocol payload, where the substring expression match criteria starts. The range is 0 to 127.

Description

See the [Description](#) parameter in section [112.1](#).

DHCP

(dhcp)

The DHCP parameter specifies whether transit IP subscribers are dynamically learned via DHCP. The options are:

- Disabled (default)
- Enabled

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Displayed Name

(appGroupName)

The Displayed Name parameter specifies an existing application group to match against to resolve an AQP action. Click on the Select button to list and choose an existing application. If no application group is chosen, no match is done. If an existing application group that does not match the ApplicationGroup class is chosen, an error is returned.

Displayed Name

(applicationName)

The Displayed Name parameter specifies an existing application to match against to resolve an AQP action. Click on the Select button to list and choose an existing application. If no existing application is chosen, no match is done. If an existing application that does not match the Application class is chosen, an error is returned.

Displayed Name

(bwLimitPolicerName)

The Displayed Name parameter specifies an existing Policer policy whose flows are to be policed using the policy's defined template. Click on the Select button to list and choose an existing policy. Validation is enforced by the [Type](#) parameter of the policy. The allowed types are single bucket bandwidth and dual bucket bandwidth.

Displayed Name

(flowCountPolicerName)

The Displayed Name parameter specifies an existing Policer policy whose flows are to be policed using the policy's defined template. Click on the Select button to list and choose an existing policy. Validation is enforced by the [Type](#) parameter of the policy. The allowed type is flow count limit.

Displayed Name

(flowRatePolicerName)

The Displayed Name parameter specifies an existing Policer policy whose flows are to be policed using the policy's defined template. Click on the Select button to list and choose an existing policy. Validation is enforced by the [Type](#) parameter of the policy. The allowed type is flow rate limit.

Divert

(divert)

The Divert parameter specifies whether the traffic for the subscriber associated with the policy is diverted to the ISA-AA MDA. The options are.

- Disabled (default)
- Enabled

Drop

(drop)

The Drop parameter specifies that flows matching the related AQP policy entry are to be dropped.

DSCP

(dscp)

The DSCP parameter specifies the DSCP name to match against to resolve to an AQP action. If Default is selected, all DHCP values are allowed. The default is be. Table 90-3 describes the parameter options.

Table 90-3 DSCP parameter

Options			
be (default)	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43

DSCP Operator

(dscpOperator)

The DSCP Operator parameter specifies the operator that is applied in conjunction with the [DSCP](#) parameter when matched against to resolve an AQP action. The options are:

- None (default)
- Equal
- Not Equal

Entry ID

(id)

The Entry ID parameter specifies a unique ID for an application filter policy identifier or an AQP. The range is 1 to 65 535.

ESM Subscriber

(subscriber)

The ESM Subscriber parameter specifies an existing subscriber to match against to resolve to an AQP action. If no entry is provided, no match is done. If no existing subscriber corresponds to the provided entry, no match is done until the entry is populated. The range is 0 to 32 characters. There is no default.

Forwarding Class

(remarkFc)

The Forwarding Class parameter specifies the forwarding class to be used to remark flows matching the related AQP policy entry. If Default is selected, the forwarding class is not modified. Table [90-4](#) describes the parameter options.

Table 90-4 Forwarding Class parameter

Options			
be (default)	l2	af	l1
h2	ef	h1	nc

Flow Count (flows)

(policerFlowCount)

The Flow Count parameter specifies the total flow count for flow-count-limit AA Policers. The range is -1, 1 to 100 000 000. The default is -1 (Max).

Flow Full High Watermark

(flowFullHighMark)

The Flow Full High Watermark parameter specifies that an alarm is raised when the high flow table capacity threshold is reached. The range is 0 to 100. The default is 95.

Flow Full Low Watermark

(flowFullLowMark)

The Flow Full Low Watermark parameter specifies the level the flow table capacity must reach before the high watermark alarm is cleared. The range is 0 to 100. The default is 90.

Flow Setup High Watermark

(flowSetupHighMark)

The Flow Setup High Watermark parameter specifies the flow setup rate on the ISA-AA when an ISA-AA group flow setup warning alarm will be raised by the 5620 SAM. Entering a value of -1 or selecting the MAX check box will set the parameter value to the maximum possible value and will prevent the NE from raising flow setup alarms. The range is 1 to 200000. The default is MAX.

Flow Setup Low Watermark

(flowSetupLowMark)

The Flow Setup Low Watermark parameter specifies the flow setup rate on the ISA-AA when an ISA-AA flow setup warning alarm will be cleared by the 5620 SAM. The value of this parameter cannot be higher than the value of the [Flow Setup High Watermark](#) parameter. The range is 0 to 199999. The default is 0.

Flow Set-up Direction

(flowSetupDir)

The Flow Set-up Direction parameter specifies the flow set up direction to which the application filter entry is to be applied. Table [90-5](#) describes the parameter options.

Table 90-5 Flow Set-up Direction parameter

Option	Option description
Subscriber to Network	The application filter entry is applied to flows initiated by a local subscriber.
Network to Subscriber	The application filter entry is applied to flows initiated from a remote destination towards a local subscriber.
Both (default)	The application filter entry is applied for subscriber-to-network and network-to-subscriber traffic.

Frustrated (milliseconds)**(roundTripTimeFrustrated)**

The Frustrated (milliseconds) parameter specifies the threshold between tolerable and frustrated (failed) network round trip times. This parameter is used by the 5670 RAM for application performance index analysis. The range is -1 to 600000. A value of -1 disables this threshold for the application. The default is -1.

Frustrated (milliseconds)**(meanTotalDelayFrustrated)**

The Frustrated (milliseconds) parameter specifies the threshold between tolerable and frustrated (failed) network mean total delay times. This parameter is used by the 5670 RAM for application performance index analysis. The range is -1 to 600000. A value of -1 disables this threshold for the application. The default is -1.

Frustrated (milliseconds)**(stdDevTotalDelayTolerated)**

The Frustrated (milliseconds) parameter specifies the threshold between tolerable and frustrated (failed) network total delay standard deviation. This parameter is used by the 5670 RAM for application performance index analysis. The range is -1 to 600000. A value of -1 disables this threshold for the application. The default is -1.

Frustrated (%)**(packetLossFrustrated)**

The Frustrated (%) parameter specifies the threshold between tolerable and frustrated (failed) network packet loss. This parameter is used by the 5670 RAM for application performance index analysis. The range is -1 to 600000. A value of -1 disables this threshold for the application. The default is -1.

Granularity**(policerGranularity)**

The Granularity parameter specifies the scope of traffic over which an AA Policer is applied. Table 90-6 describes the parameter options:

Table 90-6 Granularity parameter

Option	Option description
System	Creates a system policer profile that limits the scope of all traffic entering the ISA-AA MDA.
Subscriber	Creates a policer profile for a subscriber that limits the scope of all traffic of that subscriber.

Group ID

(groupId)

The Group ID parameter specifies the group ID of the AA group. The range is 1 to 255. The default is 1. The parameter is read-only on the ISA-AA partitions form.

Index

(id)

The Index parameter specifies the application filter expression substring index. The range is 1 to 4.

IP Protocol Number

(ipProtocolNumber)

The IP Protocol Number parameter specifies an IP protocol as a match criterion for the filter. Table 90-7 lists the parameter options. The default is ALL.

Table 90-7 IP Protocol Number parameter

Options			
ALL	SEP	IPPC	IFMP
HOPOPT	3PC	any distributed file system (68)	PNNI
ICMP	IDPR	SAT_MON	PIM
IGMP	XTP	VISA	ARIS
GGP	DDP	IPCV	SCPS
IP	IDPR_CMT	CPNX	QNX
ST	TP++	CPHB	A/N Active Networks (107)
TCP	IL	WSN	IPComp
CBT	IPv6	PVP	SNP
EGP	SDRP	BR_SAT_MON	Compaq_Peer
IGP	IPv6Route	SUN_ND	IPX_in_IP
BBN_RCC_MON	IPv6Frag	WB_MON	VRRP
NVP_II	IDRP	WB_EXPAK	PGM
PUP	RSVP	ISO_IP	any 0-hop protocol (114)
ARGUS	GRE	VMTP	L2TP
EMCON	MHRP	SECURE_VMTP	DDX
XNET	BNA	VINES	IATP
CHAOS	ESP	TTP	STP
UDP	AH	NSFNET_IGP	SRP

(1 of 2)

Options			
MUX	I_NLSP	DGP	UTI
DCN_MEAS	SWIPE	TCF	SMP
HMP	NARP	EIGRP	SM
PRM	MOBILE	OSPFGRP	PTP
XNS_IDP	TLSP	Sprite_RPC	ISIS
TRUNK_1	SKIP	LARP	FIRE
TRUNK_2	IPv6_ICMP	MTP	CRTP
LEAF_1	IPv6_No_Nxt	AX.25	CRUDP
LEAF_2	IPv6_Opts	IPIP	SSCOPMCE
RDP	any host internal protocol (61)	MICP	IPLT
IRTP	CFTP	SCC_SP	SPS
ISO_TP4	any local network (63)	ETHERIP	PIPE
NETBLT	SAT_EXPAK	ENCAP	SCTP
MFE_NSP	KRYPTOLAN	any private encryption scheme (99)	FC
MERIT_INP	RVD	GMTP	RSVP_E2E_IGNORE

(2 of 2)

IP Protocol Operator

(ipProtocolNumberOperator)

The IP Protocol Operator parameter specifies the operator applied against the value specified by the [IP Protocol Number](#) parameter. The options are:

- None (default)
- Equal
- Not Equal

ISA-AA Group ID

(isaAAGrpId)

The ISA-AA Group ID parameter specifies the ISA-AA group to which the application assurance item belongs. The range is 1 to 255. The default is 1.

ISA-AA Partition ID

(isaAAPartitionId)

The ISA-AA Partition ID parameter specifies the ISA-AA partition to which the application assurance item belongs. The range is 0 to 65 535. The default is 0.

MBS (KB)**(bwPolicerMBS)**

The MBS parameter specifies the maximum burst size of bandwidth AA Policers. To be used in conjunction with the PIR parameters. The range is 0 to 131071. The default is 0.

MBS (flows)**(frPolicerMBS)**

The MBS parameter specifies the maximum burst size for the flow count of flow setup rate AA Policers. To be used in conjunction with the PIR parameters. The range is 0 to 131071. The default is 0.

Mean Total Delay Tolerated (milliseconds)**(meanTotalDelayTolerated)**

The Mean Total Delay Tolerated (milliseconds) parameter specifies the threshold between satisfactory and tolerable total delay. This parameter is used by the 5670 RAM for application performance index analysis. The range is -1 to 600000. A value of -1 disables thresholds for the application. The default is -1.

Mirror Source All Inclusive**(mirrorSrcAllInclusive)**

The Mirror Source All Inclusive parameter specifies that all flows matching the subscriber default policy is mirrored until the protocol is identified. The [Service ID](#) parameter must be set to a valid mirror.

Operator**(appFilterExprOperator)**

The Operator parameter specifies the operator that is applied against the value specified by the String parameter. The options are:

- Equal (default)
- Not Equal

Operator**(custProcExprOperator)**

The Operator parameter specifies the comparison operator that is applied against the value specified by the String parameter. The options are:

- Equal (default)
- Not Equal

Packet Loss Tolerated (%)

(packetLossTolerated)

The Packet Loss Tolerated (%) parameter specifies the percentage threshold of tolerable packet loss. This parameter is used by the 5670 RAM for application performance index analysis. The range is -1 to 100. A value of -1 disables thresholds for the application. The default is -1.

Packet Rate High Watermark

(packetRateHighMark)

The Packet Rate High Watermark parameter specifies the packet rate on the ISA-AA when an ISA-AA packet rate warning alarm will be raised by the 5620 SAM. Entering a value of -1 or selecting the MAX check box will set the parameter value to the maximum possible value and will prevent the NE from raising packet rate alarms. The range is 1 to 14880952. The default is MAX.

Packet Rate Low Watermark

(packetRateLowMark)

The Packet Rate Low Watermark parameter specifies the packet rate on the ISA-AA when an ISA-AA group packet rate alarm will be cleared by the 5620 SAM. The value of this parameter cannot be higher than the value of the [Packet Rate High Watermark](#) parameter. The range is 0 to 14880951. The default is 0.

Partition ID

(partitionId)

The Partition ID parameter specifies the partition ID within an AA group. The range is 1 to 65 535.

PIR (Kbps)

(policerAdminPIR)

The PIR (Kbps) parameter specifies the administrative PIR of dual-packet bandwidth AA Policers. The range is -1, 1 to 100 000 000. The default is -1. A value of -1 means no limit.

PIR

(policerPIRAdaptation)

The PIR parameter specifies the adaptation rule to be used while computing the operational PIR value. The adaptation rule specifies the rules to compute the operational values while maintaining minimum offset. Table [90-8](#) describes the parameter options.

Table 90-8 PIR parameter

Option	Option description
Max	The operational PIR for the queue is equal to or less than the administrative rate specified using the rate command.
Min	The operational PIR for the queue is equal to or greater than the administrative rate specified using the rate command.
Closest (default)	The operational PIR for the queue is the rate closest to the rate specified using the rate command.

Policy ID

(id)

The Policy ID parameter specifies the numeric identifier for the transit IP policy. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 4294967295. When the value is 0 (default), the ID is generated by the 5620 SAM.

Port ID

(sapSubscrPointer)

The Port ID parameter specifies an existing subscriber SAP port to match against to resolve to an AQP action. Click on the Select button to list and choose an existing application. If no existing application is chosen, no match is done.

Port High Value

(dstPortHighValue)

The Port High Value parameter specifies the destination port high value if the parameter is set to Range. The range is 0 to 65535. The default is 0.

Port High Value

(srcPortHighValue)

The Port High Value parameter specifies the source port high value if the parameter is set to Range. The range is 0 to 65535. The default is 0.

Port Operator

(dstPortOperator)

The Port Operator parameter specifies the operator that is applied in conjunction with the parameters when matched against to resolve to an application. The options are:

- None (default)
- Equal
- Not Equal

Port Operator

(srcPortOperator)

The Port Operator parameter specifies the operator that is applied in conjunction with the parameters when matched against to resolve to an application. The options are:

- None (default)
- Equal
- Not Equal

Port Value/Low Value

(dstPortLowValue)

The Port Value/Low Value parameter specifies the destination port low value if the parameter is set to Range. The range is 0 to 65535. The default is 0.

Port Value/Low Value

(srcPortLowValue)

The Port Value/Low Value parameter specifies the source port low value if the parameter is set to Range. The range is 0 to 65535. The default is 0.

Port Value Type

The Port Value Type parameter specifies the destination port value type. The options are:

- Single (default)
- Range

Port Value Type

The Port Value Type parameter specifies the source port value type. The options are:

- Single (default)
- Range

Priority

(remarkPriority)

The Priority parameter specifies the priority to be used to remark flows matching the related AQP policy entry. If Default is selected, the priority is not modified. The options are:

- Default (default)
- High
- Low

Protocol Administrative State

(aaProtocolAdminState)

The Protocol Administrative State parameter specifies the administrative state of the AA protocol. When the administrative state is set to Out of Service, the AA protocol defaults to its parent protocol as specified in the protocol parent name. The options are:

- In Service
- Out of Service (default)

Protocol Operator

(protocolOperator)

The Protocol Operator parameter specifies whether the policy is preconfigured on the NE or if the policy is user-defined. The options are:

- None (default)
- Equal
- Not Equal

Protocol Type

(protocolType)

The Protocol Type parameter specifies the type of protocol. A custom protocol is created by the user. A system protocol is pre-populated. The options are:

- Custom Protocol
- System Protocol

RADIUS

(radius)

The RADIUS parameter specifies whether transit IP subscribers are dynamically learned via RADIUS. The options are:

- Disabled (default)
- Enabled

Remark DSCP In Profile

(remarkDscpInProfile)

The Remark DSCP In Profile parameter specifies the DSCP remark action to be used on flows matching the related AQP entry. It can only be enabled when the entry remarks forwarding class. When enabled, all packets of matching flows are remarked to the configured in-profile DSCP after all AQP policing and priority remarking is complete. The default is Default. Table 90-9 describes the parameter options.

Table 90-9 Remark DSCP In Profile parameter

Options			
be	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43
Default (default)			

Remark DSCP Out Profile

(remarkDscpOutProfile)

The Remark DSCP Out Profile parameter specifies the DSCP remark action to be used on flows matching the related AQP entry. It can only be enabled when the entry remarks forwarding class. When enabled, all packets of matching flows are remarked to the configured out-profile DSCP after all AQP policing and priority remarking is complete. The default is Default. Table 90-10 describes the parameter options.

Table 90-10 Remark DSCP Out Profile parameter

Options			
be	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43
Default (default)			

Round Trip Time Tolerated (milliseconds)

(roundTripTimeTolerated)

The Round Trip Time Tolerated (milliseconds) parameter specifies the threshold between satisfactory and tolerable network round trip times. This parameter is used by the 5670 RAM for application performance index analysis. The range is -1 to 600000. A value of -1 disables this threshold for the application. The default is -1.

SAP Subscriber

(sapSubscrPointer)

The SAP Subscriber parameter is the pointer to the instance of the service access point for an existing subscriber.

Server Address

(serverAddr)

The Server Address parameter specifies the server address to match against the IP address that a local subscriber is communicating with.

Server Address Mask

(serverAddrPrefixLength)

The Server Address Mask parameter specifies the length of the server address prefix. The range is 1 to 32. The default is 0.

Server Address Operator

(serverAddrOperator)

The Server Address Operator parameter specifies the operator applied against the value specified by the [Server Address](#) parameter. The options are:

- None (default)
- Equal
- Not Equal
- Less Than
- Greater Than
- Range

Server Port First Packet Policy

(serverPortFpp)

The Server Port First Packet Policy parameter specifies the packet policy to apply for flows that match the [Server Port Value Type](#) and [Server Port Operator](#) parameters. Table 90-11 describes the parameter options.

Table 90-11 Server Port First Packet Policy parameter

Option	Option description
None (default)	For TCP/UDP port applications with full DPI verification, AA ensures that other identifiable applications do not run over a well known port. The AA policy is applied after DPI-based identification completes.
First Packet Trusted	For TCP/UDP trusted port applications without DPI verification, the application is identified using TCP/UDP port-based filters only. The AA policy is applied from the first packet of a flow. Lack of DPI processing assumes that no other applications can run on the TCP/UDP port.
First Packet Validate	For TCP/UDP trusted port applications with DPI verification, the application is identified using TCP/UDP port-based filters. The AA policy is applied from the first packet of a flow, while DPI-based application identification continues. The application is re-identified and the AA policy is re-evaluated after DPI-based identification completes, allowing the detection of improper or unexpected applications on a well-known port.

Server Port High Value

(serverPortHighValue)

The Server Port High Value parameter specifies the server port high value when the Server Port Value Type parameter is set to Range. The range is 0 to 65 535. The default is 0.

Server Port Operator

(serverPortOperator)

The Server Port Operator parameter specifies the operator applied against the value specified by the [Server Port Value Type](#) parameter. The options are:

- None (default)
- Equal
- Not Equal
- Less Than
- Greater Than

Server Port Value Type

(serverPortValueType)

The Server Port Value Type parameter specifies the value type either in single value or in a range from low value to high value. If you choose the value Range, you must configure the [Server Port High Value](#) and the [Server Port/Low Value](#). If you choose the value Single, you must configure only the [Server Port/Low Value](#). The options are:

- Single (default)
- Range

Server Port/Low Value

(serverPort)

The Server Port/Low Value parameter specifies a port number to match against the TCP/UDP port number that a local subscriber is communicating with. The range is 0 to 65 535. The default is 0.

Service ID

(mirrorSourcePointer)

The Service ID parameter specifies an existing application-based policy mirroring service that uses the AQP policy entry as a mirror source. Click on the Select button to list and choose an existing application-based policy mirroring service. Mirror action can only be applied to AQP policy entries that specify match criteria for applications, application groups, or ASO characteristic entries. If multiple actions are to be performed on a flow, mirror action are performed on the result of the other actions. Only a single mirror action per flow is supported. AQP driven action takes precedence over a debug mirror action if both are applied to a single flow.

Spoke Subscriber

(spokeSdpSubscrPointer)

The SAP Subscriber parameter is the pointer to the instance of the spoke SDP binding point for an existing subscriber.

String

(appFilterExprStr)

The String parameter specifies a substring expression of the type specified by the Type parameter to match against an application identified by the Application Filter. The range is 3 to 66 characters. There is no default.

String

(custProcExprStr)

The String parameter specifies a printable ASCII substring expression to match against a custom protocol. The range is 1 to 16 characters. There is no default.

Subscriber name

(displayedName)

The Subscriber name parameter specifies a string that identifies a subscriber identifier. The range is 1 to 32 characters. There is no default.

Subscriber Operator

(aaSubOperator)

The Subscriber Operator parameter specifies the operator that is applied in conjunction with the [Displayed Name](#) parameter when matched against to resolve an AQP action. The options are:

- None (default)
- Equal
- Not Equal

SubscriberType

(subscriberType)

The SubscriberType parameter specifies the type of subscriber to match against to resolve to an AQP action. The options are:

- ESM
- SAP
- Spoke SDP Binding

- Transit
- None (default)

The SAP and Spoke SDP Binding options are valid only when you create a local AQP entry.

Threshold Administrative State

(ramThresholdAdminState)

The Threshold Administrative State parameter specifies the administrative state for application threshold reporting to the 5670 RAM. The options are:

- Disabled (default)
- Enabled

Total Delay Standard Deviation Tolerated (milliseconds)

(stdDevTotalDelayTolerated)

The Total Delay Standard Deviation Tolerated (milliseconds) parameter specifies the threshold between a satisfactory and tolerable total delay standard deviation. The parameter is used by the 5670 RAM for application performance index analysis. The range is –1 to 600 000. A value of -1 disables the threshold for the application. The default is –1.

Traffic Direction

(trafficDir)

The Traffic Direction parameter specifies the traffic directions to match to resolve to an AQP action. This allows different policer bandwidths to apply in each direction. The options are:

- Subscriber to Network
- Network to Subscriber
- Both (Default)

Transit Subscriber

(transitSubscriber)

The Transit Subscriber parameter specifies an existing subscriber to match against to resolve to an AQP action. If no entry is provided, no match is done. If no existing subscriber corresponds to the provided entry, no match is done until the entry is populated. The range is 0 to 32 characters. There is no default.

Tunnel ID

(pathId)

The Tunnel ID parameter specifies an existing spoke SDP binding subscriber to match against to resolve to an AQP action.

Type

(appFilterExprType)

The Type parameter specifies the Application Filter Expression type. The options are:

- HTTP Host (default)
- HTTP URI
- HTTP Referer
- SIP UA
- SIP URI
- SIP MT
- Citrix Application
- HTTP User Agent
- H323 Product ID
- TLS Certificate Subject Organization
- TLS Certificate Subject Common

Type

(policerType)

The Type parameter specifies the limiting policer type. The options are:

- Dual Bucket Bandwidth
- Flow Count Limit
- Flow Rate Control
- Single Bucket Bandwidth

91 – 802_1x parameters

91.1 802_1x parameters 91-2

91.1 802_1x parameters

This chapter describes the parameters on the 802_1x Policy form and child forms.

Accounting Port

(acctPort)

The Accounting Port parameter specifies the UDP port on the RADIUS server to which you want to connect to perform accounting activities. The range is 1 to 65 535. The default is 1813.

Administrative Status

See the [Administrative State](#) parameter in section 112.1. The default is Down.

Authorization Port

(authPort)

The Authorization Port parameter specifies the UDP port on the RADIUS server to which you want to connect to perform authorization activities. The range is 1 to 65 535. The default is 1812.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

IP Address

(ipAddress)

The IP Address parameter specifies the IP address of the RADIUS server. The range is any valid unicast IP address.

Password

(password)

The Password parameter specifies the key that is associated with the RADIUS server. You must configure the parameter. The range is any valid key that is supported by the RADIUS server of 1 to 20 characters. You must configure the parameter.

Request Timeout

(requestTimeout)

The Request Timeout parameter specifies the time, in seconds, that elapses before an attempt is made to send the same request again to the same RADIUS server. The range is 1 to 90. The default is 5.

Retry Attempts

(retryAttempts)

The Retry Attempts parameter specifies the maximum number of times an attempt is made to send a request to the same RADIUS server. The range is 1 to 1000. The default is 3.

Server Index

(serverIndex)

The Server Index parameter specifies a unique RADIUS server for the policy. The range is 1 to 5. The default is 0.

Server Type

(serverType)

The Server Type parameter specifies the type of activities to be performed by the RADIUS server. Table 91-1 describes the parameter options.

Table 91-1 Server Type parameter

Option	Option description	Dependencies
combined	The RADIUS server is used for both authorization and accounting activities.	—
accounting	The RADIUS server is used for accounting activities only.	
authorization (default)	The RADIUS server is used for authorization activities only.	

Source Address

(sourceAddress)

The Source Address parameter specifies the source IP address of the RADIUS packets. The range is any valid unicast IP address.

When the parameter specifies the address of the interface, the RADIUS client uses the address for authentication requests. When the address is in-band, the system IP address is used. When the address is out-of-band, the IP address of the management interface is used.

92 — *PBB MRP parameters*

92.1 PBB MRP parameters 92-2

92.1 PBB MRP parameters

This chapter describes the parameters on the PBB MRP form and child forms.

Action

(MrpPolicyAction)

The Action parameter specifies the action that is performed for packets that match this entry. The options are:

- Allow
- Block
- End-Station
- None (default)

Selecting the Allow option means that the matching MMRP attributes will be advertised on this SAP or SDP.

Selecting the Block option means that the matching MMRP attributes will not be advertised on this SAP or SDP.

Selecting the End-Station option means that end-station emulation is present on this SAP or SDP for the MMRP attributes related with matching ISIDs.

Selecting the None option means that the MRP policy entry will be considered incomplete and therefore rendered inactive.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Default Action

(defaultAction)

The Default Action parameter specifies the action that is performed for packets that do not match any MRP policy entries. The options are:

- Allow (default)
- Block

Selecting the Allow option means that all MMRP attributes will be advertised unless there is a specific MRP policy entry which causes them to be blocked on this SAP or SDP.

Selecting the Block option means that no MMRP attributes will be advertised unless there is a specific MRP policy entry which causes them to be advertised on this SAP or SDP.

Description

See the [Description](#) parameter in section 112.1.

Entry ID

See the [Entry ID](#) parameter in section 112.1.

High ISID

(isidHigh)

The High ISID parameter specifies the highest value of the 24-bit service instance identifier for this service that matches this entry. The value of this field can be equal to but not lower than the value of the Low ISID field. The range is 0 to 16 777 215. The default value is 0.

Consult the [Low ISID](#) parameter description for further information regarding ISID ranges and usage rules.

Low ISID

(isidLow)

The Low ISID parameter specifies the lowest value of the 24-bit service instance identifier for this service that matches this entry. The value of this field can be equal to but not higher than the value of the [High ISID](#) field.

The range is 0 to 16 777 215. The default is 0.

The Low ISID and High ISID parameters together configure an ISID value, or a range of ISID values, to be matched by the MRP policy when looking at the related MMRP attributes (Group BMACs).

Multiple ISID ranges are allowed per entry. The following rules govern the usage of multiple ISID statements:

- Overlapping values are allowed. For example:
 - Low ISID: 1 and High ISID: 10
 - Low ISID: 5 and High ISID: 15
 - Low ISID: 16 and High ISID: 16

The behavior on the network element is to merge the overlapping ranges into a single range. The overlapping ranges shown above would therefore be merged into a range of Low ISID: 1 and High ISID: 16
- When a policy with overlapping ranges is distributed to a network element, the network element merges any overlapping ranges. This could result in an inconsistency between the local policy and global policy. Therefore, when you create or modify ISID ranges in a global policy, overlapping ranges are merged in 5620 SAM to create a range that would match the result on the network element.

Name

(displayedName)

The Name parameter specifies the policy name. This property is mandatory on creation. You cannot edit this property after creation. This is an alphanumeric string from 1 to 32 characters in length.

Scope

(scope)

The Scope parameter specifies the scope of this policy. The options are:

- exclusive
- template (default)

Selecting the exclusive option means that the policy can only be applied to a single SAP or SDP entity per network element.

Selecting the template option means that the policy can be applied to multiple SAP or SDP entities per network element.

93 – AOS Ethernet Service parameters

93.1 AOS Ethernet Service parameters 93-2

93.1 AOS Ethernet Service parameters

This chapter describes the parameters on the Ethernet Services Policies form and child forms.

802.1AB

(uni8021ABTreatment)

The 802.1AB parameter how the bridge handles 802.1AB PDUs on a UNI. Table 93-1 describes the parameter options.

Table 93-1 802.1AB parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

802.1x

(uni8021xTreatment)

The 802.1x parameter how the bridge handles 802.1x PDUs on a UNI. Table 93-2 describes the parameter options.

Table 93-2 802.1x parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

802.3ad

(uni8023adTreatment)

The 802.3ad parameter how the bridge handles 802.3ad PDUs on a UNI. Table 93-3 describes the parameter options.

Table 93-3 802.3ad parameter

Option	Option description
Drop	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer (default)	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

AMAP

(uniAmapTreatment)

The AMAP parameter how the bridge handles Adaptive Mobile Access Protocol (AMAP) PDUs on a UNI. Table 93-4 describes the parameter options.

Table 93-4 AMAP parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

Bandwidth Sharing

(bandwidthSharing)

The Bandwidth Sharing parameter specifies how bandwidth is shared on multiple ports of a SAP. The Bandwidth Sharing parameter is ignored if the [Ingress Bandwidth \(Mb\)](#) parameter is set to 0. Table 93-5 describes the parameter options.

Table 93-5 Bandwidth Sharing parameter

Option	Option description
Enabled	All ports that are part of the SAP use aggregated bandwidth, sharing some part of the bandwidth limit.
Disabled	Each port assigns some part of its bandwidth to the SAP.

CDP

(uniCdpTreatment)

The CDP parameter how the bridge handles CDP PDUs on a UNI. Table 93-6 describes the parameter options.

Table 93-6 CDP parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

CVLAN Treatment

(cVlanTreatment)

The CVLAN Treatment parameter specifies the type of VLAN stacking operation to be performed on a customer frame entering this service. Table 93-7 describes the parameter options.

Table 93-7 CVLAN Treatment parameter

Option	Option description
Stack SVLAN	The SVLAN tag is pre-pended to the frame before any existing 802.1Q tag.
Translate	The existing 802.1Q tag is replaced by the SVLAN tag.

Description

(description)

See the [Description](#) parameter in section 112.1.

Displayed Name

(displayName)

See the [Displayed Name](#) parameter in section 112.1.

DTP

(uniDtpTreatment)

The DTP parameter how the bridge handles Dynamic Trunking Protocol (DTP) PDUs on a UNI. Table 93-8 describes the parameter options.

Table 93-8 DTP parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

GVRP

(gvrpTreatment)

The GVRP parameter specifies how the bridge handles Generic Attribute Registration Protocol (GVRP) PDUs on a UNI. Table 93-9 describes the options for this parameter.

Table 93-9 GVRP parameter

Option	Option description
Tunnel (default)	The PDUs are allowed to tunnel across the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Drop	The PDUs are discarded and do not enter the provider network.

Ingress Bandwidth (Mb)

(ingressBW)

The Ingress Bandwidth parameter specifies the ingress bandwidth limit, in megabits, for traffic to which this profile is applied. A value of 0 indicates that there is no bandwidth limit. The default is 0.

LACPMARKER

(uniLacpTreatment)

The LACPMARKER parameter how the bridge handles Link Aggregation Control Protocol (LACP) marker PDUs on a UNI. Table 93-10 describes the parameter options.

Table 93-10 LACPMARKER parameter

Option	Option description
Drop	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer (default)	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

OAM

(uniOamTreatment)

The OAM parameter how the bridge handles Operations, Administration, and Management (OAM) PDUs on a UNI. Table [93-11](#) describes the parameter options.

Table 93-11 OAM parameter

Option	Option description
Drop	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer (default)	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

MVRP

(uniMvrpTreatment)

The MVRP parameter how the bridge handles Multiple VLAN Registration Protocol (MVRP) PDUs on a UNI. Table [93-12](#) describes the parameter options.

Table 93-12 MVRP parameter

Option	Option description
Drop	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel (default)	The PDUs are allowed to tunnel across the provider network.

PAGP

(uniPagpTreatment)

The PAGP parameter how the bridge handles Port aggregation protocol (PAGP) PDUs on a UNI. Table 93-13 describes the parameter options.

Table 93-13 PAGP parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

Priority

(fixedPriority)

The Priority parameter specifies the value of the priority field of the 802.1q SVLAN tag pre-pended to customer data frames when the fixed priority mapping mode is selected. The range is 0 to 7. The default is 0.

Priority Mapping

(priorityMapMode)

The Priority Mapping parameter specifies the source of the value used to populate the priority field of the SVLAN 802.1q tag when the tag is pre-pended to the customer data frame. Table 93-14 describes the options for this parameter.

Table 93-14 Priority Mapping parameter

Option	Option description
Fixed	Uses the value of the Priority parameter entered by the user.
Map Inner Pt to Outer P Bit	Uses the priority field value of an incoming tagged frame to fill in the priority field of the SVLAN tag.
Map Inner DSCP to Outer P Bit	Uses the priority value of the DSCP field of an incoming tagged frame to fill in the priority field of the SVLAN tag.

PVST

(uniPvstTreatment)

The PVST parameter how the bridge handles Per-VLAN Spanning Tree (PVST) PDUs on a UNI. Table 93-15 describes the parameter options.

Table 93-15 PVST parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

STP

(stpBpduTreatment)

The STP parameter specifies how the bridge handles Spanning Tree Protocol (STP) BPDUs on a UNI. Table 93-16 describes the options for this parameter.

Table 93-16 STP parameter

Option	Option description
Tunnel (default)	The BPDUs are allowed to tunnel across the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Drop	The BPDUs are discarded and do not enter the provider network.

Tunnel MAC

(tunnelMac)

The Tunnel MAC parameter specifies the MAC address used when configuring a protocol with the MAC-Tunnel option. The default address is the global MAC tunnel address of 01:00:0C:CD:CD:D0.

UDLD

(uniUddTreatment)

The UDLD parameter how the bridge handles Unidirectional Link Detection (UDLD) PDUs on a UNI. Table 93-17 describes the parameter options.

Table 93-17 UDLD parameter

Option	Option description
Drop	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer (default)	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

UPLINK

(uniUplinkTreatment)

The UPLINK parameter how the bridge handles UPLINK PDUs on a UNI. Table [93-18](#) describes the parameter options.

Table 93-18 UPLINK parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

VLAN

(uniVlanTreatment)

The VLAN parameter how the bridge handles VLAN PDUs on a UNI. Table [93-19](#) describes the parameter options.

Table 93-19 VLAN parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

VTP

(uniVtpTreatment)

The VTP parameter how the bridge handles VLAN Trunk Protocol (VTP) PDUs on a UNI. Table 93-20 describes the parameter options.

Table 93-20 VTP parameter

Option	Option description
Drop (default)	The PDUs are discarded and do not enter the provider network.
MAC-Tunnel	The destination MAC address of L2 control frames is changed to a unique tunnel MAC address, specified by the Tunnel MAC parameter.
Peer	On the assigned port, the bridge participates in the protocol.
Tunnel	The PDUs are allowed to tunnel across the provider network.

94 — Connection profile parameters

94.1 Connection profile policy parameters 94-2

94.1 Connection profile policy parameters

This chapter describes the parameters on the Connection Profile form and child forms.

Connection Profile ID

(id)

The Connection Profile ID parameter specifies the ID of the connection profile.

Description

See the [Description](#) parameter in section 112.1.

VCI

(vci)

The VCI parameter specifies the VCI of the connection profile. The options are 1, 2 or within the range 5 to 65535.

VPI

(vpi)

The VPI parameter specifies the VPI of the connection profile. The range is 0 to 4095. The default is 0.

95 – Service PW Template parameters

95.1 Service PW Template parameters 95-2

95.1 Service PW Template parameters

This chapter describes the parameters on the Service PW Template Manager form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Collect Stats

(collectAcctStats)

The Collect Stats parameter specifies whether the agent collects accounting statistics for the SDP Binding. When the value is set to true, the agent collects accounting statistics on the SDP Binding. The default is false.

Description

(shgDescription)

The Description parameter specifies a user-provided description for the split-horizon group on the SDP Binding. The range is 0 to 80 characters.

Discard Unknown Source

(discardUnknownSource)

The Discard Unknown Source parameter specifies whether packets with an unknown source MAC are dropped. Packets are dropped when the parameter is enabled. The default is disabled.

Egress Filter Type

The Egress Filter Type parameter specifies the type of egress filter to be used. The options are:

- No filter defined (default)
- Egress IP
- Egress IPv6
- Egress MAC

Enable Control Word

(controlWord)

The Control Word parameter specifies whether or not to use a control word on pseudowire packets in VPLS, and enables the use of the control word individually on each mesh or spoke SDP. When the Control Word parameter is enabled, all VPLS packets, including the BPDU frames, are encapsulated with the control word when sent over the pseudowire. The T-LDP control plane behavior is the same as in the implementation of the control word for VLL services. The configuration for the two directions of the Ethernet pseudowire should match. The options are:

- enabled
- disabled (default)

IGMP Fast Leave

(igmpFastLeave)

The IGMP Fast Leave parameter specifies whether fast-leave is allowed on the SDP Binding. If it is enabled, the system prunes the port on which an IGMP “leave” message has been received, without waiting for the Group Specific Query to timeout. The default is disabled.

IGMP General Query Interval (seconds)

(igmpGenQueryIntvl)

The IGMP General Query Interval (seconds) parameter specifies the interval (in seconds) between two consecutive general queries sent by the system on the SDP. The value of this object is only meaningful when the [IGMP Send Queries](#) parameter is enabled. The range is 2 to 1024. The default is 125.

IGMP Import Policy

(igmpImportPly)

The IGMP Import Policy parameter specifies a policy statement that must be applied to all incoming IGMP messages on the SDP Binding. The range is 0 to 32 characters.

IGMP Last Member Interval (deciseconds)

(igmpLastMembIntvl)

The IGMP Last Member Interval (deciseconds) parameter specifies the maximum response time (in tenths of a second) used in Group-Specific and Group-Source-Specific Queries that are sent in response to “leave” messages. This is also the amount of time between Group-Specific Query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The range is 1 to 50. The default is 10.

IGMP Max Number Groups

(igmpMaxNbrGrps)

The IGMP Max Number Groups parameter specifies how many group addresses are allowed for the SDP Binding. The value 0 means that no limit is imposed. The range is 0 to 1000. The default is 0.

IGMP Max Number Sources Per Group

(igmpMaxNbrGrps)

The IGMP Max Number Sources Per Group parameter specifies how many source addresses are allowed for each group for the SDP Binding. The value 0 means that no limit is imposed. The range is 0 to 1000. The default is 0.

IGMP Query Response Interval (seconds)

(igmpQueryRespIntvl)

The IGMP Query Response Interval (seconds) parameter specifies the maximum response time (in seconds) advertised in IGMPv2/v3 queries. The value of this object is only meaningful when the [IGMP Send Queries](#) parameter is enabled. The range is 1 to 1023. The default is 10.

IGMP Robust Count

(igmpRobustCount)

The IGMP Robust Count parameter specifies the value of the Robust count. This object allows tuning for the expected packet loss on the SDP. If an SDP is expected to be lossy, the Robustness Variable may be increased. IGMP snooping is robust to (Robustness Variable-1) packet losses. The value of this object is only meaningful when the [IGMP Send Queries](#) parameter is enabled. The range is 2 to 7. The default is 2.

IGMP Send Queries

(igmpSendQueries)

The IGMP Send Queries parameter specifies whether the system generates General Queries by itself on the SDP. Queries are generated when the parameter is enabled. The default is disabled.

IGMP Version

(igmpVersion)

The IGMP Version parameter specifies the version of IGMP for the PW template.

- Version 1
- Version 2
- Version 3 (default)

Import Route Target

(pwTemplateRouteTarget)

The Import Route Target parameter specifies the RT value that is used for import under the PW Template Binding. The default is target:0:0.

Ingress Filter Type

The Ingress Filter Type parameter specifies the type of ingress filter to be used. The options are:

- No filter defined (default)
- Ingress IP
- Ingress IPv6
- Ingress MAC

Limit MAC Move

(limitMacMove)

The Limit MAC Move parameter specifies the behavior when the re-learn rate specified by the [Move Frequency](#) parameter is exceeded. When Limit Mac Move is set to “blockable”, the MAC re-learn rate on the SDP Binding is monitored. It is blocked when the re-learn rate specified by the [Move Frequency](#) parameter is exceeded. When the parameter is set to “non-Blockable”, the SDP Binding is not blocked. Instead, another blockable SDP Binding is blocked. The default is blockable.

MAC Address Limit

(macAddressLimit)

The MAC Address Limit parameter specifies the maximum number of learned and static entries allowed in the FDB for the SDP Binding. The value 0 specifies no limit for the SDP Binding. The command is valid only for spoke SDPs. When the value of the chassis mode is not C or D, the maximum value of the parameter is 131071. The range is 0 to 196607. The default is 0.

MAC Aging

(macAgeing)

The MAC Aging parameter specifies whether the MAC aging process is enabled for the SDP Binding. The value is ignored if MAC aging is disabled at the service level. The default is disabled.

MAC Learning

(macLearning)

The MAC Learning parameter specifies whether the MAC learning process is enabled for the SDP Binding. The value is ignored if MAC learning is disabled at service level. The default is enabled.

MAC Pinning

(macPinning)

The MAC Pinning parameter specifies whether MAC address pinning is active on the SDP Binding (mesh or spoke). Setting the parameter to enabled disables re-learning of MAC addresses on other SAPs or SDPs within the same VPLS. The MAC address remains attached to the SDP Binding for the duration of its age-timer. This object has effect only for MAC addresses learned using the normal MAC learning process, and not for entries learned using DHCP. The parameter is set by default to disabled. However for a spoke SDP that belongs to a residential SHG, the value is set to enabled by the system, and cannot be altered by the operator. The default is disabled.

Policy ID

(policyId)

The Policy ID parameter specifies a numeric identifier for the policy. The parameter is configurable when the Auto Assign ID parameter is disabled. The minimum value is 1. There is no maximum value. The default is 0, which means that no value is specified.

Restrict Protected Source

(shgRestProtSrcMac)

The Restrict Protected Source parameter specifies how the agent handles re-learn requests for protected MAC addresses. When the value of this parameter is “true”, requests to re-learn a protected MAC address are ignored. The default is disabled.

Restrict Unprotected Destination

(shgRestUnprotDstMac)

The Restrict Unprotected Destination parameter specifies how the system forwards packets destined to an unprotected MAC address. When the value of this parameter is “true”, packets destined to an unprotected MAC address are dropped. The default is false.

Split Horizon Group Name

(shgName)

The Split Horizon Group Name parameter specifies the name of the SHG that the spoke SDP binding belongs to. By default, a spoke SDP binding does not belong to an SHG. Specify the name of an SHG in the TLS that contains the spoke SDP binding. The range is 0 to 32 characters. There is no default.

Use Provisioned SDP

(useProvisionedSdp)

The Use Provisioned SDP parameter specifies whether to use an already provisioned SDP. A value of “true” specifies that the tunnel manager is consulted for an existing active SDP. Otherwise, a value of “false” specifies that the default SDP template is used for instantiation of the SDP. The default is false.

VC Type

(vcType)

The VC Type parameter specifies the type of virtual circuit (VC) associated with the SDP Binding. The choices are:

- Ethernet (default)
- VLAN

VLAN VC Tag

(vlanVcTag)

The VLAN VC Tag parameter specifies the VLAN VC tag for the SDP Binding. The range is 0 to 4095. The default is 4095.

96 — Residential Subscriber parameters

96.1 Residential Subscriber parameters 96-2

96.1 Residential Subscriber parameters

This chapter describes the parameters on the Manage Residential Subscribers form and child forms.

Action

See the [Action](#) parameter in section [112.1](#).

Accounting Enabled

(accountingOn)

The Accounting Enabled parameter specifies the administrative state for the collection of accounting statistics. The options are:

- Enabled
- Disabled (default)

Active

(isActive)

The Active parameter indicates if the subscriber instance is present on the NE at this time. This is a read-only parameter. Table [96-1](#) lists the parameter options.

Table 96-1 Residential subscriber status options

Option	Option description
True	The Residential Subscriber Instance object is present on the NE.
False	The Residential Subscriber Instance object is absent from the NE.

Activity Threshold (kbps)

(activityThreshold)

The Activity Threshold parameter specifies the threshold (in kbps) that is applied to determine whether or not activity is going on. The range is 0 to 100 000 000. The default is 0.

Administrative State

See the [Administrative State](#) parameter in section [112.1](#).

Administrative State

(adminState)

The Administrative State parameter specifies whether a peer object is administratively enabled. Disabled peers are not used to exchange diameter messages. The options are:

- Disabled (default)
- Enabled

Administrative Version

(adminVersion)

The Administrative Version parameter specifies the configured IGMP version that is running for a host. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP. The options are:

- Version 1
- Version 2
- Version 3 (default)

Administrative State

(mcastReportingAdminState)

The Administrative State parameter specifies the administrative state of the multicast reporting destination. When the state is Down no multicast reports are sent. When the state is Up multicast reports are sent. The options are:

- Down (default)
- Up

Aggregate Rate Limit (kbps)

(hsmdaEgressAggRateLimit)

The Aggregate Rate Limit (kbps) parameter specifies the maximum total rate of all HSMDA egress queues for the subscriber. The parameter is only configurable when the associated “Assign Aggregate Rate Limit” check box is enabled. When the parameter is set to a value greater than 0, you cannot specify an egress scheduler. The range is –1, which means that the rate is unlimited, or 1 to 100 000 000.

ANCP String

(ancpString)

The ANCP String parameter specifies the ANCP string encoded in the identification strings. The range is 0 to 63 characters. There is no default.

Application

(application)

The Application parameter specifies a string that categorizes an SLA profile by the type of application to which the SLA profile applies. Specify a text string for the parameter. The range is 0 to 32 characters. There is no default.

Application Profile

(aaApplicationProfile)

The Application Profile parameter specifies a string that categorizes an application profile. The range is 0 to 32 characters. There is no default.

Application Profile String

(appProfileString)

The Application Profile String parameter specifies a string that categorizes an application profile. Specify a text string for the parameter. The range is 0 to 16 characters. There is no default.

Authentication Key

(md5AuthKey)

The Authentication Key parameter specifies the authentication key to be used between BGP peer neighbors when establishing sessions. Specify a string of up to 255 characters.

Assign Aggregate Rate Limit

The Assign Aggregate Rate Limit parameter specifies whether or not to use the aggregate rate limit to you set using the associated [Aggregate Rate Limit \(kbps\)](#) parameter. The options are:

- Disabled (default)
- Enabled

Average Frame Size

(averageFrameSize)

The Average Frame Size parameter specifies the average frame size value to be used in the adjustment of the subscriber aggregate rate to account for the per packet variable expansion of the last mile for the specific session used by the subscriber host. The range is 64 to 4096. A value of 0 disables the parameter.

BGP Keychain

(authKeyChain)

The BGP Keychain parameter specifies the keychain used to sign and/or authenticate the BGP protocol stream.

Circuit ID

(circuitId)

The Circuit ID parameter specifies the circuit ID to match against. When the value is not configured, the parameter is not used during the search. The range is 0 to 255.

Circuit ID Format

(circuitIdFormat)

The Circuit ID Format parameter specifies the how the circuit data is presented. The options are:

- Ascii (default)
- Hex

Cluster ID

See the [Cluster ID](#) parameter in section [189.1](#).

Connection Timer (seconds)

(connectionTimer)

The Connection Timer parameter specifies the delay (in seconds) before attempting to reconnect to a peer after a lost connection. This timer value is applied to all peer connections through the diameter policy. The range is 1 to 1000. The default is 30.

Credit Control Server

(crdtCtrlServer)

The Credit Control Server parameter specifies the credit control server type. The options are:

- RADIUS (default)
- Diameter

Credit Exhaust Threshold (%)

(creditExhstThrshld)

The Credit Exhaust Threshold parameter specifies the credit exhaust threshold taken into account to take action. The range is 50 to 100. The default is 100.

Credit Type

(creditType)

The Credit Type parameter specifies whether volume- or time-based accounting is performed. The options are:

- Volume (default)
- Time

Credit Type Override

(creditTypeOverride)

The Credit Type Override parameter specifies whether or not the accounting type specified by the [Credit Type](#) parameter will be inherited or overridden. A value of None inherits the previously specified accounting type. The options are:

- None (default)
- Time
- Volume

Custom Option Number

(optionId)

The Custom Option Number parameter specifies the number of the custom option. You must choose a number that has not been previously assigned to a standard option that is defined in RFC 2131.

The range is 1 to 254. The default is 1.

Days

(days)

The Days parameter specifies the number of days for a lease option. Table [96-2](#) lists the options that use the timing parameters and the descriptions. The range is 0 to 3650. The default is 0.

Table 96-2 Options that require time configuration

Option	Option description
Lease Time	This option is used in a client request (DCHCPDISCOVER or DHCPREQUEST) to allow a client to request a lease time for the IP address. In a DHCP OFFER the DHCP server uses this option to specify the lease time it can offer.
Lease Renew Time	This option is used to specify the time interval from address assignment to when the client transitions to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval from address assignment to when the client transitions to the REBINDING state.

Default Application Profile

(defaultApplicationProfile)

The Default Application Profile parameter specifies the default Application Profile for this MSAP. This parameter can have 0 to 32 characters.

Default Credit Time (seconds)

(defaultCreditTime)

The Default Credit Time parameter specifies the default value for the Time credit. This parameter is only configurable when the [Default Credit Type](#) parameter is set to Time. The range is 900 to 4 294 967 295. The default is 0.

Default Credit Type

(defaultCreditType)

The Default Credit Type parameter specifies the type of credit to be used by default. The options are:

- None (default)
- Time
- Volume

Default Credit Volume

(defaultCreditVolume)

The Default Credit Volume parameter specifies the default value for the Volume credit. This parameter is only configurable when the [Default Credit Type](#) parameter is set to Volume. The range is 0 to 4 294 967 295. The default is 0.

Default Credit Volume Unit

(defaultCreditVolUnit)

The Default Credit Volume Unit parameter specifies the unit in which the default value for the Volume credit is expressed. This parameter is only configurable when the [Default Credit Type](#) parameter is set to Volume. The options are:

- Bytes (default)
- Kilobytes
- Megabytes
- Gigabytes

Default Intermediate Destination Id Type

(defInterDestId)

The Default Intermediate Destination Id Type parameter specifies what type of information is used as the default intermediate destination identifier for an MSAP. This parameter is used in cases where no other source (such as RADIUS) provides an intermediate destination identifier. Table [96-3](#) lists the parameter options.

Table 96-3 Default Intermediate Destination Id Types

Option	Option description
String	The value of the Default Intermediate Destination Id parameter is used as the default intermediate destination identifier.
Use Top Queue Tag	The top q-tag of the MSAP is used as the default intermediate destination identifier.
None (default)	No default intermediate destination identifier is specified.

Default Intermediate Destination Id

(defInterDestIdStr)

The Default Intermediate Destination Id parameter specifies the default subscriber identification string for an MSAP. This parameter can have up to 32 characters.

Default SLA Profile

(defaultSlaProfile)

The Default SLA Profile parameter specifies the default SLA profile for this MSAP.

Default Subscriber ID

(defSubscriberIdString)

The Default Subscriber ID parameter specifies the Subscriber ID for the MSAP policy. This parameter can have 0 to 32 characters.

Default Subscriber Identification Policy

(defaultSubIdentPolicy)

The Default Subscriber Identification Policy parameter specifies the default Subscriber Identification Policy for this MSAP.

Default Subscriber Identification Type

(defSubscriberIdType)

The Default Subscriber Identification Type parameter specifies the type of subscriber identification to use for the MSAP policy. Table 96-4 lists the parameter options.

Table 96-4 Default subscriber identification types

Option	Description
SAP-ID	Use the SAP ID
String	Use a string that can contain up to 32 characters
None	There is no subscriber identification configured

Default Subscriber Profile

(defaultSubProfile)

The Default Subscriber Profile parameter specifies the default subscriber profile for this MSAP.

Description

See the [“Description”](#) parameter in section 112.1.

Destination Host

(destHost)

The Destination Host parameter specifies the value of the destination host attribute-value pair. The parameter is specified as a string of up to 80 characters.

Destination IP

See the [Destination IP](#) parameter in section 112.1.

Destination Name

(mcastReportingDestName)

The Destination Name parameter specifies the name of the multicast reporting destination as defined by a multicast reporting destination policy.

Destination Realm

(destRealm)

The Destination Realm parameter specifies the value of the destination realm attribute-value pair. The parameter is specified as a string of up to 80 characters.

DHCP String

(dhcpString)

The DHCP String parameter specifies the DHCP string of the Option 82 suboption to match against during host identification. When the value of this parameter is not specified, the parameter is not used for the search. The range is 0 to 255. There is no default.

Disable AC Cookies

(disableAcCookies)

The Disable AC Cookies parameter specifies whether the use of AC cookie tags are disabled during the PPPoE discovery phase. The options are:

- true
- false (default)

Disable SHCV

(disableSHCV)

The Disable SHCV parameter specifies whether SHCV is suspended if a port-down message is received. SHCV remains suspended until the NE sends a port-up message. The options are:

- true
- false (default)

When this parameter is set to True and the [Disable SHCV Hold Time \(seconds\)](#) parameter is set to 1 to 7200 s, the NE suspends SHCV for the period of time defined. When the Disable SHCP Hold Time parameter is set to 0, the NE suspends SHCV until a port-up message is received.

Disable SHCV Hold Time (seconds)

(disableSHCVHoldTime)

The Disable SHCV Hold Time (seconds) parameter specifies how long SHCV is suspended before the NE sends a port-up message. The range is 0 to 7200 s. The default is 0. This parameter is used in conjunction with the [Disable SHCV](#) parameter.

Disable SHCV Notification

(disableSHCVNtf)

The Disable SHCV parameter specifies whether an alarm should be raised before SHCV is suspended on the NE. The options are:

- true
- false (default)

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Domain Name

(domainName)

The Domain Name parameter specifies the name of a domain that is used to host users. The range is 0 to 32 characters. There is no default. If no value is specified, the domain name is an empty string.

DSCP

See the [DSCP](#) parameter in section [112.1](#).

Dst Mask

See the [Dst Mask](#) parameter in section [112.1](#).

Egress Aggregate Rate Limit (kbps)

(egressAggRateLimit)

The Egress Aggregate Rate Limit (kbps) parameter specifies the maximum total rate, in kb/s, of all egress queues for the subscriber. The parameter is configurable when the “No Egress Aggregate Rate Limit” check box is disabled. When the parameter is set to a value greater than 0, you cannot specify an egress scheduler. The range is –1, which means that the rate is unlimited, or 1 to 40 000 000.

Egress Aggregate Rate Limit (kbps)

(hsmdaEgressAggRateLimit)

The Egress Aggregate Rate Limit (kbps) parameter specifies the maximum total rate of all HSMDA egress queues for the subscriber. The parameter is configurable when the “No Egress Aggregate Rate Limit” check box is disabled. When the parameter is set to a value greater than 0, you cannot specify an egress scheduler. The range is –1, which means that the rate is unlimited, or 1 to 40 000 000.

Enable Reply On PADT

(enableReplyOnPadt)

The Enable Reply On PADT parameter specifies whether the system replies with a PADT packet when a PADT packet is received for an existing PPPoE session. The options are:

- true
- false (default)

Encapsulation Offset

(encapOffset)

The Encapsulation Offset parameter specifies the fixed packet offset. This fixed packet offset will be used in the adjustment of the subscriber aggregate rate, to account for the fixed offset and per packet variable expansion of the last mile for the specific session used by the subscriber host. The options are:

- None
- PPPoA LLC
- PPPoA NULL
- PPPoEoA LLC
- PPPoEoA FCS
- PPPoEoA Tagged
- PPPoEoA Tagged FCS
- PPPoEoA NULL
- PPPoEoA NULL FCS
- PPPoEoA NULL Tagged
- PPPoEoA NULL Tagged FCS
- IPoA LLC
- IPoA NULL
- IPoAoE LLC
- IPoAoE LLC FCS
- IPoAoE LLC Tagged
- IPoAoE LLC Tagged FCS
- IPoAoE NULL
- IPoAoE NULL FCS
- IPoAoE NULL Tagged
- IPoAoE NULL Tagged FCS
- PPOE
- PPOE Tagged
- IPOE
- IPOE Tagged

Encapsulation Offset Mode

(encapOffsetMode)

The Encapsulation Offset Mode parameter specifies how the fixed packet offset will be delivered. This fixed packet offset will be used in the adjustment of the subscriber aggregate rate, to account for the fixed offset and per packet variable expansion of the last mile for the specific session used by the subscriber host. A value of none(0) disables the adjustments. A value of auto(1) will derive the fixed packet offset from the encapsulation type value signaled in the Access-loop-encapsulation sub-TLV in the Vendor-Specific PPPoE Tags or DHCP Relay Options [rfc4679].

This parameter can only be configured using OSSl.

Entry ID

(id)

See the [ID](#) parameter in section [112.1](#).

Error Handling Action

(errorHandlingAction)

The Error Handling Action parameter specifies the action to be taken when an error occurs in the CC determination. The options are:

- Continue (default)
- Block

Failover Support

(failover)

The Failover Support parameter specifies whether the 5620 SAM supports moving the credit control (CC) message stream to a backup server during an ongoing CC session. The parameter is enabled by default.

Failure Handling

(failureHandling)

The Failure Handling parameter specifies what action is taken in the event of a DCCA session failure. The options are:

- Terminate (default)
- Continue
- Retry and Continue

Fast Leave

(fastLeave)

The Fast Leave parameter specifies whether fast leave is allowed for a host. If the parameter is enabled, the system prunes a port on which an IGMP “leave” message is received without waiting for the group specific query to timeout. The parameter is enabled by default.

Filter Direction

(direction)

The Filter Direction parameter specifies whether this entry applies to the egress or ingress SAP. The options are:

- Ingress (default)
- Egress

Fragment

See the [Fragment](#) parameter in section [112.1](#).

Frame Base Accounting

(schedulerPolicyFrameBasedAccnt)

The Frame Base Accounting parameter specifies whether to use frame-based accounting or packet-based accounting. Frame-based accounting uses the inter-frame gap and instructions to calculate overhead.

Group Name

The Group Name parameter specifies the name of the L2TP tunnel group. There is no default.

Host Limit

(hostLimit)

The Host Limit parameter specifies the maximum number of hosts that use this SLA profile. Enable the parameter to configure a maximum number of subscriber hosts for the SLA profile. The range is –1 to 100. The default is –1, which means that no limit is specified.

Host MAC

(hostMac)

The Host MAC parameter specifies whether this field is included in the multicast reporting messages. You must enable the check box to include the field in the multicast reporting message. The options are:

- Disabled (default)
- Enabled

Host Name

(hostName)

The Host Name parameter specifies the name of the local user database. The range is 1 to 32. There is no default.

Hours

(hours)

The Hours parameter specifies the number of hours for a lease option. Table [96-2](#) lists the options that use the timing parameters and the descriptions. The range is 0 to 23. The default is 0.

Include RADIUS User

(includeRadiusUsr)

The Include RADIUS User parameter specifies whether the diameter User-Name attribute-value pair is included in Credit Control Request (CCR) messages. The parameter is disabled by default.

Ingress Aggregate Rate Limit (kbps)

(hsmdaIngressAggRateLimit)

The Ingress Aggregate Rate Limit (kbps) parameter specifies the maximum total rate of all HSMDA ingress queues for the subscriber. The parameter is configurable when the “No Ingress Aggregate Rate Limit” check box is disabled. When the parameter is set to a value greater than 0, you cannot specify an ingress scheduler. The range is –1, which means that the rate is unlimited, or 1 to 40 000 000.

Inner Encapsulation Value

(innerEncapValue)

The Inner Encapsulation Value parameter specifies the inner encapsulation value for the port. This parameter is configurable when the encapsulation type for the port is Q in Q. The range is 0 to 4094, or 4095 or * to indicate that all tags are accepted, regardless of value. The default is 0, which means that the port has no inner encapsulation value.

Intermediate Destination

(intermediateDestId)

The Intermediate Destination parameter specifies to which intermediate destination, for example a DSLAM network device, the host belongs. Specify a text string for the parameter. The range is 0 to 32 characters. There is no default.

Intermediate Destination ID

(interDestIdString)

The Intermediate Destination String parameter specifies a string that identifies an Intermediate Destination. Specify a text string for the parameter. The range is 0 to 32 characters. There is no default.

IP Address

(peerAddress)

The IP Address parameter specifies the IP address of a peer. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

IP Address 1

(address1)

The IP Address parameter specifies an IP address for the Subnet Option in dotted-decimal format for an IPv4 address. The default is 0.0.0.0. IP Address 1 parameters is available when the [Type](#) parameter is set to IP Address

IP Address 2

(address2)

See the [IP Address 1](#) parameter in this section for more information.

IP Address 3

(address3)

See the [IP Address 1](#) parameter in this section for more information.

IP Address 4

(address4)

See the [IP Address 1](#) parameter in this section for more information.

IP Address

See the [IP Address](#) parameter in section [112.1](#).

IP Address Pool Name

(poolName)

The IP Address Pool Name parameter specifies the IP address pool that is used to search for the IP address of the host. This parameter can be set when the Address Type parameter value is set to unknown and the [Use GI Address](#) parameter value is set to false. The range is 0 to 32. There is no default.

IP Address Prefix Length

(addrPrefixLength)

The IP Address Prefix Length parameter specifies the prefix length of the address. The value is only relevant if the value of the object address type is not unknown. If the value is unknown, this parameter is ignored. The range is 0 to 32. The default is 0.

IP Option

(ipOptionValue)

See the [IP Option](#) parameter in section [112.1](#).

IP Opt Mask

(ipOptionMask)

See the [IP Opt Mask](#) parameter in section [112.1](#)

IPCP Subnet Negotiation

(ipcpNegotiation)

The IPCP Subnet Negotiation parameter specifies whether or not IPCP subnet negotiation is enabled. The options are:

- false
- true (default)

IPv6 Address

(ipv6Address)

The IPv6 Address parameter specifies the IPv6 address of the DHCP server. Specify an address in IPv6 format. The default is 0:0:0:0:0:0:0, which means that the parameter is not configured.

IPv6 Prefix

(ipv6Prefix)

The IPv6 Prefix parameter specifies the address prefix of the DHCP server. If you configure this parameter, you must configure the [IPv6 Prefix Length](#) parameter as well. The default is 0:0:0:0:0:0:0, which means that the parameter is not configured.

IPv6 Prefix Length

(ipv6PrefixLen)

The IPv6 Prefix Length parameter specifies the length of the address prefix stored in the [IPv6 Prefix Length](#) parameter. The range is 0 or 48 to 64. The default is 0.

Last Active State Change

(activeLastChange)

The Last Active State Change parameter specifies the GMT time for the last change of the [Active](#) property. This time indicates when a residential subscriber was deleted on an NE or re-created on an NE, depending on its current active state. This is a read-only parameter.

LCP Keep-Alive Hold Up Multiplier

(lcpKaHoldUpMplier)

The LCP Keep-Alive Hold Up Multiplier parameter specifies number of LCP keep alive messages that can be missed before the PPPoE session is terminated. The range is 10 to 300. The default is 30.

LCP Keep-Alive Interval (seconds)

(lcpKaInterval)

The LCP Keep-Alive Interval (seconds) parameter specifies the time, in s, between transmitted LCP echo requests. Table 96-5 lists the ranges for different device releases. The default is 30.

Table 96-5 LCP Keep-Alive Interval (seconds) parameter

Device release	Range
Release 8.0 and earlier	10 to 300
Release 9.0 and later	4 to 300

Local Address

See the [Local Address](#) parameter in section 189.1.

MAC Address

(clientMacAddress)

The MAC address parameter specifies the MAC address to match against. When the value is set to 00-00-00-00-00-00 (default), the MAC address is not used.

MAC Address

(clientMacAddress)

The MAC address parameter specifies the MAC address to match against. When the value is set to 00-00-00-00-00-00 (default), the MAC address is not used.

Mandatory Bandwidth (kbps)

(preRsvdMandatoryBandwidth)

The Mandatory Bandwidth parameter specifies the bandwidth that has been pre-reserved for all the mandatory channels associated with multicast CAC policy traffic in kilobits per second (kbps). Enable the No Constraint checkbox to set the parameter to the default value of -1. The range is -1 to 2 147 483 647. The No Constraint checkbox is enabled by default.

Match Type

(matchTypeDhcp)

The Match Type parameter specifies an object used to configure local user database masking for DHCP hosts.

There is no default. The options are:

- Circuit ID
- Option 60
- Remote ID
- SAP ID
- String
- System ID

Match Type

(matchTypePppoe)

The Match Type parameter specifies an object used to configure local user database masking for DHCP PPPoE hosts.

There is no default. The options are:

- Circuit ID
- Remote ID
- Service Name
- User Name

Match Type DHCP 1

(matchTypeDhcp1)

The Match Type DHCP 1 parameter specifies the second type of search criteria to identify subscribers.

There is no default. The options are:

- Circuit ID
- MAC Address
- None
- Option 60
- Remote ID
- SAP ID
- Service ID
- String
- System ID

Match Type DHCP 2

(matchTypeDhcp2)

The Match Type DHCP 2 parameter specifies the second type of search criteria to identify subscribers.

There is no default. The options are:

- Circuit ID
- MAC Address
- None
- Option 60
- Remote ID
- SAP ID
- Service ID
- String
- System ID

Match Type DHCP 3

(matchTypeDhcp3)

The Match Type DHCP 3 parameter specifies the second type of search criteria to identify subscribers.

There is no default. The options are:

- Circuit ID
- MAC Address
- None
- Option 60
- Remote ID
- SAP ID
- Service ID
- String
- System ID

Match Type DHCP 4

(matchTypeDhcp4)

The Match Type DHCP 4 parameter specifies the second type of search criteria to identify subscribers.

There is no default. The options are:

- Circuit ID
- MAC Address
- Option 60
- None
- Remote ID
- SAP ID
- Service ID
- String
- System ID

Match Type PPPoE 1

(matchTypePppoe1)

The Match Type PPPoE 1 parameter specifies the search criteria to identify subscribers. The order of the user match criteria determines the evaluation order. For example if the Match Type PPPoE 1 value is MAC Address, and the Match Type PPPoE 2 value is User Name, the database searches for users that match the MAC address before searching for users that match the User Name.

If the value of Match Type PPPoE 1 parameter is set to None, all subsequent Match Type PPPoE parameters must be set to none. The [Administrative State](#) parameter value must be set to Down before you can set any of the Match Type PPPoE parameters. There is no default. The options are:

- Circuit ID
- MAC Address
- None
- Remote ID
- User Name
- Service Name

Match Type PPPoE 2

(matchTypePppoe2)

The Match Type PPPoE 2 parameter specifies the second type of search criteria to identify subscribers. See the [Match Type PPPoE 1](#) parameter in this section for more information.

Match Type PPPoE 3

(matchTypePppoe3)

The Match Type PPPoE 3 parameter specifies the second type of search criteria to identify subscribers. See the [Match Type PPPoE 1](#) parameter in this section for more information.

Maximum Cumulative Buffer Space

See the [Cumulative MBS Contribution](#) parameter in section [59.1](#).

Maximum Frame Based Bandwidth

See the [Maximum Frame Based Bandwidth](#) parameter in section [59.1](#).

Maximum Host Lost Connectivity Rate (traps per second)

(maxHostLostConnectivityRate)

The Maximum Host Lost Connectivity Rate parameter specifies the number of lost host connectivity traps that the NE receives in one second before it raises a “Maximum Host Lost Connectivity rate exceeded” alarm. The parameter is configurable when the Rate Exceeded Raises Alarm parameter is enabled. When the Rate Exceeded Raises Alarm parameter is disabled, this parameter has no effect. The range is 1 to 10 000. The default is 20.

Maximum Number of Groups

(hostMaxGroups)

The Maximum Number of Groups parameter specifies the maximum number of groups for which IGMP can have local receiver information, based on received IGMP reports for a host. The range is 0 to 16000. The default is 0.

When this configuration is changed dynamically to a value lower than currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups are not allowed. When the parameter value is 0, there is no limit to the number of groups.

Maximum Sessions Per MAC

(maxSessionsPerMac)

The Maximum Sessions Per MAC parameter specifies the maximum number of PPPoE sessions that can be created per MAC address. The range is 1 to 63. The default is 1.

MD5 Authentication

(md5Auth)

The MD5 Authentication parameter specifies whether authentication using the MD5 message-based digest protocol is enabled. The parameter is set to False by default.

MED Source

See the [MED Source](#) parameter in section [189.1](#).

Minimum Separation Buffer Space

See the [Minimum Separation Buffer Space](#) parameter in section [59.1](#).

Minutes

(minutes)

The Minutes parameter specifies the number of minutes for a lease option. Table [96-2](#) lists the options that use the timing parameters and the descriptions. The range is 0 to 59. The default is 10.

Monitoring Period

(monitoringPeriod)

The Monitoring Period specifies the length of time that selected residential subscriber hosts or SAPs are actively monitored for specific DHCP event changes. You enter a numeric value for this parameter and use it in conjunction with the [Units](#) parameter, which specifies the unit of time measurement, for example, “10” and “hours”.

The maximum possible period is 72. However, the actual maximum period may be less than this, since it is also dependent on how many events are recorded during the monitoring period you specify. For residential subscriber hosts, the actual maximum period is also affected by the [Polling Interval](#) parameter option that you choose.

MSAP Group Interface Name

(msapGroupInterfaceName)

The MSAP Group Interface Name parameter specifies the group interface name for RADIUS-authenticated MSAPs. The range is 0 to 32. The default is 0.

MSAP Policy Name

(msapPolicyName)

The MSAP Policy Name parameter specifies the name of the MSAP policy for RADIUS-authenticated MSAPs. The range is 0 to 32. The default is 0.

MSAP Service ID

(msapServiceId)

The MSAP Service ID parameter specifies the service ID for RADIUS-authenticated MSAPs. The range is 0 to 2 147 483 648. The default is 0.

Multiple Option

(multipleOption)

See the [Multiple Option](#) parameter in section [112.1](#).

Netbios Node Type

(netbiosNodetype)

The Netbios Node Type parameter specifies the order and method to resolve a Netbios name into an IP address. Table [96-7](#) lists the parameter options and the option numbers.

Table 96-6 Netbios parameter options

Option	Option Description
Unspecified	Unspecified
B	The DHCP server uses broadcast for name resolution and registration.
P	The DHCP server uses peer to peer for name resolution and registration.
M	The DHCP server uses a combination of broadcast and peer to peer. If broadcast cannot resolve the name, it uses peer to peer.
H	The DHCP server uses a combination of peer to peer and broadcast. If peer to peer cannot resolve the name, it uses broadcast.

New Subscriber Identification

(newSubscrIdent)

The New Subscriber Identification parameter specifies the new identifier for the subscriber. The range is 1 to 32 characters. There is no default.

No Constraint

The No Constraint parameter specifies whether the [Mandatory Bandwidth \(kbps\)](#) or [Unconstrained Bandwidth \(kbps\)](#) parameters are set to their default values, or can be configured. The options are:

- disabled
- enabled (default)

When the No Constraint parameter is set to enabled, you cannot configure the associated parameters.

Non-Subscriber Traffic Application Profile

(nonSubTrafficAppProfile)

The Non-Subscriber Traffic Application Profile parameter specifies the default Application Profile on the MSAP policy.

Non-Subscriber Traffic SLA Profile

(nonSubTrafficSlaProfile)

The Non-Subscriber Traffic SLA Profile parameter specifies the default non-subscriber traffic SLA profile on the MSAP policy and is meaningful when the Subscriber Limit parameter is set to 1.

Non-Subscriber Traffic Identification

(nonSubTrafficIdent)

The Non-Subscriber Traffic Identification parameter specifies the string for non-subscriber traffic subscriber identification on the MSAP policy and is meaningful when the Subscriber Limit parameter is set to 1. The string can have 0 to 32 characters.

Non-Subscriber Traffic Subscriber Profile

(nonSubTrafficSubProfile)

The Non-Subscriber Traffic Subscriber Profile parameter specifies the default non-subscriber traffic subscriber profile on the MSAP policy and is meaningful when the Subscriber Limit parameter is set to 1.

Number

(optionNumber)

The Number parameter is used to identify options. All other DHCP protocol options are available and can be set by entering the option number, defined in RFC 2131

The range is 1 to 254. The default is 1.

Option

(option)

The Option parameter specifies the option that the DHCP server uses to search for DHCP or PPPoE clients. The values for the Option parameter match the CLI option list. When the parameter value is Custom Option, you must enter an “[Option Number](#)”. For all other Option values the “[Option Number](#)” value is entered automatically. Table 96-7 lists the parameter options and the option numbers.

Table 96-7 Option parameter

Option	Option Number
Custom Option(default)	999
Subnet Mask	1
Default Routers	3
DNS Name Servers	6
Domain Name	15
Netbois Name Server	44
Netbois Node Type	46
Lease Time	51
Lease Renew Timer	58
Lease Rebind Timer	59

Option 60

(dhcpOption60)

The Option 60 parameter specifies the option to match against during host identification. When the value is not specified the parameter is not used for a search. The range is 0 to 32. There is no default.

Option Number

(optionNumber)

The Option Number parameter specifies the option number that the DHCP server uses to send the identification strings to the DHCP or PPPoE client. When the parameters value is set to 0, no identification strings are sent. The range is 0 to 254. The default is 0.

Option Present

(optionPresent)

See the [Multiple Option](#) parameter in section 112.1.

Option Protocol

(protocol)

The Option Protocol parameter specifies which protocol is used to configure, enable and disable the IP protocol on both ends of the point to point link. The options are:

- LCP (default)
- IPCP

Option Type

(optionType)

The Option Type parameter specifies the format for storing the [Option Value](#) parameter. For a PPPoE policy, the [Option Value](#) parameter value must be IPv4 Address. The options are:

- IPv4 Address (default)
- String
- Hex

Option Value

(optionValue)

The Option Value parameter specifies the value of this option. The range is 0 to 80. There is no default.

Origin Subscription ID

(subscriptionIdOrigin)

The Origin Subscription ID parameter specifies the origin of the information stored in the Subscription-Id-Data attribute-value pair. The options are:

- Subscriber ID (default)
- Circuit ID

Out Of Credit Action

(outOfCreditAction)

The Out Of Credit Action parameter specifies the action to be taken if the credit is exhausted. The options are:

- None (default)
- Continue
- Block Category
- Change Service Level

Outer Encapsulation Value

(outerEncapValue)

The Outer Encapsulation Value parameter specifies the outer encapsulation value for the port. This parameter is configurable when the encapsulation type for the port is Dot1q or Q in Q. Table 96-8 lists the parameter ranges for different encapsulation types. The default is 0, which means that the port has no outer encapsulation value.

Table 96-8 Outer Encapsulation Value parameter

Encapsulation type	Range
Dot1q	0 to 4094
Q in Q	0 to 4094 or 1 to 4094

Packet Byte Offset (bytes)

(hsmdaEgrPackByteOffOvr)

The Packet Byte Offset (bytes) parameter specifies the packet byte offset of an HSM DA egress policy for this subscriber. The parameter is only configurable when the associated “Override” check box is enabled. The range is -32 to +31. The value 0 means that there is no override. There is no default value.

PADO Delay (100’s of milliseconds)

(padoDelay)

The PADO Delay parameter specifies the delay timeout before sending a PADO. The range is 0 to 30. The default is 0.

Password Type

(passwordType)

The Password Type parameter specifies the PPP protocol used to authenticate a PPPoE session. The value None indicates that no PPP authentication is done. When you choose the value For PAP (Password Authentication Protocol) and For CHAP (Challenge Handshake Authentication Protocol) as the Password Type parameter value, you must set the [Password](#) parameter. The options are:

- None
- ignore
- For PAP
- For CHAP

Password

(password)

The Password parameter specifies the password of the host. The Password parameter is configurable when [User Name](#) parameter is configured.

PIR (kbps)

(pir)

The PIR parameter specifies the PIR rate override value (in kbps) for this category. The range is -2 to 1 000 000 000. The default is -2.

Policy 1

(exportPolicy1)

The Policy 1 parameter specifies the first export policy for a peer. Specify a string of up to 32 characters or use the Select button beside the Policy parameter to choose a policy from the list of policies. There is no default.

The Policy parameters specify the names of export route policies used to determine which routes are sent to peers and which routes are advertised to peers. When multiple Policy parameters are specified, the policies are evaluated in the order in which they are specified. The first policy that matches is applied.

Policy 2

(exportPolicy2)

See the [Policy 1](#) parameter in this section for more information.

Policy 3

(exportPolicy3)

See the [Policy 1](#) parameter in this section for more information.

Policy 4

(exportPolicy4)

See the [Policy 1](#) parameter in this section for more information.

Policy 5

(exportPolicy5)

See the [Policy 1](#) parameter in this section for more information.

Policy 1

(importPolicy1)

The Policy 1 parameter specifies the first import policy for a peer. Specify a string of up to 32 characters or use the Select button beside the Policy parameter to choose a policy from the list of policies. There is no default.

The Policy parameters specify the names of import route policies used to determine which routes are sent to peers and which routes are advertised to peers. When multiple Policy parameters are specified, the policies are evaluated in the order in which they are specified. The first policy that matches is applied.

Policy 2

(importPolicy2)

See the [Policy 1](#) parameter in this section for more information.

Policy 3

(importPolicy3)

See the [Policy 1](#) parameter in this section for more information.

Policy 4

(importPolicy4)

See the [Policy 1](#) parameter in this section for more information.

Policy 5

(importPolicy5)

See the [Policy 1](#) parameter in this section for more information.

Polling Interval

(pollingInterval)

The Polling Interval specifies the SNMP interval at which selected residential subscriber hosts are polled for specific DHCP event changes. You choose the value for the Polling Interval from the associated drop-down menu, with a range of 1 to 60 minutes. The default is 10 minutes. This parameter is used in conjunction with the Monitoring Period parameter.

Port Number

(transportPort)

The Port Number parameter specifies the port number assigned to a peer. The default is 3868.

PPP MTU

(mtu)

The PPP MTU parameter specifies the largest IP packet that can be sent out without being fragmented over the specific PPPoE tunnel. The range is 0 to 9212. The default is 0.

PPPoE Session ID

(pppoeSessionId)

The PPPoE Session ID parameter specifies whether this field is included in the multicast reporting messages. You must enable the check box to include the field in the multicast reporting message. The options are:

- Disabled (default)
- Enabled

Preference

(preference)

The Preference parameter specifies the priority level assigned to a peer object, relative to other peers associated with the same diameter policy. The lowest Preference value (1) indicates the highest priority level. If multiple peers are associated with a diameter policy, the peer with the lowest Preference value is used. If multiple peers with the same Preference value are assigned to a diameter policy, one of them is used.

The range is 1 to 100. The default is 50.

Prefix Length

(maskPrefixNum)

The Prefix Length parameter specifies the number of characters to remove from the start of the incoming string before it is matched against the value configured in the corresponding object in the local user database table. The range is 0 to 127. The default is 0. At least one of the values of the Prefix Length and Prefix String parameters must be equal to the default value.

Prefix String

(maskPrefixStr)

The Prefix String parameter specifies a substring that is stripped off the start of the incoming string before it is matched against the value configured in the corresponding object in the local user database table. The string must contain printable ASCII characters. You can use * as a wildcard. The range is 0 to 127. The default is the empty string. At least one of the values of the Prefix Length and Prefix String parameters must be equal to the default value.

Primary Script Administrative State

(script1AdministrativeState)

The Primary Script Administrative State parameter specifies the administrative state for the primary subscriber identification script. The options are:

- Disabled (default)
- Enabled

Primary Script URL

(script1Url)

The Primary Script URL parameter specifies the location of the primary subscriber identification script. The range is 0 to 180 characters. The default is 0, which means that no value is specified.

Profiled Traffic Only

(profiledTrafficOnly)

The Profiled Traffic Only parameter specifies the use of profiled traffic when set to True.

Protocol

See the [Protocol](#) parameter in section 112.1.

Protocol

(transportProtocol)

The Protocol parameter specifies the transport protocol used by a peer. The default is TCP.

RADIUS Called-Station-ID

(calledStationId)

The RADIUS Called-Station-ID parameter specifies the RADIUS Called-Station-ID attribute-value pair (AVP). If specified, the AVP is included in Credit Control Request (CCR) messages. The parameter is specified as a string of up to 64 characters.

Rate Adjustment

(egrRateAdjustment)

The Rate Adjustment parameter specifies the rate adjustment for the rate modification scheduler. This parameter is used when the rate returned by the DSLAM is calculated with a different encapsulation than the rate of the 7450 ESS or the 7750 SR. The range is 1 to 200. The default is 100.

Rate Adjustment

(ingRateAdjustment)

The Rate Adjustment parameter specifies the rate adjustment for the rate modification scheduler. This parameter is used when the rate returned by the DSLAM is calculated with a different encapsulation than the rate of the 7450 ESS or 7750 SR. The range is 1 to 200. The default is 100.

Rate Exceeded Raises Alarm

(rateExceededRaisesAlarm)

The Rate Exceeded Raises Alarm parameter specifies whether exceeding the trap rate specified by the Maximum Host Lost Connectivity Rate (traps per second) parameter generates a “HostConnectivityLostRateExceeded” alarm. The options are:

- enabled
- disabled (default)

Rate Modification

(egrRateModificationType)

The Rate Modification parameter specifies the egress rate modification that is applied to the ANCP policy. The options are:

- None (default)
- Agg-rate-limit
- Scheduler

When this parameter is set to Scheduler, the scheduler specified in the Rate Modification Scheduler parameter is used.

Rate Modification

(ingRateModificationType)

The rate Modification parameter specifies the ingress rate modification that is applied to the ANCP policy. The options are:

- None (default)
- Scheduler

When this parameter is set to Scheduler, the scheduler specified in the Rate Modification Scheduler parameter is used.

Rate Modification Scheduler

(egrRateModSchedulerName)

The Rate Modification Scheduler parameter specifies the scheduler used to modify the egress traffic rate for the subscriber. You can only configure this parameter when the [Rate Modification](#) parameter is set to Scheduler.

Rate Modification Scheduler

(egrRateModSchedObjPointer)

The Rate Modification Scheduler parameter specifies the scheduler where you apply the egress rate modification rate.

Rate Modification Scheduler

(ingRateModSchedObjPointer)

The Rate Modification Scheduler parameter specifies the scheduler to which you apply the ingress rate modification.

Rate Monitor (kbps)

(egrRateMonitor)

The Rate Monitor (kbps) parameter specifies the egress rate below which an NE generates an event. When the [Rate Monitor Notification](#) parameter is set to true, an alarm is raised. The range is 0 to 4294967295. The default is 0.

Rate Monitor (kbps)

(ingRateMonitor)

The Rate Monitor (kbps) parameter specifies the ingress rate below which an NE generates an event. When the [Rate Monitor Notification](#) parameter is set to true an alarm is raised. The range is 0 to 4294967295. The default is 0.

Rate Monitor Notification

(egrRateMonitorNtf)

The Rate Monitor Notification parameter specifies whether an egress monitored event generates an SNMP notification. The options are:

- true
- false (default)

Rate Monitor Notification

(ingRateMonitorNtf)

The Rate Monitor Notification parameter specifies whether an ingress monitored event generates an SNMP notification. The options are:

- true
- false (default)

Rate Reduction (kbps)

(egrRateReduction)

The Rate Reduction (kbps) parameter specifies the constant rate reduction to the egress rate specified by the DSLAM. This parameter is used if an NE needs to adjust the egress rate to a value that is offset compared to the total that is available on the DSLAM. The range is 0 to 4 294 967 295. The default is 0.

Rate Reduction (kbps)

(ingRateReduction)

The Rate Reduction (kbps) parameter specifies the constant rate reduction to the ingress rate specified by the DSLAM. This parameter is used if an NE needs to adjust the ingress rate to a value that is offset compared to the total that is available on the DSLAM. The range is 0 to 4 294 967 295. The default is 0.

Rating Group

(ratingGroup)

The Rating Group parameter specifies the rating group that will be applicable for a given category. The range is 0 to 4 294 967 295. The default is 0.

Redirection Policy

(redirectionPolicy)

The Redirection Policy parameter specifies the redirection policy to be used to filter IGMP packets. Click on the Select button to choose a policy from the list of redirection policies.

Remote ID

(remoteId)

The Remote ID parameter specifies the remote ID to match against during host identification. When the value of this parameter is not specified, the parameter is not used for the search. The range is 0 to 255. There is no default.

Remote ID Format

(remoteIdFormat)

The Remote ID Format parameter specifies how the value of the remote ID is specified. The options are:

- ASCII—contains seven-bit ASCII characters
- Hex—contains octets. The value must be in hexadecimal format.

The default is ASCII.

Remove oldest Subscriber Host

(removeOldestHostOn)

The Remove oldest Subscriber Host parameter specifies the action that the NE hosting the SAP takes when the number of subscriber hosts using the SLA profile reaches the maximum specified by the Host Limit parameter. The parameter is configurable when the Host Limit parameter is enabled. Table 96-9 lists the parameter options:

Table 96-9 Remove oldest Subscriber Host parameter

Option	Option description
disabled (default)	Specifies that the 5620 SAM rejects a new subscriber host that requests the SLA profile
enabled	Specifies that the 5620 SAM accepts a new subscriber host that requests the SLA profile and removes the subscriber host that has had the longest association with the SLA profile

Residential Subscriber Creation

(creationTime)

The Residential Subscriber Creation parameter specifies the GMT time of the initial creation of a residential subscriber instance in the 5620 SAM. This is a read-only parameter.

Retail Service ID

(retailServiceId)

The Retail Service ID parameter specifies the retailer VPRN service ID that is configured as a part of the business PPPoE. The range is 0 to 2147483647. The default is 0.

Retention Time (hours)

(retentionInterval)

The Retention Time (hours) parameter specifies the minimum time that the 5620 SAM database stores the log files. The range is 1 to 8760. The default is 720.

SAP ID

Table 96-10 lists where to find more information about the SAP ID parameter.

Table 96-10 SAP ID parameter

Parameter	See
SAP ID to match against for host identification	SAP ID parameter in this section

(1 of 2)

Parameter	See
SAP ID to include in multicast reporting messages	SAP ID parameter in this section

(2 of 2)

SAP ID

(sapId)

The SAP ID parameter specifies the SAP ID to match against during host identification. This parameter is a suboption of option 82. When the value of this parameter is not specified, the parameter is not used for the search. The range is 0 to 255. There is no default.

SAP ID

(sapId)

The SAP ID parameter specifies whether to include the SAP ID field in the multicast reporting messages. You must enable the check box to include the field in the message. The options are:

- Disabled (default)
- Enabled

Scheduler Type

(schedulerType)

The Scheduler Type parameter specifies the type of scheduling for queued traffic. The options are:

- port scheduler (default)
- virtual port scheduler

Secondary Script Administrative State

(script2AdministrativeState)

The Secondary Script Administrative State parameter specifies the administrative state for the secondary subscriber identification script. The options are:

- Disabled (default)
- Enabled

Secondary Script URL

(script2Url)

The Secondary Script URL parameter specifies the location of the secondary subscriber identification script. The range is 0 to 180 characters. The default is 0, which means that no value is specified.

Seconds

(seconds)

The Seconds parameter specifies the number of seconds for a lease option. Table 96-2 lists the options that use the timing parameters and the descriptions. The range is 0 to 3650. The default is 0.

Server Address

(dhcpServerAddress)

The Server Address parameter specifies the address of the DHCP server to relay to. The default is 0.0.0.0.

Service Context ID

(serverContextId)

The Service Context ID parameter specifies the DCCA Service-Context-Id attribute-value pair (AVP). If specified, the AVP is included in Credit Control Request (CCR) messages. The parameter is specified as a string of up to 32 characters.

Service ID

(serviceId)

The Service ID parameter specifies a unique ID for the service. The range is 1 to 2 147 483 647. The default is 0, which indicates that the parameter is not set.

Service ID

(svcId)

The Service ID parameter specifies whether this field is included in the multicast reporting messages. You must enable the check box to include the field in the multicast reporting message. The options are:

- Disabled (default)
- Enabled

Service Name

(serviceName)

The Service Name parameter specifies the PPPoE service name to match against. The range is 0 to 255. The default is 0.

SLA Profile String

(slaProfileString)

The SLA Profile String parameter specifies a string that identifies a SLA profile. Specify a text string for the parameter. The range is 0 to 32 characters. There is no default.

SLA Profile String

(displayName)

The SLA Profile String parameter specifies an alias for the SLA profile. The range is 1 to 32 characters.

Source IP

See the [Source IP](#) parameter in section [112.1](#).

Src Mask

See the [Src Mask](#) parameter in section [112.1](#).

Static Multicast Group

(staticGrp)

The Static Multicast Group parameter specifies the IP multicast group address for which an entry contains information. Specify an IPv4 address. the default is 224.0.1.0.

Static Source

(staticSrcGrp)

The Static Source parameter specifies the address of the source sending multicast traffic to the group identified in the [Static Multicast Group](#) parameter. Specify an IPv4 address. the default is 0.0.0.0.

Strings From Option

(stringFromOption)

The Strings From Option parameter specifies how the SLA profile and subscriber profile identification strings are derived. When the parameter is set to 0, the strings are obtained using the identification scripts. A value greater than 0 specifies the DHCP option number from which the strings are directly obtained. The range is 0 to 4 294 967 295. The default is 0.

Subscriber ID Alias

(subscrAlias)

The Subscriber ID Alias parameter specifies an alias for the subscriber ID. The range is 0 to 64 characters.

Subscriber ID

(subscriberIdString)

The Subscriber ID parameter specifies the option number that the DHCP server uses to send the identification strings to the DHCP and PPPoE client. When the parameter value is 0, no identification strings are sent. The range is 0 to 32 characters.

Subscriber Identification

(displayName)

The Subscriber Identification parameter specifies an identifier for the subscriber in the explicit map. The range is 1 to 32 characters.



Note — You cannot use the colon symbol in the subscriber identifier. The 5620 SAM uses colons as separators for the object full name.

Subscriber Identification

(subscrIdent)

The Subscriber Identification parameter specifies an identifier for the subscriber for a PPPoE session. The range is 1 to 32 characters. There is no default.

Subscriber Limit

(subscriberLimit)

The Subscriber Limit parameter specifies the maximum number of subscribers allowed for this MSAP. If the value is 1, the Profiled Traffic Only, Non-Subscriber Traffic Identification, Non-Subscriber Traffic Profile, and Non-Subscriber Traffic SLA Profile parameters are meaningful. The value zero specifies that there is no limit. The range is 0 to 20 000. The default value is 1.

Subscriber Mapped Profile String

(subscrProfileString)

The Subscriber Mapped Profile String parameter specifies the mapped string to the subscriber profile assigned to the subscriber host. The range is 0 to 16 characters. There is no default.

Subscriber Mapped SLA Profile String

(subscrProfileString)

The Subscriber Mapped SLA Profile String parameter specifies the mapped string to the subscriber SLA profile assigned to the subscriber host. The range is 0 to 16 characters. There is no default.

Subscriber Profile String

(displayedName)

The Subscriber Profile String parameter specifies an alias for the subscriber profile. The range is 1 to 32 characters.

Subscriber Profile String

(subscriberProfileString)

The Subscriber Profile String parameter specifies a string that identifies a subscriber profile. Specify a text string for the parameter. The range is 0 to 16 characters. There is no default.

Subscription ID Type

(subscriptionIdType)

The Subscription ID Type parameter specifies the type of identifier stored in the Subscription-Id-Data attribute-value pair. The options are:

- Private (default)
- E164

Suffix Length

(maskSuffixNum)

The Suffix Length parameter specifies the number of characters to remove from the end of the incoming string before it is matched against the value configured in the corresponding object in the local user database table. The range is 0 to 127. The default is 0. At least one of the values of the Suffix Length and Suffix String parameters must be equal to the default value.

Suffix String

(maskSuffixStr)

The Suffix String parameter specifies a substring that is stripped off the end of the incoming string before it is matched against the value configured in the corresponding object in the local user database table. The string must contain printable ASCII characters. You can use * as a wildcard. The range is 0 to 127. The default is the empty string. At least one of the values of the Suffix Length and Suffix String parameters must be equal to the default value.

System ID

(systemId)

The System ID parameter specifies the system ID of the Option 82 suboption to match against during host identification. When the value of this parameter is not specified, the parameter is not used for the search. The range is 0 to 255. There is no default.

Tertiary Script Administrative State

(script3AdministrativeState)

The Tertiary Script Administrative State parameter specifies the administrative state for the tertiary subscriber identification script. The options are:

- Disabled (default)
- Enabled

Tertiary Script URL

(script3Url)

The Tertiary Script URL parameter specifies the location of the tertiary subscriber identification script. The range is 0 to 180 characters. The default is 0, which means that no value is specified.

Transaction Timer (seconds)

(transactionTimer)

The Transaction Timer parameter specifies the wait time (in seconds) for an answer from a peer after sending a connection request. This timer value is applied to all peer connections through the diameter policy. The range is 1 to 1000. The default is 30.

Trap Dropped Raises Alarm

(trapDroppedRaisesAlarm)

The Trap Dropped Raises Alarm parameter specifies whether the 5620 SAM raises a “Maximum Host Lost Connectivity rate exceeded” alarm against the subscriber when the NE drops a sapHostConnectivityLost trap. Dropping a trap can indicate a connectivity problem when alarm blocking is enabled and multiple connectivity-loss events generate a flood of traps. Enabling this parameter helps to alert 5620 SAM operators to potential connectivity problems that may otherwise not be immediately noticed. The options are:

- enabled
- disabled (default)

Tx Timer (seconds)

(txTimer)

The Tx Timer parameter specifies the DCCA Tx timer value (in seconds). The range is 10 to 1000. The default is 10.

Type

(optionType)

The Type parameter specifies the format the DHCP host sends the option to the DHCP client. The options are:

- IP Address
- ASCII String
- Hex String

Unconstrained Bandwidth (kbps)

(unconstrainedBandwidth)

The Unconstrained Bandwidth parameter specifies the bandwidth assigned for the interface's multicast CAC policy traffic in kilobits per second (kbps). Enable the No Constraint checkbox to set the parameter to the default value of -1. If a default value of -1 is set, then the value is set to the physical bandwidth available for the interface. The range is -1 to 2 147 483 647. The No Constraint checkbox is enabled by default.

Units

(units)

The Units parameter is used in conjunction with the [Monitoring Period](#) parameter, which specifies the length of time that selected residential subscriber hosts or SAPs are actively monitored for specific DHCP event changes. You choose the value of Units from the associated drop-down menu. The default is minutes.

Use Client Pool

(useClientPool)

The Use Client Pool parameter specifies if the IP address pool used to search for an IP address for the host is indicated by the vendor-specific sub-option 13 of the DHCP option 82. This object can only be set to true (1) when the value of `tmnxLocUsrDbPppoeAddrType` is unknown (0) and `tmnxLocUsrDbPppoePool` contains the empty string. The options are:

- true
- false (default)

Use Direct Map as Default

(useDirectMapAsDefault)

The Use Direct Map as Default parameter specifies whether an SLA or subscriber profile string in the DHCP option information maps directly to an SLA or subscriber profile. When the parameter is set to true and no matching profile string is found, the profile string is used as the profile name. The options are:

- true
- false (default)

Use Egress QoS Marking From SAP

(egrQosMarkingFromSap)

The Use Egress QoS Marking From SAP parameter specifies whether the egress QoS marking is based on the egress QoS policy associated with a SAP (default) or derived from the egress QoS policy associated with the SLA profile. The options are:

- enabled (default)
- disabled

Use GI Address

(useGiAddress)

The Use GI Address parameter specifies whether the GI address is used to search for the IP address of the host. If the value is set to true, the gateway IP address is used. The value can only be set to true, when the value for the Address Type is set to 0 and the [IP Address Pool Name](#) parameter value contains an empty string. The options are:

- True
- False (default)

Use Multipoint Shared Queue

(multipointSharedQueueOn)

The Use Multipoint Shared Queue parameter specifies whether the SLA profile uses the multipoint shared queue on the device. The options are:

- enabled
- disabled (default)

Use Shared Queue

(sharedQueueOn)

The Use Shared Queue parameter specifies whether the SLA profile uses the shared queue on the device. The options are:

- enabled
- disabled (default)

User Name

(userName)

The User Name parameter specifies the name to match when searching for a PPPoE Host. The range is 0 to 32 characters. When 0 is used, a user name is not specified.

User Name Format

(userNameFormat)

The User Name Format parameter specifies the format of the user name. When the Full value is selected the both the host and domain parts of the user name is specified. For example, john@alcatel-lucent.com. The options are:

- None
- Full
- Domain only
- Host only

Virtual Router Type

(virtualRouterType)

The Virtual Router Type parameter specifies the type of virtual router used for communication with peers. The options are:

- Base Router (default)
- Management Router
- VPRN Service (you must specify a VPRN service name)

VLAN for all Services (Bridged)

(vlanAllServicesBridged)

The VLAN for all Services (Bridged) parameter specifies the intent to include bridged VLAN for all services functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

VLAN for all Services (Routed)

(vlanAllServicesRouted)

The VLAN for all Services (Routed) parameter specifies the intent to include routed VLAN for all services functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

VLAN per ISP per Service (Bridged)

(vlanPerISPPerServiceBridged)

The VLAN per Subscriber (Bridged) parameter specifies the intent to include bridged VLAN per ISP per service functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

VLAN per ISP per Service (Routed)

(vlanPerISPPerServiceRouted)

The VLAN per Subscriber (Routed) parameter specifies the intent to include routed VLAN per ISP per service functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

VLAN per Service (Bridged)

(vlanPerServiceBridged)

The VLAN per Service (Bridged) parameter specifies the intent to include bridged VLAN per service functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

VLAN per Service (Routed)

(vlanPerServiceRouted)

The VLAN per Service (Routed) parameter specifies the intent to include routed VLAN per service functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

VLAN per Subscriber (Bridged)

(vlanPerSubscrBridged)

The VLAN per Subscriber (Bridged) parameter specifies the intent to include bridged VLAN per Subscriber functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

VLAN per Subscriber (Routed)

(vlanPerSubscrRouted)

The VLAN per Subscriber (Routed) parameter specifies the intent to include routed VLAN per Subscriber functionality in the service model for the policy. The parameter acts as a reference for the 5620 SAM operator during policy application.

Watchdog Timer (seconds)

(watchdogTimer)

The Watchdog Timer parameter specifies the device/client watchdog timer used on all connections through the diameter policy. The range is 1 to 1000. The default is 30.

97 – Network and Service Audits policy parameters

97.1 Network and Service Audits policy parameters 97-2

97.1 Network and Service Audits policy parameters

This chapter describes the parameters on the Audit Policy form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Administrative State

(adminState)

See the [Administrative State](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Enabled

(enabled)

The Enabled parameter specifies whether the audit policy is enabled for the object. The options are:

- Enabled (default)
- Disabled

ID

(id)

See the [ID](#) parameter in section 112.1.

Remove Empty Service

(removeEmptyService)

The Remove Empty Service parameter specifies whether the empty service is removed when you perform an audit fix. If you set this parameter to Enabled, the 5620 SAM deletes the service after all the service sites are moved to the new service. The options are:

- Enabled
- Disabled (default)

98 – Diameter Peer Profile parameters

98.1 Diameter Peer Profile parameters 98-2

98.1 Diameter Peer Profile parameters

This chapter describes the parameters on the Diameter Peer Profile forms and the child forms.

Application Type

(appType)

The Application Type parameter specifies the application where the diameter peer profile is used. The options are:

- none (default)
- gx
- rf

Auto-Assign ID

See “[Auto-Assign ID](#)” in section 112.1 for the parameter description.

Description

See [Description](#) in section 112.1 for the parameter description.

Destination Realm

(destRealm)

The Destination Realm parameter specifies the destination realm of the diameter peer. The range is 0 to 80. There is no default value.

Displayed Name

See “[Displayed Name](#)” in section 112.1 for the parameter description.

Load Balance Enabled

(loadBalanceEnabled)

The Load Balance Enabled parameter specifies whether load balancing is enabled. When load balancing is enabled, that is, selected, all of the peers are used in round-robin mode. When load balancing is disabled, that is, unselected, only the first peer is used for the diameter sessions. The options are:

- enabled
- disabled (default)

Peer Administrative State

(peerListAdminState)

The Peer Administrative State parameter specifies whether the peer object is administratively enabled. The options are:

- Down (default)
- Up

Peer ID

(id)

The Peer ID parameter specifies the unique identifier for the peer. The parameter is available only when the Auto-Assign ID parameter unselected. The range is 1 to 65 535. The default is 0.

Peer IP Address

(peerListAddr)

See “[Peer IP Address](#)” in section [112.1](#) for the parameter description.

Peer Port

(peerListPort)

The Peer Port parameter specifies the port number of the peer list entry. The range is 1 to 65 535. The default is 3868.

Transport Protocol

(transport)

The Transport Protocol parameter specifies the type of diameter signaling to be used by the diameter peer. The value is TCP and cannot be changed.

99 – *Diameter Profile parameters*

99.1 Diameter Profile parameters 99-2

99.1 Diameter Profile parameters

This chapter describes the parameters on the Diameter Profile forms and the child forms.

Connection Timer (s)

(connTimer)

The Connection Timer (s) parameter specifies the length of time that the node attempts to reconnect to a diameter peer after a connection is lost because of a transport failure. The range is 0 to 180. The default is 30.

Description

See [Description](#) in section 112.1 for the parameter description.

Displayed Name

See [“Displayed Name”](#) in section 112.1 for the parameter description.

DPR Timeout (s)

(dprTimeout)

The DPR Timeout (s) parameter specifies the length of time that the node waits before restarting the diameter connection setup when a remote peer is intentionally disconnected by a DPR. The range is 1 to 3600. The default is 1800.

IP DSCP

(ipDscp)

The IP DSCP parameter specifies the DSCP value in the IP header for diameter signaling messages. This value can be configured to treat a packet as a network control packet ahead of the expedited forwarding packets. The range is 0 to 63. The default is 56.

IP TTL (s)

(ipTtl)

The IP TTL (s) parameter specifies the IP TTL value that is used for diameter signaling messages. The range is 1 to 255. The default is 255.

Refresh Time (s)

(dprRefreshTime)

The Refresh Time parameter specifies the amount of time that a node waits before sending a DNS query to refresh the FQDN resolution to a list of IP addresses. The TTL value received in a DNS response is not used by the Gateway. The range is 0 to 86 400. The default is 21 600.

Retry Count

(retryCount)

The Retry Count parameter specifies the number of times that the system attempts to retransmit a message before indicating that the attempt failed. The range is 1 to 8. The default is 3.

Retry Time (min)

(dprFailRetryTime)

The Retry Time (min) parameter specifies the time that the node waits before retrying the diameter connection setup to dynamically start the connection when there are permanent failures on the remote peer. A value of zero means that no attempt will be made to re-establish the connection. The range is 0 to 1 440. The default is 0.

Transaction Timer (s)

(transTimer)

The Transaction Timer (s) parameter specifies the maximum amount of time that the node waits for a diameter peer to respond before trying another peer. The range is 1 to 180. The default is 5.

Watch Dog Timer (s)

(watchdogTimer)

The Watch Dog Timer (s) parameter specifies the maximum amount of time that the node waits for a diameter peer to respond to a Device-Watchdog Request. If the node does not receive a Device-Watchdog-Answer message from the peer before the timer expires, a transport failure is detected. The range is 1 to 180. The default is 30.

100 –GTP Prime Server Group Profile parameters

100.1 GTP Prime Server Group Profile parameters 100-2

100.1 GTP Prime Server Group Profile parameters

This chapter describes the parameters on the GTP Prime Server Group Profile forms and the child forms.

Administrative State

(adminState)

The Administrative State parameter specifies the administrative state of the GTP prime server. The options are:

- Down (default)
- Up

Administrative State

(gtpPrimaryServerAdminState)

The Administrative State parameter specifies the administrative state of a GTP primary server. The options are:

- Down (default)
- Up

Description

See [Description](#) in section 112.1 for the parameter description.

Displayed Name

See [“Displayed Name”](#) in section 112.1 for the parameter description.

Configuration File Limit (Mbytes)

(cf1Limit)

The Configuration File Limit (Mbytes) specifies the maximum space that can be used to store ACR files on compact flash Cf1. When the limit is reached, the system can no longer support accurate charging. The range is 0 to 4 294 967 295. The default is 0.

Configuration File Limit (Mbytes)

(cf2Limit)

The Configuration File Limit (Mbytes) specifies the maximum space that can be used to store ACR files on compact flash Cf2. When the limit is reached, the system can no longer support accurate charging. The range is 0 to 4 294 967 295. The default is 0.

Dead Time (seconds)**(deadTime)**

The Dead Time (seconds) parameter specifies the time that a server is considered unavailable before it can be used again. The range is 0 to 3600. The default is 0.

Echo Interval (seconds)**(echoInterval)**

The Echo Interval (seconds) parameter specifies the interval at which the system sends echo requests for the GTP prime server PDUs. The range is 1 to 3 600. The default is 60.

File Closure Lifetime (hours)**(fileClosureLifeTime)**

The File Closure Lifetime (hours) parameter specifies the maximum time that a file can remain open. The file is closed when the specified duration has elapsed. The range is 1 to 24. The default is 1.

File Closure Max Records**(fileClosureMaxRecords)**

The File Closure Max Records parameter specifies a limit for the maximum number of CDRs that can be stored in a file. The file is closed when the specified limit is reached. The range is 100 to 75 000. The default is 50 000.

File Closure Size (Mbytes)**(fileClosureSize)**

The File Closure Size (Mbytes) parameter specifies a maximum file size limit. When the specified limit is reached the file is closed. The range is 1 to 100. The default is 50.

File Extension**(fileExtension)**

The File Extension parameter specifies a file extension field that is used in the file name. The range is 0 to 8 characters. There is no default.

File Obsolete Time (days)**(obsoleteTime)**

The File Obsolete Time (days) parameter specifies a time duration, after which a file is deleted. The range is 1 to 31. The default is 7.

File Private Info

(filePrivateInfo)

The File Private Info parameter specifies a file private information field that is used in the file name. The range is 0 to 32 characters. There is no default.

Inactive Time (minutes)

(inactiveTimer)

The Inactive Time (minutes) parameter specifies the time that a peer must remain inactive while storing all of the cached GTP packets onto a compact flash card. The range is 1 to 60. The default is 10.

Maximum CDRs per PDU

(maxCdrsPerPdu)

The Maximum CDRs per PDU parameter specifies the maximum number of CDRs that can be placed into a single GTP prime server PDU. The range is 0 to 100. The default is 0.

Maximum Requests

(maxRequests)

The Maximum Requests parameter specifies the maximum number of unacknowledged GTP prime server PDUs that are sent before the system stops sending the CDR. The range is 1 to 512. The default is 256.

Primary Compact Flash

(primaryCompactFlash)

The Primary Compact Flash parameter specifies which compact flash is used as the primary storage for CDRs. You cannot specify a compact flash that is unavailable. If you specify a compact flash that is unavailable the system selects a compact flash that is available.

- cf1 (default)
- cf2

Primary Server Address

(gtpPrimaryServerAddr)

The Primary Server Address parameter specifies the IP address of a peer primary GTP server. If the peer address type is DNS, then the IP address for this peer is obtained using a DNS A-Record query. The value of this parameter cannot be modified after it is created. Specify a unicast IPv4 address in dotted-decimal format or an IPv6 address in the form x:x:x:x:x:x or x:x:x:x:x.d.d.d, where x ranges from 0 to FFFF (hex) and d ranges from 0 to 255 (decimal). There is no default

Queue Size

(queueSize)

The Queue Size parameter specifies the maximum number of cached GTP packets that are waiting for a CGF to become available. When the specified value is reached, all of the cached GTP packets are stored on a compact flash card. The range is 10 000 to 500 000. The default is 100 000.

Retries

(retries)

The Retries parameter specifies the number of times that the system attempts to send a GTP prime server PDU to a CGF. The range is 1 to 8. The default is 4.

Server Port

(serverPort)

The Server Port parameter specifies the destination TCP or UDP port number for the GTP prime server. The value of this parameter cannot be modified after it has been saved. The range is 1 to 65 535. The default is 3386.

Server Priority

(serverPriority)

The Server Priority parameter specifies the priority of the GTP primary server. The range is 0 to 100. The default is 0.

Time Out (seconds)

(timeout)

The Time Out parameter specifies the interval between GTP prime server PDU retries. The range is 1 to 180. The default is 20.

101 –GTP Profile parameters

101.1 GTP Profile parameters 101-2

101.1 GTP Profile parameters

This chapter describes the parameters on the GTP Profile form and the child forms.

Description

See “Description” in section 112.1 for the parameter description.

Displayed Name

See “Displayed Name” in section 112.1 for the parameter description.

IP DSCP

(ipDscp)

The IP DSCP parameter specifies the DSCP value in the IP header for GTP signaling messages sent. The value can be configured to treat a packet as a network control packet ahead of the expedited forwarding packets. The range is 0 to 63. The default is 56.

IP TTL

(ipTtl)

The IP TTL parameter specifies the IP TTL value that is used for GTP signaling messages. The range is 1 to 255. The default is 255.

Keep-Alive Retry Count

(keepAlvRetryCnt)

The Keep-Alive Retry Count parameter specifies the maximum number of times that the GTP signaling component attempts to send an echo-request message for which there is no reply from the remote peer. If the retry count reaches the specified value, the remote peer is treated as unreachable. The range is 1 to 8. The default is 3.

Keep-Alive T3 Response Time (s)

(keepAlvResp)

The Keep-Alive T3 Response Time (s) parameter specifies the time that the SGW waits before resending a GTP signaling request message when a response to a request has not been received. The time is doubled for every retry. The range is 1 to 8. The default is 3.

Keep-Alive Timeout (s)

(keepAlvTimeout)

The Keep-Alive Timeout (s) parameter specifies the time that the GTP signaling component waits for a response from an MME, and after receiving a response, the number of seconds that the component waits before sending the next echo-request message. The range is 0 to 180. The default is 60.

Message Retransmit Retry Count

(msgReTxRetryCnt)

The Message Retransmit Retry Count parameter pertains to GTP-C signaling and specifies the number of times that a message is retransmitted before the system treats the retransmission attempt as a failure. The range is 1 to 8. The default is 3.

Message Retransmit Timeout (s)

(msgReTxTimeout)

The Message Retransmit Timeout (s) parameter specifies the time that the GTP-C signaling component waits for a response from the remote peer before sending another transmit request. The parameter applies to all control messages, except the GTP-C keep-alive message. The range is 1 to 30. The default is 5.

102 –PGW Charging Profile parameters

102.1 PGW Charging Profile parameters 102-2

102.1 PGW Charging Profile parameters

This chapter describes the parameters on the PGW Charging Profile form and the child forms.

Charging Profile ID

See “Charging Profile ID” in section 112.1 for the parameter description.

Description

See “Description” in section 112.1 for the parameter description.

Offline Charging

See “Offline Charging” in section 112.1 for the parameter description.

Time Limit (s)

See “Time Limit (s)” in section 112.1 for the parameter description.

Volume Limit

See “Volume Limit (Kbytes)” in section 112.1 for the parameter description.

103 –PLMN List Group parameters

103.1 PLMN List Group parameters 103-2

103.1 PLMN List Group parameters

This chapter describes the parameters on the PLMN List Group forms and the child forms.

Displayed Name

See “[Displayed Name](#)” in section 112.1 for the parameter description.

Description

See “[Description](#)” in section 112.1 for the parameter description.

Mobile Country Code

(mcc)

The Mobile Country Code parameter specifies the unique three-digit identifier that represents the country of the mobile subscriber. Choose a value from the drop-down menu. The default is unspecified.

Mobile Network Code

(mnc)

The Mobile Network Code parameter specifies the unique two- or three-digit identifier that is used with the MCC and represents the mobile network operator or carrier. The range is 2 to 3 characters in the range 0-9. There is no default.

104 –QCI Policy parameters

104.1 QCI Policy parameters 104-2

104.1 QCI Policy parameters

This chapter describes the parameters on the QCI Policy form and the child forms.

Description

See [Description](#) in section 112.1 for the parameter description.

Displayed Name

See [“Displayed Name”](#) in section 112.1 for the parameter description.

DSCP for In Profile Packets

(dscpIn)

The DSCP for In Profile Packets parameter specifies the DSCP that is used while marking the in-profile packets. Table 104-1 lists the parameter options.

Table 104-1 DSCP for in and out profile packets options

Options			
none (default)	ef	nc1	nc2
be	cp2	cp3	cp4
cp1	cp6	cp7	cp9
cp5	cp13	cp15	cp17
cp11	cp21	cp23	cp25
cp19	cp29	cp31	cp33
cp27	cp37	cp39	cp41
cp35	cp43	cp44	cp45
cp42	cp49	cp50	cp51
cp47	cp53	cp54	cp55
cp52	cp58	cp59	cp60
cp57	cp62	cp63	cs1
cp61	cs3	cs4	cs5
cs2	af12	af13	af21
af11	af23	af31	af32
af22	af41	af42	af43
af33	—	—	—

DSCP for Out Profile Packets

(dscpOut)

The DSCP for Out Profile Packets parameter specifies the DSCP that is used while marking the out-profile packets. Table 104-1 lists the parameter options.

DSCP Preserve

(dscpPreserve)

The DSCP Preserve parameter specifies whether the DSCP bits are preserved. When the check box is selected, the parameter is set to enabled and the DSCP bits are preserved. When the check box is not selected, the parameter is set to disabled and the DSCP bits are not preserved. The options are:

- disabled
- enabled (default)

Forwarding Class Name

(fcName)

The Forwarding Class Name parameter specifies the the Forwarding Class name. The options are:

- | | |
|------|------|
| • l1 | • ef |
| • l2 | • h1 |
| • be | • h2 |
| • af | • nc |

Profile

(qciProfile)

The Profile parameter specifies the QCI profile that is assigned to the packet. The options are:

- None (default)
- In
- Out
- Apply CIR

105 –SGW Charging Profile parameters

105.1 SGW Charging Profile parameters 105-2

105.1 SGW Charging Profile parameters

This chapter describes the parameters on the SGW Charging Profile form and the child forms.

Charging Profile ID

See “Charging Profile ID” in section 112.1 for the parameter description.

Description

See “Description” in section 112.1 for the parameter description.

Maximum Number of Changes

See “Maximum Number of Changes” in section 112.1 for the parameter description.

MS Time Zone Changes

See “MS Time Zone Change” in section 112.1 for the parameter description.

Offline Charging

See “Offline Charging” in section 112.1 for the parameter description.

QoS Change

See “QoS Change” in section 112.1 for the parameter description.

Time Limit (s)

See “Time Limit (s)” in section 112.1 for the parameter description.

User Location Change

See “User Location Change” in section 112.1 for the parameter description.

Volume Limit (Kbytes)

See “Volume Limit (Kbytes)” in section 112.1 for the parameter description.

106 –ANR Profile parameters

106.1 ANR Profile parameters 106-2

106.1 ANR Profile parameters

This section describes the parameters of the ANR Profile form. See the *5620 SAM LTE Parameter Reference* for descriptions of the eNodeB MIM parameters that are referred to in this section.

Active Phase Measurement Report Hysteresis

(activePhaseMeasReportHysteresis)

The Active Phase Measurement Report Hysteresis parameter defines the minimum number of consecutive measurement reports received by the eNodeB without discovering a new neighbour relation that is required to exit the active phase of ANR. The other condition is given by the activePhaseMeasReportThreshold parameter. The range is 5 to 500. The default value is 200.

Active Phase Measurement Report Threshold

(activePhaseMeasReportThreshold)

The Active Phase Measurement Report Threshold parameter defines the minimum number of measurement reports received by the eNodeB that is required to exit the active phase of ANR. The other condition is given by parameter activePhaseMeasReportHysteresis. The range is 10 to 2000. The default value is 1000.

Dormant Phase Timer For ECGI Discovery

(dormantPhaseTimerForEcgiDiscovery)

The Dormant Phase Timer For ECGI Discovery parameter specifies the time in minutes that the eNodeB dedicates to actively attempt identifying the ECGI associated to a newly discovered PCI during the dormant phase of ANR. The range is 5 to 60. The default value is 5.

DRX Cycle For Report CGI

(drxCycleForReportCGI)

The DRX Cycle For Report CGI parameter defines the DRX long cycle length that is used when a UE is requested to report the ECGI of a neighbor cell, as part of the ANR function. The options are:

- Sf 160 (default)
- Sf 320

Second Threshold EUTRAN RSRP

(threshold2EutraRsrp)

The Second Threshold EUTRAN RSRP parameter specifies the second threshold to be used for event A5 measurement reporting. See the *5620 SAM LTE Parameter Reference* for a list of configurable values.

Second Threshold EUTRAN RSRQ

(threshold2EutraRsrq)

The Second Threshold EUTRAN RSRQ parameter specifies the second threshold to be used for event A5 measurement reporting. See the *5620 SAM LTE Parameter Reference* for a list of configurable values.

Threshold EUTRAN RSRP

(thresholdEutraRsrp)

The Threshold EUTRAN RSRP parameter specifies the RRC IE Threshold EUTRAN RSRP included in the IE reportConfigEUTRA in the Measurement Configuration IE. See the *5620 SAM LTE Parameter Reference* for a list of configurable values.

Threshold EUTRAN RSRQ

(thresholdEutraRsrq)

The Threshold EUTRAN RSRQ parameter specifies the RRC IE Threshold EUTRAN RSRQ included in the IE reportConfigEUTRAN in the Measurement Configuration IE. See the *5620 SAM LTE Parameter Reference* for a list of configurable values.

UE Contribution In Wake Up Phase

(ueContributionInWakeUpPhase)

The UE Contribution In Wake Up Phase parameter specifies the number of established UE that will be configured with ANR and Report CGI measurements during the wake-up phase. The range is 0 to 20. The default is 10.

107 –eNodeB IPsec Profile parameters

107.1 eNodeB IPsec Profile parameters 107-2

107.1 eNodeB IPsec Profile parameters

This section describes the parameters of the eNodeB IPsec Profile form.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

IKE Authentication Method

(ikeAuthMethod)

The IKE Authentication Method parameter specifies the IKE v2 authentication method. The options are:

- Pre Shared Keys (default)
- Certificates

IKE SA Life Duration (s)

(ikeSALifeDurationSec)

The IKE SA Life Duration parameter specifies the life duration of the IKE security association in seconds. The range is 0 to 4 294 967 295. The default is 28 800.

IPsec Anti-Replay Windows Size

(ipsecAntiReplayWindowSize)

The IPsec Anti-Replay Windows Size parameter specifies the anti-replay window size that is used by the IPsec profile. The size is measured in the number of packets. A value of 0 means that the IPsec anti-replay mechanism is disabled. The range is 0 to 64. The default is 32.

IPsec Keep Alive Period

(ipsecKeepalivePeriod)

The IPsec Keep Alive Period parameter specifies the period that IKE keep-alives are sent. The range is 0 to 120. The default is 10.

IPsec Perfect Forward Secrecy

(ipsecPerfectForwardSecrecyOn)

The IPsec Perfect Forward Secrecy parameter specifies whether perfect forward secrecy is turned on. The default is true.

IPsec Policy

(eNBIPsecpolicy)

The IPsec Policy parameter specifies the IPsec policy settings on the eNodeB. The options are:

- S1 C and X2 C Protected
- No IPsec (default)
- S1 C And UP And X2 C And UP Protected
- Integrityprotection
- Integrityprotectionandencrypted

IPsec SA Life Duration (Kbytes/s)

(ipsecSALifeDurationbytes)

The IPsec SA Life Duration (Kbytes/s) parameter specifies the duration of IPsec security association in kilobytes. The range is 0 to 4 294 967 295. The default is 1 620 000.

IPsec SA Life Duration (s)

(ipsecSALifeDurationSec)

The IPsec SA Life Duration Sec parameter specifies the life duration of IPsec security association in seconds. The range is 0 to 4294967295. The default is 28 800.

IPsec Tunnel Address (IPv4)

(ipv4AddressEnbIPsecTunnel)

The IPsec Tunnel Address (IPv4) parameter specifies the outer IP address of the IPsec tunnel at the eNodeB. The default is 0.0.0.0.

IPsec Tunnel Subnet Mask (IPv4)

(ipv4SubNetMaskEnbIPsecTunnel)

The IPsec Tunnel Subnet Mask (IPv4) parameter specifies the subnet mask of the outer IP address of the IPsec tunnel at the eNodeB. The default is 0.0.0.0.

Pre-Shared Secret

(eNBpreSharedSecret)

The ENB pre Shared Secret parameter specifies the pre-shared secret key. The range is 0 to 40.

SEG Address (IPv4)

(ipv4AddressSegIPsecTunnel)

The SEG Address (IPv4) parameter specifies the outer IP address of the IPsec tunnel at the security gateway. The default is 0.0.0.0.

108 –CPE Test-Head Profile parameters

108.1 CPE Test-Head Profile parameters 108-2

108.1 CPE Test-Head Profile parameters

This chapter describes the parameters of the CPE Test-Head form and child forms.

Description

See the [Description](#) parameter in section 112.1.

Destination Endpoint

(testDstEndpoint)

The Destination Endpoint parameter specifies the identity of the of the remote DUT. For unidirectional tests, this parameter identifies the analyzer DUT. For bidirectional tests, this parameter identifies the DUT that needs to activate the loopback function. The range is 1 to 32. The default is DEFAULT.

Destination IP

(dstIpAddress)

The Destination IP parameter specifies the destination IP address of the generated test frame. The default is 0.0.0.0.

Destination MAC

(frameDstMacAddress)

The Destination MAC parameter specifies the destination MAC address of the test frame. The default is 00-00-00-00-00-00.

Destination Port

(dstPort)

The Destination Port parameter specifies the destination port of the generated test frame. The range is 0 to 65535. The default is 33024.

Direction

(testDUTDirection)

The Direction parameter specifies the test direction. The options are:

- UniDirectional (default)
- BiDirectional

Drop Enable

(dropEnable)

The Drop Enable parameter specifies the CFI bit present in the generated test frame. The options are:

- Disabled (default)
- Enabled

Ether Type

(etherType)

The Ether Type parameter specifies the ether-type for the L2 packet. The range is 1536 to 65534. The default is 1536.

Frame Size (bytes)

(frameSize)

The Frame Size (bytes) parameter specifies the size of packets in bytes. The range is 64 to 9212. The default is 64.

Frame Type

(frameType)

The Frame Type parameter specifies the type of frame. The options are:

- unspecified (default)
- Ethernet
- IPV4

Name

See the [Name](#) parameter in section [112.1](#).

Pattern

(dataPattern)

The Pattern parameter specifies the data pattern present in the generated test frame. The range is 0 to 65535. The default is 0.

Priority

(priority)

The Priority parameter specifies the priority in the generated test frame. The range is 0 to 7. The default is 7.

Protocol

(frameProtocol)

The Protocol parameter specifies the protocol information about the packet. The options are:

- Reserved (default)
- TCP
- UDP

Role

(testDUTRole)

The Role parameter specifies the role of the DUT based on the direction. The options are:

- unspecified (default)
- Generator
- Analyzer
- Loopback

Source Endpoint

(testSrcEndpoint)

The Source Endpoint parameter specifies the identity of the local or transmitting DUT. For bidirectional tests, this parameter also specifies the analyzer DUT. The range is 1 to 32. The default is DEFAULT.

Source IP

(srcIpAddress)

The Source IP parameter specifies the source IP address of the generated test frame. The default is 0.0.0.0.

Source MAC

(frameSrcMacAddress)

The Source MAC parameter specifies the source MAC address of the test frame. The default is 00-00-00-00-00-00.

Source Port

(srcPort)

The Source Port parameter specifies the source port of the generated test frame. The range is 0 to 65535. The default is 33024.

TOS

(frameTos)

The TOS parameter specifies the type of service for the generated test frame. The range is 0 to 255. The default is 0.

TTL

(frameTtl)

The TTL parameter specifies the time to live of the generated test frame. The range is 0 to 255. The default is 0.

Tx Rate (kbps)

(txRate)

The Tx Rate parameter specifies the rate at which the traffic generator shall generate the traffic. The value should be a multiple of 8. The range is 8 to 100000. The default is 8.

VLAN-Tag

(cVlanTag)

The VLAN-Tag parameter specifies the customer VLAN for the packet. The range is 1 to 4094. The default is 100.

109 –Remote Network Monitoring (RMON) parameters

109.1 Remote Network Monitoring (RMON) parameters 109-2

109.1 Remote Network Monitoring (RMON) parameters

This chapter describes the parameters on the RMON menu forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Community

(community)

The Community parameter specifies the name of the community that is shared between the 5620 SAM and the 7250 SAS or 7250 SAS-ES, Release 2.0. The range is 0 to 127 characters. The default is private.

Description

See the [Description](#) parameter in section 112.1.

Displayed Name

See the [Displayed Name](#) parameter in section 112.1.

Falling Threshold

(fallingThreshold)

The Falling Threshold parameter specifies a falling threshold for the sampled statistic. The 5620 SAM generates an information alarm when the following conditions apply:

- The current sampled value is less than or equal to the configured threshold, and
- The previously sampled value is greater than the configured threshold

The 5620 SAM also generates an information alarm for the following conditions:

- The first sample of the statistic is less than or equal to the configured threshold, and
- The [Start Up Alarm](#) parameter is set to Falling or Either

After the 5620 SAM generates a falling threshold alarm, another alarm for the same event condition does not occur until the sampled statistic is equal to or greater than the configured value of the [Rising Threshold](#) parameter.

The range is -2 147 483 648 to 2 147 483 647.

ID

See the [ID](#) parameter in section 112.1.

Interval (seconds)

(interval)

The Interval (seconds) parameter specifies the polling period during which the data is sampled and compared with the rising and falling thresholds. Consider the following guidelines when you configure the polling interval.

- The interval should be low enough so that the sampled variable is unlikely to increase or decrease by more than 2 147 483 647 during an interval
- The interval should not be excessively low as to create unnecessary processing overhead

The range is 1 to 2 147 483 647.

Monitored Object OID

(monitoredObjectId)

The Monitored Object OID parameter specifies the SNMP object identifier for the sampled variable. You can only sample SNMP variables that resolve to an ASN.1 primitive type of integer (integer, Integer32, Counter32, Counter64, Gauge, or TimeTicks). You can use a dotted-string format for the OID string format; for example, 1.3.6.1.2.1.2.2.1.10.184582144.

The range is 1 to 255 characters.

Owner

(owner)

The Owner parameter specifies the creator of the alarm. The range is 0 to 127 characters. The default is 5620sam.

Rising Threshold

(risingThreshold)

The Rising Threshold parameter specifies a rising threshold for the sampled statistic. The 5620 SAM generates an information alarm when the following conditions apply:

- The current sampled value is greater than or equal to the configured threshold, and
- The previously sampled value is less than the configured threshold

The 5620 SAM also generates an information alarm when the following conditions apply:

- The first sample of the statistic is greater than or equal to the configured threshold, and
- The [Start Up Alarm](#) parameter is set to Rising or Either

After the 5620 SAM generates a rising threshold alarm, another alarm for the same event condition does not occur until the sampled statistic is equal to or less than the configured value for the [Falling Threshold](#) parameter.

The range is -2 147 483 648 to 2 147 483 647.

Sample Type

(sampleType)

The Sample Type parameter specifies the method that is used to sample the NE data. The 5620 SAM compares the value against the configured threshold. Table [109-1](#) describes the parameter options.

Table 109-1 Sample Type parameter

Option	Option description
Absolute (default)	Specifies that the value of the selected variable is compared against the thresholds at the end of the sampling interval
Delta	Specifies that the value of the selected variable at the last sample is subtracted from the current value, and the difference is compared to the thresholds

Start Up Alarm

(startupAlarm)

The Start Up Alarm parameter specifies an alarm for a rising or falling value. Table [109-2](#) describes the parameter options.

Table 109-2 Start Up Alarm parameter

Option	Option description
Rising	Specifies an alarm for a rising threshold crossing event. The 5620 SAM creates an alarm for a rising threshold crossing event when the following conditions apply: <ul style="list-style-type: none">• first sample is greater than or equal to the rising threshold value• Start Up Alarm parameter is set to Rising or Either
Falling	Specifies an alarm for a falling threshold crossing event. The 5620 SAM creates an alarm for a falling threshold crossing event when the following conditions apply: <ul style="list-style-type: none">• first sample is less than or equal to the falling threshold value• Start Up Alarm parameter is set to Falling or Either
Either (default)	Specifies an alarm for a rising or falling threshold crossing event

Type

(type)

The Type parameter specifies the notification action associated with an event. Table 109-3 describes the parameter options.

Table 109-3 Type parameter

Option	Option description
None	No notification action associated with the event
Log	Specifies that the 5620 SAM creates a log entry for the event
Trap	Specifies that an SNMP trap is sent to one or more management stations
Log + Trap (default)	Specifies the creation of a log entry and sending of an SNMP trap

110 –Size Constraint parameters

110.1 Size Constraint parameters 110-2

110.1 Size Constraint parameters

This chapter describes the parameters on the Size Constraint Policy form and child forms.

Apply Threshold To

(thresholdPolicy)

The Apply Threshold To parameter specifies how the [Threshold \(# of objects\)](#) parameter value applies to the selected classes. Table 110-1 lists the parameter options.

Table 110-1 Apply Threshold To parameter

Option	Option description
Each selected class individually (default)	The threshold is reached when the number of objects for one class exceeds it.
All selected classes collectively	The threshold is reached when the total number of objects for all classes exceeds it.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Description

See the [Description](#) parameter in section 112.1.

Objects To Be Deleted When Threshold Exceeded (# of objects)

(rowsToDelete)

The Objects To Be Deleted When Threshold Exceeded (# of objects) parameter specifies the number of database objects that are removed when a threshold is reached, as determined by the Threshold (# of objects) and Apply Threshold To parameters. The minimum value is 1. There is no maximum value. The default is 5000.

Policy Id

(policyId)

The Policy Id parameter specifies a numeric identifier for the policy. The parameter is configurable when the Auto Assign ID parameter is disabled. The minimum value is 1. There is no maximum value. The default is 0, which means that no value is specified.

Threshold (# of objects)

(rowThreshold)

The Threshold (# of objects) parameter specifies the number of database objects to use as a threshold for size-constraint purposes. The minimum value is 1000. There is no maximum value. The default is 100 000.

111 –Format and Range Policies parameters

111.1 Format and Range Policies parameters 111-2

111.1 Format and Range Policies parameters

This chapter describes the parameters on the forms opened from the Format and Range Policies form.

Administrative State

See the [Administrative State](#) parameter in section 112.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Auto Assign By Default

The Auto Assign By Default parameter specifies whether the [Auto-Assign ID](#) check box is enabled by default. The options are:

- enabled
- disabled

Auto Assignment Enabled

The Auto Assignment Enabled parameter specifies whether the Auto-Assign ID parameter is enabled by default. The options are:

- enabled
- disabled

Copy Text From Position

The Copy Text From Position parameter specifies the source attribute text that is copied. This parameter is configurable when you choose the Auto-Filled option for the text block format parameters. The range is 1 to 1000 characters.

Default Value

The Default Value parameter specifies the default of the text field. The parameter is configurable when the text block format option is Text Parameter. The range is 0 to 250 characters.

Displayed Text

(Placeholder)

The Displayed Text (Placeholder) parameter specifies the text that is displayed in the GUI for an attribute that has a format policy applied. The text is automatically filled. This parameter can be configured when the Auto-Filled Parameter option is specified for text blocks.

Mask

The Mask parameter specifies the text that is entered for a parameter value when the parameter value is configured by a format policy. For example, when a format policy is created for a service description, you can configure the text that automatically populates the description field. You cannot enter values that do not comply with the mask. The range is 0 to 250 characters.

Table 111-1 lists the special formatting characters available for the Mask parameter.

Table 111-1 Special formatting characters

Character	Source object property options
'	Used to escape any of the special formatting characters
#	Any valid number
U	Any letter, where lowercase characters are mapped to uppercase characters
L	Any letter, where uppercase characters are mapped to lowercase characters
A	Any letter or number
?	Any letter
*	Anything
H	Any hexadecimal character: <ul style="list-style-type: none"> • 0 to 9 • a to f • A to F

Maximum

The Maximum parameter specifies the highest number in the ID range for a range policy. The range is 0 to 1000000999999. The default is automatically set when the range policy is created. You can click on the Reset to Default button to reset the value.

Max. Length

The Max. Length parameter specifies the maximum length of a text field parameter that is configured in a format policy text block. The range is 1 to 250 characters.

Minimum

The Minimum parameter specifies the lowest number that can be used in the ID range for a range policy. The range is 0 to 1000000999999. The default is automatically set when the range policy is created. You can click on the Reset to Default button to reset the value.

Min. Length

The Min. Length parameter specifies the minimum length of a field text parameter that is configured in a format policy text block. The range is 0 to 250 characters.

Name

(**displayName**)

See the [Name](#) parameter in section 112.1.

Object Type

The Object Type parameter specifies the object class that is configured in the format or range policy. Choose an object type by clicking on the Select button.

Policy ID

(**policyId**)

The Policy ID parameter specifies a numeric identifier for the policy. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 5 000 000. When the value is 0 (default), the ID is generated by 5620 SAM.

Priority

The Priority parameter specifies the sequence in which multiple instances of a policy are sorted. The range is 1 to 1000 (lowest priority). The list of policies returned by the policy that matches a query is listed using the priority value.

Property Name

The Property Name parameter specifies the parameter to which the format or range policy applies. The options are:

- Name
- Service Name
- Description
- Service ID
- ID
- Interface ID
- Outer Encapsulation Value

Read Only

The Read Only parameter specifies when the [Min. Length](#) and [Max. Length](#) parameters are read-only. The Read Only parameter is configured in the Text Format option of the Text Block Format window.

- Enabled
- Disabled (default)

Source Object Name

The Source Object Name parameter specifies the object type to be used as the source to create the text string. This parameter is set during Auto-Filled Parameter configuration.

Source Property Name

The Source Property Name parameter specifies the object attributes to be used as the source to create the text string. This parameter is configured when the Auto-Filled Parameter option is configured.

Tooltip Text

The Tooltip Text parameter allows the operator to create a description for the parameter value to inform users that a format policy is applied to the parameter. The range is 0 to 1000 characters.

Through To Position

The Through To Position parameter copies the text of the source parameter up to the position that is configured by this parameter. This parameter is configurable when the auto-filled option is selected for the text block format and the [Unlimited](#) parameter is disabled. The range is 1 to 1000.

Unlimited

The Unlimited parameter specifies the amount of source attribute text to be copied. The parameter is configurable when the auto-filled option is selected for the text block format. When the parameter is enabled, the source attribute text is copied from the [Copy Text From Position](#) parameter value to the end. When the parameter is disabled you can copy the source parameter text to a specified position. The options are:

- enabled
- disabled

112 –Common Policies menu parameters

112.1 Common Policies menu parameters 112-2

112.1 Common Policies menu parameters

This chapter describes the parameters that are common to the 5620 SAM Policies menu forms and child forms.

Action

(defaultAction)

The Action parameter specifies the action that should be performed with the packet when the match specified criteria are met. Table 112-1 describes the parameter options.

Table 112-1 Action parameter

Option	Option description	Dependencies
drop	Discard the packet.	—
forward	Forward the packet based on the specified next hop parameters.	You must configure the parameters on the Next Hop Routing tab
default (default)	Perform the action specified by the Default Action parameter for the filter.	—
HTTP redirect	Forward the packet to the URL configured in the Redirect URL parameter.	Not selectable for an ACL IPv6 filter entry
forward (SAP)	Forward the packet based on the specified SAP parameters.	You must configure the parameters on the Forwarding Destination tab of the SAP. Not selectable for an ACL IPv6 filter entry
forward (SDP)	Forward the packet based on the specified SDP parameters.	You must configure the parameters on the Forwarding Destination tab of the SDP. Not selectable in an ACL IPv6 filter entry

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled. The options are:

- Up
- Down

The default value depends on the type of policy.

Administrative State

(hiAdminStatus)

The Administrative State parameter specifies whether the high slope is administratively enabled. The options are:

- Enabled
- Disabled (default)

Administrative State

(loAdminStatus)

The Administrative State parameter specifies whether the low slope is administratively enabled. The options are:

- Enabled
- Disabled (default)

Administrative State

(nonTcpAdminStatus)

The Administrative State parameter specifies whether the non-Tcp slope is administratively enabled. The options are:

- Enabled
- Disabled (default)

Application

(groupEntriesApplication)

The Application parameter specifies for which application the inserted entries must be group. The options are:

- CreditControl (default)
- RADIUS

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

Burst Limit (bytes)

(burstLimit)

The Burst Limit (bytes) parameter specifies the explicit shaping burst size of an HSMDA queue. The range is -1 and 1 to 1 000 000. The default is -1.

Burst Limit (kb)

(burstLimit)

The Burst Limit (kb) parameter specifies the explicit shaping burst size of a queue. The range is -1 to 14000000. The default is -1.

Charging Profile ID

(chargingId)

The Charging Profile ID parameter specifies the charging profile ID. The range is 0 to 255. There is no default.

CIR (kbps)

(cir)

The CIR (kbps) parameter specifies the administrative committed information rate for a queue or a policer. The parameter specifies the rate at which the system prioritizes the queue over other queues that are competing for the same bandwidth.

For access ingress interfaces, the CIR also defines the rate that packets are considered in-profile by the system. In-profile packets are preferentially queued by the system at egress and at subsequent next-hop nodes that the packet traverses. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The range depends on the queue type and on the line rate of the object to which the policy is applied. Table 112-2 lists the parameter ranges for different queue types. You can also choose the MAX check box, which specifies the maximum available CIR. The default is 0.

Table 112-2 CIR (kbps) parameter

Object	Range
HSMDA queues	-1 to 100 000 000
Queues (except HSMDA queues)	-1 to 100 000 000
7210 meters	-1 to 2 000 000

The MAX check box specifies whether the CIR (kbps) parameter is set to infinity or can be configured. The options are:

- disabled (default)
- enabled

When the MAX check box is enabled, you cannot configure the CIR parameter.

The CIR (kbps) parameter can only be set when the [Rate Type](#) parameter is set to kbps. When [Rate Type](#) is not set to kbps, then the [CIR Percent \(%\)](#) parameter is configurable instead.

CIR (%)

(cir)

The CIR (%) (kb/s) parameter specifies the committed information rate, as a percentage of available bandwidth, for a queue on a network port or daughter card. The range is 0 to 100. The default is 100.

The CIR defines the rate at which the device prioritizes the queue over other queues that are competing for the same bandwidth. On network ingress interfaces, the CIR also defines the rate that packets are considered in-profile by the system.

CIR Adaptation

(cirAdaptation)

The CIR Adaptation parameter specifies the method used by the device to derive the operational CIR setting when the queue is provisioned in hardware. Table 112-3 describes the parameter options.

Table 112-3 CIR Adaptation parameter

Option	Option description	Dependencies
Closest (default)	The operational CIR for the queue is the rate closest to the rate specified by the CIR (kbps) parameter.	—
Min	The operational CIR for the queue is equal to or greater than the administrative rate specified by the CIR (kbps) parameter.	
Max	The operational CIR for the queue is equal to or less than the administrative rate specified by the CIR (kbps) parameter.	

CIR Level

Table 112-4 lists where to find more information about the CIR Level parameter.

Table 112-4 CIR Level parameter

Parameter	See
CIR Level for Parent Scheduler	CIR Level parameter in this section
CIR Level for Port Parent	CIR Level parameter in this section

CIR Level

(cirLevel)

The CIR Level parameter specifies the CIR priority level of the tier 2 or tier 3 child scheduler in comparison to other child schedulers with the same parent that are contending for a CIR from the parent. The parameter is configurable when the Tier parameter is set to the 2 or 3 option. The range is Default, 1 to 8. The default is Default. The higher the number, the higher the CIR priority level of the child scheduler within CIR request from the parent.

Child schedulers with the CIR Level parameter set lower than other child schedulers do not receive CIR bandwidth distribution until all child schedulers with a higher level have reached their maximum bandwidth allocation, or have no packets to pass.

When two child schedulers have the same CIR Level parameter value, the CIR Weight parameter determines which scheduler first receives the CIR bandwidth.

For example, there are three tier 2 child schedulers with the same tier 1 parent scheduler:

- child scheduler ABC has its CIR Level parameter set to 3
- child scheduler DEF has its CIR Level parameter set to 6
- child scheduler GHI has its CIR Level parameter set to 7

When the parent scheduler receives traffic within its CIR, bandwidth is allocated to the child schedulers. Child scheduler GHI receives its CIR bandwidth requirement from the parent scheduler before DEF and ABC. When GHI reaches its maximum CIR requirements and there is CIR bandwidth remaining, scheduler DEF receives the CIR bandwidth before scheduler ABC.

CIR Level

(portParentCirLevel)

The CIR Level parameter specifies the CIR priority level of child schedulers and queues in comparison to other child schedulers and queues for within-CIR distribution. The range is 1 (lowest priority) to 8 (highest priority). The default is 1.

CIR Percent (%)

(cirPercent)

The CIR Percent (%) parameter specifies the administrative committed information rate for an access ingress/egress queue or policer. The parameter specifies the rate as a percentage of the available bandwidth, which the system uses to prioritize the queue over other queues that are competing for the same bandwidth.

For access ingress interfaces, the CIR also defines the percent rate that packets are considered in-profile by the system. In-profile packets are preferentially queued by the system at egress and at subsequent next-hop nodes that the packet traverses. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.

The range is 0 to 100%, in increments of 0.01%. The default value is 0.

The CIR Percent (%) parameter can only be set when the [Rate Type](#) parameter is not set to kbps. When [Rate Type](#) is set to kbps, then the [CIR \(kbps\)](#) parameter is configurable instead.

CIR Weight

Table 112-5 lists where to find more information about the CIR Weight parameter.

Table 112-5 CIR Weight parameter

Parameter	See
CIR Weight for Parent Scheduler	CIR Weight parameter in this section
CIR Weight for Port Parent	CIR Weight parameter in this section

CIR Weight

(cirWeight)

The CIR Weight parameter specifies the relative importance of a child scheduler in comparison to other child schedulers that have the identical [CIR Level](#) parameter settings. The parameter is configurable when the Tier parameter is set to the 2 or 3 option. The range is 000 to 100. The default is 001.

A setting of 000 specifies that the child scheduler receives CIR bandwidth only after all non-000 weighted child schedulers have received CIR bandwidth.

CIR Weight

(portParentCirWeight)

The CIR Weight parameter specifies the relative importance of a child scheduler or queue in comparison to other child schedulers or queues that have the identical [CIR Level](#) parameter settings. The range is 000 to 100. The default is 001.

Committed Burst Size (kbps)

(cbs)

The Committed Burst Size (kbps) parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the CBS value then the packets are marked as in-profile by the meter to indicate that the traffic is complying to the meter configured parameters. Enable the Default checkbox to set the parameter to the default value of -1, indicated by MAX. Disable the Default checkbox to enter a value. The parameter value is an integer expression of the number of kilobytes reserved for the meter. For example, if you need to configure a value of 10KBits, then enter the value 10. The range depends on the policy. The Default checkbox is enabled by default.

Committed Burst Size (kb)

(committedBurstSize)

The Committed Burst Size (kb) parameter specifies the committed burst pool size for a queue and overrides the default reserved pool burst for the queue. The range is -1 to 131 072, with -1 indicating default. Default specifies that the device calculates committed burst pool size based on the CIR and the PIR. The default is default.

Configuration Mode

(configurationMode)

The Configuration Mode parameter specifies the mode in which the global policy is configured and determines whether the policy can be distributed to the network elements. Table 112-6 describes the parameter options.

Table 112-6 Configuration Mode parameter

Option	Option description	Dependencies
Draft (default)	The policy is not reviewed or approved for distribution to network elements. The policy can be synchronized. The 5620 SAM creates a global policy in draft mode for local policies discovered from the network or created through CLI.	Cannot be distributed
Released	The policy is reviewed and approved for distribution to network elements. Releasing a global policy also distributes the policy to existing local definitions. The policy can be synchronized.	Can be distributed

Credit Control Count

(creditControlCount)

The Credit Control Count parameter specifies how many filter entries received from Credit Control can be inserted in the filter. The range is 0 to 65 535. The default is 0. If the [Credit Control Start Entry](#) parameter is set to 0, then this object will be put to 0 as well. Any change attempts will be silently discarded in this case.

Credit Control Start Entry

(creditControlStartEntry)

The Credit Control Start Entry parameter specifies at what place the filter entries received from Credit Control for a particular subscriber host will be inserted in the filter. No regular entries, nor Radius provided entries can be configured in this range. The range is 0 to 65 535. The default is 0.

Default

The Default parameter specifies whether a parameter is set to the default value or can be configured. The options are:

- disabled
- enabled (default)

When the Default parameter is set to enabled, you cannot configure the associated parameters.

Default Action

(action)

The Default Action parameter specifies the action to be applied to packets when no action is specified in the IP filter entries or when the packets do not match the specified criteria. The options are:

- drop (default)
- forward

Default FC

(defaultFc)

The Default FC parameter specifies the default forwarding class for packets that ingress a network interface which uses the network policy. All packets with undefined DSCP or LSP EXP bits are mapped to the specified forwarding class and associated profile. The default profile is specified by the Default FC Profile parameter. Table 112-7 describes the parameter options.

Table 112-7 Default FC parameter

Option	Option description	Dependencies
be (default)	Specifies that packets in the class are treated, at best, as out-of-profile assured service packets. There are no delivery guarantees. The best-effort and low-2 forwarding class options are intended for best effort traffic.	—
l2		
af	Specifies that packets in the class are forwarded or discarded based on the availability of bandwidth on network elements. The assured and low-1 forwarding class options are intended for assured traffic. Packets transmitted that are at or below the committed rate are marked in-profile. Packets transmitted that are above the committed rate are marked out-of-profile.	
l1		
h2	Specifies that packets in the class are always serviced at congestion points over other forwarding classes. These options are intended for high-priority traffic. <ul style="list-style-type: none">• The h2 and ef forwarding class options are intended for delay/jitter sensitive traffic.• The h1 forwarding class option is intended for secondary network control traffic or delay/jitter sensitive traffic.• The nc forwarding class option is intended for network control traffic.	
ef		
h1		
nc		

Description

(description)

The Description parameter specifies a description for the created object. The range is 0 to 80 characters.

Destination IP

(destinationIpAddress)

The Destination IP parameter specifies the destination IP address to use as a packet match criterion in an ACL IP filter entry or QoS policy. When the parameter is configured in a QoS policy, the matching packets are mapped to the forwarding class specified by the [Forwarding Class](#) parameter and the priority specified by the [Priority](#) parameter.

If you are configuring an ACL IP filter policy or QoS policy, specify an IP address in dotted-decimal format.

If you are configuring an ACL IPv6 filter policy, specify an IP address in colon-hexadecimal format.

There is no default.

Destination Port

(destinationOperator, destinationPort1, destinationPort2)

The Destination Port parameter specifies the destination port match criterion for a packet. The parameter is configurable when the Protocol parameter value is TCP or UDP. Table [112-8](#) describes the parameter options.

Table 112-8 Destination Port parameter

Option	Option description	Dependencies
NONE (default)	No match criterion is specified.	—
EQUAL	Match the value specified in the first field. The second field is not accessible. The range is 0 to 65 535.	
RANGE	Match the range configured in the first and second fields. The range is 0 to 65 535.	
LESS_THAN	Match a value less than that specified. Enter a value in the first field. The second field is not accessible. The range is 0 to 65 535.	
GREATER_THAN	Match a value greater than that specified. Enter a value in the first field. The second field is not accessible. The range is 0 to 65 535.	

Dest Port

(destinationOperator, destinationPort1, destinationPort2)

The Dest Port parameter specifies the destination port match criterion for a packet. This parameter is configurable when the Protocol parameter is TCP or UDP. The range is 0 to 65 535. The default is 0.

Displayed Name

(displayedName)

The Displayed Name parameter specifies a name for the created policy object.



Note — You cannot use the colon symbol in a policy name. The 5620 SAM uses colons as separators for the object full name.

The range depends on the type of object being configured. Table 112-9 lists the Name parameter ranges for different policy object types.

Table 112-9 Displayed Name parameter

Object	Range (characters)
Forwarding subclass	0 to 29
Residential Subscriber policy	0 to 32
PBB MRP policy	0 to 32
Shared Risk Link Group policy	0 to 32
Static Configuration for SRLG policy	0 to 32
802.1x policy 7210 SAS Network Queue policy 7210 SAS Slope policy Host Tracking policy Multicast Info policy Ingress/Egress Queue Group Template policies WRED Slope policy HSMDA WRR Policy Diameter Peer Profile Diameter Profile GTP Prime Server Group Profile GTP Profile PLMN List Group QCI Policy	1 to 32
OmniSwitch QoS action, condition, or policy	1 to 31
9500 MPR QoS action, condition, or policy	0 to 10
Other	0 to 80

Distribution Mode

(distributionMode)

The Distribution Mode parameter specifies whether the local policy is synchronized with the associated global policy. Table 112-10 describes the parameter options.

Table 112-10 Distribution Mode parameter

Option	Option description	Dependencies
Sync With Global (default)	The local policy is synchronized with the global policy at all times. The local instance cannot be modified. Local policies discovered from the network or created through CLI are in Sync With Global mode.	—
Local Edit Only	You can modify the local instance only which affects the associated network element. Changes to the global policy do not affect the local policy unless a synchronization operation is manually performed.	—

Dot1p

(dot1p)

The Dot1p parameter specifies the IEEE 802.1p value to forwarding class and profile mapping of packets that ingress the network interface or access uplink port that uses the policy. When a packet is marked with the value specified by the Dot1p parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the profile specified by the Profile parameter. The range is 0 to 7. The default is 0.

Dot1p In Profile

(dot1pInProfile)

The Dot1p In Profile parameter specifies the forwarding class to IEEE 802.1p value mapping for in-profile packets that egress the network interface or access uplink port that uses the network policy. When an in-profile packet is marked with the forwarding class that is specified by the Forwarding Class parameter, the packet is mapped to the IEEE 802.1p value that is specified by the Dot1p In Profile parameter. The default for the Dot1p In Profile parameter depends on the forwarding class. The range is 0 to 7, or default. The 7210 SAS range is 0 to 7, or Not Set (-1).

Dot1P-LSP-EXP-Shared In Profile

(dot1pLspExpSharedInProfile)

The Dot1P-LSP-EXP-Shared In Profile parameter specifies the forwarding class to LSP-EXP mapping of in-profile LSP packets that egress the network interface that uses the network policy. When an in-profile packet is marked with the forwarding class that is specified by the Forwarding Class parameter, the packet is mapped to the Dot1P-LSP-EXP-Shared value that is specified by the Dot1P-LSP-EXP-Shared In Profile parameter. The default for the Dot1P-LSP-EXP-Shared In Profile parameter depends on the forwarding class. The range is 0 to 7, or default.

Dot1P-LSP-EXP-Shared Out Profile

(dot1pLspExpSharedOutProfile)

The Dot1P-LSP-EXP-Shared Out Profile parameter specifies the forwarding class to LSP experimental bit mapping of out-of-profile LSP packets that egress the network interface that uses the network policy. When an out-of-profile packet is marked with the forwarding class that is specified by the Forwarding Class parameter, the packet is mapped to the LSP experimental bit value that is specified by the Dot1P-LSP-EXP-Shared Out Profile parameter. The default for the Dot1P-LSP-EXP-Shared Out Profile parameter depends on the forwarding class. The range is 0 to 7, or default.

Dot1p Out Profile

(dot1pOutProfile)

The Dot1p Out Profile parameter specifies the forwarding class to IEEE 802.1p value mapping for out of profile packets that egress the network interface or access uplink port which uses the network policy. When an out of profile packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the IEEE 802.1p value specified by the Dot1p Out Profile parameter. The default for the Dot1p Out Profile parameter depends on the forwarding class. The range is 0 to 7, or default. The 7210 SAS range is 0 to 7, or Not Set (-1).

DSAP

(dsap)

The DSAP parameter specifies an Ethernet 802.2 LLC DSAP value or range as the match criterion. You must enable the parameter to specify a value. The range is -1 to 255. The default is -1, which means that filtering for this parameter is disabled. This parameter is configurable when the Frame Type parameter is set to e802dot2LLC.

DSAP Mask

(dsapMask)

The DSAP Mask parameter specifies a mask value as a match criterion when you filter on a DSAP value. The parameter is configurable when the DSAP parameter is enabled. The range is -1 to 255. The default is -1, which means that filtering for this parameter is disabled. This parameter is configurable only when the Frame Type parameter is set to e802dot2LLC.

DSCP

(dscp)

The DSCP parameter specifies the DiffServ Code Point value to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied.

When a packet is marked with the value specified by the DSCP parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and in some cases, the priority specified by the Priority parameter. When configuring a policy for a 7210 SAS, you must enable the checkbox before you can choose a value. The checkbox is disabled by default. Table 112-11 lists the parameter options.

Table 112-11 DSCP parameter

Options			
be (default)	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43

Dst Mask

(destinationIpAddressMask)

The Dst Mask parameter specifies the subnet mask length for the [Destination IP](#) parameter. The parameter is configurable when the [Destination IP](#) is enabled. The range is 0 to 32. The default is 0.

Egress Remark

(egressRemark)

The Egress Remark parameter specifies the remarking on all packets that egress on a specified network port. The remarking is based on the forwarding class to DSCP and LSP EXP bit mapping that is defined under the egress node of the network QoS policy. The options are:

- true (default)
- false

Entry ID

(id)

The Entry ID parameter specifies a unique identifier for the filter entry. This identifier determines the order of entries in a filter. Packets are compared to filter entries in ascending entry order. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. Table 112-12 lists the parameter ranges for different NE types. The default is 0, which means that the parameter is not configured.

Table 112-12 Entry ID parameter

NE type	Range
7705 SAR	1 to 64
All other NE types	1 to 65 535

Ether Type

(ethernetType)

The Ether Type parameter specifies an Ethernet type II value as the match criterion. When configuring a policy for the 7210 SAS, disable the checkbox to set the parameter to the default value and enable the checkbox to enter a value. The range is 1536 to 65 535, or -1. The default is -1, indicating that filtering for this parameter is disabled. The Ether Type parameter appears only when the Frame Type parameter value is Ethernet II.

Expedite

(expedite)

The Expedite parameter specifies the method that the device uses to service the queue in hardware. Although parental virtual schedulers can be defined for the queue, they only enforce how the queue vies for bandwidth with other queues associated with the same scheduler hierarchy. Expediting provides an internal mechanism which defines access rules when the queue competes for bandwidth with queues in other virtual schedulers. Table 112-13 describes the parameter options.

Table 112-13 Expedite parameter

Option	Option description	Dependencies
Auto (default)	Specifies that the device automatically defines the way that the queue is serviced in hardware. Specifies that the queue is treated in an expedited manner when all forwarding classes mapped to the queue are expedited types (nc, ef, h1 or h2). The queue is treated in a non-expedited manner when a single non-expedited forwarding class (be, af, l1, or l2) is mapped to the queue.	You cannot configure the parameter for network policy queue 9. It is set to Auto by default and cannot be changed. The Auto option is not available for ingress/egress queue group template policy queues.
Yes	Specifies that the queue is treated in an expedited manner regardless of the forwarding classes that are mapped to the queue	
No	Specifies that the queue is treated in a non-expedited manner regardless of the forwarding classes that are mapped to the queue	

Filter ID

(id)

See the [ID](#) parameter in this section for information.

Forwarding Class

(forwardingClass)

The Forwarding Class parameter specifies the forwarding class to map to an object. Table [112-14](#) describes the parameter options.

Table 112-14 Forwarding Class parameter

For	Description	Options
Queue mapping	Specifies the forwarding class that is mapped to the queue specified by the Queue ID, Multicast Queue ID, Broadcast Queue ID, Egress HSMDA Queue ID, and Unknown Queue ID parameters.	<ul style="list-style-type: none"> • be (default) • l2 • af • l1 • h2 • ef • h1 • nc
Dot1p, DSCP, EXP, Precedence, IP, and MAC mapping	<p>Specifies the forwarding class to which packets with the specified match criteria are mapped. The default option specifies that packets maintain their previous forwarding class. The parameter options are described in Table 112-7.</p> <p>The parameter is configurable as a DSCP, Precedence, or IP match criterion in an access egress policy for a 7210 SAS, 7450 ESS, 7710 SR, or 7750 SR.</p> <p>The parameter is configurable as an EXP criterion in an access egress policy for a 7450 ESS, 7710 SR, or 7750 SR, Release 8.0 or later.</p>	<ul style="list-style-type: none"> • default (default) • be • l2 • af • l1 • h2 • ef • h1 • nc

Fragment

(fragment)

The Fragment parameter specifies whether fragmented or non-fragmented packets are used as a packet match criterion. When the parameter is configured in a QoS policy, the matching packets are mapped to the forwarding class specified by the [Forwarding Class](#) parameter and the priority specified by the [Priority](#) parameter. Table 112-15 describes the parameter options.

Table 112-15 Fragment parameter

Option	Option description
off (default)	No match criterion is specified.
false	Specifies a match on all non-fragmented IP packets. Non-fragmented IP packets have the MF bit and the Fragment Offset field set to zero.
true	Specifies a match on all fragmented IP packets. A match occurs for each packet that has a non-zero value in the MF bit or the Fragment Offset field of the IP header.

High Priority Reserved

(highPriorityReserved)

The High Priority Reserved parameter specifies the percentage of buffer pool space for the queue that is only used by high-priority packets. The range is -1 to 100, with -1 indicating default. The default is default, which means that the device calculates high priority reserved pool size based on the CIR and the PIR values.

High WaterMark (%)

(highWaterMark)

The High WaterMark parameter specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be raised. The range is 0 to 100. The default is 95.

HSMDA Counter Override

(hsmdaCntrOvr)

The HSMDA Counter Override parameter specifies the counter to use for traffic that matches the specified entry. The range is 0 to 8. The default is 0. A value of 0 means that the default counters should be used.

When an EXP value is specified, packets matching value are mapped to the defined HSMDA exception counter for the packets queue group.

HSMDA Egress Profiling

(hsmdaDot1pProfile)

The HSMDA Egress Profiling parameter specifies whether egress profiling on HSMDA queues is performed. The options are:

- false (default)
- true

HSMDA Packet Byte Offset

(bytes)

Table 112-16 lists where to find information about the HSMDA Packet Byte Offset (bytes) parameter.

Table 112-16 HSMDA Packet Byte Offset (bytes) parameter

Parameter	See
HSMDA Packet Byte Offset (bytes) for egress	HSMDA Packet Byte Offset (bytes) parameter in this section
HSMDA Packet Byte Offset (bytes) for ingress	See the HSMDA Packet Byte Offset (bytes) parameter in this section

HSMDA Packet Byte Offset (bytes)

(hsmdaEgrPackByteOff)

The Packet Byte Offset parameter specifies the offset of an HSMDA egress policy. The parameter is configurable when the Override check box is enabled. The range is -32 to 31. The default is no override. When the Override check box is enabled, the value entered overrides the configured offset of the HSMDA egress policy.

HSMDA Packet Byte Offset (bytes)

(hsmdaIngPackByteOff)

The Packet Byte Offset parameter specifies the offset of an HSMDA ingress policy. The parameter is configurable when the Override check box is enabled. The range is -32 to 31. The default is no override. When the Override check box is enabled, the value entered overrides the configured offset of the HSMDA ingress policy.

ICMP Code

(icmpCode)

The ICMP Code parameter specifies the ICMP code of a packet as match criterion for the filter. The parameter is configurable when the [Protocol](#) parameter is ICMP. The range is 1 to 255. The default is None, which specifies that ICMP code matching is disabled.

ICMP Type

(icmpType)

The ICMP Type parameter specifies the ICMP type of a packet as match criteria for the filter. The parameter is configurable when the [Protocol](#) parameter is set to ICMP. The range is 1 to 255. The default is None, which specifies that ICMP type matching is disabled.

ID

(id)

The ID parameter specifies a unique ID for the object. You can configure the parameter for policies when the [Auto-Assign ID](#) parameter is set to disabled. Table 112-17 lists the parameter values for different applications.

Table 112-17 ID (id) parameter

Application	Value
Queues	1 to 8 1 to 12 for 7210 SAS-M Uplink mode
Policy ID	1 to 65 535
IKE policies	1 to 2048
RCA audit policies	1 000 000 999 999
7210 SAS Access Ingress policy meter ID	1 to 18; cannot create or delete meter ID 1 or 11

In Profile

(inDot1p)

The In Profile parameter specifies that packets matching the Dot1p value and that belong to the forwarding class specified by the Forwarding Class parameter are remarked as in-profile. If the parameter is set to default, packets are remarked according to the default access egress policy. The range is 0 to 7, or default. The default value is default.

Ingress Meter

(sapIngressWithAggregateMeter)

The Ingress Meter parameter specifies whether the SAP aggregate meter is enabled. The options are:

- true
- false (default)

Ingress Meter Burst

(sapIngressAggregateMeterBurst)

The Ingress Meter Burst parameter specifies the burst size for the SAP aggregate policer. You must configure the Ingress Meter Rate parameter before you can configure the Ingress Meter Burst parameter. The range is -1 to 2 146 959 kb. The default is 0. To configure the parameter, deselect the Disabled check box.

Ingress Meter Rate (kbps)

(sapIngressAggregateMeterRate)

The Ingress Meter Rate (kbps) parameter specifies the rate of the ingress meter. The range is 0 to 20 000 000. The default is 0. To configure the parameter, deselect the Disabled check box.

Inner Encap Value

(fwdSapInnerEncapValue)

The Inner Encap Value parameter specifies the SAP Inner encapsulation of the destination for this filter entry. A value of 0 indicates that either the SAP encapsulation value is not specified when Port Name and Service Id have valid values or there is no SAP destination. A value different from 0 can only be specified if the value of the Action property of this entry is forward SAP. The default is 0.

Inner Tag Value

(innerTagValue)

The Inner Tag Value parameter specifies the value to match against the VID of the second VLAN tag in the packet (after the service delimiting tags) that is carried transparently through the service. This parameter can only be set to a non-default value if the [MAC Filter Type](#) is set to the VID option. The default value of -1 indicates that no inner VLAN tag matching will be performed. The range is -1 to 4095.

Inner Tag VID Mask

(innerTagMask)

The Inner Tag Value parameter is applied as a mask to the VID of the inner VLAN tag of the packet prior to comparing it with the [Inner Tag Value](#). This parameter can only be set to a non-default value if the [MAC Filter Type](#) is set to the VID option. The range is 1 to 4095. The default is 4095.

IP Address

(address)

The IP Address parameter specifies the IP address of the host. You can configure the parameter when the [IP Address Pool Name](#) parameter is not configured and the [Use GI Address](#) parameter is set to False. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

IP Option

(ipOptionValue)

The IP Option parameter specifies the optional header field to be included in a packet as match criterion for the filter. Table 112-18 describes the parameter options.

Table 112-18 IP Option parameter

Option	Option description	Dependencies
EOOL (000) (default)	End of Options List	—
NOP (001)	No Operation	
RR (007)	Record Route	
ZSU (010)	Experimental Measure	
MTUR (012)	MTU Reply	
MTUP (011)	MTU Probe	
ENCODE (015)		
TS (068)	Time Stamp	
TR (082)	Traceroute	
SEC (130)	Security	
LSR (131)	Loose Source Route	
E_SEC (133)	Extended Security	
CIPSO (134)	Commercial Security	
SID (136)	Stream ID	
SSR (137)	Strict Source Route	
VISA (142)	Experimental Access Control	
IMITD (144)	IMI Traffic Descriptor	
EIP (145)	Extended Internet Protocol	
ADDEXT (147)	Address Extension	
RTRALT (148)	Router Alert	
SDB (149)	Selective Directed Broadcast	
NSAPA (150)	NSAP Addresses	
DPS (151)	Dynamic Packet State	
UMP (152)	Upstream Multicast Packet	
FINN (205)	Experimental Flow Control	

IP Opt Mask

(ipOptionMask)

The IP Opt Mask parameter specifies the IP mask value to use as a match criterion for the IP Option parameter specified. The parameter is configurable when the Option IP parameter is configured. The range is 0 to 255. The default is 0.

Level

Table 112-19 lists where to find more information about the Level parameter.

Table 112-19 Level parameter

Parameter	See
Level for Parent Scheduler	Level parameter in this section
Level for Port Parent	Level parameter in this section

Level

(level)

The Level parameter specifies the priority level of the tier 2 or tier 3 child scheduler in comparison to other child schedulers with the same parent scheduler. The Level parameter helps determine relative importance when children are contending for bandwidth. The parameter is configurable when the Tier parameter is set to the 2 or 3 option. The range is 1 to 8. The default is 1. The higher the number, the higher the priority level of the child scheduler bandwidth request.

Child schedulers with the Level parameter set lower than other child schedulers do not receive bandwidth until all child schedulers with a higher level have reached their maximum bandwidth allocation, or have no packets to pass.

When two child schedulers have the same Level parameter value, the [Weight](#) parameter determines which scheduler first receives bandwidth.

For example, there are three tier 2 schedulers with the same tier 1 parent scheduler:

- child scheduler alpha has its Level parameter set to 3
- child scheduler beta has its Level parameter set to 6
- child scheduler omega has its Level parameter set to 7

When the parent scheduler receives traffic above its CIR, bandwidth is allocated to the child schedulers. Child scheduler omega receives the bandwidth from the parent scheduler before beta and alpha. When omega reaches its maximum bandwidth requirements, and there is bandwidth remaining, scheduler beta receives the bandwidth before scheduler alpha.

Level

(portParentLevel)

The Level parameter specifies the priority level of child schedulers or queues in comparison to other child schedulers or queues with the same parent scheduler for above-CIR bandwidth distribution. The Level parameter helps determine relative importance when child schedulers or queues contend for bandwidth. The range is 1 (lowest priority) to 8 (highest priority). The default is 1.

Child schedulers or queues with the Level parameter set lower than other child schedulers or queues do not receive bandwidth until all of the schedulers and queues with a higher level reach their maximum bandwidth allocation, or have no packets to pass.

When two child schedulers or queues have the same Level parameter value, the **Weight** parameter determines which scheduler first receives bandwidth.

For example, there are three tier 2 schedulers with the same tier 1 parent scheduler:

- child scheduler alpha has its Level parameter set to 3
- child scheduler beta has its Level parameter set to 6
- child omega has its Level parameter set to 7

When the parent scheduler receives traffic above its CIR, bandwidth is allocated to the child schedulers. Child scheduler omega receives the bandwidth from the parent scheduler before beta and alpha. When omega reaches its maximum bandwidth requirements, and there is bandwidth remaining, scheduler beta receives the bandwidth before scheduler alpha.

Location

(groupEntriesLocation)

The Location parameter specifies at what location the inserted entries must be grouped. The options are:

- Top (default)
- Bottom

Loggable

(loggable)

The Loggable parameter specifies whether logging information about MAC filtering is generated and how this information, if any, is managed. Table 112-20 describes the options.

Table 112-20 Loggable parameter

Option	Option description
None (default)	No logging information is generated.
Log	An informational logging message about the packet that matches the entry is sent to the 7250 SAS or Telco console.

(1 of 2)

Option	Option description
Log Input	An informational logging message about the packet that matches the entry and includes input source information is stored on the 7250 SAS or Telco device.

(2 of 2)

Log ID

The Log ID parameter specifies the filter log for the filter entry. Click on the Select button beside the parameter to choose a filter, or type in a value. The range is 101 to 199. The default is 0, which means that the parameter is not configured.

Low WaterMark (%)

(lowWaterMark)

The Low WaterMark parameter specifies the utilization of the filter ranges for filter entry insertion, at which a table full alarm will be cleared. The range is 0 to 100. The default is 90.

MAC Monitoring

(dosProtectionMonitorMac)

The MAC Monitoring parameter specifies whether the tmnxCpmProtPolPerSrcRateLimit value as specified in the DoS Protection policy is applied. Select the MAC Monitoring check box to enable. This parameter is not supported on SR-1 and ESS-1 chassis types.

Max Average

(hiMaxAverage)

The Max Average parameter specifies the maximum average (high slope) for an in-profile WRED. The range is 0 to 100. The default is 90.

Max Average

(loMaxAverage)

The Max Average parameter specifies the maximum average (low slope) for an out-of-profile WRED. The range is 0 to 100. The default is 75.

Max Average

(nonTcpMaxAverage)

The Max Average parameter specifies the maximum average (non Tcp slope) for a WRED. The range is 0 to 100. The default is 75.

Max Probability

(hiMaxProbability)

The Max Probability parameter specifies the maximum probability (high slope) for an in-profile WRED. The range is 1 to 99. The default is 75.

Max Probability

(loMaxProbability)

The Max Probability parameter specifies the maximum probability (low slope) for an out-of-profile WRED. The range is 1 to 99. The default is 75.

Max Probability

(nonTcpMaxProbability)

The Max Probability parameter specifies the maximum probability (non Tcp slope) for a WRED. The range is 1 to 99. The default is 75.

Maximum Burst Size (kbps)

(mbs)

The Maximum Burst Size (kbps) parameter specifies the maximum amount of tokens allowed for a specific meter in kilobytes, and overrides the default value for the context. The function of this parameter depends on the value of the [Mode](#) parameter. Enable the Default checkbox to set the parameter to the default value of -1, indicated by MAX. Disable the Default checkbox to enter a value. The parameter value is an integer expression of the number of kilobytes reserved for the meter. For example, if you need to configure a value of 10KBits, then enter the value 10. The range depends on the policy. The default is Default enabled.

Maximum Burst Size (kb)

(maximumBurstSize)

The Maximum Burst Size (kb) parameter specifies the maximum burst pool size for a queue and overrides the default reserved burst pool for the queue. The range is -1 to 131 072, with -1 indicating default. Default specifies that the device calculates committed burst pool size based on the CIR and the PIR. The default is Default enabled.

Maximum Burst Size (bytes)

(maximumBurstSizeBytes)

The Maximum Burst Size (bytes) parameter specifies the maximum burst pool size for a queue and overrides the default reserved burst pool for the queue. The range is -1 to 134 217 728, with -1 indicating default. Default specifies that the device calculates committed burst pool size based on the CIR and the PIR. The default is Default enabled.

Maximum Number of Changes

(prctMaxNumberOfChanges)

The Maximum Number of Changes parameter specifies the maximum number of change conditions, such as a tariff or location change, that can occur before a partial record is created. The range is 0 to 32. The default is 4.

Maximum Queue Size (msec)

(maxQueueSize)

The Maximum Queue Size (msec) parameter specifies the buffer queue size for a specific egress class. The range is 1 to 1000. Table 112-21 lists the default value for each MLPPP and MCFR class.

Table 112-21 Maximum Queue Size (msec) parameter

Type	Class 0	Class 1	Class 2	Class 3
MLPPP	25	5	200	100
MCFR(msec)	10	50	150	750

MIR (%)

(mir)

The MIR(%) parameter specifies the MIR as a percentage of the available bundle rate. The range is 0 to 100. A value of 0 indicates that this parameter is not applicable to the class. Table 112-22 lists the default values assigned to each MLPPP and MCFR class. The MIR(%) is 100 for Class 0 and cannot be changed.

Table 112-22 MIR (%) parameter

Type	Class 0	Class 1	Class 2	Class 3
MLPPP	100	85	Not applicable	Not applicable
MCFR	100	90	Not applicable	Not applicable

MS Time Zone Change

(prctMsTimeZoneChange)

The MS Time Zone Change parameter specifies whether the MS time zone change partial record trigger is enabled. When the parameter is enabled, a partial record is created after an MS time zone change is detected. The options are:

- Disabled (default)
- Enabled

Mode

(mode)

The mode parameter specifies whether the queue supports color-aware profiling or priority forwarding and real-time rate-limiting functions. Table 112-23 describes the parameter options.

Table 112-23 Mode parameter

Option	Option description
priority (default)	Specifies that the queue is to support the access-ingress priority state for each packet. Packets may be classified by the SAP ingress QoS policy classification commands as either high- or low-priority. High-priority packets receive preferential buffering during queue congestion. Forwarding classes and subclasses configured as in-profile or out-of-profile are not allowed to map to queues configured as priority-mode. Setting the mode parameter to priority is only allowed during queue creation. Real-time rate limiting is supported when the queue is operating in priority mode.
profile	Specifies that the queue is to support color -aware profiling of the forwarding class and sub-classes mapped to the queue. Color-aware operational behavior is as follows: <ul style="list-style-type: none"> Classes defined as in-profile are handled as high priority and are never marked out-of-profile. In-profile packets consume queue CIR bandwidth. Classes defined as out-of-profile are handled as low priority and are never marked in-profile. Out-of-profile packets do not consume queue CIR bandwidth. Classes not set to in-profile or out-of-profile are marked according to the dynamic rate as they are scheduled from the queue. Packets scheduled from the queue when the queue is below or equal to CIR are marked in-profile, and packets scheduled from the queue when the queue is above CIR are marked out-of-profile. Non-profiled packets consume queue CIR bandwidth. Real-time rate limiting is not allowed on a queue operating in profile mode.

Multipoint

(multicast)

The Multipoint parameter specifies whether a queue applies only to multicast or unicast traffic. The options are:

- false (default)
- true (applies to 7210 SAS-M uplink access node)

Multiple Option

(multipleOption)

The Multiple Option parameter specifies whether to perform a match for a packet that contains more than one optional header field. This parameter is configurable when the Option Present parameter is enabled. Table 112-24 describes the parameter options.

Table 112-24 Multiple Option parameter

Option	Option description	Dependencies
off (default)	Specifies that filtering for this parameter is disabled.	—
false	Does not match when a packet contains more than one optional header field.	
true	Matches when a packet contains more than one optional header field.	

MultiPoint

(mCast)

The MultiPoint parameter specifies whether a meter can receive ingress packets that need to be sent to multiple destinations. Within non-multipoint services, such as Epipe services, all traffic is considered unicast due to the nature of the service type. Multicast and broadcast-destined traffic in an Epipe service are not mapped to a multipoint service meter. The options are:

- false (default)
- true

Name

(displayName)

The Name parameter specifies a name for the created object. The range is 1 to 32 characters. The characters must be 7-bit ASCII characters, excluding double quotation marks.

For MSAP policies, this parameter is the unique identifier of the MSAP policy. Two MSAP policies with the same name cannot exist in the 5620 SAM or on the same NE.



Note — The multicast information policy bundle named “default” cannot be modified or deleted.

Named Buffer Pool

(poolName)

The Named Buffer Pool parameter specifies the name of the pool for the ingress queue. Click on the Select button to list and choose a named buffer pool for the queue.

NE DoS Protection

(dosProtectionPolicyPointer)

The NE DoS Protection parameter allows you to specify the DoS protection policy for the MSAP Policy. Choose the required policy from the list of existing DoS protection policies. This parameter is not supported on SR-1 and ESS-1 chassis types.

New Entry ID

The New Entry ID parameter specifies the new identifier of the filter entry. The parameter value becomes the Entry ID of the filter entry. A filter policy compares the contents of a packet to each filter entry until it finds a match, beginning with the lowest Entry ID. The range is 1 to 65535. There is no default.

Offline Charging

(offlineState)

The Offline Charging parameter specifies whether offline charging is enabled for the charging profile. The options are:

- Disabled (default)
- Enabled

Option Present

(optionPresent)

The Option Present parameter specifies whether to perform a match on a packet that contains an optional header field. Table 112-25 describes the parameter options.

Table 112-25 Option Present parameter

Option	Option description	Dependencies
off (default)	Specifies that filtering for this parameter is disabled.	—
false	Does not match when a packet contains an optional header field.	
true	Matches when a packet contains an optional header field.	

Out Profile

(outDot1p)

The Out Profile parameter specifies that packets matching the Dot1p value and that belong to the forwarding class specified by the Forwarding Class parameter are remarked as out-of-profile. If the parameter is set to default, packets are remarked according to the default access egress policy. The range is 0 to 7, or default. The default value is default.

Outer Encap Value

(fwdSapOuterEncapValue)

The Outer Encap Value parameter specifies the SAP outer encapsulation of the destination for this filter entry. A value of 0 indicates that either the SAP encapsulation value is not specified when Port Name and Service Id have valid values or there is no SAP destination. A value different from 0 can only be specified if the value of the Action property of this entry is forward SAP. The default is 0.

Outer Tag Value

(outerTagValue)

The Outer Tag Value parameter specifies the value to match against the VID of the first VLAN tag in the packet (after the service delimiting tags) that is carried transparently through the service. This parameter can only be set to a non-default value if the [MAC Filter Type](#) is set to the VID option. The default value of -1 indicates that no outer VLAN tag matching will be performed. The range is -1 to 4095.

Outer Tag VID Mask

(outerTagMask)

The Outer Tag Value parameter is applied as a mask to the VID of the outer VLAN tag of the packet prior to comparing it with the [Outer Tag Value](#). This parameter can only be set to a non-default value if the [MAC Filter Type](#) is set to the VID option. The range is 1 to 4095. The default is 4095.

Override CIR

The Override CIR parameter specifies the override value for the administrative committed information rate for the queue or the policer. The default is MAX which specifies the maximum available CIR.

The CIR override is configured in kbps if the [Rate Type](#) for the queue or policer was originally set to kbps. The CIR override is configured as a Percent (%) if the [Rate Type](#) for the queue or policer was originally set to either Percent Port Limit (queues only) or Percent Local Limit.

The range depends on the type of object being configured. Table [112-26](#) lists the ranges.

Table 112-26 Override CIR parameter

Object type	Range
Queue	The range is 0 to 100 000 000 kbps (0 to 100%), depending on the line rate of the object to which the policy is applied. A value of -2 specifies that no override is applied. A value of -1 specifies that the maximum override is applied.
Policer	The range is 0 to 20 000 000 kbps (0 to 100%), depending on the line rate of the object to which the policer is applied. A value of -2 specifies that no override is applied. A value of -1 specifies that the maximum override is applied.

Override CIR Adaptation

The Override CIR Adaptation parameter specifies the override value for the method used by the device to derive the operational CIR setting when the queue is provisioned in hardware

Table 112-27 describes the parameter options. You can also choose the Default option, which specifies that the operational CIR for the queue is the rate closest to the rate specified by the CIR (kbps) parameter.

Table 112-27 Override CIR Adaptation parameter

Option	Option description	Dependencies
Closest (default)	The operational CIR for the queue is the rate closest to the rate specified by the CIR (kbps) parameter.	—
Min	The operational CIR for the queue is equal to or greater than the administrative rate specified by the CIR (kbps) parameter.	
Max	The operational CIR for the queue is equal to or less than the administrative rate specified by the CIR (kbps) parameter.	

Override Committed Burst Size

The Override Committed Burst Size parameter specifies the override value for the Committed burst pool size for a queue.

The range is -1 to 131 072, with -1 indicating default. Default specifies that the device calculates committed burst pool size based on the CIR and the PIR. The default is default.

Override High Priority Reserved

The Override High Priority Reserved parameter specifies the override value for the percentage of buffer pool space for the queue that is only used by high-priority packets.

The range is -1 to 100, with -1 indicating default. The default is default, which means that the device calculates the high priority reserved pool size based on the CIR and the PIR values.

Override Maximum Burst Size

The Override Maximum Burst Size parameter specifies the override value for the maximum burst pool size for a queue.

The range is -1 to 131 072, with -1 indicating default. Default specifies that the device calculates the committed burst pool size based on the CIR and PIR.

Override Packet Offset

The Override Packet Offset parameter specifies the number of offset bytes to add to (or remove from) a packet handled by a policer. A positive number adds bytes. A negative number removes bytes. The range is -128 and -32 to 31. The -128 value indicates that no override is applied. The default is -1.

Override PIR

The Override PIR parameter specifies the override value for the administrative peak information rate for the queue or the policer. The default is MAX which specifies the maximum available PIR.

For policers and non-HSMDA queues, the PIR override is configured in kbps if the [Rate Type](#) for the queue or policer was originally set to kbps. The PIR override is configured as a Percent (%) if the [Rate Type](#) for the non-HSMDA queue or policer was originally set to either Percent Port Limit (queues only) or Percent Local Limit.

The range depends on the type of object being configured. Table [112-28](#) lists the ranges.

Table 112-28 Override PIR parameter

Object type	Range
HSMDA queue	The range is 0 to 100 000 000 kbps, depending on the line rate of the object to which the policy is applied. A value of -2 specifies that no override is applied. A value of -1 specifies that the maximum override is applied.
Queue	The range is 0 to 100 000 000 kbps (0 to 100%), depending on the line rate of the object to which the policy is applied. A value of -2 specifies that no override is applied. A value of -1 specifies that the maximum override is applied.
Policer	The range is 0 to 20 000 000 kbps (0 to 100%), depending on the line rate of the object to which the policer is applied. A value of -2 specifies that no override is applied. A value of -1 specifies that the maximum override is applied.

Override PIR Adaptation

The Override PIR Adaptation parameter specifies the override value for the method used by the device to derive the operational PIR setting when the queue is provisioned in hardware

Table [112-29](#) describes the parameter options. You can also choose the Default option, which specifies that the operational PIR for the queue is the rate closest to the rate specified by the PIR (kbps) parameter.

Table 112-29 Override PIR Adaptation parameter

Option	Option description	Dependencies
Closest (default)	The operational PIR for the queue is the rate closest to the rate specified by the PIR (kbps) parameter.	—
Min	The operational PIR for the queue is equal to or greater than the administrative rate specified by the PIR (kbps) parameter.	
Max	The operational PIR for the queue is equal to or less than the administrative rate specified by the PIR (kbps) parameter.	

Override Port Average Overhead

The Override Port Average Overhead parameter specifies the override value for the average percentage that the offered load to a queue is expected to expand during the frame encapsulation process before sending traffic on queues that egress a SONET or SDH port or channel.

The range is 0 to 100. Default specifies that the egress QoS policy for the queue is applied.

Override Queue CIR Weight

The Override Queue CIR Weight parameter specifies the override value for the weight that should be assigned to this queue by the parent scheduler among all the entities feeding into the parent when the traffic is conforming to the committed rate.

The range is -2 to 100. Default specifies that the egress or ingress QoS policy for the queue is applied. A value of '0' specifies that the queue will not receive bandwidth for the 'within-cir' pass on its parent scheduler.

Override Queue Weight

The Override Queue Weight parameter specifies the weight that needs to be used by the scheduler to which this queue would be feeding.

The range is -2 to 100. Default specifies that the egress or ingress QoS policy for the queue is applied.

Override Summed CIR

The Override Summed CIR parameter specifies the override value for the summed CIR.

The options are:

- true
- false (default)

Packet Byte Offset

(pktOffset)

The Packet Byte Offset parameter specifies the number of offset bytes to add to (or remove from) a packet handled by a policer. A positive number adds bytes. A negative number removes bytes. The range is -32 to 31. The default is 0.

Parent Arbiter

(parentArbiter)

The Parent Arbiter parameter specifies the parent arbiter to the current arbiter. For a tier 1 arbiter, the parent must be root. For a tier 2 arbiter, the parent can be either root or a tier 1 arbiter under the same policy.

Path ID

(fwdSdpBindPathId)

The Path ID parameter specifies the ID of the SDP binding path of the destination for this filter entry. A value of 0 indicates that there is currently no SDP binding defined. A value different from 0 can only be specified if the value of the Action object of this entry is forward (SDP).

Peer IP Address

(peerListAddr)

The Peer IP Address parameter specifies the IP address for the peer. The default is 0.0.0.0, which means that the parameter is not configured. The formats are:

- for an IPv4 address—dotted-decimal format
- for an IPv6 address—colon-hexadecimal format
- for FQDN—up to 255 characters, must be configured for both peers

PIR (%)

(pir)

The PIR (%) parameter specifies the peak information rate, as a percentage of available bandwidth, for an ingress network MDA queue or an egress network port queue. The range is 0 to 100. The default is 100.

On ingress, the PIR defines the maximum rate that the queue can transmit packets through the switch fabric. On egress, the PIR defines the maximum rate that the queue can transmit packets out an egress interface.

The specified PIR (%) value does not guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

PIR (kbps)

(pir)

The PIR (kbps) parameter specifies the administrative peak information rate for a queue or a policer. The parameter specifies the maximum rate that the queue can transmit packets through the switch fabric for access ingress, or out an egress interface for access egress queues. Specifying a value for the PIR parameter does not guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The range is 1 to 100 000 000 kbps, dependant on the line rate of the object to which the policy is applied.

The range for a 7210 network ingress meter is -1 to 2 000 000.

The MAX check box specifies whether the PIR (kbps) parameter is set to infinity or can be configured. The options are:

- disabled
- enabled (enabled)

When the MAX check box is enabled, you cannot configure the PIR parameter.

The PIR (kbps) parameter can only be set when the [Rate Type](#) parameter is set to kbps. When [Rate Type](#) is not set to kbps, then the [PIR Percent \(%\)](#) parameter is configurable instead.

PIR Adaptation

(pirAdaptation)

The PIR Adaptation parameter specifies the method used by the device to derive the operational PIR setting when the queue is provisioned in hardware. Table [112-30](#) describes the parameter options.

Table 112-30 PIR Adaptation parameter

Option	Option description	Dependencies
Closest (default)	The operational PIR for the queue is the rate closest to the rate specified by the PIR (kbps) parameter.	—
Min	The operational PIR for the queue is equal to or greater than the administrative rate specified by the PIR (kbps) parameter.	
Max	The operational PIR for the queue is equal to or less than the administrative rate specified by the PIR (kbps) parameter.	

PIR Percent (%)

(pirPercent)

The PIR Percent (%) parameter specifies the administrative peak information rate for an access ingress/egress queue or policer. The parameter specifies the maximum rate as a percentage of the total available bandwidth that the queue can transmit packets through the switch fabric for access ingress, or out an egress interface for access egress queues. Specifying a value for the PIR Percent (%) parameter does not guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The range is 0 to 100%, in increments of 0.01%. The default value is 100.

The PIR Percent (%) parameter can only be set when the [Rate Type](#) parameter is not set to kbps. When [Rate Type](#) is set to kbps, then the [PIR \(kbps\)](#) parameter is configurable instead.

Policed

(policed)

The Policed parameter specifies that the out-of-profile traffic feeding into the physical queue instance should be dropped. The options are:

- true
- false (default)

Setting the parameter to true overrides the bandwidth specified by the SAP ingress queue administrative CIR.

Policer ID

(policerId)

The Policer ID parameter specifies a policer to be mapped to a forwarding class for unicast traffic. The range is 0 to 32. The default is 0.

You can click on the Select button to list and choose a policer. The policer must be preexisting on the access ingress policy.

Policing

(policing)

The Policing parameter specifies whether ingress traffic is policed. Policing is valid for CBR, RT-VBR and NRT-VBR. For 9500 MPR, policing is valid for CBR, UBR and UBR+. The options are:

- enabled
- disabled (default)

The parameter applies only to ingress traffic. Similarly, the Shaping parameter applies only to egress traffic. For example, if a traffic descriptor has both options, policing and shaping enabled, the policing option is enforced for the ingress traffic, while the shaping option is enforced for the egress traffic.

Port Average Overhead (%)

(portAvgOverhead)

The Port Average Overhead (%) parameter specifies the average percentage that the offered load to a queue is expected to expand during the frame encapsulation process before sending traffic on queues that egress a SONET or SDH port or channel. The default is 0. The range is 0 to 100.

Port Name

(fwdSapPortName)

The Port Name parameter specifies the destination SAP port for this filter entry. A value of empty string indicates that there is currently no SAP destination defined.

Port Parent

(portParent)

The Port Parent parameter specifies whether you can define a direct child-parent relationship between a queue and a port scheduler priority level. The options are:

- true
- false (default)

Precedence

(precedence)

The Precedence parameter specifies the IP precedence value to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress or egress the access interface to which the access ingress or egress policy is applied. The range is default, 0 to 7. The default is 0.

When a packet is marked with the value specified by the Precedence parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter.

Priority

(priority)

The Priority parameter specifies the enqueueing priority with which to map packets that are marked with the specified Dot1p, DSCP, EXP, Precedence, IP, or MAC value. Table [112-31](#) describes the parameter options.

Table 112-31 Priority parameter

Option	Option description	Dependencies
default (default)	Specifies that the probability of enqueueing a packet decreases when the ingress queue is congested	—
low	Specifies that the probability of enqueueing a packet decreases when the ingress queue is congested	—
high	Specifies that the probability of enqueueing a packet increases when the ingress queue is congested	

Profile

(profile)

The Profile parameter specifies how a packet is to be considered when associated with an access ingress or 7210 SAS network policy that involves forwarding classes. In-profile packets have a higher transmission priority than out-of-profile packets, which have a higher probability of being discarded if NE bandwidth is limited. Packets that are not explicitly marked as in-profile or out-of-profile have the status assigned by their forwarding class. Table 112-32 describes the parameter options.

Table 112-32 Profile parameter

Option	Option description	Dependencies
none (default)	Specifies that the packet forwarding class determines the status	Does not apply to the 7210 SAS.
in	Specifies that the NE considers the packet to be in-profile	—
out	Specifies that the NE considers the packet to be out-of-profile	—

The parameter is configurable as a DSCP, Precedence or IP match criterion in an access egress policy for a 7450 ESS, 7710 SR, or 7750 SR.

Profile ID

(id)

The Profile ID parameter specifies a unique ID for the object. The parameter is configurable for profiles when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 65 535.

Protocol

(protocol)

The Protocol parameter specifies the protocol to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied.

When a packet uses the protocol specified by the Protocol parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter. Table 112-33 lists the parameter options.

Table 112-33 Protocol parameter

Options			
ALL (default)	SEP	any distributed file system (68)	PIM
UDPTCP (*)	3PC	SAT_MON	ARIS
HOPOPT	IDPR	VISA	SCPS
ICMP	XTP	IPCV	QNX
IGMP	DDP	CPNX	A/N Active Networks (107)
GGP	IDPR_CMT	CPHB	IPComp
IP	TP++	WSN	SNP
ST	IL	PVP	Compaq_Peer
TCP	IPv6	BR_SAT_MON	IPX_in_IP
CBT	SDRP	SUN_ND	VRRP
EGP	IPv6Route	WB_MON	PGM
IGP	IPv6Frag	WB_EXPAK	any 0-hop protocol (114)
BBN_RCC_MON	IDRP	ISO_IP	L2TP
NVP_II	RSVP	VMTP	DDX
PUP	GRE	SECURE_VMTP	IATP
ARGUS	MHRP	VINES	STP
EMCON	BNA	TTP	SRP
XNET	ESP	NSFNET_IGP	UTI
CHAOS	AH	DGP	SMP
UDP	I_NLSP	TCF	SM
MUX	SWIPE	EIGRP	PTP
DCN_MEAS	NARP	OSPF_IGP	ISIS
HMP	MOBILE	Sprite_RPC	FIRE
PRM	TLSP	LARP	CRTP
XNS_IDP	SKIP	MTP	CRUDP
TRUNK_1	IPv6_ICMP	AX.25	SSCOPMCE
TRUNK_2	IPv6_No_Nxt	IPIP	IPLT
LEAF_1	IPv6_Opts	MICP	SPS

(1 of 2)

Options			
LEAF_2	any host internal protocol (61)	SCC_SP	PIPE
RDP	CFTP	ETHERIP	SCTP
IRTP	any local network (63)	ENCAP	FC
ISO_TP4	SAT_EXPAK	any private encryption scheme (99)	RSVP_E2E_IGNORE
NETBLT	KRYPTOLAN	GMTP	
MFE_NSP	RVD	IFMP	
MERIT_INP	IPPC	PNNI	

(2 of 2)

QoS Change

(citQosChange)

The QoS Change parameter specifies whether the QoS change detection is enabled. When QoS change detection is enabled, information about a QoS change is added to the CDR. The options are:

- Disabled (default)
- Enabled

Queue CIR Weight

(queueCirWeight)

The Queue CIR Weight parameter specifies the weight that should be assigned to this queue by the parent scheduler among all the entities feeding into the parent when the traffic is conforming to the committed rate. The range is 0 to 100. The default is 1. A value of '0' specifies that the queue will not receive bandwidth for the 'within-cir' pass on its parent scheduler.

Queue ID

(queueId)

The Queue ID parameter specifies a unicast queue to be mapped to a forwarding class. Click on the Select button to list and choose a queue. For network policies, enter a queue ID. The range for network policies is 0 to 8. The default is 0.

The queue is mapped to the forwarding class specified by the Forwarding Class parameter. The mapping that you specify overrides the default forwarding class-to-queue mapping for unicast traffic.

Queue Weight

(queueWeight)

The Queue Weight parameter specifies the weight that needs to be used by the scheduler to which this queue would be feeding. The range is 0 to 100. The default is 1.

RADIUS Count

(radiusCount)

The value specifies how many filter entries received from Radius for subscriber hosts can be inserted in the filter. The range is 0 to 65 535. The default is 0. If the [RADIUS Start Entry](#) parameter is set to 0, then this object will be put to 0 as well. Any change attempts will be silently discarded in this case.

RADIUS Start Entry

(radiusStartEntry)

The RADIUS Start Entry parameter specifies at what place the filter entries received from Radius will be inserted in the filter. No regular entries, nor Credit Control provided entries can be configured in this range. The range is 0 to 65 535. The default is 0. The value 0 means that no Radius provided filter entries can be inserted in the filter. If the [RADIUS Count](#) parameter is set to 0, then this object will be set to 0 as well. Any change attempts will be silently discarded in this case.

Rate Type

(rateType)

The Rate Type parameter specifies whether an absolute rate or percentage-based rate is used to specify the CIR and PIR when configuring queues and policers in access ingress and access egress policies. The parameter is also applicable when configuring queue and policer overrides on SAPs. The options are:

- kbps (default)
- Percent Port Limit (not available for policers or policer overrides)
- Percent Local Limit

Reassembly Timeout (msec)

(reassemblyTimeout)

The Reassembly Timeout (msec) parameter specifies the reassembly timeout for a specific ingress class. The range is 0 to 1000. Table 112-34 lists the default reassembly timeout value for each MLPPP and MCFR class.

Table 112-34 MLPPP Reassembly Timeout (msec) parameter

Type	Class 0	Class 1	Class 2	Class 3
MLPPP	10	10	100	1000
MCFR	25	25	100	1000

Redirect URL

(redirectURL)

The Redirect URL parameter specifies the URL to redirect a subscriber to when the [Action](#) parameter is set to HTTP redirect in an ACL IP or ACL MAC filter entry. The subscriber web browser closes the original TCP connection and opens a new connection to the web portal. The subscriber can use the web portal to create or modify a service profile. The web portal updates the ACL policy, directly or through another system, to remove the redirection policy. The range is 0 to 255 characters.

Remarking

(remarking)

The Remarking parameter specifies whether remarking applies to the packets that egress on the specified network port. The remarking is based on the forwarding class to DSCP and LSP EXP bit mapping that is defined for the egress node of the network QoS policy. The options are:

- true
- false (default)

Scheduler button

Click on the Scheduler button to list and choose a virtual scheduler for the object.

Scope

(scope)

The Scope parameter specifies whether the policy can be applied to individual or multiple SAPs and network ports. Table [112-35](#) describes the parameter options.

Table 112-35 Scope parameter

Option	Option description	Dependencies
template (default)	Policy can be applied to multiple SAPs or network ports. You can override Access Ingress or Access Egress policies that have the Scope parameter set to template.	—
exclusive	Policy can only be applied to a single SAP or network port. An error message appears if you attempt to assign the policy to another SAP or network port. You can reassign the policy if you remove the assignment to the original SAP or network port.	—

Service Category

(serviceCategory)

The Service Category parameter determines the priority a connection receives when requesting network bandwidth. Table 112-36 describes the Service Category parameter options listed from highest to lowest priority. Table 112-37 describes the Service Category parameter options for the 9500 MPR.

Table 112-36 Service Category parameter

When the Service Category parameter is set to	Traffic descriptor parameters	Option description
CBR	PIR (kbps) Shaping (enabled)	For applications such as voice and video that require high priority and have a known peak transmission rate. CBR guarantees bandwidth for constant bit rate traffic, very low cell loss, and very low delay. For circuit-switched data paths, the Service Category parameter is set to the CBR option and cannot be changed.
rt-VBR	SIR (kbps) MBS (cells) PIR (kbps) Shaping (enabled)	For time-sensitive applications, such as voice and video, that have unpredictable, bursty traffic characteristics. It guarantees very low cell loss and very low delay. The 5620 SAM handles rt-VBR and nrt-VBR identically for routing and rerouting purposes, and uses both to calculate the total VBR bandwidth usage. You cannot exceed the physical speed of the ATM interface when setting the traffic descriptors.
nrt-VBR		Choose nrt-VBR for applications, such as video ad frame relay, that have known or predictable traffic characteristics. It guarantees low cell loss and low delay. You cannot exceed the physical speed of the ATM interface when setting the traffic descriptors.
UBR (default)	MDCR (cells per second) PCR (cells per second) Shaping (disabled)	For applications that do not require guarantees of low cell loss or low delay. UBR paths emulate the connectionless services provided by conventional bridged and routed data networks.

Table 112-37 Service Category parameter for 9500 MPR

When the Service Category parameter is set to	Traffic descriptor parameters	Option description
CBR	Policing PCR (cells/second) CDVT (microseconds)	For applications such as voice and video that require high priority and have a known peak transmission rate. CBR guarantees bandwidth for constant bit rate traffic, very low cell loss, and very low delay. For circuit-switched data paths, the Service Category parameter is set to the CBR option and cannot be changed.
UBR (default)	Policing PCR (cells per second) CDVT(ms)	For applications that do not require guarantees of low cell loss or low delay. UBR paths emulate the connectionless services provided by conventional bridged and routed data networks.

(1 of 2)

When the Service Category parameter is set to	Traffic descriptor parameters	Option description
UBR+	Policing PCR (cells per second) CDVT(ms) MDCR (cells per second)	For ATM interface applications which require the ability to communicate both the minimum and maximum cell rates to the ATM network, so that the necessary QoS for traffic flow can be assured.

(2 of 2)

SGW Change

(citSgwChange)

The SGW Change parameter specifies whether SGW change detection is enabled. When SGW change detection is enabled, information about an SGW change is added to the CDR. The options are:

- Disabled (default)
- Enabled

Source IP

(sourceIpAddress)

The Source IP parameter specifies the source IP address to use as a packet match criterion in an ACL IP filter entry or QoS policy. When the parameter is configured in a QoS policy, the matching packets are mapped to the forwarding class specified by the [Forwarding Class](#) parameter and the priority specified by the [Priority](#) parameter.

If you are configuring an ACL IP filter policy or QoS policy, specify an IP address in dotted-decimal format.

If you are configuring an ACL IPv6 filter policy, specify an IP address in colon-hexadecimal format.

There is no default.

Source Port

(sourceOperator, sourcePort1, sourcePort2)

The Source Port parameter specifies the source port match criterion for packets. The parameter is configurable when the [Protocol](#) parameter is set to TCP or UDP. Table [112-38](#) describes the parameter options.

Table 112-38 Source Port parameter

Option	Option description	Dependencies
NONE (default)	No match criterion is specified.	—
EQUAL	Match the value specified in the first field. The second field is not accessible. The range is 0 to 65 535.	
RANGE	Match the range configured in the first and second fields. The range is 0 to 65 535.	
LESS_THAN	Match a value less than that specified. Enter a value in the first field. The second field is not accessible. The range is 0 to 65 535.	
GREATER_THAN	Match a value greater than that specified. Enter a value in the first field. The second field is not accessible. The range is 0 to 65 535.	

Src Mask

(sourceIpAddressMask)

The Src Mask parameter specifies the subnet mask length for the [Source IP](#) parameter. This parameter is configurable when the [Source IP](#) parameter is enabled. The range is 0 to 32. The default is 0.

SSAP

(ssap)

The SSAP parameter specifies an Ethernet 802.2 LLC SSAP value or range as match criterion. You must enable the parameter to specify a value. The range is -1 to 255. The default is -1, which means that filtering on this parameter is disabled. This parameter is configurable only when the Frame Type parameter is set to e802dot2LLC.

SSAP Mask

(ssapMask)

The SSAP Mask parameter specifies a mask value to use as a match criterion when you filter on an SSAP value. The parameter is configurable when the SSAP parameter is enabled. The range is -1 to 255. The default is -1, indicating that filtering on this parameter is disabled. This parameter is configurable only when the Frame Type parameter is set to e802dot2LLC.

Start Average

(hiStartAverage)

The Start Average parameter specifies the starting average (high slope) for an in-profile WRED. The range is 0 to 100. The default is 70.

Start Average

(loStartAverage)

The Start Average parameter specifies the starting average (low slope) for an out-of-profile WRED. The range is 0 to 100. The default is 50.

Start Average

(nonTcpStartAverage)

The Start Average parameter specifies the starting average (non Tcp slope) for a WRED. The range is 0 to 100. The default is 50.

Stats Mode

(statsMode)

The Stats Mode parameter specifies the counter allocation when generating statistics. Table 112-39 describes the parameter options.

Table 112-39 Stats Mode parameter

Option	Option description
Minimal (default)	The system creates one offered-output counter in the network processor and one discard counter in the QChip. Packet priority, initial profile, and CIR profile output are ignored, and are not individually visible in the policer statistics. Use the Minimal option when only basic policer accounting is required.
No Stats	The system does not allocate any counters to the policer. The absence of counters does not affect the operation of the policer. Use the No Stats option when policer accounting is not required. You cannot enable this option if the policer has a parent arbiter assigned to it.
Offered Limited Profile CIR	The system creates three offered-output counters in the network processor and three discard counters in the QChip. Use the Offered Limited Profile CIR when ingress color aware profiling is in use but packets are not being classified as in-profile. In most color aware instances, only undefined and explicit out-of-profile packets are used in service offerings. If an in-profile classified packet is offered to the policer, it is included in the offered-undefined statistic. Packet priority is ignored, and is not separated in the accumulated statistics.
Offered Priority CIR	The system creates four offered-output counters in the network processor and four discard counters in the QChip. Use the Offered Priority CIR option when the ingress policer is used on a non-color aware mode (all ingress packets have an undefined initial profile), but packet priority input and CIR state output visibility is required.

(1 of 2)

Option	Option description
Offered Priority No CIR	The system creates two offered-output counters in the network processor and two discard counters in the QChip. Use the Offered Priority No CIR option when ingress packet priority (high profile and low profile classification) accounting is the primary requirement. The initial and output profile of the packets offered to the policer is ignored in the offered, discarded, and forwarded statistics. This mode does not inhibit the function of CIR on the ingress policer and it does not prevent explicit in-profile and out-of-profile classification for packets offered to the policer.
Offered Profile CIR	The system creates four offered-output counters in the network processor and four discard counters in the QChip. The Offered Profile CIR option is similar to the Offered Limited Profile CIR option, except that it includes the in-profile packet classification along with the out-of-profile and undefined-profile classifications. As with the Offered Limited Profile CIR option, packet priority is ignored and not separated in the statistics.
Offered Profile No CIR	The system creates two offered-output counters in the network processor and two discard counters in the QChip. Use the Offered Profile No CIR option when all ingress packets are either in-profile or out-of-profile. Undefined-profile packets are treated as offered out from a statistics perspective. Undefined-profile packets are affected by the current state of the policer's CIR and are output as either in-profile or out-of-profile, depending on the CIR output state. The offered, discarded, and forwarded statistics do not reflect this behavior because they are based on the initial profile of the packets.
Offered Total CIR	The system creates two offered-output counters in the network processor and two discard counters in the QChip. Use the Offered Total CIR option when ingress priority and initial profile visibility is not required, and CIR profiling is in use. In many cases, all packets offered to a policer are of one priority level and all have the same initial profile (in-profile, out-of-profile, or undefined-profile). This option is different from the Minimal option because it provides visibility into the policer's CIR output.

(2 of 2)

Summed CIR

(summedCir)

The Summed CIR parameter specifies that the CIR rate be used as the summed CIR values of the children schedulers or queues. The options are:

- true (default)
- false

TCP Ack

(tcpAck)

The TCP Ack parameter specifies whether a match occurs for a packet that contains a cumulative acknowledgement, but no data. ACK filtering uses TCP data-driven loss recovery mechanisms. The parameter is configurable when the Protocol parameter is TCP. Table 112-40 describes the parameter options.

Table 112-40 TCP Ack parameter

Option	Option description	Dependencies
off (default)	Specifies that filtering for this parameter is disabled.	—
false	Does not match when a packet contains a cumulative acknowledgement, but no data.	
true	Matches when a packet contains a cumulative acknowledgement, but no data.	

TCP Syn

(tcpSyn)

The TCP Syn parameter specifies whether a match occurs for a packet that contains a cumulative acknowledgement, and also may contain data. The parameter is configurable when the Protocol parameter is TCP. Table 112-41 describes the parameter options.

Table 112-41 TCP Syn parameter

Option	Option description	Dependencies
off (default)	Specifies that filtering for this parameter is disabled.	—
false	Does not match when a packet contains a cumulative acknowledgement, and also may contain data.	
true	Matches when a packet contains a cumulative acknowledgement, and also may contain data.	

Termination of SDF

(citTerminationSdf)

The Termination of SDF parameter specifies whether termination of SDF detection is enabled. When termination of SDF detection is enabled, information about a termination of SDF is added to the CDR. The options are:

- Disabled (default)
- Enabled

Time Average Factor

(timeAvgFactor)

The Time Average Factor parameter specifies a weight factor between the previous shared buffer average utilization and current shared buffer instantaneous utilization when a new shared buffer average utilization is calculated. The range is 0 to 15. The default is 7, which indicates an instantaneous shared buffer utilization of 0.8%

Weighting occurs when the buffer pool uses a portion of the previous shared buffer average and adds the factor to the instantaneous shared buffer utilization. A low value, such as 3, weights the new shared buffer average utilization more towards the shared buffer instantaneous utilization. A high value, such as 11, weights the new shared buffer average utilization more towards the previous shared buffer average utilization value. The Time Average Factor parameter must be set to 3 on the 7705 SAR.

Time Limit per Rating Group (s)

(citTimeLimitRatingGroup)

The Time Limit per Rating Group (s) parameter specifies a time limit during which accounting information is collected for a rating group. After the specified time limit, information is added to the CDR. The range is 1 to 86 400. The default is 1800.

Time Limit (s)

(prctTimeLimit)

The Time Limit (s) parameter specifies a time limit, per session or bearer, for collecting accounting information. A partial record is created after the specified time limit is reached. The range is 0 to 86 400. The default is 3600.

Type

(type)

The Type parameter specifies the type of packet that egresses the network interface. The options are:

- DOT1P
- DOT1P-DSCP
- DOT1P-LSP-EXP SHARED (default)
- DSCP
- LSP-EXP

Use WRED Queue

(wredQueue)

The Use WRED Queue parameter specifies whether a WRED queue is to be created on the queue or not. The options are:

- Enabled
- Disabled (default)

User Location Change

(citUserLocationChange)

The User Location Change parameter specifies whether user location change detection is enabled. When user location change detection is enabled, information about a user location change is added to the CDR. The options are:

- Disabled (default)
- Enabled

VC ID

(fwdSdpBindVcId)

The VC ID parameter specifies the identification number of the virtual circuit for the SDP binding destination of this filter entry. A value of 0 indicates that there is currently no SDP binding defined.

VLAN Priority Tag

(vpt)

The VLAN Priority Tag parameter specifies the Dot1p priority value as a match criterion. The parameter is configurable when the check box is selected. Table 112-42 lists the parameter options.

Table 112-42 VLAN Priority Tag parameter

Option	Option description
default (default)	—
0	Best effort
1	Background
2	Spare
3	Excellent effort
4	Controlled load
5	Video
6	Voice
7	Network control

Volume Limit (Kbytes)

(prctVolumeLimit)

The Volume Limit (Kbytes) parameter specifies a volume limit, per session or bearer, for collected accounting information. A partial record is created after the volume limit is reached. The range is 0 to 65 535. The default is 4096.

Volume Limit per Rating Group (koctets)

(citVolumeLimitRatingGroup)

The Volume Limit per Rating Group (kocets) parameter specifies a volume limit, per rating group, for collected accounting information. When volume limit per rating group change detection is enabled, information is added to the CDR after the volume limit is reached. The range is 1 to 32 768. The default is 2048.

Weight

Table 112-43 lists where to find more information about the Level parameter.

Table 112-43 Weight parameter

Parameter	See
Weight for Parent Scheduler	Weight parameter in this section
Weight for Port Parent	Weight parameter in this section

Weight

(weight)

The Weight parameter specifies the relative importance of a child scheduler in comparison to other child schedulers that have the identical [Level](#) parameter settings. The parameter is configurable when the Tier parameter is set to the 2 or 3 option. The range is 000 to 100. The default is 001.

A setting of 000 specifies that the child scheduler receives bandwidth from the parent only after all non-000 weighted child schedulers have received bandwidth.

Weight

(portParentWeight)

The Weight parameter specifies the relative importance of a child scheduler or queue in comparison to other child schedulers or queues that have identical [Level](#) parameter settings. The range is 000 to 100. The default is 001. The higher the number, the higher the priority of the child scheduler bandwidth request.

A setting of 000 specifies that the child scheduler or queue receives bandwidth from the parent only after all non-000 weighted child schedulers and queues have received bandwidth.

Weight (%)

(weight)

The Weight (%) parameter specifies the weight, as a percentage, that is assigned to an egress class. The range is 0 to 100. A value of 0 indicates that this parameter is not applicable to the class. Table 112-44 lists the default value for each MLPPP and MCFR class.

Table 112-44 Weight (%) parameter

Type	Class 0	Class 1	Class 2	Class 3
MLPPP	Not applicable	Not applicable	66	33
MCFR	Not applicable	Not applicable	90	10

WRR Weight

(wrrWeight)

The WRR Weight parameter specifies the weight with which this queue should parent into the HSMDA scheduler, provided it is not superseded by the Weighted Round Robin (WRR) policy. The weight of each queue determines how much bandwidth that queue gets out of the total rate for the scheduling class. The queue ranges are as follows:

- Queue 1: 1 to 4
- Queue 2: 1 to 32
- Queue 3: 1 to 32

In each case, the default is 1.

113 –LTE LI delivery function peer parameters

113.1 LTE LI delivery function peer parameters 113-2

113.1 LTE LI delivery function peer parameters

This chapter describes the parameters on the LTE LI Delivery Function Peer form and the child forms.

Description

See “[Description](#)” in section [112.1](#) for the parameter description.

Address

(df2Addr)

The Address parameter specifies the IP address of the delivery function 2 peer associated with the target. The address can be an IPv4 address in dotted-decimal format. There is no default.

Address

(df3Addr)

The Address parameter specifies the IP address of the delivery function 3 peer associated with the target. The address is an IPv4 address in dotted-decimal format. There is no default.

ID

(id)

The ID parameter specifies a target for LI. The range is 1 to 16. There is no default.

Port

(df2Port)

The Port parameter specifies the port number of the delivery function 2 peer. The range is 1 to 65 535. The default is 1002.

Port

(df3Port)

The Port parameter specifies the port number of the delivery function 3 peer. The range is 1 to 65 535. The default is 1003.

114 –LTE LI interception target parameters

114.1 LTE LI interception target parameters 114-2

114.1 LTE LI interception target parameters

This chapter describes the parameters on the LTE LI Interception Target form and the child forms.

Content Type

(contentType)

The Content Type parameter specifies the interception type for the target. The options are:

- IRI (default)
- IRICC

Description

See “[Description](#)” in section [112.1](#) for the parameter description.

Target ID

(targetId)

The Target ID parameter identifies a unique target for the interception. The range is 1 to 15 digits. There is no default.

Target Type

(targetType)

The Target Type parameter specifies a target type for the interception. The only valid option is IMSI.

Content Type

(contentType)

The Content Type parameter specifies the interception type for the target. The options are:

- IRI (default)
- IRICC

115 –Trusted Peer List parameters

115.1 Trusted Peer List parameters 115-2

115.1 Trusted Peer List parameters

This chapter describes the parameters on the Trusted Peer List Policy forms and the child forms.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled. The options are:

- Up
- Down

The default value depends on the type of policy.

Displayed Name

See “[Displayed Name](#)” in section 112.1 for the parameter description.

Description

See “[Description](#)” in section 112.1 for the parameter description.

GTP Echo

(keepAlive)

The GTP Echo parameter specifies whether the General Packet Radio Services Tunneling Protocol (GTP) echo is enabled. The parameter is selectable using a checkbox.

Mobile Country Code

(mcc)

The Mobile Country Code parameter specifies the unique three-digit identifier that represents the country of the mobile subscriber. Choose a value from the drop-down menu. The default is unspecified.

Mobile Network Code

(mnc)

The Mobile Network Code parameter specifies the unique two- or three-digit identifier that is used with the MCC and represents the mobile network operator or carrier. The range is 2 to 3 characters in the range 0-9. There is no default.

Node Type

foreign

The Node Type parameter specifies whether the peer is a foreign or home node. The options are:

- Home (default)
- Foreign
- None

Peer IP Address

(peerListAddr)

The Peer IP Address parameter specifies the IP address for the peer. The default is 0.0.0.0, which means that the parameter is not configured. The formats are:

- for an IPv4 address—dotted-decimal format
- for an IPv6 address—colon-hexadecimal format
- for FQDN—up to 255 characters, must be configured for both peers

Prefix

(prefix)

The Prefix parameter specifies the IP address for a prefix list entry. Specify an IPv4 address in dotted-decimal format, or an IPv6 address in colon-hexadecimal format.

Radio Access Technology

ratType

The Radio Access Technology parameter specifies the radio access technology type being served by the peer. The options are:

- GERAN
- UTRAN (default)
- EUTRAN

Tools menu parameters

- 116 – Service Test Manager parameters
- 117 – Ethernet CFM parameters
- 118 – Scripts parameters
- 119 – Auto-Provision Profiles parameters
- 120 – Bulk Operations parameters
- 121 – Card Migration Event Manager parameters
- 122 – MIB Policies parameters
- 123 – Server Performance Statistics parameters
- 124 – Accounting Policies parameters
- 125 – File Policies parameters
- 126 – Statistics Browser parameters
- 127 – TCA Policies parameters
- 128 – RAN Performance Management Policies parameters
- 129 – Schedules parameters
- 130 – Policies Audit parameters
- 131 – Time Range Entry Assignment parameters

- 132 – Copy/Move SAPs parameters
- 133 – NE Sessions parameters
- 134 – Common Tools menu parameters

116 –Service Test Manager parameters

116.1 Service Test Manager parameters 116-2

116.1 Service Test Manager parameters

This chapter describes the parameters on the Service Test Manager form and child forms.

Accounting Files

(accountingFiles)

The Accounting Files parameter specifies whether the test suite uses SAA accounting. The options are:

- disabled (default)
- enabled

When the parameter is enabled, the [Ignore Probe Results](#) parameter and the [Lightweight Execution](#) parameter are not configurable.

Administrative State

See the [Administrative State](#) parameter in section [134.1](#).

Age (seconds)

(age)

The Age (seconds) parameter specifies how long, in s, an OAM MAC address ages in the FIB. The default is 3600.

Alarm Threshold (%)

(dualEndedLossRaiseThreshold)

The Alarm Threshold (%) parameter specifies the loss threshold at which an alarm is raised for a Y.1731 Dual Ended Loss Test. The value is specified in hundredths of a percent. The range is 0.00 to 100. The default is .25.

Alarm Clearing Threshold (%)

(dualEndedLossClearThreshold)

The Alarm Clearing Threshold (%) parameter specifies the loss threshold at which an alarm is cleared for a Y.1731 Dual Ended Loss Test. The value is specified in hundredths of a percent. The range is 0.00 to 100. The default is 0.

ANCP String

(ancpString)

The ANCP String parameter specifies an ANCP string that is the ASCII representation of the DSLAM circuit ID. The range is 0 to 63 characters. There is no default.

ATM Interface ID

(pvcConnection)

The ATM Interface ID parameter specifies the ID of the ATM PVC against which the ATM ping is performed. Click on the Select button to choose an ATM PVC connection.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [134.1](#).

Bypass Routing

(bypassRouting)

The Bypass Routing parameter specifies whether to bypass the routing table and send the ICMP ping request to a host on a directly attached network. The options are:

- disabled (default)
- enabled

When the [Egress Interface Index](#) parameter is set to a value other than 0, you must disable the parameter.

Clear Alarm on Falling Threshold

(clearAlarmOnFalling)

The Clear Alarm on Falling Threshold parameter specifies whether to clear a threshold-crossing alarm when a falling threshold is crossed and the threshold condition no longer exists. The options are:

- enabled
- disabled (default)



Note — To provide meaningful test results, the tested devices must use a common timing source; for example, NTP.

Continuously Executed

(contExecution)

The Continuously Executed parameter specifies whether a test suite that employs this test policy should be continuously executed by the node. This parameter can only be configured when the [NE Schedulable](#) and [Accounting Files](#) parameters are enabled. The options are:

- enabled
- disabled (default)

Control MEP

(controlMep)

The Control MEP parameter specifies whether to include the CC state in the protection algorithm. Alcatel-Lucent recommends including the CC state if fast failure detection is required, for example, when Link Layer OAM does not provide the required detection time. The parameter applies only to Ethernet tunnel path endpoint MEPs. The options are:

- True
- False (default)

Control Plane

(sendControl)

The Control Plane parameter specifies whether the OAM request is to be sent on the control plane. The options are:

- Enabled
- Disabled (default)

Count

The Count parameter specifies the number of frames to be sent during an OS 6850, or OS 6850E ping. The range is 0 to 2 147 483 647. The default is 6.

Count

(count)

The count parameter specifies the number of messages that an access node uses to test a circuit. The range is 1 to 32. The default is 1.

Count

(mepSingleEndedLossCount)

The count parameter specifies the number of LMM frames for a Single Ended Loss test. The range is 2 to 5. The default is 2.

Customer ID

The Customer ID parameter specifies the customer associated with the ANCP loopback diagnostic.

Data Pattern

(pattern)

The Data Pattern parameter specifies a number that represents the binary pattern that is inserted into the data field of an ICMP ping. The parameter is configurable when the [Positional Data Pattern](#) parameter is disabled. The range is -1, or 0 to 65 535. The default is -1, which means that the parameter is not configured.

Data Size

(mepTransmitLbmDataTlv)

The Data Size parameter specifies the size of the loopback message. The range is 1 to 1500. The default is 0, which means that the parameter is not configured.

Data Size (octets)

(mepEthTestDataLen)

The Data Size (octets) parameter specifies the number of data octets in an Eth test frame. The range is 64 to 1500. The default is 64.

Description

(description)

See the [Description](#) parameter in section [134.1](#).

Destination Address

(destinationIpAddr)

The Destination Address parameter specifies the destination IP address for a multicast trace OAM diagnostic. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Destination IP Address

(targetIpAddress)

The Destination IP Address parameter specifies the IP address of the CPE device that is the target of a ping. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Destination Path Address

(pathDest)

The Destination Path Address parameter specifies a unique path for an LSP ping, such as an ECMP path. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Destination Type

(destinationType)

The Destination Type parameter specifies the type of ping destination. Table 116-1 describes the parameter options.

Table 116-1 Destination Type parameter

Option	Description
End-to-End (default)	Sends a unidirectional ping to the connection endpoint
Segment	Sends a unidirectional ping to the segment termination point

DiffServ Field

(diffServField)

The DiffServ Field parameter specifies the DiffServ value for a test packet. The value is used to populate the Differentiated Services field in the IP packet that contains the OAM probe. The Differentiated Services field is defined as the ToS octet in an IPv4 header. The range is 0 to 255. The default is 0.

The parameter can be used to determine the effect of an explicit Differentiated Services value has on a trace response. A Differentiated Services value is typically not supported in IP implementations. A value of 0 means that the function represented by this option is not supported. Useful service octet values include 16 for low delay and 8 for high throughput.

DMR Frames Transmitted

(dmrTxCount)

The DMR Frames Transmitted parameter is a read only counter that specifies number of DMR frames transmitted on the MEP.

DNS Name

(dnsName)

The DNS Name parameter specifies the DNS name to resolve to an IP address. The range is 1 to 32 characters. There is no default.

DNS Server Address

(targetIpAddress)

The DNS Server Address parameter specifies the IP address of a DNS server that is reachable by the managed devices. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

DNS Server Type

(dnsServerType)

The DNS Server Type parameter specifies the type of DNS server for name resolution. The options are:

- User Choice
- Primary (default)
- Secondary
- Tertiary

Do Not Fragment

(doNotFragment)

The Do Not Fragment parameter specifies whether the Don't Fragment, or DF bit is set in an ICMP ping packet. The options are:

- disabled (default)
- enabled

When the parameter is disabled, the bit is not set.

Duration (minutes)

(timer)

The Duration (minutes) parameter specifies the duration of the continuity check test in minutes. A duration of 0 denotes continuous execution of Continuity Check (CCM Messages). The range is 0 to 1439. The default is 0.

Egress Interface Index

(egressIfIndex)

The Egress Interface Index parameter specifies the interface index of the interface that transmits ICMP ping packets. The options are 0 to 2 147 483 647. The default is 0, which means that the parameter is not configured.

When the [Bypass Routing](#) parameter is enabled, the parameter must be set to 0.

Enable Test

(dualEndedLossEnable)

The Enable Test parameter specifies whether a Y1731 Dual Ended Loss Test is enabled when Continuity Check messages are enabled. The options are:

- disabled (default)
- enabled

Entity Type

(testedEntityType)

The Entity Type parameter specifies the type of object to which the test policy or test suite applies. In the context of a test policy, the parameter determines the types of available test definitions. In the context of a test suite, the parameter determines the types of tests that the 5620 SAM generates. Table 116-2 lists the parameter options.

Table 116-2 Entity Type parameter

Option	Option Description	Dependencies
None	Places no restrictions on the test types available for inclusion in a test suite	Available for test suite only
VLL Service (default)	—	—
VPLS	—	—
VPRN Service	—	—
Mirror Service	—	—
P2MP LSP	—	—
Tunnel (SDP)	—	—
LSP	—	—
Service Connector	—	—
ATM PVC	—	—
Router	—	—
EPS Path (LTE)	—	—
Mobile Service	—	—

EPS Path ID

(id)

The EPS Path ID parameter specifies the 5620 SAM identifier for the EPS path.

First Run Execution Sequence

(firstGroupExecutionSequence)

The First Run Execution Sequence parameter specifies, for a test suite, the order of execution for the tests in the First Run Tests list. Table 116-3 lists the parameter options.

Table 116-3 First Run Execution Sequence parameter

Option	Option description
In Parallel (default)	Specifies that the tests run concurrently
All In Sequence	Specifies that the tests run sequentially

Flood

(flood)

The Flood parameter specifies the method of sending an OAM MAC address during a MAC populate or MAC purge operation. Table 116-4 describes the parameter options.

Table 116-4 Flood parameter

Option	Option description
Enabled	Specifies that the OAM MAC address is sent to all upstream devices, and each upstream device adds or deletes the MAC address, depending on the type of OAM
Disabled (default)	Specifies that the OAM MAC address is sent to the local FIB

Force OAM

(force)

The Force OAM parameter specifies that the MAC address is converted to an OAM-generated MAC address, even if the MAC address is set by another method. The options are:

- Enabled
- Disabled (default)

Forwarding Class

(forwardingClass)

The Forwarding Class parameter specifies the forwarding class for OAM packets. The options are:

- be (default)
- l2
- af
- ll
- h2
- ef
- h1
- nc



Note 1 – For LSP ping and MAC ping, the parameter value is automatically set to the SDP forwarding class.

Note 2 – For LSP ping and LSP trace, the parameter value is automatically set to the LSP tunnel forwarding class.

Note 3 – For VCCV ping, the parameter value is automatically set to the VLL forwarding class.

Forwarding Profile

(profile)

The Forwarding Profile parameter specifies whether the test packets are in or out of profile, as compared to the forwarding class of the test packet. The options are:

- in (default for VCCV ping)
- out (default)

From Access Gateway

(originatingEpsSite)

The From Access Gateway parameter specifies the IP address of the NE on which an SGW or PGW instance exists and which is used as the origin of the test.

From IP Address

(originatingNode)

The From IP Address parameter specifies the IP address of the managed device that is the origin of the OAM test. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

When the [Target Type](#) parameter is set to VPRN Site, the routing instance is displayed.

Generate Alarm on Rising Threshold

(generateAlarmOnRising)

The Generate Alarm on Rising Threshold parameter specifies whether to raise a threshold-crossing alarm when a rising threshold is crossed. The options are:

- enabled (default)
- disabled



Note — To provide meaningful test results, the tested devices must use a common timing source, for example, NTP.

Generator Frame Size (bytes)

(frameSize)

The Generator Frame Size (bytes) parameter specifies the size of packets in bytes. The range is 64 to 9212. The default is 64.

Generator Tx Rate

(txRate)

The Generator Tx Rate parameter specifies the rate at which the traffic generator shall generate the traffic. The value should be a multiple of 8. The range is 8 to 10000. The default is 8.

ID

(id)

The ID parameter specifies a unique numeric identifier for the created object. The parameter is configurable when the Auto-Assign ID parameter is disabled. Table 116-5 lists the parameter ranges for different object types. The default is 0, which means that no value is specified.

Table 116-5 ID parameter

Object	Range
OAM test	1 to 99 999 999
STM test policy or test suite	1 to 268 435 455

ID

(lsp)

The ID parameter specifies the ID of the LSP being tested. The parameter is configurable when the [Target Type](#) parameter is set to LSP or LSP Path and the [Site ID](#) parameter is configured.

ID

(mepId)

The ID parameter specifies the ID of the remote MEP being tested. The range is 1-8191. The default is 0, which means that the parameter is not configured.

Ignore Probe Results

(ignoreResults)

The Ignore Probe Results parameter specifies that the 5620 SAM ignores all test probe result records. The options are:

- Disable (default)
- Enable

When the [Lightweight Execution](#) parameter is enabled, the parameter is also enabled and read-only.

Include Falling Threshold

The Include Falling Threshold parameter specifies whether to generate a threshold-crossing alarm for an OAM test if the value falls below a specified level. The options are:

- Enabled
- Disabled (default)

Increase Tx Rate Every Iteration

(txRateIteration)

The Increase Tx Rate Every Iteration by parameter specifies the value added to the traffic generator rate after each iteration. The value must be a multiple of 8. The range is 8 to 9992. The default is 8.

Inhibit Learning

(inhibitLearning)

The Inhibit Learning parameter specifies whether MAC entries are learned (created in the router table) during an OAM MAC purge diagnostic activity. The options are:

- Enabled
- Disabled (default)

Initial Time to Live

(initialTimeToLive)

The Initial Time to Live parameter specifies the minimum TTL value in the packet label for the OAM diagnostic. The range is 0 to 255. The default is 1.

Interface Type

(sapOrBinding)

The Interface Type parameter specifies the type of object that the MEP is associated with. The options are:

- SAP (default)
- SdpBinding
- Ethernet Tunnel Path Endpoint
- Ethernet Ring Path Endpoint
- Network Interface
- Port
- LAG

Interval (seconds)

The Interval (seconds) parameter specifies the polling interval that is used for the ping. The range is 1 to 10 000. The default is 1.

Interval (seconds)

(interval)

The Interval (seconds) parameter specifies the minimum amount of time, in seconds, that must expire before the next message request is sent. The range is 1 to 10. The default is 1. A value of 0 indicates that only one message request is sent.

Interval

(mepSingleEndedLossInterval)

The Interval parameter specifies the interval at which to send LMM frames in a single-ended loss test. The range is 1 s or 100 ms. The default is 1 s.

IP Address

The IP Address parameter specifies the IP address of the OS 6850, or OS 6850E that is the object of the ping. The value is an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

IP Address

(srcIpAddrPointer)

The IP Address parameter specifies the source IP address for the LSP Ping or LSP Trace test. You configure this by clicking the associated Select button and choosing the required entry in the Select LDP Site form that is displayed. The parameter is only configurable when the [Target Type](#) parameter is set to Any LSP, and when the [LDP Site ID](#) is configured.

This parameter only needs to be specified when the OAM packet must be generated from a different address than the node's system interface address. The OAM messages which operate over an LDP LSP, and/or over a PW signalled by T-LDP, and which require a response using the IP path, must use a source IP address which is reachable within the same routing domain as that of the LSR ID of the LDP or T-LDP session. The NE sender source address of the echo request message for either LSP Ping or LSP Trace LDP FEC messages must be one that is reachable within the domain of the FEC destination.

Last Run Execution Sequence

(lastGroupExecutionSequence)

The Last Run Execution Sequence parameter specifies, for a test suite, the order of execution for the tests in the Last Run Tests list. Table [116-6](#) lists the parameter options.

Table 116-6 Last Run Execution Sequence parameter

Option	Option description
In Parallel (default)	Specifies that the tests are run concurrently
All in Sequence	Specifies that the tests are run in sequence

LDP Prefix

(ldpPrefix)

The LDP Prefix parameter specifies the IP address of the LDP for the MPLS path being probed by an LSP OAM diagnostic. You can configure the parameter when the Target Type parameter is set to *Type of Site*. Specify the IP address of the LDP prefix. The default is 0.0.0.0, which means that the parameter is not configured.

LDP Prefix Length

(ldpPrefixLen)

The LDP Prefix Length parameter specifies the prefix length of the LDP IP address for the MPLS path being probed by an LSP OAM diagnostic. You can configure the parameter when the Target Type parameter is set to *type_of Site*. The parameter can be set to 32. The default is 32.

LDP Prefix Length

(ldpPrefixLen)

The LDP Prefix Length parameter specifies the IP address prefix length for the LDP-based LSP for the OAM LDP tree discovery test. You can configure the parameter when the [LDP Prefix](#) value has been specified. The prefix length value can be set to 32. The default is 32.

Lightweight Execution

(sla)

The Lightweight Execution parameter specifies that the 5620 SAM only displays results for tests that fail, generate threshold crossing alarms, or time out. The options are:

- Disabled (default)
- Enabled

When the parameter is enabled, the [Ignore Probe Results](#) parameter is enabled and the [Trap Generation](#) parameter options are enabled.

Loopback Location (hex)

(loopbackLocation)

The Loopback Location (hex) parameter specifies the ID used in the ATM OAM loopback cell, for example, FF:FF:01:FF:00:FF:02:FF. If all bits in the ID are 1, the destination of the ATM OAM ping is the far end of the virtual circuit. Otherwise, the destination is a specific ATM node. The range is 16 hexadecimal numbers separated by a “.”, up to 47 characters. Each number ranges from 00 to FF. The default is FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF.FF, which means that the parameter is not configured.

Maximum Concurrent Pings

(maxConcurrentPings)

The Maximum Concurrent Pings parameter specifies the maximum number of simultaneous pings that can be performed on the managed device. The parameter is configurable when the [Unlimited Concurrent Pings](#) parameter is disabled. The range is 0 to 2 147 483 647. The default is 10.

Maximum Concurrent Traces

(maxConcurrentTraces)

The Maximum Concurrent Traces parameter specifies the maximum number of simultaneous traces that can be performed on the managed device. The parameter is configurable when the [Unlimited Concurrent Traces](#) parameter is disabled. The range is 0 to 2 147 483 647. The default is 10.

Maximum Failures

(maxFailures)

The Maximum Failures parameter specifies how many packet arrival failures are allowed before the OAM test is considered failed. The range is 0 to 255. The default is 5. A value of 0 or 255 specifies no maximum number of failures.

Maximum Hop

The Maximum Hop parameter specifies the maximum number of hops in the path to the target OS 6850, or OS 6850E. The range is 0 to 2 147 483 647. The default is 5.

Maximum Number of Hops

(hopCount)

The Maximum Number of Hops parameter specifies the maximum number of hops along the path to the source device. The range is 1 to 255. The default is 5.

Maximum Number of Results to Keep

(maxNumObjectTokeep)

The Maximum Number of Results to Keep parameter specifies the sum of the Test Results, Aggregated Results, and the number of probes results in the database (viewed from the Test Results-Probe Tab), and any other objects that may be required to store the test results in the database. The range is 60 000 to 20 000 000. The default is 1 000 000.

Maximum Time to Live

(maxTimeToLive)

The Maximum Time to Live parameter specifies the maximum TTL value, in hops, in the packet label for the OAM diagnostic. The parameter value must be greater than the [Initial Time to Live](#) parameter value. The range is 1 to 255. The defaults are as follows:

- 4 for VPRN trace and MAC trace
- 8 for VCCV trace
- 30 for LSP trace, LDP tree trace, ICMP trace, and P2MP LSP trace

MTU End Size (octets)

(mtuEndSize)

The MTU End Size (octets) parameter specifies the size, in octets, of the end frame in an MTU OAM diagnostic test. The parameter value must exceed the [MTU Start Size \(octets\)](#) parameter value, which is the frame size at the beginning of the test. During the test, the frame grows incrementally by the number of bytes specified by the [MTU Step Size \(octets\)](#) parameter value. The test is complete when the frame size reaches the end frame size, or when three messages at the current step size time out. The range is 41 to 9198. The default is 9198.

MTU Start Size (octets)

(mtuStartSize)

The MTU Start Size (octets) parameter specifies the size, in octets, of the start frame in an MTU OAM diagnostic test. During the test, the frame grows incrementally by the number of bytes specified by the [MTU Step Size \(octets\)](#) parameter value. The test is complete when the frame size reaches the [MTU End Size \(octets\)](#) parameter value, or when three messages at the current step size time out. The range is 40 to 9197. The default is 40.

MTU Step Size (octets)

(mtuStepSize)

The MTU Step Size (octets) parameter specifies by how many bytes a frame grows during each pass in an MTU OAM diagnostic test. The [MTU Start Size \(octets\)](#) parameter value determines the size of the start frame. During the test, the frame grows incrementally by the number of bytes specified by the parameter. The next frame is sent only after a reply is received. The test is complete when the frame size reaches the [MTU End Size \(octets\)](#) parameter value, or when three messages at the current step size time out. The range is 1 to 512. The default is 32.

Multicast Group

(groupMcastAddress)

The Multicast Group parameter specifies the destination multicast address for an OAM request. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Multicast Source

(sourceMcastAddress)

The Multicast Source parameter specifies the source multicast address for the OAM request. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Name

Table [116-7](#) lists where to find information about the Name parameter.

Table 116-7 Name parameter

Parameter	See
Name for aggregation scheduler	Name parameter in this section
Name for service site	Name parameter in this section
Name for subscriber	Name parameter in this section
Name for test, test policy or test suite	Name parameter in chapter 134

Name

(aggregationSchedulerName)

The Name parameter specifies a name for the aggregation scheduler. The range is 1 to 32 characters. There is no default.

Name

(siteName)

The Name parameter specifies the name of the service site. Click on the Select button and choose a service site from the list.

For CPE, MAC, and multicast FIB pings, the parameter is configurable when the [Service Name](#) parameter is configured.

Name

(subscriberName)

The Name parameter specifies a name for the subscriber. The range is 0 to 32 characters. There is no default.

NE Persistent

(nePersistent)

The NE Persistent parameter specifies whether the OAM test is deployed to a device after the first run. When you enable the parameter, the OAM test is deployed to the NE and remains on the NE. The options are:

- Disabled (default)
- Enabled

NE Schedulable

(neSchedulable)

The NE Schedulable parameter specifies whether the associated OAM test, or the test suite generated from the policy, can be scheduled and run on managed NEs. The options are:

- Disabled (default)
- Enabled

When you enable the parameter for an OAM test, the test is deployed to the managed NE.

If you want the test suite that is associated with the test policy to become an NE scheduled task, you must enable the parameter in the test policy.

The [Ignore Probe Results](#) and [Lightweight Execution](#) parameters are configurable when the parameter is enabled.



Note — This parameter does not apply to CFM or Y.1731 tests for all 7210 SAS nodes.

Next Hop Address

(nextHopAddr)

The Next Hop Address parameter specifies the IP address of the next hop for VPRN ICMP diagnostics. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

You can configure the parameter when the [Target Type](#) parameter is set to VPRN Site and [Bypass Routing](#) is disabled.

Next Hop Interface Address

(nhAddress)

The Next Hop Interface Address parameter specifies the interface address to the next hop in which the LSP ping test is transmitted. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

The parameter is configurable when the [Next Hop Interface Name](#) parameter is not configured.

Next Hop Interface Name

(nhIntfName)

The Next Hop Interface Name parameter specifies the administrative name of the next hop interface. The value must be unique within the VR. The range is 0 to 32 characters.

The parameter is configurable when the [Next Hop Interface Address](#) parameter is not configured.

Number of Loopback Sent

(mepTransmitLbmMessages)

The Number of Loopback Sent parameter specifies the number of loopback messages to transmit. The range is 1 to 1024. The default is 1.

Number of Test Iterations

(testIterations)

The Number of Test Iterations parameter specifies the number of iterations for the CPE test. The range is 1 to 5. The default is 1.

Number of Test Probes

(packetsToSend)

The Number of Test Probes parameter specifies the number of OAM probes to send. Table 116-8 describes the range and default values for each OAM test type.

Table 116-8 Number of test packets parameter

Test type	Range	Default
ICMP Trace, LSP Trace, LSP Ping, LDP Tree Trace	1 to 100	3
P2MP LSP Trace	1 to 10	10
ICMP or VCCV Ping	1 to 100000	5
MEF MAC Ping	2 to 15	2

Packet Size (octets)

(packetSize)

The Packet Size (octets) parameter specifies the size, in octets, of the message in an OmniSwitch OAM trace diagnostic. Table 116-9 lists the ranges and defaults, which depend on the test type and Target Type value.

Table 116-9 Packet Size (octets) parameter

Test type	Range	Default
LSP ping	98 to 9198, if Target Type is set to LSP or LSP path	98
	84 to 9198, if Target Type is set to Any LSP	84
LSP trace	108 to 9198	108
P2MP LSP ping	97 to 9198	1200
P2MP LSP trace	128 to 9198	128

Path ID

(sdpBindingPathId)

The Path ID parameter specifies the spoke SDP binding of the VLL service that the OAM diagnostic is to test. Click on the Select button to choose an SDP binding. There is no default.

Port ID

(sapPortId)

The Port ID parameter specifies the interface that is to send a MAC populate request. Click on the Select button to choose an access interface.

Positional Data Pattern

(positionalPattern)

The Positional Data Pattern parameter specifies the repeated pattern that is inserted in the data field of an ICMP ping. The options are:

- disabled (default—a value of –1 is sent to the device)
- enabled

When you enable the parameter, a data pattern is inserted into each ICMP ping packet.

Priority

(mepOneWayDelayPriority)

The Priority parameter specifies the one-way delay priority. The range is 0 to 7. The default is 0.

Priority

(mepTwoWayDelayPriority)

The Priority parameter specifies the two-way delay priority. The range is 0 to 7. The default is 0.

Priority

(mepSingleEndedLossPriority)

The Priority parameter specifies the priority of LMM frames in a single-ended loss test. The range is 0 to 7. The default is 0.

Probe Failure Threshold

(packetFailureThreshold)

The Probe Failure Threshold parameter specifies the number of times a probe can fail before the test fails. The parameter has no effect if the value is higher than the [Number of Test Probes](#) parameter value. The range is 0 to 15. The default is 1.

Probe History Size (rows)

(maxHistoryRows)

The Probe History Size (rows) parameter specifies the number of OAM history rows that are stored in the managed device probe results table. The range is 1 to 99 000 000. The default is 50. When the value is exceeded, the device removes the oldest entry in the table to allow for a new history row.

Probe Interval (seconds)

(packetInterval)

The Probe Interval (seconds) parameter specifies how often, in s, to send a probe. The range is 1 to 10. The default is 1.

Probe Timeout (seconds)

(packetTimeout)

The Probe Timeout (seconds) parameter specifies how soon, in s, a message request times out and is aborted. The message request depends on receiving a message reply from the target. The parameter value must be less than the [Probe Interval \(seconds\)](#) value. Table 116-10 describes the parameter options.

Table 116-10 Probe Timeout (seconds) parameter

For	Range	Default
LSP ping, LSP trace, LDP tree trace	1 to 3	1
ATM ping, MTU ping, VPRN ping, Tunnel ping, MAC trace, VPRN trace, MAC ping, ICMP trace, VCCV ping	1 to 10	1
ICMP ping, DNS ping	1 to 10	5
MEF MAC ping	1 to 60	1
VCCV trace	1 to 60	3
P2MP LSP ping	1 to 10	5
P2MP LSP trace	1 to 60	1

Rapid

(rapid)

The Rapid parameter specifies whether to send ICMP ping probes in rapid sequence, as part of one group of ping probes. The options are:

- disabled (default)
- enabled

When you enable the parameter, the [Probe Interval \(seconds\)](#) parameter is measured in tens of ms.

Reply Control

(replyControl)

The Reply Control parameter specifies whether the OAM response arrives on the control plane. The options are:

- Enabled
- Disabled (default)

Reply Type

(replyType)

The Reply Type parameter specifies the method of reply expected from the far-end device after a VCCV ping request. Table 116-11 describes the parameter options.

Table 116-11 Reply Type parameter

Option	Option description
IP	Specifies that the reply is sent out-of-band using IPv4.
Control Channel (default)	Specifies that the reply is sent in-band using the VCCV control channel

Reply Via Control Plane

(replyViaControlPlane)

The Reply Via Control Plane parameter specifies whether the OAM response arrives on the control plane. The options are:

- Enabled
- Disabled (default)

Response Address

(responseIpAddr)

The Response Address parameter specifies the response IP address for the multicast trace OAM diagnostic. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Retry Counter

(retryCount)

The Retry Counter parameter specifies the number of consecutive timeouts allowed before a path probe is considered failed. The range is 1 to 255. The default is 3.

Return LSP

(returnLsp)

The Return LSP parameter specifies the name of the LSP to use for sending an LSP ping response. The name must be unique in the VR. The range is 0 to 32 characters. There is no default.

Return Tunnel

(returnTunnel)

The Return Tunnel parameter specifies the unique ID of the return service tunnel for a tunnel ping. The range is 0 to 17 407. The default is 0, which means that the parameter is not configured.

Select All S2L Paths

(allS2l)

The Select All S2L Paths parameter specifies whether or not all the S2L paths will be pinged. The options are:

- Enabled (default)
- Disabled

When this parameter is disabled, you can select a specific S2L path to ping.

Send Via Control Plane

(sendViaControlPlane)

The Send Via Control Plane parameter specifies whether the OAM request is sent on the control plane. The options are:

- Enabled
- Disabled (default)

Service Name

(serviceName)

The Service Name parameter specifies the name of a VPLS to test. Click on the Select button to choose a VPLS.

Site ID

(siteId)

The Site ID parameter specifies the IP address of a network object that is to participate in a test. Click on the Select button to choose an IP address from a list. Table [116-12](#) lists the types of object IP addresses that are listed for each test type.

Table 116-12 Site ID parameter

Test type	Object IP addresses listed
LSP Ping LSP Trace LDP Tree Trace	MPLS path
Multicast Router Information	VP RN PIM site or core routing PIM site
Multicast Trace	VP RN or core routing PIM site Multicast group
MEP	MEP

Size (octets)

(packetSize)

The Size (octets) parameter specifies the OAM packet size, in octets, of the probe for a trace diagnostic. Table 116-13 lists the range and default for each diagnostic type.

Table 116-13 Size (octets) parameter

Test type	Range	Default
VP RN ping MAC ping	1 to 65 535	40
VP RN trace	80 to 9198	128
MTU ping Tunnel ping Multicast FIB ping	40 to 9198	40
LSP ping LSP trace	84 to 9198	98
P2MP LSP ping P2MP LSP trace	97 to 9198	1200
VCCV ping VCCV trace	88, or 93 to 9198	88
ICMP Ping	0 to 16 384	56
MEF MAC ping	64 to 1468	64

Source Address

(srcAddr)

The Source Address parameter specifies the unicast IP address of a multicast-capable source at the start of the traceable route. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Source IP Address

(sourceIpAddress)

The Source IP Address parameter specifies the source IP address for an OAM diagnostic. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

For a CPE ping, the source IP address must be in the same subnet as the destination IP address.

Source MAC Address

(sourceMacAddress)

The Source MAC Address parameter specifies the source MAC address in the format *xx-xx-xx-xx-xx-xx*. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The default is FF-FF-FF-FF-FF-FF or 00-00-00-00-00-00, depending on the diagnostic.

Source Site ID

The Source Site ID parameter specifies the IP address of the service tunnel origin. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Strategy

(generationStrategy)

The Strategy parameter specifies the approach used to run the generated OAM tests on VLL services. It is only configurable when the [Entity Type](#) parameter is set to VLL Service.

The options are:

- All (default)
- End to End

Using a VCCV ping test as an example, the two different strategies for test generation mean the following:

- All: the test will generate all the single segment VCCV pings for all spoke SDP bindings in the VLL service
- End To End: the test will create end-to-end multiple segment VCCV pings for all VLL paths in the service

Subscriber Ident String

(subscriberIdent)

The Subscriber Ident String parameter specifies a subscriber identification string that the device uses to identify the circuit of the access node. The range is 0 to 32 characters. There is no default.

System ID (Loopback Ip Address)

(systemAddress)

The System ID (Loopback Ip Address) parameter specifies the system ID of the originating device. Specify an IP address in dotted-decimal format. The default is 0.0.0.0, which means that the parameter is not configured. Click on the Select button to choose a site.

Target IP Address

(targetIpAddress)

The Target IP Address parameter specifies the target IP address for an OAM diagnostic. Specify an IPv4 address in dotted-decimal format, or an IPv6 address in colon-hexadecimal format, or a DNS name. The default is 0.0.0.0, which means that the parameter is not configured.

Target MAC

(mepTransmitLtmTargetMacAddress)

The Target MAC parameter specifies the MAC address of a MEP. Specify a MAC address in the format *xx-xx-xx-xx-xx-xx*.

Target MAC Address

(targetMacAddress)

The Target MAC Address parameter specifies the MAC address of the target device in the format *xx-xx-xx-xx-xx-xx*. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. There is no default.

When you configure an MEF MAC ping, the parameter specifies the base shelf MAC address of a Release 3.0 7250 SAS-ES or 7250 SAS-ESA.

Target Type

Table 116-14 lists where to find information about the Target Type parameter.

Table 116-14 Target Type parameter

Parameter	See
Target Type for diagnostic test other than ANCP loopback	Target Type parameter in this section
Target Type for ANCP loopback diagnostic test	Target Type parameter in this section

Target Type

(targetType)

The Target Type parameter specifies the type of reference for ANCP loopback diagnostic. The options are:

- ANCP String
- Subscriber Ident String (default)

Target Type

(testTargetType)

The Target Type parameter specifies the type of object against which the OAM diagnostic is performed. Table 116-15 lists the parameter options.

Table 116-15 Target Type parameter

For	Options
MAC purge MAC trace MAC populate MAC ping MEF MAC Ping	VLL Site VPLS Site (default) 7250 SAS-ES and 7250 SAS-ESA 3.0 VPLS Site
LSP ping LSP trace	LSP (default) LSP Path Any LSP
Multicast router information Multicast trace	Core Routing PIM Site (default) VPRN PIM Site
ICMP ping	Core Routing Site (default) VPRN Site EPS Site EPS Path
ICMP trace	Core Routing Site (default) VPRN Site EPS Site EPS Path

Test Failure Threshold

(testFailureThreshold)

The Test Failure Threshold parameter specifies the number of test failures that occur before an NE sends a trap about the test failure. The range is 0 to 15. The default is 1.

Test Iteration Duration

(testDuration)

The Test Iteration Duration parameter specifies the duration of the test for which the traffic generator is active, in seconds. The range is 5 to 3600. The default is 5.

Threshold Reporting State

(thresholdReportingState)

The Threshold Reporting State parameter specifies whether to generate threshold alarms when the number of log entries exceeds the Max Log Records parameter value. The options are:

- Up (default)
- Down

Threshold Value

(thresholdValue)

The Threshold Value parameter specifies the value to monitor to determine whether a threshold-crossing alarm should be raised or cleared, based on the rising or dropping count. The range is 0 to 2 147 483 647. The default is 0.



Note — To provide meaningful test results, the tested devices must use a common timing source, for example, NTP.

Time To Live

(timeToLive)

The Time To Live parameter specifies the TTL value, in hops, that is added to the test packet to ensure that the packet does not circulate in a routing loop past the configured time. Table 116-16 lists the range and default for each diagnostic type.

Table 116-16 Time To Live parameter

Object	Range	Default
ICMP ping	1 to 128	64
MAC ping multicast FIB ping VPRN ping VPRN trace	1 to 255	5
P2MP ping	1 to 255	255
P2MP trace	1 to 255	Initial TTL default = 1 Maximum TTL default = 30

Time To Wait (milliseconds)

(waitMilliSec)

The Time to Wait (milliseconds) parameter specifies how long, in ms, the ICMP trace waits for a response before sending the next probe packet. The range is 10 to 60000. The default is 10.

Timeout

Table 116-17 lists where to find more information about the Timeout parameter.

Table 116-17 Timeout parameter

Parameter	See
Timeout for message responses	Timeout (seconds) parameter in this section
Timeout for an OS 6850, or OS 6850E ping test	Timeout parameter in this section.
Timeout for ANCP loopback diagnostic	Timeout (seconds) parameter in this section
Timeout for an LSP trace request during tree discovery	Timeout (seconds) parameter in this section

Timeout (seconds)

The Timeout (seconds) parameter specifies the time, in s, to wait for a message response. All reply messages that arrive after the specified time are silently discarded. The range is 1 to 100. The default is 5.

Timeout

(seconds)

The Timeout (seconds) parameter specifies the time, in s, that the OS 6850, or OS 6850E ping waits for a response before timing out. The range is 1 to 10 000. The default is 5.

Timeout (seconds)

(timeOut)

The Timeout (seconds) parameter specifies the timeout value, in s, for an LSP trace request during tree discovery. The range is 1 to 60. The default is 30.

Timeout (seconds)

(timeout)

The Timeout (seconds) parameter specifies the time, in s, that the device waits for a result from the ANCP loopback diagnostic. The range is 0 to 255. The default is 0.

Trap Generation

(trapGenerationPolicy)

The Trap Generation parameter specifies the conditions under which a device sends a trap during an OAM test. You can select multiple options. Not all options are available for every type of test. The options are:

- Test Completion (default)
- Test Failure
- Probe Failure
- Path Change

When the [Lightweight Execution](#) parameter is enabled, all of the options are selected and the parameter is not configurable.

TTL

(ltrTtl)

The TTL parameter specifies the number of hops remaining in the Link Trace Message. As each Link Trace Responder handles the message, the value decreases by 1. The value returned in a Link Trace Responder is 1 less than the value that is received in the associated Link Trace Message. When the value is 0 or 1, the Link Trace Message is not forwarded to the next hop. The range is 0 to 255. The default is 64.

Type

(type)

The Type parameter specifies which type of threshold crossing event generates an alarm. The options are:

- | | |
|----------------------------|---------------------|
| • Inbound Jitter (default) | • Roundtrip Loss |
| • Outbound Jitter | • Inbound Latency |
| • Roundtrip Jitter | • Outbound Latency |
| • Inbound Loss | • Roundtrip Latency |
| • Outbound Loss | |



Note — To provide meaningful test results, the tested devices must use a common timing source, for example, NTP.

Unlimited Concurrent Pings

(unlimitedMaxPings)

The Unlimited Concurrent Pings parameter specifies whether to allow an unlimited number of simultaneous pings on the managed devices. The options are:

- enabled (default)
- disabled

Use the check box to change the parameter.

Unlimited Concurrent Traces

(unlimitedMaxTraces)

The Unlimited Concurrent Traces parameter specifies whether to allow an unlimited number of simultaneous traces on the managed devices. The options are:

- enabled (default)
- disabled

Use the check box to change the parameter.

Update Test Result Status

(updateResultStatus)

The Update Test Result Status parameter specifies whether the Threshold Crossing Event should change the test result status. The options are:

- enabled
- disabled (default)

Use Local Tunnel

(useLocalTunnel)

The Use Local Tunnel parameter specifies that the ping request message is sent using the same service tunnel encapsulation labeling as service traffic. Table [116-18](#) describes the parameter options.

Table 116-18 Use Local Tunnel parameter

Option	Option description
Enabled (default)	Specifies that the ping request message is sent from the local device using the same labeling for service tunnel encapsulation as for service traffic. The ping attempts to use an egress SDP (service tunnel) ID bound to the service, with the specified far-end IP address, with the VC label for the service.
Disabled	Specifies that the ping request message is sent with GRE with the OAM label from the local device.

Use Remote Tunnel

(useRemoteTunnel)

The Use Remote Tunnel parameter specifies which path mechanism the far end uses for an OAM ping diagnostic. Table 116-19 describes the parameter options.

Table 116-19 Use Remote Tunnel parameter

Option	Option description
Enabled (default)	Specifies that the ping response message from the remote device attempts to use an egress SDP (service tunnel) ID bound to the service, with the message originator as the destination IP address, with the VC label for the service
Disabled	Specifies that the ping request message is sent with GRE with the OAM label from the remote device

Using EPS Path

(originatingEpsPath)

The Using EPS Path parameter specifies if the selected EPS path is single-sided or double-sided. A single-sided EPS path has one side managed by the 5620 SAM. A double-sided EPS path has both sides managed by the 5620 SAM.

Validation Test Suite

(sasValidator)

The Validation Test Suite parameter specifies whether the test suite is used to validate the operational status of the tested service or service tunnel. The validation test results are displayed using the operational state cause flags of the associated service or service tunnel. You can configure the parameter when the [Entity Type](#) parameter is set to VPLS, VLL, VPRN, or Tunnel. The options are:

- Enabled
- Disabled (default)

VC's Label Time Live

(vcLabelTtl)

The VC's Label Time Live parameter specifies the TTL value that is added to the test packet, to ensure that the packet does not circulate in a routing loop past the configured time. The range is 1 to 255. The default is 255 for CPE pings. When the parameter is set to 1, the CPE ping is done on the local SAP.

Virtual Router ID

(vRtrID)

The Virtual Router ID parameter specifies a number used to identify a virtual router instance. The range is 1 to 4096. The default is 1.

VC Type

See the [VC Type](#) parameter in section 36.1.

VLAN ID

(vlanId)

The VLAN ID parameter specifies the identification number of the VLAN. The range is 0 to 4094. The default is 0.

VLAN Priority

(mepTransmitLbmVlanPriority)

The VLAN Priority parameter specifies the priority of the VLAN. The range is 0 to 7. The default is 0.

VLAN VC Tag

See the [VLAN VC Tag](#) parameter in section 36.1.

117 –Ethernet CFM parameters

117.1 Ethernet CFM parameters 117-2

117.1 Ethernet CFM parameters

This chapter describes the parameters on the Manage Maintenance Domain Policies form and child forms.

AIS Enabled

(aisEnable)

The AIS Enabled parameter specifies whether AIS frames are generated by the MEG. The options are:

- disabled (default)
- enabled

AIS Interval (seconds)

(aisInterval)

The AIS Interval (seconds) parameter specifies how often, in s, AIS frames are transmitted. The range is 1 to 60. The default is 1.

AIS Meg Level

(aisMegLevel)

The AIS Meg Level parameter specifies the MEG levels that are to suppress alarms when the MEP detects a defect condition. The options are:

- Level 1
- Level 2
- Level 3
- Level 4
- Level 5
- Level 6
- Level 7

There is no default.

AIS Priority

(aisPriority)

The AIS Priority parameter specifies the assigned priority to transmitted AIS frames. The range is 0 to 7. The default is 7.

Auto-Assign ID

See [Auto-Assign ID](#) in section 134.1 for the parameter description.

Auto MEG Site Creation

(autoMegSite)

The Auto MEG Site Creation parameter specifies whether MEG sites are generated for the service. The options are:

- enabled (default)
- disabled

CCM interval

(ccmInterval)

The CCM Interval parameter specifies, in s or ms, how often continuity messaging is performed on the MEP or MEG. The options are:

- 10 ms
- 100 ms
- 1 s
- 10 s (default)
- 60 s
- 600 s



Note — The 7705 SAR supports only the following options:

- 10 ms
- 100 ms

CCM Messages Enabled

(ccEnable)

The CCM Messages Enabled parameter specifies whether to perform continuity messaging on the MEP. The options are:

- Enabled
- Disabled (default)

CFM Hold Down Timer (centiseconds)

(cfmHoldDownTimer)

The CFM Hold Down Timer (centiseconds) parameter specifies the time, in centiseconds, that a MEP in the association will delay in declaring a fault. This parameter can only be set when the [CCM interval](#) parameter is set to either 10 ms or 100 ms. The range is 0 to 1000. The default is 0.

Data Size (octets)

(twDataSize)

The Data Size (octets) parameter specifies the data size, in bytes, contained in the padding TLV for the two-way Synthetic Loss Measurement (SLM) test. A value of zero (0) specifies that no padding TLV is inserted in the SLM packet. Any non-zero value will increase the packet size by the specified data size plus 3 bytes for the TLV header. The range is 0 to 1500. The default is 0.

Description

See [Description](#) in section 112.1 for the parameter description.

Direction

(direction)

The Direction parameter specifies the direction of the MEP. The options are:

- Up
- Down (default)

When the direction is Up, the MEP sends CCM packets into the NE. When the direction is Down, the MEP sends CCM packets away from the NE.



Note 1 – The parameter is not configurable on the 7705 SAR.

Note 2 – Only the Down option is configurable on the 7210 SAS nodes.

Direction

(mepDirectionAccessInterface)

The Direction parameter specifies the direction of the automatically created MEPs when the [MEP\(s\) Creation on Access Interfaces](#) parameter is enabled. The options are:

- up (default)
- down

When the direction is up, the packets are sent toward the managed device. When the direction is down, the packets are sent to the CE device.



Note 1 – The 7705 SAR does not support the parameter.

Note 2 – The ‘down’ option is applicable only to the 7210 SAS-M uplink node.

Direction

(mepDirectionSdpBindings)

The Direction parameter specifies the direction of the automatically created MEPs when the [MEP\(s\) Creation on SDP Bindings](#) parameter is enabled. The options are:

- up (default)
- down

When the direction is up, the packets are sent toward the managed device. When the direction is down, the packets are sent to the CE device.



Note — The 7705 SAR does not support the parameter,

Eth Test Enabled

(ethTestEnable)

The Eth Test Enabled parameter specifies whether ETH Test frames are generated by the MEG. The options are:

- disabled (default)
- enabled

Eth Test Pattern

(ethTestPattern)

The Eth Test Pattern parameter specifies the data content of the AIS test frames. The options are:

- AllZerosNoCrc (default)
- AllZerosCrc
- AllOnesNoCrc
- AllOnesCrc

Eth Test Threshold (number of bit errors)

(ethTestThreshold)

The Eth Test Threshold (number of bit errors) parameter specifies the number of bit errors after which to send an Eth Test completion notification. The range is 0 to 11 840. The default is 0, which means that a notification is sent after the completion of each test on the MEP.

Facility Fault Notify

(fcltyFaultNotify)

The Facility Fault Notify parameter specifies whether or not a fault detected on the facility MEP will notify the associated SAP MEPs and facility MEPs. This parameter is configurable only on port facility MEPs and LAG facility MEPs. The options are:

- Enabled
- Disabled

Facility VLAN ID

(**facilityVlanId**)

The Facility VLAN ID specifies whether the MEP is a LAG MEP or a tunnel MEP. If the value is set to 0, the MEP is considered a LAG MEP. If VLAN ID has a value other than 0, the MEP is considered a tunnel MEP. In this instance, a logical tunnel is created and the tunnel MEP is associated with a service SAP, where the Outer Encap Value of the SAP is the same value as the VLAN ID.

Fault Alarm Time (centiseconds)

(**mepFngAlarmTime**)

The Fault Alarm Time (centiseconds) parameter specifies the time, in centiseconds, that a defect is present before an alarm is raised. The parameter is configurable only on an OmniSwitch. The range is 250 to 1000, in increments of 10. The default is 250.

Fault Propagation

(**faultPropagation**)

The Fault Propagation parameter specifies the action to be taken by a MEP if a fault is detected by the related service. Table 117-1 describes the parameter options.

Table 117-1 Fault Propagation parameter

Option	Option description
Disabled (default)	Specifies that no additional fault propagation will occur
useIfStatusTLV	Specifies that the MEP will send an interface status TLV in the next CCM indicating fault
suspendCCM	Specifies that the MEP will stop regular CCM transmission entirely until the fault is cleared

Fault Reset Time (centiseconds)

(**mepFngResetTime**)

The Fault Reset Time (centiseconds) parameter specifies the time, in centiseconds, that a defect is absent before an alarm is cleared. The parameter is configurable only on an OmniSwitch. The range is 250 to 1000, in increments of 10. The default is 1000.

ID

(id)

The ID parameter specifies the numeric identifier of the MEP. The range is 1 to 8191. The default is 0, which means that the parameter is not configured.

Id-Permission

(mhfIdPermission)

The Id-Permission parameter, which is configurable only for OmniSwitch NEs, specifies what is to be included in the Sender ID TLV (21.5.3) transmitted by MPs in the MD. The options are:

- defer (default)
- chassis
- chassisManage
- manage
- none

Initial CCM Interval

(ccmInterval)

The Initial CCM Interval parameter specifies, in s or ms, how often continuity messaging is performed on the MEP or MEG. The options are:

- 10 ms
- 100 ms
- 1 s
- 10 s (default)
- 60 s
- 600 s



Note – The 7705 SAR supports only the following options:

- 10 ms
- 100 ms

Initial CFM Hold Down Timer (centiseconds)

(cfmHoldDownTimer)

The Initial CFM Hold Down Timer (centiseconds) parameter specifies the time, in centiseconds, that a MEP in the association will delay in declaring a fault. This parameter can only be set when the [Initial CCM Interval](#) parameter is set to either 10 ms or 100 ms. The range is 0 to 1000. The default is 0.

Initial MHF-Creation

(mhfCreation)

The Initial MHF-Creation parameter specifies how the initial MFG creation is performed. The options are:

- none (default)
- default
- explicit

Interface Type

(sapOrBinding)

The Interface Type parameter specifies the type of object that the regular MEP is associated with. The options are:

- SAP (default)
- SdpBinding
- Ethernet Tunnel Path Endpoint
- Ethernet Ring Path Endpoint
- Network Interface
- Port
- LAG

Interval (seconds)

(twInterval)

The Interval (seconds) parameter specifies the delay, in seconds, between Synthetic Loss Measurement (SLM) messages for the two-way SLM test. The range is 1 to 10. The default is 5.

Level

(maintDomainLevel)

The Level parameter specifies the level for the MD. The range is 0 to 7. The default is 0.

Low-priority Defect

(mepLowestPrDefect)

The Low-priority Defect parameter specifies the level at which an alarm is raised by the MEP. The options are:

- allDef
- macRemErrXcon
- remErrXcon (default)
- errXcon

- xon
- noXon

Mac Address

(macAddress)

The Mac Address parameter specifies the configured MAC Address for the MEP. Specify a MAC address in the form *nn-nn-nn-nn-nn-nn*. The default is 00-00-00-00-00-00, which means that the parameter is not configured.

MC-LAG Prop Hold Time

mcLagPropHoldTime

The MC-LAG Prop Hold Time parameter specifies the configuration delay between redundant MC-LAGs when they switch between the standby and active state. When the timer is activated, fault changes are not propagated to the MC-LAG SAP CFM MEPs.

If the parameter is set to zero, delays in response to a port or protocol change are ignored. The range is 0 to 60. The default is 1s.



Note — The [MC-LAG Standby Inactive](#) must be enabled to configure Ethernet CFM redundancy.

MC-LAG Standby Inactive

mcLagStdbyInactive

The MC-LAG Standby Inactive parameter specifies whether Ethernet CFM MEPs configured on an MC-LAG port monitor the active or standby redundancy states of the MC-LAG port. When the parameter is enabled, MEPs configured on an MC-LAG standby port are in standby status, whereas MEPs configured on an MC-LAG active port are operational. When the parameter is disabled, MEPs configured on an MC-LAG port operate regardless of the MC-LAG port state. The options are:

- Enabled
- Disabled (default)



Note — The [MC-LAG Prop Hold Time](#) must be configured to configure Ethernet CFM redundancy.

MD Mgr Object ID

(maintDomainId)

The MD Mgr Object ID parameter specifies a unique MD ID. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 4 294 967 295. There is no default.

MEP ID

(id)

The MEP ID parameter specifies the identification number given to the unmanaged remote MEP. The range is 0 to 8191. The default is 0.

MEP Mac Address

(macAddress)

The MEP Mac Address parameter specifies the MAC address of the remote MEP. Specify a MAC address in the form *nn-nn-nn-nn-nn-nn*. There is no default.

MEP(s) Creation on Access Interfaces

(autoMepCreationAccessInterface)

The MEP(s) Creation on Access Interfaces parameter specifies whether a MEP is created on each access interface in the service. The options are:

- Enabled (default)
- Disabled

MEP(s) Creation on SDP Bindings

(autoMepCreationSdpBindings)

The MEP(s) Creation on SDP Bindings parameter specifies whether a MEP is created on each SDP binding in the service. The options are:

- Enabled
- Disabled (default)

MHF-Creation

(mhfCreation)

The MHF-Creation parameter specifies how the MHFs are created, which depends on the device type. Table [117-2](#) lists and describes the parameter options for each device type.

Table 117-2 MHF-Creation parameter

Option	Non-OmniSwitch description	OmniSwitch description
None (default)	No MHFs can be created.	No MHFs can be created

(1 of 2)

Option	Non-OmniSwitch description	OmniSwitch description
Explicit	Specifies whether MEPs in a specific MD level are recognized as MIPs on other MD levels. For example, if a set of MEPs are configured on MD1 and the parameter is set to explicit, when a CFM test is run on MD2, the MEPs from MD1 are included in the test and are recognized as MIPs. Not supported on the 7705 SAR.	MHFs can be created for the specified VLAN ID only on bridge ports through which this VLAN can pass and only if a MEP is created at a lower MA level.
Default	MHFs can be created.	MHFs can be created on the specified VLAN on any bridge port through which this VLAN can pass.

(2 of 2)

MIP(s) Creation on Access Interfaces

(autoMipCreationAccessInterface)

The MIP(s) Creation on Access Interfaces parameter specifies whether a MIP is created on each access interface in the service. The options are:

- Enabled (default)
- Disabled

MIP(s) Creation on SDP Bindings

(autoMipCreationSdpBindings)

The MIP(s) Creation on SDP Bindings parameter specifies whether a MIP is created on each SDP binding in the service. The options are:

- Enabled
- Disabled (default)

Name

See [Name](#) in section 112.1 for the parameter description.

Name

(maintAssocName)

The Name parameter specifies a name for the MEG. The range is 0 to 45 characters. There is no default.

Name Format

(maintAssocNameType)

The Name Format parameter specifies the MEG address type. The options are:

- vid
- string (default)
- integer
- vpn-id
- icc-based



Note 1 – If you select icc-based as the Name Format, then the associated [Name](#) value must be exactly 13 characters long.

Note 2 – The MEG name type supports Y1731 meps and tests.

Name Type

(maintDomainNameType)

The Name Type parameter specifies the name type of the MD, and defines the type of entry that the [Name](#) parameter accepts. The options are:

- string (default)
- dns
- mac
- none



Note – The 'none' option is applicable to the 7210 SAS-M uplink and the 7210 SAS-D node.

Object ID

(id)

The Object ID parameter specifies the ID of the CC Test ethernet test object. The range is 1 to 2 147 483 647. The default is 0, which means that the parameter will be automatically assigned.

One-way-delay Test Threshold (seconds)

(owdtThreshold)

The One-way-delay Test Threshold (seconds) parameter specifies how often, in s, a notification is sent during a MEP one-way delay test. The range is 0 to 600. The default is 0, which means that a notification is sent on the completion of each one-way delay test.

Originating MEP

(originatingMep)

The Originating MEP parameter specifies which MEP is the test origin. The range is 1 to 8191. The default is 1.

Priority

(twPriority)

The Priority parameter specifies the priority used in the generated test frame for the two-way Synthetic Loss Measurement (SLM) test. The range is 0 to 7. The default is 0.

Priority Level for CCM Messages

(ccmLtmPriority)

The Priority Level for CCM Messages parameter specifies the CCM interval for the MEP. The range is 0 to 7. The default is 7.

Run Continuity Check Protocol

(runCCOnSelection)

The Run Continuity Check Protocol parameter specifies whether or not to create Maintenance Associations and local and remote MEPs. Any existing Remote MEPs that do not match the local MEPs are deleted. MEPs are turned up and CCM Messages are enabled. The options are:

- Enabled (default)
- Disabled

Send Count (packets)

(twSendCount)

The Send Count (packets) parameter specifies the number of Synthetic Loss Measurement (SLM) packets to send during the two-way SLM test. The range is 1 to 100. The default is 1.

Service ID

(serviceId)

The Service ID parameter specifies a unique service ID. The range is 0 to 2 147 483 647. The default is 0, which means that the parameter is not configured.

Set Control MEP property on created MEPs

(setControlMep)

The Set Control MEP property on created MEPs parameter specifies whether or not to set up a Control MEP on the MEPs that are created on the specified ethernet path. The options are:

- Enabled (default)
- Disabled

Timeout (seconds)

(twTimeout)

The Timeout (seconds) parameter specifies the timeout value, in seconds, to wait for a Synthetic Loss Measurement (SLM) message to reply for the two-way SLM test. Upon expiration of the timeout period, the agent assumes that the message response will not be received. Any response received after the timeout period has expired is discarded. The range is 1 to 10. The default is 5.

Type

(type)

The Type parameter specifies the MEP type. Table 117-3 lists the parameter options.

Table 117-3 Type parameter

Option	Description
Regular (default)	The MEP is associated with a SAP or an SDP binding.
Virtual	The MEP is associated with a B-VPLS.

Virtual MEP(s) Creation on B-Sites

(autoVirtualMepCreation)

The Virtual MEP Creation on B-sites parameter specifies whether the MEPs on the service B-sites are enabled. The options are:

- Enabled
- Disabled

VLAN ID

(vlanId)

The VLAN ID parameter specifies the identification number of the VLAN. The range is 0 to 4094. The default is 0.

118 –Scripts parameters

118.1 Scripts parameters 118-2

118.1 Scripts parameters

This chapter describes the parameters on the Script Manager form and child forms.

Answer

The Answer parameter specifies the answer to a command sent by the system in response to a question intervention tag.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [134.1](#).

Comment

(comment)

The Comment parameter is an optional parameter that specifies additional information about the version of the script and the NE associated with the script.

Content Type

(contentType)

The Content Type parameter specifies the types of commands that appear in the contents the CLI script. Table [118-1](#) describes the parameter options.

Table 118-1 Content Type parameter options

Option	Description	Dependencies
CLI (default)	The script version contains CLI substitution	—
Velocity	The script version contains Velocity engine support	—

Continue On Command Failure

(continueOnCommandFailure)

The Continue On Command Failure parameter specifies whether the script continues to execute in its entirety if an error occurs. The options are:

- Enabled
- Disabled (default)

Default Value

The Default Value parameter specifies the default value that is associated with the parameter tag or intervention tag in the CLI script. The range is 0 to 255 characters. The characters ' () ? / are not allowed.

Description

(description)

The Description parameter specifies a description for the created script. The range is 0 to 255 characters.

Label

The Label parameter specifies the CLI script parameter tag in a CLI script. The range is 1 to 255 characters. Only alphanumeric characters, underscores, and dashes are allowed.

Mode

(scriptMode)

The Mode parameter specifies the state of the script. When in Released mode, any attempt to edit the script causes the script to automatically enter Draft mode. When in Draft mode, only one version of the script can be edited. This version is replaced with every save and can only be executed by users with edit permissions. The options are:

- Draft (default)
- Released

Name

(scriptName)

The Name parameter specifies a name for the script. The range is 1 to 255 characters.

Network Element Version Information

(neVersionInformation)

The Network Element Version Information parameter is an optional parameter that specifies additional information about the NE version that is associated with the script.

Question

The Question parameter specifies a question that is expected in response to a command in a script. The system responds to the question with the answer specified by the [Answer](#) parameter.

Reserve Targets

The Reserve Targets parameter specifies whether the script instances or targets that the current 5620 SAM user creates are locked by the user. When a script is locked by a user and the user associates a target or an instance with the script, no other user can subsequently execute, modify, or delete the instance or target. Another user can, however, create a new instance or target, or copy an existing instance or target, and then execute, modify, or delete it, as required. The options are:

- disabled (default)
- enabled

Script ID

(id)

The Script ID parameter specifies a unique numeric identifier for the created script. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 65 535. The default is 0.

State

(state)

The State parameter specifies whether the script can be executed against the configured targets. The options are:

- Enabled (default)
- Disabled

Type

The Type parameter specifies the category of the script. The range is 0 to 255 characters.

Use Latest Version

(useLatestVersion)

The Use Latest Version parameter specifies whether the latest version of the script is executed on the targets that are associated to a script instance. Select the check box to enable this parameter. The options are:

- Enabled
- Disabled (default)

Version Number

(mtosi_version)

The Version Number parameter specifies the version of the script that is added to the instance.

119 –Auto-Provision Profiles parameters

119.1 Auto-Provision Profiles parameters 119-2

119.1 Auto-Provision Profiles parameters

This chapter describes the parameters used for Auto- provision.

Adjacent NE Managed

(adjacentNeManaged)

The Adjacent NE Managed parameter specifies whether the adjacent device is managed by the 5620 SAM. When the adjacent device is managed by the 5620 SAM, the IP address of the device is automatically populated. When the adjacent device is not managed by the 5620 SAM, the IP address must be configured. The options are:.

- enabled (default)
- disabled

Adjacent Site ID

(adjacentNeSiteId)

The Adjacent Site ID parameter specifies the IP address of the node that is adjacent to the device that is targeted for auto-provision. This device can be any device in a network. The default IP address is 0.0.0.0.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [112.1](#).

Description

(mtosi_description)

The Description parameter specifies a description of the script. The range is 1 to 252 characters.

Name

(scriptName)

The Name parameter specifies the name of the script. The range is 1 to 252 characters.

Name

The Name parameter specifies the site name of the managed NE that is selected as the adjacent device.

Network Element Type

The Network Element Type parameter specifies the type of NE that supports auto provisioning.

Network Element Version Information

The Network Element Version Information parameter specifies the version of the NE that supports auto provisioning.

Script ID

(mtosi_id)

The Script ID parameter specifies the unique ID of the script. The range is 1 to 65 535. The default is 0.

Type

(mtosi_type)

The Type parameter specifies the category of the script. The range is 0 to 255 characters.

View the newly created Auto-Provisioning

The View the newly created Auto-Provisioning parameter specifies whether you need to view the configuration details of the newly created Auto-Provision. The options are:

- Enabled
- Disabled (default)

120 –Bulk Operations parameters

120.1 Bulk Operations parameters 120-2

120.1 Bulk Operations parameters

This chapter describes the parameters on the bulk operation forms and child forms.

Admin State

The Admin State parameter specifies whether the operation can be executed. The options are:

- Enable
- Disable (default)

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [134.1](#).

Batch ID

The Batch ID parameter displays the system-generated ID of the batch.

Batch Size

The Batch Size parameter specifies the size of each batch. The range is 100 to 5000. The default is 2000.

Batch Status

The Batch Status parameter displays the bulk change status of all of the batch items. The value is not configurable.

If all of the batch items have the same bulk change status, the Batch Status parameter displays that status. If one or more of the batch items has a different bulk change status, the Batch Status parameter displays the Mixed status.

Table [120-1](#) lists the generated statuses and their descriptions.

Table 120-1 Batch Status descriptions

Status	Description
Cancelled	The operation has been manually stopped.
DB Failures	A database error occurred with the batch change.
Deployment Failure ⁽¹⁾	Deployment to the node failed.
Exception	An internal error occurred during the batch execution.
Execution Failures	An error occurred with the operation.
In Progress	The operation is executing.
Mixed	One or more of the batch items has a different bulk change status.

(1 of 2)

Status	Description
No Change	No objects were changed.
Not Applicable	—
Not Executed	The operation has never been executed before.
Not in User Span	Objects were not in the user span.
Object Not Found	The object to modify no longer exists in the 5620 SAM.
Queued	The operation is queued to execute.
Successful	The operation completed successfully.

(2 of 2)

Note

⁽¹⁾ This status does not update automatically if or when the deployment failure clears.

Batch Status Summary

The Batch Status Summary parameter displays the status of all of the batches. The value is not configurable.

If all of the batches have the same batch status, the Batch Status Summary parameter displays that status. If one or more of the batches has a different batch status, the Batch Status Summary parameter displays the Mixed status.

See Table [120-1](#) for a list of generated statuses and their descriptions.

Changed

The Changed parameter displays the number of objects that were modified in the batch. The value is not configurable.

Continue on Failure

The Continue on Failure parameter specifies whether the operation stops if a failure occurs or if the operation continues until the operation is complete regardless of failures. The options are:

- Enabled
- Disabled (default)

Creator

The Creator parameter displays the name of the 5620 SAM user that created the last operation. The value is not configurable.

Description

The Description parameter specifies a description of the operation. The range is 0 to 255 characters. There is no default.

Duration

The Duration parameter specifies how long the last operation took to execute. The value is not configurable.

Execution Status

The Execution Status parameter displays the status of the bulk change operation. The value is not configurable.

Table 120-2 lists the generated statuses and their descriptions.

Table 120-2 Execution Status descriptions

Status	Description
Cancelled	The operation has been manually stopped.
Completed	The operation has been executed.
Generating...	Batch generation is in progress.
Generation Complete	Batch generation is complete.
In Progress	The operation is executing.
No Deployers Available	All available deployers are busy, or the deployment failed.
Not Applicable	—
Not Executed	The operation has never been executed.
Queued	The operation is queued for execution.

Failures

The Failures parameter displays the number of objects in the batch that failed to be changed. The value is not configurable.

Last Total Changed

The Last Total Changed parameter displays the number of objects that were changed by the last executed operation. The value is not configurable.

Name

The Name parameter specifies the name of the bulk change. The range is 1 to 255 characters. The value must be unique for each bulk change.

Not Changed

The Not Changed parameter displays the number of objects in the batch that did not change. The value is not configurable.

Not Found

The Not Found parameter displays the number of objects in the executed batches that could not be changed because they no longer exist in the 5620 SAM. The value is not configurable.

Not in Span

The Not in Span parameter displays the number of objects in the executed batches that could not be changed because they are not in the user span of control. The value is not configurable.

Object Type

The Object Type parameter specifies the object class to which the bulk change applies. Choose an object type using the pull-down list.

Operation ID

The Operation ID parameter specifies a unique numeric identifier for the operation. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 65 535. The default is 0, which means that a value is not specified.

Range

The Range parameter displays the range of objects that are included in the batch. The range is not configurable.

Time Last Started

The Time Last Started parameter specifies the time that the last operation execution started. The value is not configurable.

Time Last Finished

The Time Last Finished parameter specifies the time that the last operation execution finished. The value is not configurable.

121 –Card Migration Event Manager parameters

121.1 Card Migration Event Manager parameters 121-2

121.1 Card Migration Event Manager parameters

This chapter describes the parameters on the Card Migration Event Manager form and child forms.

Additional Information

The Additional Information parameter specifies information about the card migration event. The range is 0 to 4000 characters. There is no default.

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique numeric identifier to the card migration event. The options are:

- Enabled (default)
- Disabled

Auto Reboot

The Auto Reboot parameter specifies whether the 5620 SAM reboots a target NE automatically after the migration tasks on the NE are complete. The parameter is configurable at the card migration event level, which applies to each target NE, and at the target NE level, which applies only to the selected NEs. The options are:

- Enabled
- Disabled (default)

Description

The Description parameter specifies a description for the card migration event. The range is 0 to 80 characters. There is no default.

ID

The ID parameter specifies a unique numeric identifier for the card migration event. The parameter is configurable when the [Auto-Assign ID](#) parameter is set to Disabled.

New Type

The New Type parameter specifies the new IOM or MDA type, depending on which panel contains the parameter, and on the Current Type value in the panel. The parameter options for IOMs are:

- No Change (default)
- 2 x XP MDA IOM 3

Table [121-1](#) lists the parameter options for MDAs. The default is No Change.

Table 121-1 New Type parameter

Current Type	New Type
10 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
5 x 1-Gig Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-Gig Ethernet	4 x 10Gig Extended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance SFP
20 x 100 Ethernet Fx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
20 x 10/100/1000 Ethernet Tx	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
2 x 10-Gig Ethernet XFP	2 x 10Gig Extended Performance XFP 4 x 10Gig Extended Performance XFP
20 x 10/100/1000 Ethernet SFP	20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
1 x 10-gig Ethernet XFP	4 x 10GigExtended Performance XFP 2 x 10Gig Extended Performance XFP 1 x 10Gig Extended Performance XFP
5 x 10/100/1000	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX
10 x 10/100/1000 Ethernet SFP	10 x 1Gig Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance SFP 20 x 10/100/1000 Ethernet Extended Performance TX

122 –MIB Policies parameters

122.1 MIB Policies parameters 122-2

122.1 MIB Policies parameters

This chapter describes the parameters on the Manage MIB Statistics Policies form and child forms.

Administrative State

See the [Administrative State](#) parameter in section 134.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 134.1.

Displayed Name

See the [Displayed Name](#) parameter in section 134.1.

Number of Varbind per PDU

(numberOfVarPerPdu)

The Number of Varbind per PDU parameter specifies the maximum number of variable bindings, or varbinds, in the SNMP PDUs associated with the MIB statistics policy. The parameter is used to adjust the PDU size with respect to the network MTU size. The range is 20 to 200. The default is 100.



Caution — Changing the parameter value may affect the time required for subsequent NE resynchronizations and degrade 5620 SAM server performance. Do not change the parameter value from the default without contacting Alcatel-Lucent technical support.

Policy ID

(id)

The Policy ID parameter specifies a unique ID for the policy. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 65535. The default is 0.

Polling Admin State

(administrativeState)

The Polling Admin State parameter specifies whether the polling of managed devices is enabled (up). The options are:

- Up (default)
- Down

Polling Interval

(pollingInterval)

The Polling Interval parameter specifies how often MIB elements of discovered and managed devices are polled for changes. When changes are detected, the 5620 SAM rereads the MIB element and updates the database. The default is 15 minutes. When this parameter is disabled, synchronization between network elements and the database do not occur. The options are:

- 5 minutes
- 15 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 1 hour, 15 minutes
- 1 hour, 30 minutes
- 1 hour, 45 minutes
- 2 hours
- 2 hours, 15 minutes
- 2 hours, 30 minutes
- 2 hours, 45 minutes
- 3 hours
- 4 hours
- 8 hours
- 12 hours
- 24 hours
- 48 hours

Polling Synchronization Time

See the [Polling Synchronization Time](#) parameter in section [134.1](#).

123 –Server Performance Statistics parameters

123.1 Server Performance Statistics parameters 123-2

123.1 Server Performance Statistics parameters

This chapter describes the parameters on the Server Performance Statistics form and its child forms.

Accounting Stats Failure Periodic Threshold

The Accounting Stats Failure Periodic Threshold parameter specifies the number of accounting statistics failures that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. Accounting statistics failures can be caused by conditions such as failed file transfers. When the counter reaches this number, a threshold-crossing alarm is raised.

Accounting Stats Pending Periodic Threshold

The Accounting Stats Pending Periodic Threshold parameter specifies the number of accounting statistics that are pending to be processed that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Accounting Stats Processed Periodic Threshold

The Accounting Stats Processed Periodic Threshold parameter specifies the number of accounting statistics processed that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Accounting Stats Total Periodic Threshold

The Accounting Stats Total Periodic Threshold parameter specifies the number of accounting statistics received that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Administrative State

See the [Administrative State](#) parameter in section [134.1](#).

Alarm Total Periodic Threshold

The Alarm Total Periodic Threshold parameter specifies the number of alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Cleared Periodic Threshold

The Cleared Periodic Threshold parameter specifies the number of cleared alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Collection Interval

([pollingInterval](#))

The Collection Interval parameter specifies the frequency with which the statistics counters for the selected statistics class are logged. The default is 15 minutes.

Condition Periodic Threshold

The Condition Periodic Threshold parameter specifies the number of condition alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Critical Periodic Threshold

The Critical Periodic Threshold parameter specifies the number of critical alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Dropped Backpressure Periodic Threshold

The Dropped Backpressure Periodic Threshold parameter specifies the number of traps dropped because of backpressure during the interval specified by the [Collection Interval](#) parameter. Backpressure conditions occur when the 5620 SAM server is very busy processing other traps. When the SNMP Trap counter reaches this number, a threshold-crossing alarm is raised.

Dropped Duplicate Periodic Threshold

The Dropped Duplicate Periodic Threshold parameter specifies the number of duplicate SNMP traps dropped during the interval specified by the [Collection Interval](#) parameter. When the SNMP Trap counter reaches this number, a threshold-crossing alarm is raised.

Dropped Full Resync Periodic Threshold

The Dropped Full Resync Periodic Threshold parameter specifies the number of SNMP traps that are not processed because of a pending full resync during the interval specified by the [Collection Interval](#) parameter. When the SNMP Trap counter reaches this number, a threshold-crossing alarm is raised.

Dropped Not Managed Periodic Threshold

The Dropped Not Managed Periodic Threshold parameter specifies the number of SNMP traps associated with an unmanaged NE dropped during the interval specified by the [Collection Interval](#) parameter. When the SNMP Trap counter reaches this number, a threshold-crossing alarm is raised.

Dropped Out Of Sequence Periodic Threshold

The Dropped Out Of Sequence Periodic Threshold parameter specifies the number of SNMP traps with non-sequential trap IDs dropped during the interval specified by the [Collection Interval](#) parameter. When the SNMP Trap counter reaches this number, a threshold-crossing alarm is raised.

Incoming Periodic Threshold

The Incoming Periodic Threshold parameter specifies the number of SNMP traps received during the interval specified by the [Collection Interval](#) parameter. When the SNMP Trap counter reaches this number, a threshold-crossing alarm is raised.

Indeterminate Periodic Threshold

The Indeterminate Periodic Threshold parameter specifies the number of indeterminate alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Info Periodic Threshold

The Info Periodic Threshold parameter specifies the number of log entries for info alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Major Periodic Threshold

The Major Periodic Threshold parameter specifies the number of major alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Minor Periodic Threshold

The Minor Periodic Threshold parameter specifies the number of minor alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Polling Synchronization Time

See the [Polling Synchronization Time](#) parameter in section [134.1](#).

Retention Time (hours)

See the [Retention Time \(hours\)](#) parameter in section 134.1.

Scheduled Polling Stats Pending Periodic Threshold

The Scheduled Polling Stats Pending Periodic Threshold parameter specifies the number of scheduled SNMP statistics awaiting processing that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Scheduled Polling Stats Processed Periodic Threshold

The Scheduled Polling Stats Processed Periodic Threshold parameter specifies the number of processed scheduled SNMP statistics that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Scheduled Polling Stats Total Periodic Threshold

The Scheduled Polling Stats Total Periodic Threshold parameter specifies the number of scheduled SNMP statistics received that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Scheduled Resync Failure Periodic Threshold

The Scheduled Resync Failure Periodic Threshold parameter specifies the number of scheduled node resync failures that the Node Resync counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Scheduled Resync Processed Periodic Threshold

The Scheduled Resync Processed Periodic Threshold parameter specifies the number of scheduled processed node resyncs that the Node Resync counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Scheduled Resync Received Periodic Threshold

The Scheduled Resync Received Periodic Threshold parameter specifies the number of scheduled node resyncs that the Node Resync counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Scheduled Stats Failure Periodic Threshold

The Scheduled Stats Failure Periodic Threshold parameter specifies the number of scheduled SNMP statistics processing failures that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. Statistics failures may occur if an NE is unreachable or if collection takes longer than the collection interval time. When the counter reaches this number, a threshold-crossing alarm is raised.

Threshold Reporting State

See the [Threshold Reporting State](#) parameter in section 116.1.

Unscheduled Resync Failure Periodic Threshold

The Unscheduled Resync Failure Periodic Threshold parameter specifies the number of unscheduled node resync failures that the Node Resync counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Unscheduled Resync Processed Periodic Threshold

The Unscheduled Resync Processed Periodic Threshold parameter specifies the number of unscheduled processed node resyncs that the Node Resync counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Unscheduled Resync Received Periodic Threshold

The Unscheduled Resync Received Periodic Threshold parameter specifies the number of unscheduled node resyncs that the Node Resync counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Used Heap Memory Periodic Threshold

The Used Heap Memory Periodic Threshold parameter specifies the amount of heap memory currently in use that the SAM Memory counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Used Non Heap Memory Periodic Threshold

The Used Non Heap Memory Periodic Threshold parameter specifies the amount of non-heap memory currently in use that the SAM Memory counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Unscheduled Polling Stats Pending Periodic Threshold

The Unscheduled Polling Stats Pending Periodic Threshold parameter specifies the number of unscheduled SNMP statistics awaiting processing that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Unscheduled Polling Stats Processed Periodic Threshold

The Unscheduled Polling Stats Processed Periodic Threshold parameter specifies the number of processed unscheduled SNMP statistics that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Unscheduled Polling Stats Total Periodic Threshold

The Unscheduled Polling Stats Total Periodic Threshold parameter specifies the number of unscheduled SNMP statistics received that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Unscheduled Stats Failure Periodic Threshold

The Unscheduled Stats Failure Periodic Threshold parameter specifies the number of unscheduled SNMP statistics processing failures that the Stats Collection counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

Warning Periodic Threshold

The Warning Periodic Threshold parameter specifies the number of warning alarms that the Alarm Rate counter records during the interval specified by the [Collection Interval](#) parameter. When the counter reaches this number, a threshold-crossing alarm is raised.

124 –Accounting Policies parameters

124.1 Accounting Policies parameters 124-2

124.1 Accounting Policies parameters

This chapter describes the parameters on the Manage Accounting Policies form and child forms.

All Overrides

(allOverrides)

The All Overrides parameter specifies whether an NE monitors all override counters for the change in value specified by the [Significant Change Delta](#) parameter. The options are:

- Disabled (default)
- Enabled

All Queues

(allQueues)

The All Queues parameter specifies whether an NE monitors all queues for the change in value specified by the [Significant Change Delta](#) parameter. The options are:

- Disabled (default)
- Enabled

Application Assurance Counters

(applicationAssuranceCounter)

The Application Assurance Counters parameter specifies the general AA statistics counters that are to be included in a Custom AA Subscriber record. You can select multiple options. The options are:

- Short Duration Flows
- Medium Duration Flows
- Long Duration Flows
- Total Flow Duration
- Total Flows Completed

You can select all counters by clicking on the Select All button. You can deselect all counters by clicking on the Deselect All button.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [134.1](#).

Administrative

See the [Administrative State](#) parameter in section [134.1](#).

Collection Interval (m)

(collectionInterval)

The Collection Interval (m) parameter specifies how frequently, in minutes, the statistics are collected and written to their destination. This parameter will have a default value assigned when the associated [Use Default Interval](#) parameter is set to true. The Collection Interval (m) parameter is only configurable when the associated [Use Default Interval](#) parameter is set to false. The range is 5 to 120, except for NE Schedulable tests (saa) record types, where the range is 1 to 120.

Table [124-1](#) lists the default values for different object types.

Table 124-1 Collection Interval (m) parameter

Object type	Default
AA records	15
Network records	15
Service records	5
Subscriber records	5
LSP records	5
NE Schedulable tests (saa) records	5
Video records	10
No record type specified	5

Counters

Table [124-2](#) describes where to find information about the Counters parameter.

Table 124-2 Counters parameter

Object	See
Egress queue or override	Counters parameter in this section
Ingress queue or override	Counters parameter in this section
Significant change criteria	Counters parameter in this section

Counters

The Counters parameter in the Egress panel of the CustomQueueConfig or CustomOverrideConfig form specifies the ingress statistics counters or override queue counters to monitor. See the [Egress Counters](#) parameter in this section for the parameter options.

Counters

The Counters parameter in the Ingress panel of the CustomQueueConfig or CustomOverrideConfig form specifies the ingress statistics counters or override queue counters to monitor. See the [Ingress Counters](#) parameter in this section.

Counters

(significantApplicationAssuranceCounter)

The Counters parameter in the Application Assurance panel specifies whether an NE monitors the statistics counters specified in a custom AA policy for the change in value that the [Significant Change Delta](#) parameter specifies. Table 124-3 describes the parameter options.

Table 124-3 Counters parameter

Option	Description
Any	Specifies that the parameter is enabled

- Disabled (default)
- AnyEnabled

Default

(isDefault)

The Default parameter specifies whether the policy is the default policy. The options are:

- false (default)
- true

Description

See the [Description](#) parameter in section 134.1.

Displayed Name

See the [Displayed Name](#) parameter in section 134.1.

Egress Counters

(significantEgressOverrideCounter)

The Egress Counters parameter specifies the reference-queue egress statistics counters that an NE monitors for the change in value specified by the [Significant Change Delta](#) parameter. The options are:

- In Profile Packets Forwarded
- In Profile Packets Dropped
- Out Of Profile Packets Forwarded
- Out Of Profile Packets Dropped
- In Profile Octets Forwarded
- In Profile Octets Dropped
- Out Of Profile Octets Forwarded
- Out Of Profile Octets Dropped



Note — You must select at least one egress counter for the reference override that you specify to monitor for significant change.

Egress Counters

(significantEgressQueueCounter)

The Egress Counters parameter specifies the reference-queue egress statistics counters that an NE monitors for the change in value specified by the [Significant Change Delta](#) parameter. The options are:

- In Profile Packets Forwarded
- In Profile Packets Dropped
- Out Of Profile Packets Forwarded
- Out Of Profile Packets Dropped
- In Profile Octets Forwarded
- In Profile Octets Dropped
- Out Of Profile Octets Forwarded
- Out Of Profile Octets Dropped



Note — You must select at least one egress counter for the reference queue that you specify to monitor for significant change.

File ID

(fileId)

The File ID parameter specifies a file policy identifier. Click on the Select button to choose a file policy.

From Subscriber Counters

(fromSubCounter)

The From Subscriber Counters parameter specifies the AA statistics counters for traffic from a subscriber that are to be included in a Custom AA Subscriber record. You can select multiple options. The options are:

- Allowed Flows
- Denied Flows
- Active Flows
- Total Packets
- Total Octets
- Total Discarded Packets
- Total Discarded Octets

You can select all counters by clicking on the Select All button. You can deselect all counters by clicking on the Deselect All button.

ID

The ID parameter specifies the numeric identifier of a queue or an override counter. Table 124-4 lists the ranges for different object types. The default is 0, which means that the parameter is not configured.

Table 124-4 ID parameter

Object type	Range
Override counter	1 to 8
Egress queue	1 to 8
Ingress queue	1 to 32

ID

(id)

See the ID parameter in section 134.1.

Ingress Counters

(significantIngressOverrideCounter)

The Ingress Counters parameter specifies the override ingress statistics counters that an NE monitors for the change in value specified by the [Significant Change Delta](#) parameter. The options are:

- All Packets Offered
- High Packets Dropped
- Low Packets Dropped
- In Profile Packets Forwarded
- Out Of Profile Packets Forwarded
- All Octets Offered
- High Octets Dropped
- Low Octets Dropped
- In Profile Octets Forwarded
- Out Of Profile Octets Forwarded



Note — You must select at least one ingress counter for the reference override that you specify to monitor for significant change.

Ingress Counters

(significantIngressQueueCounter)

The Ingress Counters parameter specifies the reference-queue ingress statistics counters that an NE monitors for the change in value specified by the [Significant Change Delta](#) parameter. The options are:

- All Packets Offered
- Uncolored Packets Offered
- High Packets Offered
- Low Packets Offered
- High Packets Dropped
- Low Packets Dropped
- In Profile Packets Forwarded
- Out Of Profile Packets Forwarded
- All Octets Offered
- Uncolored Octets Offered
- High Octets Offered
- Low Octets Offered
- High Octets Dropped
- Low Octets Dropped
- In Profile Octets Forwarded
- Out Of Profile Octets Forwarded



Note — You must select at least one ingress counter for the reference queue that you specify to monitor for significant change.

Name

(fileName)

Use the Select button to choose a file policy.

Significant Change Delta

(delta)

The Significant Change Delta parameter specifies the collective amount by which the statistics counters must change before an NE saves the custom statistics record to a file. The parameter takes effect when the [All Overrides](#) parameter is enabled. The range is 0 to 4 294 967 295, or 0 to 1 when the [Counters](#) parameter is enabled. The default is 0.

To Subscriber Counters

(toSubCounter)

The From Subscriber Counters parameter specifies the AA statistics counters for traffic from a subscriber that are to be included in a Custom AA Subscriber record. You can select multiple options. The options are:

- Allowed Flows
- Denied Flows
- Active Flows
- Total Packets
- Total Octets
- Total Discarded Packets
- Total Discarded Octets

You can select all counters by clicking on the Select All button. You can deselect all counters by clicking on the Deselect All button.

Type

(recordType)

The Type parameter specifies the type of accounting statistics to collect. The options are:

- AA Application
- AA Application Group
- AA Protocol
- AA Subscriber Application
- AA Subscriber Protocol
- Combined MPLS LSP Egress
- Combined MPLS LSP Ingress
- Combined Network Ing Egr Octets
- Combined Queue Group
- Combined Service Ing Egr Octets
- Combined Service Ingress
- Combined Service SDP Ingress Egress
- Compact Service Ingress Octets
- Complete Service Ingress Egress
- Complete Service SDP Ingress Egress
- Complete Subscriber Ingress Egress
- Custom Record AA Subscriber
- Custom Record Service
- Custom Record Subscriber
- NE Schedulable Tests
- Network Egress Octet
- Network Egress Packet
- Network Ingress Octet
- Network Ingress Packet
- None (default)
- Queue Group Octets
- Queue Group Packets
- Service Ingress Octet
- Service Ingress Packet
- Service Egress Octet
- Service Egress Packet

Use Default Interval

(useDefaultInterval)

The Use Default Interval parameter specifies whether the default NE collection interval is used as the collection interval for the accounting policy.

The options are:

- false (default)
- true

When the parameter is set to false, the [Collection Interval \(m\)](#) parameter is configurable.

125 –File Policies parameters

125.1 File Policies parameters 125-2

125.1 File Policies parameters

This chapter describes the parameters on the Manage File Policies form and child forms.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [134.1](#).

Description

See the [Description](#) parameter in section [134.1](#).

Displayed Name

See the [Displayed Name](#) parameter in section [134.1](#).

Drive

(drive)

The Drive parameter specifies where statistics are to be collected for backup purposes. You cannot specify the same location for both the Drive and the Storage Drive - Backup parameters. The options are:

- Application Specific Default (default)
- cf1:
- cf2:
- cf3:

ID

See the [ID](#) parameter in section [134.1](#).

Retention (hours)

(retentionInterval)

The Retention (hours) parameter specifies the minimum time, in hours, that an NE stores accounting statistics log files. An NE deletes a log file that is older than the parameter value if the NE requires storage space. The range is 1 to 500. The default is 12.

Ensure that the NE resources are sufficient to support the file policy and associated accounting policy specifications. The collection, retention, and rollover intervals must be appropriate, and the statistics must be regularly retrieved from each NE.

Rollover (minutes)

(collectionInterval)

The Rollover (minutes) parameter specifies the file rollover time, in minutes, of the accounting statistics files. Table 125-1 lists the parameter ranges for various device types. The default is 1440.

Table 125-1 Rollover (minutes) parameter

Device type	Range
7450 ESS, 7710 SR, and 7750 SR	5 to 10080
7705 SAR, Release 1.0 or later	5 to 2880

When the parameter value is greater than 2880 in a new file policy and the policy is applied to an NE that does not support the value, the default value is used on the NE.

When the parameter value in an existing file policy is increased above 2880 and the policy is applied to an NE that does not support the value, the local value remains unchanged.

Ensure that the NE resources are sufficient to support the file policy and associated accounting policy specifications. The collection, retention, and rollover intervals must be appropriate, and the statistics must be regularly retrieved from the NEs.

Storage Drive - Backup

(backupPath)

The Storage Drive - Backup parameter specifies where statistics are backed up. You can specify different flash drives for different policies, depending on your needs and the size of the logging data to be stored. You cannot specify the same location for both the Drive and the Storage Drive - Backup parameters. The options are:

- Application Specific Default (default)
- cf1:
- cf2:
- cf3:

126 –Statistics Browser parameters

126.1 Statistics Browser parameters 126-2

126.1 Statistics Browser parameters

This chapter describes the parameters on the statistics records forms and child forms.

Administrative State

See the [Administrative State](#) parameter in section [134.1](#).

Statistics Type

The Statistics Type parameter specifies the type of logged data that is displayed in the search list. Table [126-1](#) describes the parameter options.

Table 126-1 Statistics Type parameter

Option	Description
Current Data (default)	The most recent available statistics record
Statistics Policy	The statistics policy configured for the statistics class
Statistics Record	All available records for the statistics class

Retention Time (hours)

See the [Retention Time \(hours\)](#) parameter in section [134.1](#).

Threshold Reporting State

See the [Threshold Reporting State](#) parameter in section [116.1](#).

127 –TCA Policies parameters

127.1 TCA Policies parameters 127-2

127.1 TCA Policies parameters

This chapter describes the parameters on the UtilizationTCA form and child forms.

Alarm Severity

(severity)

The Alarm Severity parameter specifies the severity that the 5620 SAM assigns to an alarm when the utilization reaches the threshold specified by the [Threshold \(%\)](#) and [Threshold Direction](#) parameters. The options are:

- cleared
- condition
- critical
- indeterminate
- info
- major (default)
- minor
- warning

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [134.1](#).

Displayed Name

See the [Displayed Name](#) parameter in section [134.1](#).

Flow Direction

(direction)

The Flow Direction parameter specifies the direction of traffic flow to which the policy applies. The options are:

- Ingress
- Egress
- Ingress/Egress (default)

Policy ID

(id)

The Policy ID parameter specifies the numeric identifier of the policy. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 65 535. The default is 0, which means that the parameter is not configured.

Rule ID

(id)

The Rule ID parameter specifies the numeric identifier of the rule. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to infinity. The default is 0, which means that the parameter is not configured.

Threshold (%)

(threshold)

The Threshold (%) parameter specifies the percentage of resource utilization that triggers the alarm condition. The range is 1 to 100. The default is 80.

Threshold Direction

(crossDirection)

The Threshold Direction parameter specifies the direction of the utilization change that triggers the alarm condition. The options are:

- Falling Below
- Rising Above (default)

128 –RAN Performance Management Policies parameters

128.1 RAN Performance Management Policies parameters 128-2

128.1 RAN Performance Management Policies parameters

This chapter describes the parameters on the RAN Performance Management Policies form.

Administrative State

(administrativeState)

The Administrative State parameter allows operators to start and stop performance management statistics collection. The options are:

- Up
- Down

Collection Interval (min)

(pollingInterval)

The Collection Interval (min) parameter specifies the collection interval for performance management statistics. The options are:

- 5
- 15
- 30
- 60

129 –Schedules parameters

129.1 Schedules parameters 129-2

129.1 Schedules parameters

This chapter describes the unique parameters on the Manage Schedules and Manage Scheduled Tasks forms and child forms.

Administrative State

See the [Administrative State](#) parameter in section 134.1.

Change Current User To

The Change Current User To parameter specifies the 5620 SAM user to which the SAM scheduled task is to be assigned. The options are all configured user accounts. The default is admin, which is the default 5620 SAM account.

Delay Time (seconds)

(delayTime)

The Delay Time (seconds) parameter specifies the delay start time for a run within a scheduled task. The delay time is applied when the execution time of a scheduled run is skipped. If a previous run is complete and a scheduled run is triggered, the run executes and is not delayed whether a delay time is configured or not. If this parameter is set to 0, there is no delay. The range is 0, 60 to 900. The default is 0.

The parameter is configurable when the [Enable](#) parameter is set to Enable.

Description

See the [Description](#) parameter in section 134.1.

Enable

The Enable parameter specifies whether to enable or disable the configurability of the [Delay Time \(seconds\)](#) parameter. The options are:

- Enable
- Disable (default)

Frequency

(frequency)

The Frequency parameter specifies how often the SAM schedule operates. Table 129-1 describes the parameter options.

Table 129-1 Frequency parameter

Option	Option description	Dependencies
Once (default)	The SAM schedule is run only once.	You cannot configure the Current Client End Time parameter.
Per Second	The SAM schedule is performed every second, based on an additional parameter.	You must configure the Run Every Second or Run Every Seconds parameter to specify the frequency.
Per Minute	The SAM schedule is performed every minute, based on an additional parameter.	You must configure the Run Every Minute or Run Every Minutes parameter to specify the frequency.
Per Hour	The SAM schedule is performed every hour, based on an additional parameter.	You must configure the Run Every Hour or Run Every Hours parameter to specify the frequency.
Per Day	The SAM schedule is performed every day, based on an additional parameter.	You must configure the Run Every Day , Run Every Days , or Run Every parameter to specify the frequency.
Per Week	The SAM schedule is performed every week, based on an additional parameter.	You must configure the Run Every Week or Run Every Weeks parameter to specify the frequency.
Per Month	The SAM schedule is performed every month, based on an additional parameter.	You must configure the Run Every Month or Run Every Months parameter to specify the frequency.

Name

(**displayName**)

The Name parameter specifies the name of the schedule. The range is 1 to 32 characters. There is no default.

Current Client End Time

(**userEndDate**)

The Current Client End Time parameter allows you to enter the user end time based on the client time zone, daylight savings mode, and time zone set in the user preferences. Depending on the time and the time zone set by the user, the user end time is converted to the server end time. The server end time is also calculated based on the server time zone and daylight savings mode set for the server. The range is any date. The default is the time that the 5620 SAM server starts, plus one minute. The parameter is configurable when the [Frequency](#) parameter is set to any value except Once and the [Ongoing](#) parameter is disabled.

You can choose the year, month, or day values using the calendar button. All values are configurable using the up and down arrows beside the parameter, the cursor keys on the keyboard, or by entering the value.

All schedules are based on the 5620 SAM server time at the time when the schedule was created. For example, if you create a schedule in a different time zone from the server, 5620 SAM converts the value and updates the server end time parameter with the converted time. The scheduled task is executed based on the server time.

Current Client Start Time

(**userStartDate**)

The Current Client Start Time parameter allows you to enter the user start time based on the client time zone, daylight savings mode and the time zone set in the user preferences. Depending on the time and the time zone set by the user, the user start time is converted to the server start time. The server start time is also calculated based on the server time zone and daylight savings mode set for the server. The range is any future date. The default is the time that the 5620 SAM server GUI started, plus one minute.

You can choose the year, month, or day values using the calendar button. All values are configurable using the up and down arrows beside the parameter, the cursor keys on the keyboard, or by entering the value.

When a SAM schedule is created using a client station in a time zone other than the 5620 SAM server time zone, you can configure the remote station time zone to match the local time zone by choosing Application → User Preferences → Time Zone. If you do not configure the time zone, the 5620 SAM uses the default client time zone.

All schedules are based on the 5620 SAM server time at the time when the schedule is created. For example, if you create a schedule in a different time zone from the server, 5620 SAM converts the value and updates the server start time parameter with the converted time. The scheduled task is executed based on the server time.

Ongoing

(onGoing)

The Ongoing parameter specifies whether a schedule has an end time. When the parameter is disabled, the schedule operates indefinitely. The options are:

- Enabled
- Disabled (default)

Run Every

Table 129-2 lists where to find more information about the Run Every parameter.

Table 129-2 Run Every parameter

Parameter	See
Run Every <i>n</i> days	Run Every parameter in this section
Run Every <i>n</i> weeks	Run Every parameter in this section
Run Every <i>n</i> months	Run Every parameter in this section

When a user chooses the [Run Every](#) parameter, they cannot set the [Ongoing](#) parameter. The [Current Client End Time](#) parameter must be set and cannot exceed the [Current Client Start Time](#) parameter.

Run Every

(runDay)

The Run Every parameter specifies that the SAM schedule runs on the days indicated by the selected check boxes. The parameter is configurable when the [Frequency](#) parameter is set to Per Day. There is no default. The options are:

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

Run Every

(runMonth)

The Run Every parameter specifies that the SAM schedule runs on the months indicated by the selected check boxes. The parameter is configurable when the [Frequency](#) parameter is set to Per Month. There is no default. The options are:

- January
- February
- March
- April
- May
- June
- July
- August
- September
- October
- November
- December

Run Every

(runWeek)

The Run Every parameter specifies that the SAM schedule runs on a specific day of the week and week of the month. For example a scheduled task can be run every second Tuesday of the month. The parameter is configurable when the [Frequency](#) parameter is set to Per Week.

The day of the week on which the SAM schedule runs is configurable using a drop-down menu. The options are:

- Monday
- Tuesday
- Wednesday
- Thursday
- Friday
- Saturday
- Sunday

The week of the month in which the SAM schedule runs is selectable using a checkbox. The options are:

- First
- Second
- Third
- Fourth
- Last

Run Every Day

(runEveryDay)

The Run Every Day parameter specifies whether the SAM schedule runs every day. The parameter is configurable when the [Frequency](#) parameter is set to Per Day. The options are:

- Enabled (default)
- Disabled

Run Every Days

The Run Every Days parameter specifies whether the SAM schedule runs every n days, where n is a numerical value that you set using the up and down arrows. The parameter is configurable when the [Frequency](#) parameter is set to Per Day. The range is 1 to 2 147 483 647. The default is 1.

Run Every Hour

(runEveryHour)

The Run Every Hour parameter specifies whether the SAM schedule runs every hour. The parameter is configurable when the [Frequency](#) parameter is set to Per Hour. The options are:

- Enabled (default)
- Disabled

Run Every Hours

The Run Every Hours parameter specifies whether the SAM schedule runs every n hours, where n is a numerical value set using the up and down arrows. The parameter is configurable when the [Run Every Hour](#) parameter is disabled. The range is 1 to 2 147 483 647. The default is 1.

Run Every Minute

(runEveryMinute)

The Run Every Minute parameter specifies whether the SAM schedule runs every minute. The parameter is configurable when the [Frequency](#) parameter is set to Per Minute. The options are:

- Enabled (default)
- Disabled

Run Every Minutes

The Run Every Minutes parameter specifies that the SAM schedule runs every n minutes, where n is a numerical value set using the up and down arrows. The parameter is configurable when the [Run Every Minute](#) parameter is disabled.

Run Every Month

(runEveryMonth)

The Run Every Month parameter specifies that the SAM schedule runs every month. The parameter is configurable when the [Frequency](#) parameter is set to Per Month. The options are:

- Enabled (default)
- Disabled

Run Every Months

The Run Every Months parameter specifies that the SAM schedule runs every n months, where n is a numerical value set using the up and down arrows. The parameter is configurable when the [Frequency](#) parameter is set to Per Month. The range is 1 to 2 147 483 647. The default is 1.

A month is based on a 30-day interval.

Run Every Second

(runEverySecond)

The Run Every Second parameter specifies whether the SAM schedule runs every second. The parameter is configurable when the [Frequency](#) parameter is set to Per Second. The options are:

- Enabled (default)
- Disabled

Run Every Seconds

The Run Every Seconds parameter specifies that the SAM schedule runs every n seconds, where n is a numerical value set using the up and down arrows. The parameter is configurable when the [Run Every Second](#) parameter is disabled. The range is 1 to 2 147 483 647. The default is 1.

Run Every Week

(runEveryWeek)

The Run Every Week parameter specifies whether the SAM schedule runs every week. The parameter is configurable when the [Frequency](#) parameter is set to Per Week. The options are:

- Enabled (default)
- Disabled

Run Every Weeks

(runWeek)

The Run Every Weeks parameter specifies that the SAM schedule runs every n weeks, where n is a numerical value set using the up and down arrows. The parameter is configurable when the [Frequency](#) parameter is set to Per Week. The range is 1 to 2 147 483 647. The default is 1.

Scheduled Task Description

(description)

The Scheduled Task Description parameter specifies the description of this association of a schedule and a scheduled task. The range is 0 to 254 characters.

Scheduled Task Name

(displayName)

The Scheduled Task Name parameter specifies the name of this association of a schedule and a scheduled task. You must configure the parameter. The range is 1 to 32 characters.

Time Alignment Setting

The Time Alignment Setting parameter specifies the base minute with which the SAM schedule aligns. The parameter is used with the [Run Every Minutes](#) parameter. The range is 0 to 59. The default is 0.

130 –Policies Audit parameters

130.1 Policies Audit parameters 130-2

130.1 Policies Audit parameters

This chapter describes the parameters on the Policy Audit form and child forms.

Include Non Applicable Attributes

(alarmAllDifferences)

The Include Non Applicable Attributes parameter specifies whether the 5620 SAM includes attributes that are not common to the policies in the audit. When the parameter is enabled, an alarm is raised during the audit when an attribute is present in one policy but not in the other. The options are:

- enabled
- disabled (default)

Set to “Local Edit Only” upon finding of differences

(localEditDifferences)

The Set to “Local Edit Only” upon finding of differences parameter specifies whether the local policy distribution mode is changed to local edit only when the audit discovers differences between local and global policy. The parameter is configurable when the [Include Non Applicable Attributes](#) parameter is disabled. The options are:

- enabled
- disabled (default)

Set to “Sync with Global” upon finding of no differences

(globalSyncNonDifferences)

The Set to “Sync with Global” upon finding no differences parameter specifies whether the local policy distribution mode is changed to sync with global when the audit discovers no differences between local and global policies. The parameter is configurable when the [Include Non Applicable Attributes](#) parameter is disabled. The options are:

- enabled
- disabled (default)

131 –Time Range Entry Assignment parameters

131.1 Time Range Entry Assignment parameters 131-2

131.1 Time Range Entry Assignment parameters

This chapter describes the parameters on the Time Range Entry Assignment Tool form and its child forms.

End Date

The End Date parameter specifies the end date and time of the time range entry assignment analysis. You can use the up and down arrows to change the year, month, day, hour, or minute. The default value is the current system time of the 5620 SAM server.

Search by Time Of Day Entry Type

The Search by Time Of Day Entry Type parameter specifies whether the time range entry assignment analysis tool uses the [Time Of Day Entry Policy Type](#) parameter as an input criterion. The options are:

- enabled
- disabled (default)

Start Date

The Start Date parameter specifies the start date and time of the time range entry assignment analysis. You can use the up and down arrows to change the year, month, day, hour, or minute. The default value is the current system time of the 5620 SAM server.

Time Of Day Entry Policy Type

The Time Of Day Entry Policy Type parameter specifies the type of time of day entry policy that the time range entry assignment analysis tool uses as an input criterion. The options are:

- | | |
|-------------------------------|--------------------------------|
| • Ingress IPV6 Filter | • Egress IPV6 Filter |
| • Egress MAC Filter | • Ingress QoS Scheduler Policy |
| • Egress QoS Scheduler Policy | • Egress QoS Policy |
| • Ingress IP Filter | • Ingress QoS Policy |

Time Range Entry Container Type

The Time Range Entry Container Type parameter specifies the type of policy string that the time range entry assignment analysis tool uses as an input criterion. The options are:

- L2 Access Interface
- L3 Access Interface
- Aggregation Suite
- Time Of Day Suite

132 –Copy/Move SAPs parameters

132.1 Copy/Move SAPs parameters 132-2

132.1 Copy/Move SAPs parameters

This chapter describes the parameters on the Copy/Move SAPs form and child forms.

Action Type

(isMoving)

The Action Type parameter specifies the operation to be performed on a SAP. The options are:

- Copy (default)
- Move

Continue on individual Failure

The Continue on individual Failure parameter specifies the action to be taken if a SAP copy or move operation fails. When the parameter is disabled, the operation stops after the first failure and all successful SAP copy or move operations are reversed. When the parameter is enabled, the operation continues until all SAP copy or move operations that can be completed successfully are finished. The options are:

- Disabled (default)
- Enabled

Current Mode

(targetType)

The Current Mode parameter specifies the type of interface on which the move and copy operations are performed. The options are:

- L2 Access Interface (default)
- L3 Access Interface
- L3 Subscriber Interface SAP

Inner Encap Value End

The Inner Encap Value End parameter specifies the ending value of the inner encapsulation label. The range is 1 to 65 535 (default is 1) for ATM channels. Otherwise, the range is 0 to 4095 (default is 0).

Inner Encap Value Offset

(innerEncapShiftOffset)

The Inner Encap Value Offset parameter specifies the offset value used to shift the inner encapsulation value of a copied or moved SAP. This value is required when the destination port has a SAP with the same encapsulation value as the SAP that is being copied or moved. The range is –65 535 to 65 535 for ATM channels. Otherwise, the range is –4095 to 4095. The default is 0.

Inner Encap Value Start

The Inner Encap Value Start parameter specifies the starting value of the inner encapsulation label. The range is 1 to 65 535 (default is 1) for ATM channels. Otherwise, the range is 0 to 4095 (default is 0).

Outer Encap Value End

The Outer Encap Value End parameter specifies the end value of the outer encapsulation label. The range is 0 to 4094. The default is 4094.

Outer Encap Value Offset

(outerEncapShiftOffset)

The Outer Encap Value Offset parameter specifies the offset value that is used to shift the outer encapsulation value of a copied or moved SAP. This value is required when the destination port has a SAP that uses the same encapsulation value as the SAP that is being copied or moved. The range is –4094 to 4094. The default is 0.

Outer Encap Value Start

The Outer Encap Value Start parameter specifies the start value of the outer encapsulation label. The range is 0 to 4094. The default is 0.

Service Type

The Service Type parameter specifies the type of service for the source interface SAPs.

When the [Current Mode](#) parameter is L2 Access Interface, the options are:

- All L2 Services (default)
- Apipe
- Epipe
- Ipipe
- VPLS
- MVPLS

When the **Current Mode** parameter is L3 Access Interface or L3 Subscriber Interface SAP, the options are:

- All L3 Services (default)
- IES
- VPRN

133 –NE Sessions parameters

133.1 NE Sessions parameters 133-2

133.1 NE Sessions parameters

This chapter describes the parameters on the Terminal Configuration form.

Append to file

The Append to file parameter specifies whether the 5620 SAM appends the console output to the file specified by the [Log File Location](#) parameter.

The parameter is configurable when the [Send Console To a File](#) parameter is enabled.

Table 133-1 describes the parameter options.

Table 133-1 Append to file parameter

Option	Description
disabled (default)	The 5620 SAM overwrites the file specified by the Log File Location parameter using the console output.
enabled	The 5620 SAM appends the console output to the file specified by the Log File Location parameter.

Background color

The Background color parameter specifies the background color of the console window. Click on the Set color button beside the parameter to choose a color using a palette form. The default is black.

Bold

The Bold parameter specifies whether the console window displays text in boldface type. The options are:

- disabled (default)
- enabled

Font Name

The Font Name parameter specifies the typeface of the text in the console window. The options are:

- Monospaced (default)
- DialogInput
- Lucida Console
- Lucida Sans Typewriter

Font Size

The Font Size parameter specifies the character size of the text in the console window. The options are:

- 8
- 9
- 10
- 11
- 12
- 13 (default)
- 14
- 15
- 16
- 17
- 18

Foreground color

The Foreground color parameter specifies the color of the text in the console window. Click on the Set color button beside the parameter to choose a color using a palette form. The default is white.

Italic

The Italic parameter specifies whether the text in the console window is italicized. The options are:

- disabled (default)
- enabled

Log File Location

The Log File Location parameter specifies the path and name of the file that is to contain the console output. The 5620 SAM creates the file if it does not exist. You can configure the parameter using one of the following methods.

- Manually type a file name.
- Click on the Change button and use the form that opens to specify a file.
- Click on the Set Default button to restore the default path and file name.

The default is *install_dir*\nms\log\client\user_name\cli_output.txt for a Solaris client or *install_dir*\nms\log\client\user_name\cli_output.txt for a Windows client

where

install_dir is the client installation directory, typically /opt/5620sam/client on Solaris or C:\5620sam\client on Windows

user_name is the Solaris or Windows login name of the current user

The parameter is configurable when the [Send Console To a File](#) parameter is enabled.

Minimum number of scrolling lines

The Minimum number of scrolling lines parameter specifies the maximum number of text lines that the console scroll buffer can contain. When the number of lines exceeds the parameter value, the 5620 SAM removes the oldest line from the buffer and the line is no longer displayed in the console window.

Send Console To a File

The Send Console To a File parameter specifies whether the 5620 SAM records the console output in a file. The options are:

- disabled (default)
- enabled

134 –Common Tools menu parameters

134.1 Common Tools menu parameters 134-2

134.1 Common Tools menu parameters

This chapter describes the parameters that are common to the Tools menu forms and child forms.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether the object can be put in service. The options are:

- Enabled (default)
- Disabled

Auto-Assign ID

(id)

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique numeric identifier to the created object. The options are:

- Enabled (default)
- Disabled

Description

(description)

The Description parameter specifies a description for the created object. The range is 0 to 80 characters.

Displayed Name

(displayName)

The Displayed Name parameter specifies a name for the created policy object. The range is 0 to 80 characters.

Forwarding Class

(forwardingClass)

The Forwarding Class parameter specifies the forwarding class to map to an object. Table [134-1](#) describes the parameter options.

Table 134-1 Forwarding Class parameter

For	Description	Options
Queue mapping	Specifies the forwarding class that is mapped to the queue specified by the Queue ID, Multicast Queue ID, Broadcast Queue ID, and Unknown Queue ID parameters.	<ul style="list-style-type: none"> • be (default) • l2 • af • l1 • h2 • ef • h1 • nc
Dot1p, DSCP, Precedence, IP, and MAC mapping	Specifies the forwarding class to which packets with the specified match criteria are mapped. The default option specifies that packets maintain their previous forwarding class. The parameter options are described in Table 112-7.	<ul style="list-style-type: none"> • default (default) • be • l2 • af • l1 • h2 • ef • h1 • nc

ID

(logId)

The ID parameter specifies a unique numeric identifier for the created log. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 99. The default is 0, which means that no value is specified.

Name

(displayName)

The Name parameter specifies the name of an object. The range is 1 to 32 characters for most objects; Table 134-2 lists the exceptions. There is no default.

Table 134-2 Name parameter

Object	Range (characters)
STM test, test policy, or test suite	0 to 32
Virtual Anycast RP	1 to 80
VR	0 to 32

Polling Synchronization Time

(pollingSyncTime)

The Polling Synchronization Time parameter specifies the polling synchronization start time from which the polling intervals are calculated in hh:mm format based on a 24-hour clock. When the server restarts, the next appropriate collection interval is calculated and polling restarts. The default is 00:00.

Retention Time (hours)

(retentionInterval)

The Retention Time (hours) parameter specifies the time, in hours, that the 5620 SAM database stores the statistics associated with a statistics policy.

The range for a performance or server performance statistics policy is 1 to 8760.

The range for an accounting statistics policy is configurable. The minimum is 1. The maximum is $24 \times$ the [Accounting Statistic Data Retention Period \(Days\)](#) value, which is initially specified during 5620 SAM database installation and is configurable using the 5620 SAM Database Manager form.

The default for each policy type is 24.

Administration menu parameters

- 135 – 5620 SAM User Security parameters
- 136 – Change Password parameters
- 137 – TCP Key Chains parameters
- 138 – 5620 SAM RADIUS/TACACS+ User Authentication parameters
- 139 – NE Management Access Filters parameters
- 140 – NE CPM Filter parameters
- 141 – NE DoS Protection parameters
- 142 – NE User Profiles parameters
- 143 – NE User Configuration parameters
- 144 – NE Password Policy parameters
- 145 – NE RADIUS Authentication parameters
- 146 – NE TACACS+ Authentication parameters
- 147 – NE AOS Security Authentication parameters
- 148 – NE System Security parameters
- 149 – Subscriber Authentication Policy Manager parameters
- 150 – NE Maintenance parameters

- 151 – Database parameters
- 152 – System Information parameters
- 153 – System Preferences parameters
- 154 – Alarm Settings parameters
- 155 – Discovery Manager parameters
- 156 – Generic NE Manager parameters
- 157 – Mediation parameters
- 158 – NE Self Config Policy Manager parameters
- 159 – RAN License Manager parameters
- 160 – Pre-Provisioned NE Manager parameters
- 161 – Common Administration menu parameters

135 –5620 SAM User Security parameters

135.1 5620 SAM User Security parameters 135-2

135.1 5620 SAM User Security parameters

This chapter describes the parameters on the 5620 SAM User Security form and its child forms.

Account Expiry

(accountExpiryEnabled)

The Account Expiry parameter specifies whether the 5620 SAM should track how long an account remains dormant. When the parameter is enabled and a user account is not used for the number of days specified in the Account Expiry (days) parameter, the user account is removed from the system. The options are:

- Enabled
- Disabled (default)

Account Expiry (days)

(accountValidityPeriod)

The Account Expiry (days) parameter specifies how long dormant accounts are kept in the system. When a user account is not used for the number of days specified in the parameter and the Account Expiry parameter is enabled, the user account is removed from the system. The range is 0 to 365 days. The default is 180 days.

Administrative State

See the [Administrative State](#) parameter in section [161.1](#).

Advance Password Expiry Notification (days)

(advancePasswdExpirNotification)

The Advance Password Expiry Notification (days) parameter specifies how many days before a user password expires that the user is notified. The range is 0 and 1 to 365 days. The default is 10 days. When the parameter is set to 0, no notification of password expiry is sent to the user.

Apply Local Authentication Only

(localAuthenticationOnly)

The Apply Local Authentication Only parameter specifies whether only local authentication is applied to the user group. If this parameter is disabled, remote authentication can be applied to the group. The options are:

- Enabled
- Disabled (default)

Attempts before e-mail

(numAuthFailuresBeforeNotification)

The Attempts before e-mail parameter specifies how many failed login attempts are allowed per user account before an e-mail is sent to indicate that login failures are occurring. The range is 0 to 10. The default is 3.

Attempts before logout

(numAuthFailuresBeforeLockout)

The Attempts before logout parameter specifies how many failed login attempts are allowed per user account before that user account is locked out of the system. The range is 0, or 1 to 10 attempts. The default is 5 attempts. If you set the parameter to 0, account lockout functionality is disabled.

Client Timeout (minutes)

(guiTimeoutMinutes)

The Client Timeout (minutes) parameter specifies whether 5620 SAM clients shut down automatically after the configured number of minutes of inactivity. The range is 0, or 1 to 9999 min. The default is 0 for all clients. A value of 0 indicates that the client GUI expiry inactivity check functionality is disabled, and client GUIs are not shut down due to inactivity.

The parameter is configured system-wide when configured from the General tab. The parameter is configured for a user group when the [Override Global Timeout](#) parameter is enabled. The timeout value is 15 minutes for a user group. The setting affects clients that are connected to the 5620 SAM server.

Confirm Password

See the [Confirm Password](#) parameter in section [161.1](#).

Created In

(addToSpanAction)

The Created In parameter specifies which spans a newly created service is added to. Table [135-1](#) describes the parameter options.

Table 135-1 Created In parameter

Option	Description
Edit Spans common to user (default)	Each service created by a user associated with the rule is added only to the spans that the user has in common with the rule.
All listed Spans	Each service created by a user associated with the rule is added to each span listed in the rule.

Description

See the [Description](#) parameter in section 161.1.

E-mail Address

(fromEmailAddress)

The E-mail Address parameter specifies the address to which an e-mail message is sent if the number of login attempts exceeds the value of the Attempts before lockout parameter. The e-mail message sent is specified using the E-mail text parameter. The value is a valid e-mail address of up to 80 characters using the format *name@name.extension*.

E-mail Subject

(authFailureNotificationSubject)

The E-mail Subject parameter specifies the subject line of the email sent to the user email address. The range is 0 to 80 characters. The default for authentication failures is 'Authentication Failure'. You cannot use double quotes in the text.

E-mail Subject

(suspendedNotificationSubject)

The E-mail Subject parameter specifies the subject line of the email sent to the user email address. The range is 0 to 80 characters. The default for suspended account email is Account Suspended. The default for authentication failure is 'Authentication Failure'. You cannot use double quotes in the text.

E-mail text

(authFailureNotificationText)

The E-mail text parameter specifies the e-mail message to be sent when the number of login attempts exceeds the value of the Attempts before lockout parameter. The range is 0 to 1024 characters. The default for authentication failure is 'Enter authentication failure email notification text here'. The default for suspended account email is 'Enter account suspended email notification text here'. You cannot use double quotes in the text.

E-mail text

(suspendedNotificationText)

The E-mail text parameter specifies the e-mail message to be sent when the account is to be suspended. The range is 0 to 1024 characters. The default is 'Enter account suspended email notification text here'. You cannot use double quotes in the text.

E-mail User Name

(mailUserId)

The E-mail User Name parameter specifies the outgoing SMTP e-mail user name. The range is 0 to 80 characters. The default is N/A.

E-mail User Password

(mailUserPasswd)

The E-mail User Password parameter specifies the outgoing SMTP mail server password. The range is 0 to 80 characters. There is no default.

Enable IP Address validation

(enableClientIpAddressValidation)

The Enable IP Address validation parameter specifies whether a user must log in to the 5620 SAM using a client with a valid IP address specified by the [Valid Client IP address](#) parameter. The options are:

- True
- False (default)

Enable

The Enable parameter specifies whether to enable or disable the ability to configure the [Maximum Sessions Allowed](#) parameter. The options are:

- enabled
- disabled (default)

Enabled

(statementEnabled)

The Enabled parameter specifies whether to display a login statement to client GUI users on the login screen. You must be logged in to the client GUI with administrator privileges to view the parameter. The options are:

- Enabled
- Disabled (default)

LI Filter Lock

(liFilterLock)

The LI Filter Lock parameter specifies which types of users are permitted to modify or delete base IPv4 and MAC filters referenced by an LI Source. 5620 SAM LI user privileges are required to view or modify this parameter. The options are:

- Locked: no users can modify the LI filters
- Unlocked For LI Users: only users with LI privileges can modify the LI filters
- Unlocked For All: all users can modify the LI filters

The default is Locked.

Maximum GUI Sessions Allowed

(maxSessionsAllowed)

The Maximum GUI Sessions Allowed parameter specifies the number of concurrent remote client GUI sessions allowed for the same user account. The parameter is configurable when the Enable check box beside the parameter is selected. When the parameter is configured, the 5620 SAM displays an error if the user tries to open a session that exceeds the allowable limit. The range is 1 to the 5620 SAM Operator Positions value in the 5620 SAM license. There is no default.

Maximum OSS Sessions Allowed

(maxOssSessionsAllowed)

The Maximum OSS Sessions Allowed parameter specifies the number of concurrent remote OSS client sessions allowed for the same user account. The parameter is configurable when the Enable check box beside the parameter is selected. The range is 1 to 30. There is no default.

Maximum Sessions Allowed

(maxSessionsAllowed)

The Maximum Sessions Allowed parameter specifies the number of concurrent client GUI sessions allowed for the user account. The parameter is configurable when the Enable check box beside the parameter is selected. When the parameter is configured, the 5620 SAM displays an error if the user tries to open a session that exceeds the allowable limit.

When the Maximum User Sessions Allowed parameter is enabled, the value for the Maximum Sessions Allowed parameter cannot exceed the Maximum User Sessions Allowed parameter value for any user account in the selected user group.

The range is 1 to the 5620 SAM Operator Positions value in the 5620 SAM license. There is no default.

Maximum User Sessions Allowed

(maxUserSessionsAllowed)

The Maximum User Sessions Allowed parameter specifies the number of concurrent client GUI sessions allowed for the user group. The parameter is configurable when the Enable check box beside the parameter is selected. When the parameter is configured, the 5620 SAM displays an error if the user tries to open a session that exceeds the allowable limit.

When the Maximum Sessions Allowed parameter is enabled, the value for the Maximum User Sessions Allowed parameter must be greater than or equal to the Maximum Sessions Allowed parameter value for any user account in the selected user group.

The range is 1 to the 5620 SAM Operator Positions value in the 5620 SAM license. There is no default.

Minimum User Name Length Allowed

(minUserNameLengthAllowed)

The Minimum User Name Length Allowed parameter specifies a minimum length for user names. This parameter is configurable when the Enable check box is selected.

Once the parameter is configured, existing user names are verified against the minimum length. The user will be prompted to delete the existing user names if the length is below the minimum user name length. The range is 5 to 40 characters.

Name

(spanRuleName)

The Name parameter specifies the name of the span rule. The range is 1 to 40 characters. There is no default.

Override Global Timeout

(guiTimeoutOverride)

The Override Global Timeout parameter specifies whether to use the same client inactivity check for all clients in the system, or whether to specify an inactivity check for all users in a specific user group. The options are:

- enabled
- disabled (default)

When the parameter is disabled, the client inactivity check is governed by a global value applicable to all clients. When the parameter is enabled, you can specify the [Client Timeout \(minutes\)](#) parameter for the user group. For user accounts associated with the modified user group, the new inactivity check period applies.

For example, if there is a user group created that allows users to view but not manage incoming alarms, and no configuration actions take place using that client GUI, you can disable the GUI inactivity check for a specific user group by setting the parameter to enabled and setting the [Client Timeout \(minutes\)](#) parameter to 0, indicating that the inactivity check is disabled.

Password Change Required

The First Time Login Password Change parameter specifies whether a user is prompted to enter a new password before they can login for the first time. The options are:

- disabled (default)
- enabled

Password Expiry

(passwordExpiryEnabled)

The Password Expiry parameter specifies whether the 5620 SAM should track how long an account password remains dormant. When a user password is not used for the number of days specified in the Password Expiry (days) parameter, the password is removed from the system and another password must be created for the account. The options are:

- Enabled
- Disabled (default)

Password Expiry (days)

(passwordValidityPeriod)

The Password Expiry (days) parameter specifies the threshold for how long a user account password can be used before the password must be modified. The range is 0, or 1 to 365 days. The default is 90 days. If you set the parameter to 0, password expiry functionality is disabled.

Password History Duration (days)

(passwordHistoryDuration)

The Password History Duration (days) parameter specifies how many days a history of previous passwords used for an account will be preserved. The range is 0 to 365. The default is 180.

Password Reuse Cycle

(passwordHistoryCount)

The Password Reuse Cycle parameter specifies the number of unique passwords required before a password can be reused. The range is 0 to 12. The default is 5.

Priority

(priority)

The Priority parameter specifies the priority that the 5620 SAM assigns to user requests. When the parameter is configured for a user group, the setting applies only to remote users in the group. When the parameter is configured for a user account, the setting applies only to the user account. The options are:

- Low (default)
- Medium
- High

Profile ID

(scopeOfCommandProfileId)

The Profile ID parameter specifies a unique ID for the scope of command profile. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled.

Profile Name

(profileName)

The Profile Name parameter specifies the scope of command profile name. The range is 1 to 80 characters.

Profile Name

(profileName)

The Profile Name parameter specifies the span of control profile name. The range is 1 to 80 characters.

Remote User

(isRemote)

The Remote User parameter specifies whether a user account is defined in a remote authentication server. The parameter is disabled by default.

Reserve Administrator Login

(reserveAdminEnabled)

The Reserve Administrator Login parameter specifies whether an administrator can reserve a login name. The options are:

- enabled
- disabled

Reserve Administrator Login

(reserveAdminEnabled)

The Reserve Administrator Login parameter specifies whether to reserve one client GUI session, from the total number of sessions allowed based on the license key, for admin login only. The options are:

- disabled (default)
- enabled

Retention Time (hours)

(retentionInterval)

The Retention Time (hours) parameter specifies the minimum time, in hours, that the NE stores log files. A log file that is not transferred from the NE before the retention time is reached is deleted if the NE requires additional storage space. The range is 1 to 8760. The default is 720.

Ensure that the NE resources are sufficient to support the policy specifications. The parameter value must be appropriate for the NE, and the statistics must be regularly retrieved from the NEs.

Role ID

(roleId)

The Role ID parameter specifies a unique number for the scope of command role. The range is 1 to 65 535. The default is 0, which means that the parameter is not configured.

Role Name

(displayName)

The Role Name parameter specifies a unique name for the scope of command role. The range is 1 to 80 characters.

Server

(outGoingServerMail)

The Server parameter specifies the outgoing SMTP mail server IP address. There is no default.

Span ID

(spanId)

The Span ID parameter specifies the administrator-defined or default span of control ID to be assigned to identify the span.

Span Name

(spanName)

The Span Name parameter specifies the user-defined name for the span. The range is 0 to 80 characters. There is no default.

Span Rule ID

(spanRuleId)

The Span Rule ID parameter specifies the numeric identifier of the span rule. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 5 000 000. There is no default.

Statement

(statement)

The Statement parameter specifies the content of the login message that client GUI users view before they log in to a client GUI session. You must be logged in to the client GUI with administrator privileges to configure the parameter. The range is 0 to 2000 characters. You must set the [Enabled](#) parameter before the statement is displayed at log in. When you do not enter a value for the parameter, a value of N/A is automatically assigned, and can be viewed when users log in. You cannot use double quotes in the text.

Test Message

(testEmailMessage)

The Test Message parameter specifies the text message that is displayed in the test e-mail that is received when a successful test of the validity of the user e-mail address is achieved. The range is 0 to 1024 characters. The default text is Enter a test message here.

Threshold Reporting State

The Threshold Reporting State parameter specifies whether to generate threshold alarms when the number of log entries exceeds Max Log Record parameter value. The options are:

- Up (default)
- Down

User Group

(defaultSystemGroupAttributePtr)

The User Group parameter specifies a user group in the 5620 SAM that represents the default user group for remote-only users (temporary 5620 SAM user account). The User Group parameter is used when remote authentication is enabled and the remote authentication server does not provide the user group to which the user belongs to the 5620 SAM. The options are:

- enabled
- disabled (default)



Note — A LI user group cannot be set as the default external user group.

User Group

(groupName)

The User Group parameter specifies an administrator-defined group of users that are likely to perform similar tasks. The range is 5 to 40 characters. There is no default. You cannot use spaces in the user group name.

User Group State

(userGroupPointer)

The User Group State parameter specifies whether the user group is active in the 5620 SAM. The options are:

- active (default)
- suspended

User Name

(userName)

The User Name parameter specifies a unique identifier for an individual that uses the 5620 SAM. You cannot use spaces in the user name. User names are case sensitive. The range is 1 to 40 characters.

User Password

(password)

The User Password parameter specifies the password for a 5620 SAM user (not the currently logged in administrator's password). Passwords must use at least one numerical character, one special character, an upper-case character, and a lower-case character, and cannot be the same as the user account name. The range is 8 to 80 characters and must conform to the site password policies configured.

User State

(state)

The User State parameter specifies whether the user is active in the 5620 SAM and allowed to log in. The options are:

- active (default)
- suspended

Valid Client IP address

(validClientIpAddress)

The Valid Client IP Address parameter specifies the IPv4 address of a client used to access the 5620 SAM. When the [Enable IP Address validation](#) parameter is True, the user can only access the 5620 SAM from a client with the specified IP address. The default is 0.0.0.0.

136 –Change Password parameters

136.1 Change Password parameters 136-2

136.1 Change Password parameters

This chapter describes the parameters on the Password Change form.

Confirm Password

The Confirm Password parameter specifies the password that was entered for a 5620 SAM user for confirmation purposes. The range is 8 to 100 characters and must match the value entered in the [New Password](#) parameter.

New Password

(password)

The New Password parameter specifies a new password for a currently logged in user. The characters entered for this parameter must conform to the rules for password creation. The range is 8 to 100 characters.

Passwords must use at least one numerical character, one special character, an upper-case character, and a lower-case character, and cannot be the same as the user account name. See the chapter [10](#) for more information.

Old Password

(password)

The Old Password parameter specifies the current password of a current user account. The range is 5 to 100 characters.

137 –TCP Key Chains parameters

137.1 TCP Key Chains parameters 137-2

137.1 TCP Key Chains parameters

This chapter describes the parameters on the TCP KeyChains form and child forms.

Admin State

(adminState)

The Admin State parameter specifies the administrative state of the key chain or key. The options are:

- In Service (default)
- Out Of Service

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 161.1.

Begin Time

(beginTime)

The Begin Time parameter specifies the time after which the NE uses the key to sign or authenticate the protocol stream. Manually enter a date in yyyy/MM/dd HH:mm format, or use the calendar icon beside the parameter to choose a value. The default is Forever. When the parameter value is set to Forever, the key is not active or used as an eligible key.

Displayed Name

(keyChainName)

See the [Displayed Name](#) parameter in section 161.1.

Description

(chainDescription)

See the [Description](#) parameter in section 161.1.

End Time

(endTime)

The End Time parameter specifies the time until which the NE uses the key to sign or authenticate the protocol stream. The parameter is configurable when the [Key Direction](#) parameter is set to Receive. Manually enter a date in yyyy/MM/dd HH:mm format, or use the calendar icon beside the parameter to choose a value. The default is Forever. When the parameter value is set to Forever, the key is valid indefinitely.

Key

(sharedSecret)

The Key parameter specifies the shared secret value that the 5620 SAM uses as input for the algorithm specified by the [Secret Key Algorithm](#) parameter to sign or authenticate a protocol packet. Specify an alphanumeric value, or accept the value that the 5620 SAM provides. The range is 1 to 20 characters. The default value is a random value that the 5620 SAM generates.



Note — For security reasons, Alcatel-Lucent recommends that you accept the default value that the 5620 SAM generates.

Key Direction

(keyDirection)

The Key Direction parameter specifies the protocol-stream direction to which an NE applies the key. The options are:

- Send
- Receive
- Send-Receive



Caution — Alcatel-Lucent recommends that you choose the Send-receive option to ensure bidirectional communication between NEs.

Key ID

(keyId)

The Key ID parameter specifies a numeric value that the 5620 SAM combines with the [Displayed Name](#) and [Key Direction](#) parameter values to create a unique identifier for the key. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 0 to 63.

Receive Option

(receiveTcpOptionNumber)

The Receive Option parameter specifies the TCP option value in a received TCP header that is associated with the key chain. The options are:

- 253
- 254 (default)
- All

Secret Key Algorithm

(algorithm)

The Secret Key Algorithm specifies the algorithm that is used to sign or authenticate the secret key. The options are:

- AES-128-CMAC-96 (default)
- HMAC-SHA-1-96

Send Option

(sendTcpOptionNumber)

The Send Option parameter specifies the TCP option value in a TCP header that the NE sends to another device. The options are:

- 253
- 254 (default)
- All

Tolerance (seconds)

(tolerance)

The Tolerance parameter specifies the time, in seconds, that an eligible receive key overlaps with an active send key. The parameter is configurable when the [Key Direction](#) parameter is set to Receive or Send-Receive. The range is 0 to 4 294 967 295. The default is 300.

138 –5620 SAM RADIUS/TACACS+ User Authentication parameters

**138.1 5620 SAM RADIUS/TACACS+ User Authentication
parameters 138-2**

138.1 5620 SAM RADIUS/TACACS+ User Authentication parameters

This chapter describes the parameters on the Remote Authentication Manager form and its child forms.

Address

See the [Address](#) parameter in section [161.1](#).

Administrative State

See the [Administrative State](#) parameter in section [161.1](#).

Authentication Order 1

(authOrder1)

The Authentication Order parameters are used to indicate the preferred type and order of password authentication used to verify the 5620 SAM user account. The value of the parameter is the first method of authentication, followed by the values for the two other authentication orders. Table [138-1](#) describes the parameter options.

Table 138-1 Authentication Order 1 parameter

Option	Option description	Dependencies
none	Specifies that no authentication type is used	—
local (default)	Specifies that locally-managed 5620 SAM password authentication is required, based on the passwords assigned by the system administrator	
radius	Specifies that RADIUS server password authentication is required	
tacplus	Specifies that TACACS+ server password authentication is required	

Authentication Order 2

(authOrder2)

See the [Authentication Order 1](#). The default is tacplus

Authentication Order 3

(authOrder3)

See the [Authentication Order 1](#). The default is radius.

Description

See the [Description](#) parameter in section 161.1.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

Exit On Reject

See the [Exit On Reject](#) parameter in section 161.1.

Port

See the [Port](#) parameter in section 161.1.

Retry Attempts

See the [Retry Attempts](#) parameter in section 161.1.

Secret

See the [Secret Name](#) parameter in section 161.1.

Single Connection

See the [Single Connection](#) parameter in section 161.1.

Timeout (seconds)

See the [Timeout \(seconds\)](#) parameter in section 161.1.

139 –NE Management Access Filters parameters

139.1 NE Management Access Filters parameters 139-2

139.1 NE Management Access Filters parameters

This chapter describes the parameters on the NE Management Access Filters form and child forms.

Action

(action)

The Action parameter specifies whether a packet that matches the selection criteria is permitted or denied access to the site. Table 139-1 describes the parameter options.

Table 139-1 Action parameter

Option	Option description	Dependencies
none	Specifies that no default action is set	—
permit	Specifies that packets that match the configured selection criteria are permitted	
deny	Specifies that packets that match the configured selection criteria are denied and an ICMP host unreachable message is sent	When you set the parameter to deny, you cannot distribute the policy to the managed device. Before setting the parameter to deny, set the parameter to permit, distribute the configuration to the managed devices, then reconfigure the parameter to deny.
Deny Host U unreachable	Specifies that packets that match the configured selection criteria are denied and a host unreachable message is sent	—

Administrative Status

See the [Administrative State](#) parameter in section 161.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 161.1.

Configuration Mode

See the [Configuration Mode](#) parameter in section 161.1.

Default Filter Action

(defaultAction)

The Default Filter Action parameter specifies which action is applied to any packets that do not meet the selection criteria. Site management access filters specify the type of access, for example, FTP or Telnet, allowed on the managed devices. These specifications apply to all users that access the device. Table 139-2 describes the parameter options.

Table 139-2 Default Filter Action parameter

Option	Option description	Dependencies
none (default)	Specifies that no default action is set	Cannot be set if one or more Site MAF Match Entries exist
permit	Specifies that packets that do not match the configured selection criteria are permitted	—
deny	Specifies that packets that do not match the configured selection criteria are denied	
deny host unreachable	Specifies that packets that do not match the configured selection criteria are denied and a host unreachable message is sent	

Description

See the [Description](#) parameter in section 161.1.

Destination Port

(destinationPort)

The Destination Port parameter specifies the destination UDP or TCP port number. Packets matching the specified port number is permitted or denied based on the option chosen by the Action parameter. The range is 0 to 65 535. The default is 0.

Destination Port Mask

(destinationPortMask)

The Destination Port Mask parameter specifies the mask bits to use, if any, when setting the Destination Port parameter. Packets matching the specified port mask are permitted or denied based on the option chosen by the Action parameter. This parameter is not configurable if the Destination Port parameter is not set. The range is 0 to 65 535. The default is 65 535.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

ID

See the [ID](#) parameter in section 161.1.

Protocol

See the [Protocol](#) parameter in section 161.1.

Source IP

See the [Source IP](#) parameter in section [161.1](#).

Source IP Mask

See the [Source IP Mask](#) parameter in section [161.1](#).

Source Port ID

(sourcePortName)

The Source Port ID parameter specifies the address of the source port. Use the format slot/daughtercard/port. For example, to configure port 3 on daughter card 2 on card 6, enter 6/2/3. This parameter is configurable when the Source Port Type parameter is set to port or lag. The range is 0 to 30 characters.

Source Port Type

(portType)

The Source Port Type parameter specifies that incoming packets are restricted and must be sent by one of the specified port types to match the criteria specified in the Source IP and Source IP Mask parameters. Packets matching the specified port type are permitted or denied based on the option chosen by the Action parameter. Table [139-3](#) describes the parameter options.

Table 139-3 Source Port Type parameter

Option	Option description	Dependencies
any (default)	Specifies that incoming packets from any port are permitted or denied access using any of the specified port types	—
cpm	Specifies to configure the Ethernet port on the primary CPM to match the criteria	
port	Specifies that incoming packets from a specific port, as identified by the Source Port ID parameter, are permitted or denied	You can configure the Source Port ID parameter
lag	Specifies that incoming packets from a specific LAG, as identified by the Source Port ID parameter, are permitted or denied	

140 –NE CPM Filter parameters

140.1 NE CPM Filter parameters 140-2

140.1 NE CPM Filter parameters

This chapter describes the parameters on the NE CPM Filter form.

Action

(action)

The Action parameter specifies whether a packet that matches the selection criteria is permitted or denied access to the site. Table 140-1 describes the parameter options.

Table 140-1 Action parameter

Option	Option description	Dependencies
drop (default)	Specifies that packets that match the configured selection criteria are dropped	—
forward	Specifies that packets that match the configured selection criteria are forwarded	
queue	Specifies that packets that match the configured selection criteria are sequentially queued for transmission.	
default	Specifies that packets that match the configured selection criteria inherit the default CPM filter action	

Administrative Status

See the [Administrative State](#) parameter in section 161.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 161.1.

CIR (kb/s)

(cir)

The CIR (kb/s) parameter specifies the administrative committed information rate for a queue. The parameter specifies the rate at which the system prioritizes the queue over other queues that are competing for the same bandwidth.

The range is 0 to 100 000 000 kb/s, depending on the line rate of the object to which the policy is applied. You can also choose the MAX option, which specifies the maximum available CIR. When the MAX parameter is set to enabled, you cannot configure the CIR or PIR parameters. The default is 0.

Committed Burst Size (KB)

(committedBurstSize)

The Committed Burst Size (KB) parameter specifies the committed burst pool size for a queue and overrides the default reserved pool burst for the queue. The range is -1 to 131 072, with -1 indicating default. Default specifies that the device calculates committed burst pool size based on the CIR and the PIR. The default is default.

Configuration Mode

See the [Configuration Mode](#) parameter in section [161.1](#).

CFM Opcode

(cfmOpCodeOper)

The CFM Opcode parameter specifies the type of operation code that is performed in an NE CPM or MAF. If you set the CFM Opcode parameter to a value other than NONE, the values of the [CFM Val 1](#) and [CFM Val 2](#) are applied. The CFM Opcode parameter is applied only when the [Frame Type](#) parameter is set to e802dot1ag.

The options are:

- NONE (default)
- EQUAL
- RANGE
- LESS_THAN
- GREATER_THAN

CFM Val 1

(cfmOpCodeValue1)

The CFM Val 1 parameter specifies a value that is applied when you configure the [CFM Opcode](#) parameter. The range is 0 to 255. The default is 0.

CFM Val 2

(cfmOpCodeValue2)

The CFM Val 2 parameter specifies a value that is applied when you configure the [CFM Opcode](#) parameter. The range is 0 to 255. The default is 0.

Default Filter Action

(defaultAction)

The Default Filter Action parameter specifies which action is applied to any packets that match the selection criteria. Table [140-2](#) describes the parameter options.

Table 140-2 Default Filter Action parameter

Option	Option description	Dependencies
forward (default)	Specifies that packets matching the filter entry are forwarded	—
drop	Specifies that packets matching the filter entry are dropped	

Description

See the [Description](#) parameter in section [161.1](#).

Destination IP

([destinationIpAddress](#))

The Destination IP parameter, combined with the Destination Mask parameter, specifies a destination IP address range as a match. When the parameter is enabled, specify an IPv4 address in dotted-decimal format, or an IPv6 address in colon-hexadecimal format. The default is 0.0.0.0 for IPv4 or 0:0:0:0:0:0:0:0 for IPv6.

Destination MAC

([destinationMacAddress](#))

The Destination MAC parameter specifies a destination MAC address or range that is applied as a MAC filter match criterion in an NE CPM or management access (destination service access point) filter. Specify a MAC address in colon-hexadecimal format. The default is 00-00-00-00-00-00.

Destination Mask

Table [140-3](#) lists where to find more information about the Destination Mask parameter.

Table 140-3 Destination Mask parameter

Parameter	See
IP mask value to use as a match criterion for the specified destination IP address	Destination Mask parameter in this section
Port mask value to use as a match criterion for the destination port of the packet	Destination Mask parameter in this section

Destination Mask

([destinationIpAddressMask](#))

The Destination Mask parameter specifies the IP mask value to use as a match criterion for the specified destination IP address. The parameter is configurable when the Destination IP parameter is enabled. The range is 0 to 32 for an IPv4 mask or 0 to 128 for an IPv6 mask. The default is 0.

Destination Mask

(destinationPortMask)

The Destination Mask parameter specifies the 16-bit mask to be applied when matching the destination TCP/UDP port. The parameter is configurable when the Destination Port parameter is enabled. The range is 0 to 65535. The default is 0.

Destination Port

(destinationPort)

The Destination Port parameter specifies the TCP/UDP port to match the destination port of the packet. The range is 0 to 65535. The default is disabled and 0.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

Dot1p

(dot1pValue)

The Dot1p parameter specifies an IEEE 802.1p value that is applied as a MAC filter match criterion in an NE CPM or MAF. The dot1p match criterion fails for the frame when a frame is missing the 802.1p bits. The options are:

- | | |
|--------------------------|-----|
| • Not Set (-1) (default) | • 4 |
| • 0 | • 5 |
| • 1 | • 6 |
| • 2 | • 7 |
| • 3 | |

Dot1p Mask

(dot1pMask)

The Dot1p Mask parameter specifies the mask that is applied as a MAC filter match criterion in an NE CPM or MAF. The options are:

- | | |
|---------------|-----|
| • 0 (default) | • 4 |
| • 1 | • 5 |
| • 2 | • 6 |
| • 3 | • 7 |

DSCP

(dscp)

The DSCP parameter specifies the DiffServ Code Point value to be used as the CPM IP filter match criterion. When a packet is marked with the value specified by the DSCP parameter, the packet is mapped to the priority specified by the Priority parameter. Table 140-4 lists the parameter options.

Table 140-4 DSCP parameter

Options			
be (default)	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43

DSAP

(dsap)

The DSAP parameter specifies an Ethernet 802.2 LLC destination service access point (DSAP) value that is applied as a MAC filter match criterion in an NE CPM or management access filter. The range is -1 to 255. The default is -1.

DSAP Mask

(dsapMask)

The DSAP Mask parameter specifies the mask that is applied as a MAC filter match criterion in an NE CPM or MAF. The range is -1 to 255. The default is -1.

Dst Mask

(destinationMacAddressMask)

The Dst Mask parameter specifies the 48-bit mask to match a range of MAC address values in an NE CPM or management access filter. Specify a MAC address in colon-hexadecimal format. The default is 00-00-00-00-00-00. The Dst Mask parameter is configurable when the [Destination MAC](#) parameter is enabled.

Entry ID

(id)

The Entry ID parameter specifies a unique identifier for the filter entry. The entry ID determines the order of all entry IDs within a specific filter ID. Packets are compared to entry IDs in ascending order. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 2048. The default is 0.

Ether Type

(ethernetType)

The Ether Type parameter specifies an Ethernet type II Ethertype value that is applied as a MAC filter match criterion in an NE CPM or MAF. The Ether Type parameter is a two-byte field that is used to identify the protocol carried by the Ethernet frame. The range is -1 to 65 535. The default is -1.

Flow Label

(flowLabel)

The Flow Label parameter specifies the flow identifier in an IPv6 packet header. Flow labeling is used to label packets that belong to specific traffic flows for which the sender requests special handling. The range is 0 to 1 048 575. The default is 0.

Fragment

(fragment)

The Fragment parameter specifies whether fragmented or non-fragmented packets are used as the match criterion for mapping packets to a forwarding class and queue priority. Fragmented packets have either the MF bit set, or have the Fragment Offset field of the IP header set to a non-zero value.

The options are:

- off (default)
- false
- true

Frame Type

(frameType)

The Frame Type parameter specifies the Ethernet frame type that is applied as the MAC filter match criterion in an NE CPM or MAF. Table 140-5 describes the parameter options.

Table 140-5 Frame Type parameter

Option	Description	Dependencies
none (default)	No frame type is used for filter match criteria	Supported only for CPM MAC match entries
e802dot3	Specifies that the frame type is Ethernet IEEE 802.3	Supported only for MAC MAF match entries
e802dot1ag	Specifies that the frame type is Ethernet IEEE 802.1 ag	—
e802dot2LLC	Specifies that the frame type is Ethernet IEEE 802.2 LLC	—
e802dot2SNAP	Specifies that the frame type is Ethernet IEEE 802.2 SNAP	Supported only for MAC MAF match entries
Ethernet II	Specifies that the frame type is Ethernet Type II	—

ICMP Code

(icmpCode)

The ICMP Code parameter specifies using the ICMP code field in the ICMP header of an IP packet as the filter match criterion. You can configure this parameter when the Protocol parameter is set to ICMP. The range is 1 to 255. The default is 1.

ICMP Type

(icmpType)

The ICMP Type parameter specifies using the ICMP type field in the ICMP header of an IP packet as the filter match criterion. You can configure this parameter when the Protocol parameter is set to ICMP. The range is 1 to 255. The default is 1.

ID

(id)

The ID parameter specifies a unique ID for the queue. The range is 33 to 2000. The default is 0.

IP Option

(ipOptionValue)

The IP Option parameter specifies the optional header field to be included in a packet as a match criterion for the filter. Table 140-6 describes the parameter options.

Table 140-6 IP Option parameter

Option	Option description	Dependencies
EOOL (000) (default)	End of Options List	—
NOP (001)	No Operation	
RR (007)	Record Route	
ZSU (010)	Experimental Measure	
MTUR (012)	MTU Reply	
MTUP (011)	MTU Probe	
ENCODE (015)	—	
TS (068)	Time Stamp	
TR (082)	Traceroute	
SEC (130)	Security	
LSR (131)	Loose Source Route	
E_SEC (133)	Extended Security	
CIPSO (134)	Commercial Security	
SID (136)	Stream ID	
SSR (137)	Strict Source Route	
VISA (142)	Experimental Access Control	
IMITD (144)	IMI Traffic Descriptor	
EIP (145)	Extended Internet Protocol	
ADDEXT (147)	Address Extension	
RTRALT (148)	Router Alert	
SDB (149)	Selective Directed Broadcast	
NSAPA (150)	NSAP Addresses	
DPS (151)	Dynamic Packet State	
UMP (152)	Upstream Multicast Packet	
FINN (205)	Experimental Flow Control	

IP Option Mask

(ipOptionMask)

The IP Option Mask parameter specifies the IP mask value to use as an additional match criterion for the specified IP Option parameter. The range is 0 to 255. The default is 0.

IPv6 Administrative Status

(`ipv6AdministrativeStatus`)

The IPv6 Administrative Status parameter specifies whether IPv6 is enabled for the IP filter policy. The options are:

- Down (default)
- Up

MAX

The MAX parameter specifies whether the PIR (kbps) parameter or CIR (kbps) parameter is set to infinity or can be configured. The options are:

- disabled (default)
- enabled

When the MAX parameter is set to enabled, you cannot configure the CIR or PIR parameters.

Maximum Burst Size (KB)

(`maximumBurstSize`)

The Maximum Burst Size (KB) parameter specifies the maximum burst pool size for a queue and overrides the default reserved burst pool for the queue. The range is -1 to 131 072, with -1 indicating default. Default specifies that the device calculates committed burst pool size based on the CIR and the PIR. The default is default.

Multiple Option

(`multipleOption`)

The Multiple Option parameter specifies whether to perform a match for a packet that contains more than one optional header field. This parameter is configurable when the Option Present parameter is enabled. Table 140-7 describes the parameter options.

Table 140-7 Multiple Option parameter

Option	Option description	Dependencies
off (default)	Specifies that filtering for this parameter is disabled.	—
false	Does not match when a packet contains more than one optional header field.	
true	Matches when a packet contains more than one optional header field.	

Next Header

See the [Protocol](#) parameter in section 161.1 for more information.

Option Present

(optionPresent)

The Option Present parameter specifies whether to perform a match on a packet that contains an optional header field. Table 140-8 describes the parameter options.

Table 140-8 Option Present parameter

Option	Option description	Dependencies
off (default)	Specifies that filtering for this parameter is disabled.	—
false	Does not match when a packet contains an optional header field.	
true	Matches when a packet contains an optional header field.	

PIR (kb/s)

(pir)

The PIR (kb/s) parameter specifies the administrative peak information rate for a queue. The parameter specifies the maximum rate that the queue can transmit packets. Specifying a value for the PIR parameter does not guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.

The range is 1 to 100 000 000 kb/s, dependant on the line rate of the object to which the policy is applied. You can also choose the MAX option, which specifies the maximum available PIR. When the MAX parameter is set to enabled, you cannot configure the CIR or PIR parameters. The default is MAX.

Protocol

See the [Protocol](#) parameter in section 161.1.

Queue ID

(id)

The Queue ID parameter specifies an integer value that identifies a CPM queue. You can configure the parameter when the [Action](#) parameter is set to queue. The range is 33 to 2000. The default is 0.

Routing Instance

(routingInstanceFor)

The Routing Instance parameter specifies the criteria used to choose the routing instance. The options are:

- none (default)
- base
- management

For example, when you set the parameter to base, the filter match is done on the base routing instance of the managed device.

Service Id

The Service Id parameter specifies the service ID that is applied as a MAC filter match criterion in an NE CPM or management access filter.

SNAP OUI

(snapOui)

The SNAP OUI parameter specifies an IEEE 802.3 LLC subnetwork access protocol (SNAP) Ethernet frame OUI zero or non-zero value that is applied as a MAC filter match criterion in an NE CPM or MAF. Table 140-9 describes the parameter options.

Table 140-9 SNAP OUI parameter

Option	Description	Dependencies
off	—	—
zero	Specifies that packets with the three-byte SNAP OUI field in the SNAP ID set to zero must be matched	—
Non Zero	Specifies that packets with the three-byte SNAP OUI field in the SNAP-ID not set to zero must be matched	—

SNAP PID

(snapPid)

The SNAP PID parameter specifies an IEEE 802.3 LLC subnetwork access protocol Ethernet frame ID value that is applied as a MAC filter match criterion in an NE CPM or management access filter. The range is -1 to 65 535. The default is -1.

Source IP

See the [Source IP](#) parameter in section 161.1.

Source IP Mask

See the [Source IP Mask](#) parameter in section 161.1.

Source MAC

(sourceMacAddress)

The Source MAC parameter specifies the source MAC address or range that is applied as a MAC filter match criterion in an NE CPM or MAF. Specify the 48-bit IEEE MAC address in colon-hexadecimal format. The default is 00-00-00-00-00-00.

Source Mask

Table [140-10](#) lists where to find more information about the Source Mask parameter.

Table 140-10 Source Mask parameter

Parameter	See
IP mask value to use as a match criterion for the specified source IP address	Source Mask parameter in this section
Port mask value to use as a match criterion for the source port of the packet	Source Mask parameter in this section

Source Mask

(sourceIpAddressMask)

The Source Mask parameter specifies the IP mask value to use as a match criterion for the specified source IP address. The parameter is configurable when the Source IP parameter is enabled. The range is 0 to 32 for IPv4 IP addresses and 0 to 128 for IPv6 IP addresses. The default is 0.

Source Mask

(sourcePortMask)

The Source Mask parameter specifies the 16-bit mask to be applied when matching the source TCP/UDP port. The parameter is configurable when the Source Port parameter is enabled. The range is 0 to 65 535. The default is 0.

Source Port

(sourcePort)

The Source Port parameter specifies the TCP/UDP port to match the source port of the packet. The range is 0 to 65535. The default is disabled and 0.

Src Mask

(sourceMacAddressMask)

The Src Mask parameter specifies the 48-bit mask that must match a range of MAC addresses in an NE CPM or management access filter. Specify a MAC address in colon-hexadecimal format. The default is 00-00-00-00-00-00. The Src Mask parameter is configurable when the [Source MAC](#) parameter is enabled.

SSAP

(ssap)

The SSAP parameter specifies an Ethernet 802.2 LLC source SSAP for a MAC filter match criterion. This is a one-byte field that is part of the 802.2 LLC header of the IEEE 802.3 Ethernet Frame. The range is -1 to 255. The default is -1.

SSAP Mask

(ssapMask)

The SSAP Mask parameter specifies the mask that is applied as a MAC filter match criterion in an NE CPM or management access filter. The range is -1 to 255. The default is -1.

TCP Ack

(tcpAck)

The TCP Ack parameter specifies matching on the ACK bit in the TCP header of an IP packet as the filter match criterion. The parameter is configurable when the TCP Syn parameter is enabled. The options are:

- off (default)
- false
- true

TCP Syn

(tcpSyn)

The TCP Syn parameter specifies matching on the SYN bit in the TCP header of an IP packet as the filter match criterion. The SYN bit is normally set when the packet source initiates a TCP session with the specified destination IP address. The options are:

- off (default)
- false
- true

141 –NE DoS Protection parameters

141.1 NE DoS Protection parameters 141-2

141.1 NE DoS Protection parameters

This chapter describes the parameters on the NE DoS Protection form.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 161.1.

Description

See the [Description](#) parameter in section 161.1.

Level Set

(levelSet)

The Level Set parameter specifies one or more MEG levels. You must specify at least one MEG level. There is no default. The options are:

- 0
- 1
- 2
- 3
- 4
- 5
- 6
- 7

Overall Rate Limit (pps)

(overallRateLimit)

The Overall Rate Limit (pps) parameter specifies the maximum rate, in packets per second, at which the interfaces and SAPs on the NE can collectively receive network-control protocol packets. The range is –1, which means that there is no maximum rate, or 1 to 65 534. The default is 6000.

Out Profile Rate (pps)

(outProfileRate)

The Out Profile Rate (pps) parameter specifies the maximum rate, in packets per second, at which incoming control packets are marked out of profile. The range is –1, which means that there is no maximum rate, or 1 to 65 534. The default is 3000.

Packet Rate Limit (pps)

(packetRateLimit)

The Packet Rate Limit (pps) parameter specifies the maximum rate, in packets per second, at which the NE receives packets from a specific subscriber or subscriber host. The range is –1, or 1 to 65 534. The default is –1, which means that there is no maximum rate.

Policy ID

(id)

The Policy ID parameter specifies a unique ID for the NE DoS protection policy, or for a CFM frame-rate limiting entry in a DoS protection policy. The parameter is configurable for a DoS protection policy when the [Auto-Assign ID](#) parameter is disabled. The default is 0, which means that the parameter is not configured. Table [141-1](#) lists the parameter range for different objects.

Table 141-1 Policy ID parameter

Object	Range
CFM frame-rate limiting entry in DoS protection policy	1 to 100
DoS protection policy	1 to 255

Receive Notification

(polAlarm)

The Receive Notification parameter specifies whether the NE generates an event if the [Packet Rate Limit \(pps\)](#) or [Overall Rate Limit \(pps\)](#) parameter value is exceeded. The options are:

- true (default)
- false

142 –NE User Profiles parameters

142.1 NE User Profiles parameters 142-2

142.1 NE User Profiles parameters

This chapter describes the parameters on the NE User Profiles form and its child forms.

Action

(action)

The Action parameter specifies how to handle CLI commands that match the selection criteria specified in the Match String parameter. Table 142-1 describes the parameter options.

Table 142-1 Action parameter

Option	Option description	Dependencies
deny (default)	Specifies that CLI commands that match the value indicated in the Match String parameter are denied access to the site (router).	—
allow	Specifies that CLI commands that match the value indicated in the Match String parameter are permitted access to the site (router).	
none	Specifies that no default action is set	

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 161.1.

Configuration Mode

See the [Configuration Mode](#) parameter in section 161.1.

Default Profile Action

(defaultAction)

Specify the Default Profile Action parameter to determine how to handle CLI commands that do not match any of the configured profile entries. Table 142-2 describes the parameter options.

Table 142-2 Default Profile Action parameter

Option	Option description	Dependencies
deny	Specifies that CLI commands that do not match any of the configured Site User Profile Match Entries are denied access to the site (router).	—

(1 of 2)

Option	Option description	Dependencies
allow (default for administration account)	Specifies that CLI commands that do not match any of the configured Site User Profile Match Entries are permitted access to the site (router).	—
none (default for all accounts except administrative)	Specifies that no default action is set	—

(2 of 2)

Description

See the [Description](#) parameter in section 161.1.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

ID

See the [ID](#) parameter in section 161.1.

LI Profile

(liProfile)

The LI Profile parameter specifies whether the profile has LI privileges. The options are:

- True
- False (default)



Note — To configure the [LI Profile](#) parameter you must have LI privileges. See chapter 32 for more information about LI.

Match String

(matchString)

The Match String parameter specifies a CLI command prefix which defines the scope of the user profile. For example, when you set the match string to “config” and specify a deny action, the user profile cannot use any CLI commands that begin with “config”. CLI commands are forwarded or denied access to the site (router) based on the Action parameter value.

143 –NE User Configuration parameters

143.1 NE User Configuration parameters 143-2

143.1 NE User Configuration parameters

This chapter describes the parameters on the NE User Configuration form and child forms.

Access

(access)

The Access parameter specifies which functions the site user can access. You can choose one or more of the available options. By default, none of the options are selected. The options are:

- li
- snmp
- console (serial port or Telnet access)
- ftp



Note — To set the li value you must have LI privileges. See chapter [32](#) for more information about LI.

Additional ID

(id)

The Additional ID parameter specifies the additional identifier for the NE user. Setting the Additional ID parameter allows you to have multiple NE users with the same value for the [User Name](#) parameter. The range is 0 to 256. The default is 0.

Authentication Protocol

(snmpAuthProtocol)

The Authentication Protocol parameter specifies the authentication method to establish communication with the managed device. SNMP authentication allows the device to validate the managing node that issued the SNMP message and determine if the message has been tampered with. Table [143-1](#) describes the parameter options.

Table 143-1 Authentication Protocol parameter

Option	Option description	Dependencies
No Authentication (default)	Specifies that no checks, with the exception of a permission check of the user account, are performed.	The authentication protocol and associated passwords should match the authentication used on the devices where the accounts reside.
MD5	MD5 specifies that the authentication protocol can be HMAC-MD5-96 or HMAC-SHA-96. The password length is specified in the Set New Authentication Password parameters.	
SHA	SHA specifies that the authentication protocol can be either HMAC-MD5-96 or HMAC-SHA-96. The password length is specified in the Set New Authentication Password parameters.	

Configuration Mode

See the [Configuration Mode](#) parameter in section [161.1](#).

Confirm New Auth Password

(snmpAuthPassword2)

The Confirm New Auth Password parameter specifies the user's authentication password for confirmation purposes. The range is 0 to 80 characters.

Confirm New Privacy Password

(snmpPrivPassword2)

The Confirm New Privacy Password parameter specifies the user's privacy password for confirmation purposes. The range is 0 to 80 characters.

Confirm Password

(password2)

The Confirm Password parameter specifies the password for a local site user for confirmation purposes. The parameter value must match the Password parameter value. The range is 0 to 129 characters and must conform to the site password policies.

Console Cannot Change Password

(consoleCannotChangePassword)

The Console Cannot Change Password parameter specifies whether a user can change their password for both FTP and console login. The options are:

- true
- false (default)

When the parameter is set to true, the user cannot change their password for FTP and console login.

Console Login Exec File

(consoleLoginExecFile)

The Console Login Exec File parameter specifies the location of the user's login exec file which executes every time a user successfully logs in to a console session. The range is 0 to 200 characters. There is no default.

Console New Password At Login

(consoleNewPasswordAtLogin)

The Console New Password At Login parameter specifies whether the user must change their password at the next console or FTP login. The options are:

- true
- false (default)

Description

See the [Description](#) parameter in section [161.1](#).

Home Directory

(homeDirectory)

The Home Directory parameter specifies the default local home directory on the managed device for the user for both console and FTP access. The directory is specified as a URL or a URL/directory structure. If the Restrict to Home parameter is set to true, then no file access is granted for the user and no home directory is created. If the Restrict to Home parameter is set to false, then the root directory of the device becomes the default home directory. The range is 0 to 200 characters.

New Authentication Password

(snmpAuthPassword)

The New Authentication Password parameter specifies the initial authentication password when the user is created or modifies the password of an existing user. The range is 0 to 80 characters.

New Privacy Password

(snmpPrivPassword)

The New Privacy Password parameter specifies the initial privacy password when the user is created or modifies the password of an existing user. The range is 0 to 80 characters.

Password

(password)

The Password parameter specifies the password for a local site user, for console or ftp access. The range is 0 to 129 characters and must conform to the site password policies.

Privacy Protocol

(snmpPrivProtocol)

The Privacy Protocol parameter specifies the encryption method that the user must use to communicate with the managed device. The options are:

- No Privacy (default)
- DES

The DES option specifies the DES privacy key. The privacy password for the DES key is specified in the Set [New Privacy Password](#) parameters. The password should match the password configured on the managed device for the user that is using DES privacy.

Restrict to Home

(isRestrictedToHome)

The Restrict to Home parameter specifies whether a user can access other directories in addition to their home directory on the managed device. The options are:

- true
- false (default)

User Name

(displayName)

The User Name parameter specifies a unique name for the site user. You must configure the parameter. The range is 1 to 16 characters.

144 –NE Password Policy parameters

144.1 NE Password Policy parameters 144-2

144.1 NE Password Policy parameters

This chapter describes the parameters on the NE Password Policy form and child forms.

Admin Password

(adminPassword)

The Admin Password parameter specifies the password for an admin user, allowing another user account to have administration privileges on the managed device for one session. No RADIUS or TACACS+ authorization is performed. After the session ends, the Admin Password is no longer valid.

The length of the password depends on the hash or encryption used. The maximum length is 20 characters unhashed, 32 characters if hashed, and 54 characters if the hash2 keyword is specified.

Authentication Order 1

(authOrder1)

The Authentication Order parameters are used to indicate the preferred type and order of password authentication used to verify the user account password. Authentication is performed in order, from 1 to 3. The first authentication method is used, if it can be used successfully. If the first authentication method cannot be used, then the second authentication method is attempted. Table 144-1 describes the parameter options.

Table 144-1 Authentication Order 1 parameter

Option	Option description	Dependencies
none	Specifies that no authentication type is used	You must configure user accounts and password policies for each type of authentication used, for example, RADIUS and local 5620 SAM server authentication. System administrators need to manage the user accounts, as described in chapter 10.
local	Specifies that locally-managed device password database authentication is required	
radius (default)	Specifies that RADIUS server password authentication is required	
tacplus	Specifies that TACACS+ server password authentication is required	

Authentication Order 2

(authOrder2)

See the [Authentication Order 1](#). The default is tacplus.

Authentication Order 3

(authOrder3)

See the [Authentication Order 1](#). The default is local.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [161.1](#).

Complexity

(complexity)

The Complexity parameter specifies the types of characters that are required in a password. Table [144-2](#) describes the parameter options.

Table 144-2 Complexity parameter

Option	Option description	Dependencies
Numeric Characters	Specifies that at least one number must be included in the password, for example 3.	—
Mixed Case	Specifies that at least one uppercase and one lowercase character must be included in the password, for example, H and h.	
Special Characters	Specifies that at least one special character must be included in the password, for example, &.	

Configuration Mode

See the [Configuration Mode](#) parameter in section [161.1](#).

Confirm Password

The Confirm Password parameter specifies a confirmation of the [Admin Password](#) parameter. Enter the same value.

Days Before Expiration

(aging)

The Days Before Expiration parameter specifies the number of days that a password can be active before a new password must be entered. When the Password Never Expires parameter is enabled, this field is not configurable. The range is 1 to 500 days. The default is 500 days.

Description

See the [Description](#) parameter in section [161.1](#).

Exit on Reject

See the [Exit On Reject](#) parameter in section [161.1](#).

Health Check

(isPasswordHealthCheck)

The Health Check parameter specifies whether to perform RADIUS or TACACS+ server monitoring, to ensure that the servers are reachable. The options are:

- true (default)
- false

When the parameter is set to true, the servers are monitored for seconds at 30 second intervals. Events are generated to indicate when a server is unreachable or when a previously unreachable server becomes reachable.

Health Check Interval

(passwordHealthCheckInterval)

The Health Check Interval parameter specifies the server polling interval, in seconds, when you enable the [Health Check](#) parameter. The range is 6 to 1500. The default is 30.

ID

See the [ID](#) parameter in section [161.1](#).

Lockout Time (minutes)

(lockoutMinutes)

The Lockout Time (minutes) parameter specifies the amount of time a user is locked out of their account if they exceed the maximum number of password site attempts in the time specified by the value of the Maximum Attempts Time (minutes) parameter. The range is 0 to 1440 min. The default is 10 min.

Maximum Attempts

(attemptsCount)

The Maximum Attempts parameter specifies the maximum number of attempts to enter a password before the user is locked out of their account. Configure this parameter in conjunction with the Lockout Time (minutes) and the Maximum Attempts Time (minutes) parameters. The range is 1 to 64. The default is 3.

Maximum Attempts Time (minutes)

(attemptsMinutes)

The Maximum Attempts Time (minutes) parameter specifies the maximum number of minutes that can elapse during a password attempt before the user is locked out of their account. Configure this parameter in conjunction with the Maximum Attempts and the Lockout Time (minutes) parameters. The range is 0 to 60. The default is 5.

Minimum Length

(minLength)

The Minimum Length parameter specifies the minimum number of characters that are required for a password. The range is 1 to 8. The default is 6.

Name

(displayName)

The Name parameter specifies a name for the created object. The range is 0 to 80 characters.

Password Never Expires

(neverExpires)

The Password Never Expires parameter specifies whether the password can expire. When the parameter is disabled, you can specify the number of days the password can be active before a new password must be entered in the Days Before Expiration parameter. The options are:

- enabled
- disabled (default)

145 –NE RADIUS Authentication parameters

145.1 NE RADIUS Authentication parameters 145-2

145.1 NE RADIUS Authentication parameters

This chapter describes the parameters on the NE RADIUS Authentication form and its child forms.

Address

See the [Address](#) parameter in section 161.1.

Administrative State

See the [Administrative State](#) parameter in section 161.1.

Configuration Mode

See the [Configuration Mode](#) parameter in section 161.1.

Description

See the [Description](#) parameter in section 161.1.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

Enable Accounting

See the [Enable Accounting](#) parameter in section 161.1.

Enable Authorization

See the [Enable Authorization](#) parameter in section 161.1.

ID

See the [ID](#) parameter in section 161.1.

Port

See the [Port](#) parameter in section 161.1.

RADIUS Authorization Algorithm

(radiusAuthAlgorithm)

The RADIUS Authorization Algorithm specifies the authorization algorithm. The options are:

- direct (default)
- round-robin

Retry Attempts

See the [Retry Attempts](#) parameter in section 161.1.

Secret

See the [Secret Name](#) parameter in section 161.1.

Source Address

See the [Source Address](#) parameter in section 161.1.

Timeout (seconds)

See the [Timeout \(seconds\)](#) parameter in section 161.1.

146 –NE TACACS+ Authentication parameters

146.1 NE TACACS+ Authentication parameters 146-2

146.1 NE TACACS+ Authentication parameters

This chapter describes the parameters on the NE TACACS+ Authentication form and child forms.

Accounting Type

(**accountingType**)

The Accounting Type parameter specifies the type of accounting to use when the Enable Accounting is set to true. Table 146-1 describes the parameter options.

Table 146-1 Accounting Type parameter

Option	Option description	Dependencies
Start and Stop	Specifies that both start and stop record accounting notices are sent during authentication transactions with the TACACS+ server. Start packets are sent whenever a user performs a command.	The Enable Accounting parameter must be set to true.
Stop Only (default)	Specifies that a stop record accounting notice is sent at the end of an authentication transaction with the TACACS+ server. Stop packets are sent whenever a user command is complete.	

Address

See the [Address](#) parameter in section 161.1.

Administrative State

See the [Administrative State](#) parameter in section 161.1.

Configuration Mode

See the [Configuration Mode](#) parameter in section 161.1.

Description

See the [Description](#) parameter in section 161.1.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

Enable Accounting

See the [Enable Accounting](#) parameter in section 161.1.

Enable Authorization

See the [Enable Authorization](#) parameter in section 161.1.

ID

See the [ID](#) parameter in section 161.1.

Secret

See the [Secret Name](#) parameter in section 161.1.

Single Connection

See the [Single Connection](#) parameter in section 161.1.

Source Address

See the [Source Address](#) parameter in section 161.1.

Timeout (seconds)

See the [Timeout \(seconds\)](#) parameter in section 161.1.

147 –NE AOS Security Authentication parameters

147.1 NE AOS Security Authentication parameters 147-2

147.1 NE AOS Security Authentication parameters

This chapter describes the parameters on the NE AOS Security Authentication form and its child forms.

Account Port

(aaasRadAcctPort)

The Account Port parameter specifies the UDP destination port for accounting requests. The range is 1 to 65 535. The default is 1813.

Authentication Port

(aaasRadAuthPort)

The Port parameter specifies the UDP destination port for authentication requests. The range is 1 to 65 535. The default is 1812.

Port

(aaasTacacsPort)

The Port parameter specifies the port number for the primary TACACS+ server. The range is 0 to 65 535. The default is 49.

Retries

(aaasRetries)

The Retries parameter specifies the number of retries that the switch makes to authenticate a user before the switch tries to use the backup server. The range is 1 to 32. The default is 3.

Secret

(aaasRadKey)

The Secret parameter specifies the secret value that is configured on the switch and the server, but which is not sent over the network. The parameter can be any text or hexadecimal string but the value must match the secret that is configured on the server. The Secret is case-sensitive and is required when creating a server. The range is 1 to 64 characters.

Secret

(aaasTacacsKey)

The Secret parameter specifies the secret value that is configured on the switch and the server, but which is not sent over the network. The parameter can be any text or hexadecimal string but the value must match the secret that is configured on the server. The Secret is case-sensitive and is required when you create a server. The range is 1 to 64 characters.

148 –NE System Security parameters

148.1 NE System Security parameters 148-2

148.1 NE System Security parameters

This chapter describes the parameters on the NE System Security form.

Access

(templateAccess)

The Access parameter specifies the type of permitted user access. Enable one or more options, as required. The options are:

- FTP
- Console (enabled by default)

Console Login Exec File

(templateConsoleLoginExecFile)

The Console Login Exec File parameter specifies the name of a login script on the NE that runs automatically when a user logs in. Specify an NE file path. The range is 0 to 200 characters. There is no default.

CPM Per-Peer-Queuing

(cpmPerPeerQueuing)

The CPM Per-Peer-Queuing parameter specifies whether to enable or disable per peer queuing. Per-peer queuing ensures that the managed device automatically allocates a separate CPM hardware queue for provisioned peers, for example, a BGP or T-LDP peer. The options are:

- true
- false (default)

Home Directory

(templateHomeDirectory)

The Home Directory parameter specifies the name of the user home directory on the NE. Specify an NE file path. The range is 0 to 100 characters. There is no default.

Link Rate Limit (pps)

(cpmProtLinkRateLimit)

The Link Rate Limit (pps) parameter specifies the maximum rate, in packets per second, at which an interface can receive link-layer protocol packets from a specific source. This limit is applied to the network and access interfaces on the NE. The range is -1, or 1 to 65 535. The default is -1, which means that there is no maximum rate.

Port Overall Rate Limit (pps)

(cpmProtPortOverallRateLimit)

The Port Overall Rate Limit (pps) parameter specifies the maximum rate, in packets per second, at which the NE can receive link-layer protocol packets from a specific source. The range is –1, which means that there is no maximum rate, or 1 to 65 535. The default is 15 000.

Protection Administrative State

(cpmProtDropUncfgdProtocolMsg)

The Protection Administrative State parameter specifies whether NE DoS protection is enabled or disabled. When the parameter is enabled, the NE enforces the limits specified by the [Link Rate Limit \(pps\)](#) and [Port Overall Rate Limit \(pps\)](#) parameters and drops packets for unconfigured protocols. The options are:

- Down (default)
- Up

Restricted to Home Directory

(templateRestrictedToHomeDirectory)

The Restricted to Home Directory parameter specifies whether the user is restricted to the directory on the NE specified by the [Home Directory](#) parameter. The options are:

- true
- false (default)

Servers Enabled

(enableServers)

The Servers Enabled parameter specifies whether to enable or disable FTP, Telnet, or SSH servers on the managed device. The enabled options are determined by how the device is configured during commissioning, and depend on whether the managed device supports the type of server. See the chapter [14](#) for more information about using CLI to configure devices as servers. The options are:

- Telnet IPv6 (available on the 7450 ESS in mixed mode and the 7750 SR only)
- FTP (enabled by default for all supporting devices)
- SSH (enabled by default for all supporting devices)
- Telnet (enabled by default for all supporting devices)

SSH

(sshServerVersion)

The SSH parameter specifies the version of SSH supported on the managed device.
The option are:

- Version 1
- Version 2 (default for 7450 ESS)
- Version 1-2 (default for 7750 SR)

149 –Subscriber Authentication Policy Manager parameters

149.1 Subscriber Authentication Policy Manager parameters 149-2

149.1 Subscriber Authentication Policy Manager parameters

This chapter describes the parameters on the Create Subscriber Authentication Policy form and its child forms.

Accept CoA

(acceptAuthenticateChange)

The Accept CoA parameter specifies whether the router handles the CoA messages from the RADIUS server and changes to the RADIUS accounting policies assigned to subscriber profiles during a subscriber host session. The options are:

- enabled
- disabled (default)

The RADIUS server sends CoA messages when the following occurs:

- the subscriber profile of the subscriber host is modified
- the SLA profile of the subscriber host is modified
- the IP configuration of the subscriber host is modified
- a subscriber host is created

Access Algorithm

(accessAlgorithm)

The Access Algorithm parameter specifies the algorithm that is used to select a RADIUS server from the list of configured servers. The options are:

- Direct (default)
- Round-robin

Append To User Name

(userNameAppend)

The Append To User Name parameter specifies the algorithm that is used to select a RADIUS server from the list of configured servers. The options are:

- Domain Name
- Nothing (default)

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [161.1](#).

Authentication Hold Down Time

(radAuthDownTime)

The Authentication Hold Down Time parameter specifies (in seconds) the amount of time the system waits before addressing a RADIUS server that had been down and has come back up. The range is 30 to 900. The default is 30.

Calling Station ID Type

(callingStationIdType)

The Calling Station ID Type parameter specifies the string for the RADIUS Calling Station ID parameter when included in RADIUS authentication request messages. The parameter is configurable when the Calling Station ID option is enabled for the RADIUS Attributes parameter. The options are:

- SAP String (default)
- MAC Address
- SAP ID
- Remote ID

Description

See the [Description](#) parameter in section 161.1.

Domain Name

(pppDomain)

The Domain Name parameter specifies the domain name to apply with PAP/CHAP user name re-write operations. The parameter is specified as a string of up to 128 characters.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

Fallback Action

(radiusFallbackAction)

The Fallback Action parameter specifies how subscriber authentication failure is handled because of RADIUS server failure. The options are:

- Deny—access to the host is blocked (default)
- Accept—the host is accepted and created using default profiles that are attached to the corresponding SAPs
- User DB—enter or choose a local user database name. The corresponding local user database is used to authenticate the subscriber host. This option is applicable only for DHCP and PPPoE hosts.

ID

See the [ID](#) parameter in section 161.1.

Password

(password)

The Password parameter specifies the password associated with a user in an authentication request sent to the RADIUS server. The range is 0 to 10. There is no default.

Port

See the [Port](#) parameter in section [161.1](#).

Port Prefix String

(nasPortPrefixString)

The Port Prefix String parameter specifies the string to be added as a prefix to the NAS Port ID option of the RADIUS Attributes parameter when included in RADIUS authentication request messages. The range is 0 to 8. A value can be specified for the prefix if the Port Prefix Type parameter is set to User String.

Port Prefix Type

(nasPortPrefixType)

The Port Prefix Type parameter specifies the prefix type to be added to the NAS Port ID option of the RADIUS Attributes parameter when included in RADIUS authentication request messages. The options are:

- None (default)
- User String

Port Suffix Type

(nasPortSuffixType)

The Port Suffix Type parameter specifies the suffix type to be added to the NAS Port ID option of the RADIUS Attributes parameter when included in RADIUS authentication request messages. The options are:

- None (default)
- Circuit Id
- Remote Id

Port Type

(nasPortTypeType)

The Port Type parameter specifies the value of the RADIUS NAS Port Type parameter when included in RADIUS authentication request messages. The Port Type parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter. The options are:

- Standard (default)
- Config

Port Type Value

(nasPortTypeValue)

The Port Type Value parameter specifies the value of the RADIUS NAS Port Type parameter when included in RADIUS authentication request messages. The Port Type Value parameter is configurable when the NAS Port Type option is enabled for the RADIUS Attributes parameter, and the Port Type is set to Config. The range is 0 to 255. The default is 0.

PPPoE Access Method

(pppoeAccessMethod)

The PPPoE parameter specifies one of the methods to authenticate PPPoE towards the RADIUS server. Table 149-1 describes the parameter options.

Table 149-1 PPPoE parameter

Option	Description
None	no PPPoE authentication
PADI	PPPoE authentication based on the received PADI packet

RADIUS Attributes

(radiusAttributes)

The RADIUS Attributes parameter specifies the RADIUS attributes that are included in RADIUS authentication request messages. Table 149-2 describes the parameter options.

Table 149-2 RADIUS Attributes parameter

Option	Description
MAC Address	The MAC address is included in the request.
DHCP Vendor Class ID	The DHCP vendor class ID is included in the request.
NAS ID	The NAS ID is included in the request.
Remote ID	The remote server ID is included in the request.

(1 of 2)

Option	Description
Calling Station ID	The calling station ID is included in the request.
Tunnel Server Attributes	The tunnel server attributes are included in the request.
NAS Port Type	The NAS port type is included in the request.
Access Loop Options	The access loop options are included in the request.
PPPoE Service Name	The PPPoE service name is included in the request.
NAS Port ID	The NAS port ID is included in the request.
Circuit ID	The circuit ID is included in the request.
Called Station ID	The called station ID is included in the request.
DHCP Options	All DHCP options are included in the request.
Accounting Session ID	The SLA or host accounting session ID is included in the request.

(2 of 2)

Re-Authenticate When DHCP Lease Expires

(reAuthenticate)

The Re-Authenticate When DHCP Lease Expires parameter specifies whether authentication is reissued when the DHCP lease state time expires. This parameter assumes that DHCP snooping is enabled on a specific IES or VPLS. The options are:

- false (default)
- true

Retry Attempts

See the [Retry Attempts](#) parameter in section 161.1.

Router Instance

(routerType)

The Router Instance parameter specifies the type of virtual router for the RADIUS authentication policy. Table 149-3 describes the options.

Table 149-3 Router Instance parameter

Option	Description	Dependencies
Matched (default)	Base and Management router instances are the same.	—
VPRN	A VPRN service that is used as the routing instance for the policy.	This option is not available for the 7450 ESS in a local policy.
Base	The routing table configuration of the router is the routing instance for the policy.	—

(1 of 2)

Option	Description	Dependencies
Management	The bof configuration of the router is the routing instance for the policy.	—

(2 of 2)

Secret Key

See the [Secret Name](#) parameter in section [161.1](#).

Server IP Address

See the [Address](#) parameter in section [161.1](#).

Source Address

(sourceAddress)

The Source Address parameter specifies the source IP address of the RADIUS packets. The range is any valid unicast address. The default is 0.0.0.0.

When the parameter specifies the address of the interface, the RADIUS client uses the address for authentication requests. When the address is in-band, the system IP address is used. When the address is out-of-band, the IP address of the management interface is used.

Timeout (seconds)

See the [Timeout \(seconds\)](#) parameter in section [161.1](#).

User Name Format

(userNameFormat)

The User Name Format parameter specifies the format of the user name in an authentication request sent to the RADIUS server. Table [149-4](#) describes the options.

Table 149-4 User Name Format parameter

Option	Option description
MAC Address (default)	The MAC address of the DHCP client is the user name.
Circuit ID	The Option 82 circuit ID from the DHCP packet is the user name. If the 7450 ESS or 7750 SR served as the DHCP relay that inserted the Option 82 information, the user name corresponds to the format defined in the information option.
Both	Both the MAC address and the Option 82 circuit ID are used as the user name.
ASCII Converted Circuit ID	The ASCII converted circuit ID of the DHCP client is the user name.

(1 of 2)

Option	Option description
ASCII Converted Both	Both the MAC address and the ASCII converted circuit ID of the DHCP client are used as the user name.
DHCP Client Vendor Options	The DHCP client-identifier option, the "@" delimiter and the DHCP vendor-class identifier option are concatenated to form the user name.
MAC GI Address	The MAC gateway IP address of the DHCP client is the user name.

(2 of 2)

User Name Operation

(pppUserNameOp)

The User Name Operation parameter specifies the re-writing operation performed on the PAP/CHAP user name. Table 149-5 describes the options.

Table 149-5 User Name Operation parameter options

Option	Option description
None (default)	No change
Append	Adds an @ delimiter and the Domain Name string after the PAP/CHAP username. Requires configuration of the Domain Name parameter.
Strip	Removes all characters after and including the @ delimiter.
Replace	Replaces the character string after the @ delimiter with the Domain Name string. Requires configuration of the Domain Name parameter.
Use As Default	Adds the Domain Name string only to usernames which have no domain name (@domain) specified. Requires configuration of the Domain Name parameter.

150 –NE Maintenance parameters

150.1 NE Maintenance parameters 150-2

150.1 NE Maintenance parameters

This chapter describes the parameters on the NE Maintenance form and child forms.

ATCA Image Root Path

(cflashImageRoot)

The ATCA Image Root Path parameter specifies the full path on the device where the NE software image file is to be downloaded. The range is 0 to 255 characters. The default value is /data0.

Auto-Activate After Successful File Transfer

(isAutoActivate)

The Auto-Activate After Successful File Transfer parameter specifies whether the device activates the new software image after an upgrade operation successfully completes. The parameter is enabled and not configurable when the [In Service Software Upgrade](#) parameter is enabled. Table 150-1 describes the parameter options.

Table 150-1 Auto-Activate After Successful File Transfer parameter

Option	Option description
enabled (default)	After the 5620 SAM transfers the software files to the NE, it does the following: <ul style="list-style-type: none">• updates the BOF with the new software image location• backs up the original boot.ldr at the location specified by the CFlash Backup Root Path parameter• replaces the currently active boot.ldr file with the new one• forces a “boot env synch” and a “config synch” on NEs that have redundant CPMs
disabled	The 5620 SAM transfers the software files to the NE for activation at a later time.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Auto Backup Scheme

(autoBackupScheme)

The Auto Backup Scheme parameter specifies under which conditions a backup to the database should occur. Table 150-2 describes the parameter options.

Table 150-2 Auto Backup Scheme parameter

Option	Option description	Dependencies
No Auto-backup (default)	Specifies that no automatic backups occur	—
Every 5620 SAM Server Initiated Save	Specifies that a backup occurs when the 5620 SAM server initiates a save operation	
Every Nth 5620 SAM Server Initiated Save	Specifies that a backup occurs only after a set number of save operations occur	The Auto Backup Threshold (operations) parameter must be configured

Auto Backup Threshold (operations)

(autoBackupSchemeTreshold)

The Auto Backup Threshold (operations) parameter specifies how many save operations occur before a backup is initiated. The parameter is configurable when the [Auto Backup Scheme](#) parameter is set to Every Nth 5620 SAM Server Initiated Save. The range is 0 to 1000. The default is 0.

Auto-Purge Scheme

(purgeMode)

The Auto-Purge Scheme parameter specifies the method of backup purging used to control the number of device configuration backups files kept by the 5620 SAM. Table [150-3](#) describes the parameter options.

Table 150-3 Auto-Purge Scheme parameter

Option	Option description	Dependencies
Limit To A Maximum Number Of Backups	The maximum number of backup files kept is the value specified by the Number of Backups parameter. When this value is reached, the oldest backup files are deleted to make room for the new ones.	You must configure the Number of Backups parameter.
By Age	All backup files older than the value specified by the Maximum Backup Age parameter are deleted.	You must configure the Maximum Backup Age (days) parameter.
By Age But Retain A Minimum Number Of Backups	Backup files older than the value specified by the Maximum Backup Age (days) parameter are deleted only if the number of files in the backup directory has reached the value specified by the Number of Backups parameter.	You must configure the following parameters: <ul style="list-style-type: none"> Maximum Backup Age (days) Number of Backups
By Age But Limit To A Maximum Number Of Backups	Backup files older than the Maximum Backup Age parameter are deleted and the number of files is limited by the Number of Backups parameter.	

Auto-Reboot After Successful Upgrade

(isAutoReboot)

The Auto-Reboot After Successful Upgrade parameter specifies whether the device initiates a reboot after an upgrade operation is successfully completed. The parameter is configurable when the [In Service Software Upgrade](#) parameter is disabled. The options are:

- enabled
- disabled (default)

When you are upgrading multiple devices, Alcatel-Lucent recommends that the parameter is set to disabled. This ensures that reboots of managed devices do not interfere with the transfer of software images from the 5620 SAM to the managed devices.



Caution — When you use the 5620 SAM client GUI to perform managed device software upgrades and disable the parameter, there is a risk that the bof.cfg file may be overwritten in the following situations:

- when a user performs ‘bof save’ using the CLI on the managed device
- If there is a gap between a software upgrade and a reboot
Perform a ‘show bof’ to ensure another user has not performed ‘bof save’.



Note — You are not required to reboot for some node software upgrades; for example ISA-AA upgrades. See the associated node documentation for additional information.

Auto-Reboot After Successful Activation

(isAutoReboot)

The Auto-Reboot After Successful Activation parameter specifies whether a reboot is required after the database is successfully restored to the device. The options are:

- Enabled
- Disabled (default)



Note — You are not required to reboot for some node software upgrades. See the associated node documentation for additional information.

When you are downloading multiple images to multiple devices, Alcatel-Lucent recommends that the automatic reboot option is disabled, to ensure that the new software is properly transferred.



Caution — When you use the 5620 SAM client GUI to perform managed device software upgrades and disable the parameter, there is a risk that the bof.cfg file may be overwritten in these situations:

- when a user performs ‘bof save’ using CLI on the managed device
- If there is a gap between a software upgrade and a reboot, perform a ‘show bof’ to ensure another user hasn’t performed a ‘bof save’.

Auto Save Scheme

(autoSaveConfigScheme)

The Auto Save Scheme parameter specifies how configuration changes are automatically saved on the managed device, and when the network device performs a save of its running configuration, and, if so, how often. Table 150-4 describes the parameter options.

Table 150-4 Auto Save Scheme parameter

Option	Option description	Dependencies
No Auto-save	Specifies that configuration changes are not saved to the device automatically.	—
Every Deployment (default)	Specifies that configuration changes are saved on the device after every configuration change is deployed to the device. This option ensures that the managed device configuration file is always up to date with the 5620 SAM database.	Ensure that this option does not cause excessive activity on the managed device when there is a high rate of network configuration; for example, when an OSS client is performing bulk service configurations through the 5620 SAM-O open interface.
Every Successful Deployment	Specifies that configuration changes are saved to the device only when a successful deployment is executed.	—
Every Nth Deployment	Specifies that configuration changes are saved to the device after every <i>N</i> deployments, where <i>N</i> is specified by the Auto Save Threshold parameter.	When <i>N</i> is set to a large number, changes deployed to a managed device are saved less often on the device. It is therefore possible to lose configuration changes if the device reboots.
Every Nth Successful Deployment	Specifies that configuration changes are saved to the device after every <i>N</i> successful deployments, where <i>N</i> is specified by the Auto Save Threshold parameter.	

Auto Save Threshold

(autoSaveConfigThreshold)

The Auto Save Threshold parameter specifies the number of deployments or successful deployments that are required before configuration changes are automatically saved to the router. The parameter is configurable when the [Auto Save Scheme](#) parameter is set to Every Nth Deployment or Every Nth Successful Deployment. The range is 0 to 10 000. The default value is 0.



Caution — When *N* is set to a large number, changes deployed to a managed device are saved less often on the device. It is therefore possible to lose configuration changes if the device reboots.

Boot Option File Mode

(bootOptionFileBackupMode)

The Boot Option File Mode parameter specifies the backup behavior for the boot option file. The options are:

- Disabled
- New Version Only
- Always (default)

CFlash Backup Root Path

(cflashBackupRoot)

The CFlash Backup Root Path parameter specifies the full path on the device where the node software image file is to be backed up. The default is cfx:/backup, where *x* is the compact flash drive. The range is 0 to 255 characters.

CFlash Image Root Path

(cflashImageRoot)

The CFlash Image Root Path parameter specifies the full path on the device where the node software image file is to be downloaded. The range is 0 to 255 characters. The default value is cf3:/images.

CLI Config File Mode

(cliConfigFileBackupMode)

The CLI Config File Mode parameter specifies the backup behavior for the CLI config file. The options are:

- Disabled (default)
- New Version Only
- Always

CLI Config Save Details

(cliConfigSaveDetails)

The CLI Config Save Details parameter specifies whether to save additional details about the CLI configuration save changes. The options are:

- Enabled
- Disabled (default)

CLI Debug Save Config File Mode

(debugConfigFileBackupMode)

The CLI Debug Save Config File Mode parameter specifies whether to save the debug config files in a backup operation. The options are:

- Enabled
- Disabled (default)

Deployment Mode

(deploymentMode)

The Deployment Mode parameter specifies whether configuration management information is sent to a network device or remains on the 5620 SAM. Table 150-5 describes the parameter options.

Table 150-5 Deployment Mode parameter

Option	Option description	Dependencies
Deployed through SNMP (default)	Specifies that 5620 SAM configurations are sent to the managed devices using SNMP. Alcatel-Lucent recommends that you use this option.	—
No Deployment	Specifies that 5620 SAM configurations are not sent to devices and remain on the 5620 SAM server. This option is useful in lab or demonstration environments, when there is a restored database available, but no network is accessible.	—

Enable Backup

(enableBackup)

The Enable Backup parameter specifies whether device backup operations are enabled in the backup policy. When the [Enable Backup](#) parameter is disabled, no other parameters on the form are configurable. The options are:

- enabled (default)
- disabled

File Compression

(compressionMode)

The File Compression parameter specifies the compression format of the backup file if compression is used. If there is no file compression, the value is None. The options are:

When you configure an AOS Based Node backup policy, the File Compression parameter only applies to files saved to the certified directory. Files saved to the network directory are always saved using ZIP file compression.

- None (default)
- ZIP
- GZIP

Forced Download

(forcedActivation)

The Forced Download parameter specifies that the NE download all of the software image files on the server. When this parameter is disabled, the 9500 MPR compares the software image files on the NE with the image files on the server and only downloads the files that differ. The options are:

- Disabled (default)
- Enabled

FTP Password

(ftpPassword)

The FTP Password parameter specifies the password that is used to log in to the FTP server that stores the software image files. The range is 0 to 255 characters.

FTP Server IP

(ftpServerIP)

The FTP Server IP parameter specifies the IP address of the FTP server that stores the software image files. The address can be IPv4 or IPv6 format. The default is 127.0.0.1.

FTP Server Port

(ftpServerPort)

The FTP Server Port parameter specifies the FTP server port used by the server that stores the software image files. The default is 21.

FTP User ID

(ftpUser)

The FTP User ID parameter specifies the user name that is used to log in to the FTP server that stores the software image files. The range is 0 to 255 characters.

Image Root Path

(cflashImageRoot)

The Image Root Path parameter specifies the full path on the device where the node software image file is to be downloaded. The range is 0 to 255 characters. The default value is /flash/.

In Service Software Upgrade

(isIssu)

The In Service Software Upgrade parameter specifies whether you want to perform a maintenance (minor) software upgrade on a redundant CPM device without service interruption. During the upgrade, service is maintained as one CPM assumes operation while the other restarts. The parameter is configurable when the [Auto-Activate After Successful File Transfer](#) parameter is enabled. The options are:

- Enabled
- Disabled (default)

Maximum Backup Age (days)

(maxBackupAge)

The Maximum Backup Age (days) parameter specifies the length of time, in days, that backup files are retained by the 5620 SAM before they are purged. The parameter is configurable when the [Auto-Purge Scheme](#) parameter is set to a value that begins with By Age. Any non-negative number is valid. The default is 100.

Name

See the [“Name”](#) parameter in section [112.1](#).

Number of Backups

(numBackupsToKeep)

The Number of Backups parameter specifies the maximum number of backup files that are saved in the 5620 SAM database. Any non-negative number is valid. Ensure that there is enough disk space to accommodate the specified number of backups.

The parameter is configurable when the [Auto-Purge Scheme](#) parameter is set to something other than By Age. The default is 30. The range is limited by the available backup disk space.

Policy ID

(policyId)

The Policy ID parameter specifies a numeric identifier for the backup policy. The parameter is configurable when the Auto Assign ID parameter is disabled. The range is 1 to 65 535. The default is 0, which means that no value is specified.

Policy Type

(policyType)

The Policy Type parameter specifies the type of backup or software upgrade policy. The options are:

- SR Based Node (default)
- AOS Based Node
- MPR Node
- MME Node
- RAN Node

Retry Interval

(retryFrequency)

The Retry Interval parameter specifies the time interval between retry attempts if deployment failed. The options are:

- | | |
|-----------------------|------------|
| • 1 minute | • 1 hour |
| • 5 minutes (default) | • 2 hours |
| • 10 minutes | • 3 hours |
| • 15 minutes | • 6 hours |
| • 20 minutes | • 12 hours |
| • 30 minutes | • 24 hours |
| • 45 minutes | • 48 hours |

Retry Scheme

(retryScheme)

The Retry Scheme parameter specifies how deployment failures should be handled. Table [150-6](#) describes the parameter options.

Table 150-6 Retry Scheme parameter

Option	Option description	Dependencies
No Retries	Specifies that a deployment retry does not occur as a result of a failed deployment.	A deployment failure does not raise an alarm until the number of deployment retries is reached. When you set the parameter to Retry Forever, there is no set number of attempts, and a deployment failure alarm is not raised.
Retry Forever (default)	Specifies that a retry of the deployment should occur continuously, based on the interval period.	
Retry Number Of Times	Specifies that a retry of the deployment should occur the number of times specified in the Retry Threshold parameter.	

Retry Threshold

(retryThreshold)

The Retry Threshold parameter specifies the number of times that a retry should occur in the event of a failed deployment. The range is 0 to 10 000. The default value is 0.

Root Directory

(ftpRootDir)

The Root Directory parameter specifies the directory on the FTP server where the software image files are stored. The default is /. The range is 0 to 255 characters.

Save Certified Directory

(saveCertifyDir)

The Save Certify Directory parameter specifies whether the OmniSwitch certified directory should be saved during a backup operation. The certified directory contains configuration files that are certified as the default startup files for the switch. These files are the trusted configuration and binary image files. They are used if there is a non-specified reload. The options are:

- Enable (default)
- Disable

Save Details

(saveConfigDetails)

The Save Details parameters specifies whether to save additional information about the configuration file save change scheme configured. The options are:

- Enabled
- Disabled (default)

When you set the parameter to Enabled, default and non-default information is saved. When you set the parameter to Disabled, only non-default information is saved.

Save Network Directory

(saveNetworkDir)

The Save Network Directory parameter specifies whether the OmniSwitch network directory should be saved during a backup operation. The network directory contains files that may be required by servers used for authentication. Other files can also be stored in this directory, if required. The options are:

- Enable
- Disable (default)

Scheduled Backup Interval

(scheduledBackupFrequency)

The Scheduled Backup Interval parameter specifies the time interval between scheduled backups to the database. The parameter is configurable when the Scheduled Backup Scheme (scheduledBackupScheme) parameter is set to something other than No Scheduled Backup. The options are:

- 15 minutes
- 30 minutes
- 1 hour
- 2 hours
- 3 hours
- 6 hours
- 12 hours
- 24 hours (default)
- 48 hours

Scheduled Backup Scheme

(scheduledBackupScheme)

The Scheduled Backup Scheme parameter specifies whether a scheduled backup to the managed device database should occur, and, if so, under what conditions. Table 150-7 describes the parameter options.

Table 150-7 Scheduled Backup Scheme parameter

Option	Option description	Dependencies
No Scheduled Backup	Specifies that backups to the database do not automatically occur	—

(1 of 2)

Option	Option description	Dependencies
Every Scheduled Interval (default)	Specifies that backups to the database should occur based on the value of the Scheduled Backup Interval parameter	The following parameters must be configured: <ul style="list-style-type: none"> Scheduled Backup Interval Scheduled Backup Threshold (operations)
Every Scheduled Interval If 5620 SAM Server Initiated Save Performed	Specifies that backups to the database should occur as scheduled but only when the 5620 SAM server initiates a save (admin save) operation during the previous backup interval. This option can be used in networks where the managed device configuration is relatively static and fixed or where the backup interval is short to prevent unnecessary backups and management traffic.	

(2 of 2)

Scheduled Backup Sync Time

(scheduledBackupSyncTime)

The Scheduled Backup Sync Time parameter specifies the start time for the first scheduled backup. The range is an allowable value in the format HH:mm. For example, to start a backup at 1 p.m., set the parameter to 13:00, then click on the Apply button. When the parameter value is reached, the backup begins. Backups are then performed at regular intervals, based on the [Scheduled Backup Interval](#) and the [Scheduled Backup Scheme](#) parameters. The parameter is configurable when the Scheduled Backup Scheme (scheduledBackupScheme) parameter is set to something other than No Scheduled Backup. The default is 02:00 (2 a.m.). The range is a valid time value, based on a 24-hour clock.

Scheduled Backup Threshold (operations)

(scheduledBackupTreshold)

The Scheduled Backup Threshold (operations) parameter works in conjunction with the [Scheduled Backup Scheme](#) parameter to specify the number of 5620 SAM server-initiated saves that occur before the 5620 SAM performs a scheduled backup. The range is 0 to 1000. The default is 0.

Scheduled Save Interval

(scheduledSaveConfigFrequency)

The Scheduled Save Interval parameter specifies the time interval that should elapse before the next save operation is performed. The parameter is configurable when the [Scheduled Save Scheme](#) parameter is set to anything other than No Scheduled Save. The options are:

- 15 minutes
- 30 minutes
- 1 hour (default)
- 2 hours
- 3 hours
- 6 hours
- 12 hours
- 24 hours
- 48 hours

Scheduled Save Scheme

(scheduledSaveConfigScheme)

The Scheduled Save Scheme specifies whether a scheduled save operation should occur, and, if so, under what deployment conditions. Table 150-8 describes the parameter options.

Table 150-8 Scheduled Save Scheme parameter

Option	Option description	Dependencies
No Scheduled Save (default)	Specifies that a save is not executed automatically	—
Scheduled Always	Specifies that a save is executed every time the specified time interval has elapsed	Requires a value to be configured for the Scheduled Save Interval parameter
Scheduled If Deployment Performed	Specifies that a save is executed only when a deployment is performed	—
Scheduled If Successful Deployment Performed	Specifies that a save is executed only when a successful deployment is performed	—

SFTP Password

(sftpPassword)

The SFTP Password parameter specifies the password that is used to log in to the SFTP server that stores the software image files. The range is 0 to 255 characters.

SFTP User ID

(sftpUser)

The SFTP User ID parameter specifies the user name that is used to log in to the SFTP server that stores the software image files. The range is 0 to 255 characters.

Timer To Wait For Fallback To Previous IP Version

(timerToWaitForFallbackToPreviousIPversion)

The Timer To Wait For Fallback To Previous IP Version parameter specifies the number of minutes to wait for an eNodeB performing a full fallback to the previous IP transport configuration version when the eNodeB failed to use a new version. A value of 0 is used to turn off the transport fallback functionality. The range is 30 to 120. The default is 30.

Timer To Wait For Fallback To Previous Software Version

(timerToWaitForFallbackToPreviousSWversion)

The Timer To Wait For Fallback To Previous Software Version parameter specifies the number of minutes to wait for an eNodeB performing a full fallback to the previous SW version when the eNodeB failed to use a new version. A value of 0 is used to turn off the software fallback functionality. The range is 30 to 120. The default is 30.

Transfer Protocol

(ftpType)

The Transfer Protocol parameter specifies the type of FTP to use for transferring software image files. The options are:

- FTP
- SFTP

Upgrade File Type

(upgradeBootFiles)

The Upgrade File Type parameter specifies the type of software upgrade to perform. The options are:

- Image and Boot Files (default)
- Image Files Only
- Boot Files Only

151 –Database parameters

151.1 Database parameters 151-2

151.1 Database parameters

This chapter describes the parameters on the Database Manager form and child forms.

Accounting Statistic Data Retention Period (Days)

(accStatsDataPartInt)

The Accounting Statistic Data Retention Period (Days) parameter specifies how long, in days, the 5620 SAM database retains collected statistics data. The range is 1 to 1000. The default is 1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [112.1](#) for more information.

Backup Interval

(backupFrequency)

The Backup Interval parameter specifies how often a backup is performed. For example, when you set the Backup Interval parameter to 5 and the [Interval Unit](#) parameter to hour, a backup is performed every 5 h. The parameter is used with the Interval Unit parameter. The range is 1 to 1000. The default is 24.

Backup Type

(scheduledBackupType)

The Backup Type parameter specifies the type of scheduled backup to perform. The options are:

- Full (default)
- Partial

Description

See the [Description](#) parameter in section [112.1](#) for more information.

Enable Backup File Compression

(enableBackupCompression)

The Enable Backup File Compression parameter specifies whether the database backup file set is automatically compressed after it is created. The file set is compressed in gzip format and archived using the tar function. The resulting file name is `samDBBackup_timestamp_5620 SAMRelease_CPU_OracleReleaseF | P.tar`

where

timestamp is the date and time of archive file creation

5620 SAMRelease is the 5620 SAM release identifier

CPU is the platform processor type

OracleRelease is the Oracle release identifier

F | P indicates whether the file contains a full or partial database backup

The options are:

- disabled (default)
- enabled

Interval Unit

([backupFrequencyUnit](#))

The Interval Unit parameter specifies the unit of time for the [Backup Interval](#) parameter. The options are:

- minute
- hour (default)
- day
- week

Manual Backup Directory

([manualBackupDest](#))

The Manual Backup Directory parameter specifies the directory that is to contain the backup file sets that are created during unscheduled backups. The range is 0 to 200 characters. The default is /opt/5620sam/dbbackup/manual.



Caution — Before the 5620 SAM performs a manual database backup, it deletes the contents of the directory specified by the [Manual Backup Directory](#) parameter. Ensure that the directory that you specify does not contain files that you want to retain.

Max (Collective) Log Size

(KB) ([maxSize](#))

The Max (Collective) Log Size (KB) parameter specifies the log size that must be reached before the archiving action occurs. You can configure the parameter when the [Purge Mode](#) parameter is set to any option except Manual. The range starts at 0 Kb and has no upper limit. The default is 100 000 KB.

When the Purge Mode parameter is set to By Max Log Size, no zipped archives are created. When there are multiple logs of each type, for example, 24 audit log files, the size of each file is considered, and when the collective size of the files reaches the parameter limit, all logs are zipped in one file.

Number of Archives

(numArchives)

The Number of Archives parameter specifies the maximum number of archive logs that must be reached before the purging action occurs. You can configure the parameter when the [Purge Mode](#) parameter is set to By Max Log Size and Number of Archives. The range is 0 to 2 147 486 347. The default is 50.

Alcatel-Lucent recommends that you store archived log files for record keeping and troubleshooting. When the parameter value is reached, the archived log files are deleted. You can move the archived log files from the database to another site for storage.

Number to Keep

(backupNumberOfSets)

The Number to Keep parameter specifies how many database backups are stored. The range is 1 to 10. The default is 3.



Note — Ensure that the backup location has enough space to contain the database. For regularly scheduled backups, ensure that there is enough space for numerous backup copies of the database.

Policy ID

(policyId)

See the [ID](#) parameter in section [112.1](#) for more information.

Purge Mode

(purgeMode)

The Purge Mode parameter specifies the criterion that must be met before database log files are purged. Table [151-1](#) describes the parameter options.

Table 151-1 Purge Mode parameter

Option	Option description	Dependencies
Manual	No purge criterion is set. If log management is required, the logs are manually handled by a user with database management permissions. When manual is selected, the following back up policy configuration parameter values are updated, the Auto-Purge Scheme parameter is set to Limit to a Maximum Number of Backups, and the Number of Backups parameter is set to 30.	Alcatel-Lucent does not recommend that users perform database management functions with Oracle tools. Such actions can damage databases and may void support contracts. You cannot configure any additional parameters.
By Max Log Size	When the log or logs reach the Max (Collective) Log Size (KB) parameter setting, the log or logs are deleted and a new log of size 0 kb is started.	You cannot configure the Number of Archives parameter. No zipped archives of logs are kept.

(1 of 2)

Option	Option description	Dependencies
By Max Log Size and Number of Archives (default)	Logs are zipped when the Max (Collective) Log Size (KB) parameter setting is reached, and then the archived log files are deleted based on the number of archives stored.	When the archive log limit is reached and the maximum log size is reached, a new archive is created and the oldest archive file is deleted. Alcatel-Lucent recommends that you store archived log files off the database system, for record keeping and troubleshooting.

(2 of 2)

Scheduled Backup Directory

(schedBackupDest)

The Scheduled Backup Directory parameter specifies the directory that is to contain the backup file sets that are created during scheduled backups. Each backup file set is stored in a subdirectory below the scheduled backup directory. The range is 0 to 200 characters. The default is /opt/5620sam/dbbackup.



Caution — Before the 5620 SAM performs a scheduled database backup, it deletes the contents of the directory specified by the [Scheduled Backup Directory](#) parameter. Ensure that the directory that you specify does not contain files that you want to retain.

Schedule Enabled

(isScheduleEnabled)

The Schedule Enabled parameter specifies whether the database backup schedule is in effect. When the parameter is enabled, the 5620 SAM backs up the 5620 SAM database

Start Time

(backupStartTime)

The Start Time parameter specifies when the database backup is scheduled to start, in the format `yyyy/MM/dd hh:mm`. For example, if the parameter were set to 2006/01/29 02:30, the first backup starts on January 29, 2006 at 2:30 a.m. The parameter uses a 24-hour clock.

When the value of the start time parameter is reached, the [Backup Interval](#) and [Interval Unit](#) parameters determine the backup frequency and successive start times. For example, the next scheduled backup starts at the time chosen and every interval thereafter. If the start time is set to Oct 26 14:15, and the interval is 6 hours, then backups are performed Oct 26 at 14:15, Oct 26 at 20:15, Oct 27 at 02:15, and so on.

To change the date, highlight the year, month, day, hour, or minute value on the client GUI and use the up and down arrow keys to modify the setting.

152 –System Information parameters

152.1 System Information parameters 152-2

152.1 System Information parameters

This chapter describes the parameters on the System Information form and child forms.

Maximum UI Sessions

(maxUISessions)

The Maximum UI Sessions parameter specifies the number of client sessions that the client delegate allows before it raises an alarm. The range is 1 to 65 535. The default is 30.

153 –System Preferences parameters

153.1 System Preferences parameters 153-2

153.1 System Preferences parameters

This chapter describes the parameters on the System Preferences form and child forms.



Caution — Changing the parameter value of a System Preference may affect the behavior of an existing 5620 SAM service. Do not change the parameter value from the default without contacting Alcatel-Lucent technical support.



Note — The System Preferences parameters can only be modified by a user with administration privileges.

Auto Discover Composite Services

(autoDiscoverCompositeSvc)

The Auto Discover Composite Services parameter specifies whether to enable or disable checking for composite services. By default, the 5620 SAM checks for composite services.

Default Service Priority

(svcPriority)

The Default Service Priority parameter specifies the default priority of the service. The options are Low, Medium, and High priority. The default is Low priority.

Maximum number of sites that can be moved

(maxNumberOfMoveSites)

The Maximum number of sites that can be moved parameter specifies the maximum number of service sites that can be moved between services at a time. The range is 1 to 50. The default is 25.

Remove Empty Service

(removeEmptyService)

The Remove Empty Service parameter specifies whether a services is deleted from the 5620 SAM when the last site is removed from the service. The default is false.



Note — When the Remove Empty Service parameter is set to True, a composite service is also deleted when the last service is deleted from the composite service.

Suppress VPRN SNMP Community String Warning

(supVprnSnmpCommunityStringMsg)

The Suppress VPRN SNMP Community String Warning parameter specify whether or not to suppress the VPRN SNMP community string warning and alarms. The default is disabled.

154 –Alarm Settings parameters

154.1 Alarm Settings parameters 154-2

154.1 Alarm Settings parameters

This chapter describes the parameters on the Alarm Settings form and its child forms.

Administrative State

See the [Administrative State](#) parameter in section [112.1](#).

Alarm deletion

(isAlarmDeletionEnabled)

The Alarm deletion parameter specifies whether alarm deletion policies are allowed. The options are:

- Enabled (default)
- Disabled

Attribute Name

(attributeName)

The Attribute Name parameter specifies the object attribute that is associated with the object type. This parameter is configurable when an Additional Text Policy has been created. Click on the Select button to list and choose an attribute.

auto

(implicitDeletionRule)

The auto parameter specifies an automatic deletion policy to use for alarms. This parameter is configurable if the Alarm Deletion parameter is set to Enabled. The options are:

- disabled
- when cleared (default)
- when acknowledged
- when cleared and acknowledged
- when cleared or acknowledged



Caution — When an escalation policy uses the default when cleared option, the escalation policy does not work. You must configure the parameter to a value other than when cleared to ensure the escalation policy is successful.

Automatically Assigned Urgency

(autoAssignedUrgency)

The Automatically Assigned Urgency parameter specifies the urgency for an alarm type. The default 5620 SAM setting is unique to the alarm type. For example, the default 5620 SAM setting may be to associate an alarm type with a minor urgency. However, in a specific network configuration, the alarm condition may be historically recognized as a precursor to a larger network problem. You may decide to change the default setting for the alarm type from minor to major urgency, raising the visibility of the issue to network operators.

The options are:

- minor
- major
- critical
- indeterminate

automatic deletion of correlated alarms

The automatic deletion of correlated alarms parameter specifies the conditions under which correlated alarms are deleted when the deletion of other alarms deleted. The options are:

- disabled
- delete correlated alarms with GUI notification (default)
- delete correlated alarms without GUI notification

automatic severity alterations

(isSeverityAutoAlterable)

The automatic severity alterations parameter specifies whether to enable automatic severity changes for alarms based on specific alarm policies. This parameter is configurable when the Severity Alterable parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

clearing (if self-clearing alarm)

(isSeverityManualClearingEnabled)

The clearing (if self-clearing alarm) parameter specifies whether to allow an operator to clear an alarm if the alarm is self-clearing. A self-clearing alarm is cleared when an alarm-clearing condition occurs. This parameter is configurable when the manual severity alterations parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

Alarms that are not self-clearing must be cleared manually. The *5620 SAM Troubleshooting Guide* describes which alarms are self-clearing.

De-escalation

Table 154-1 lists where to find information about the De-escalation parameter.

Table 154-1 De-escalation parameter

Parameter	See
De-escalation for alarm	De-escalation parameter in this section
De-escalation for policy	de-escalation (defined by specific policy) parameter in this section

De-escalation

(deEscalationEnabled)

The De-escalation parameter specifies whether to de-escalate the severity level of an alarm based on how frequently the alarm is processed by the 5620 SAM. When the parameter is enabled, you can add one or more threshold rules to the policy. This parameter is configurable when the automatic severity alterations parameter is set to Enabled. The options are:

- Enabled
- Disabled (default)

de-escalation (defined by specific policy)

(isSeverityDeEscalationEnabled)

The de-escalation (defined by specific policy) parameter specifies whether to automatically de-escalate the severity of an alarm based on the specific alarm policy. This parameter is configurable when the automatic severity alterations parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

Description

See the [Description](#) parameter in section 161.1.

Detailed Text

The Detailed Text parameter specifies the updated note information when a note for an alarm is modified. The modified note information appears under the Revision History tab as the textual explanation. The range is 1 to 255 alphanumeric characters.

Domain

(domain)

The Domain parameter specifies the type of policy to be associated with an object. You can list and choose a domain by clicking on the Select button.

Escalation

Table 154-2 lists where to find information about the Escalation parameter.

Table 154-2 Escalation parameter

Parameter	See
Escalation for specific alarm types	Escalation parameter in this section
Escalation for global alarm policy	escalation (defined by specific policy) parameter in this section

Escalation

(escalationEnabled)

The Escalation parameter specifies whether to escalate the severity level of an alarm based on how frequently the alarm is processed by the 5620 SAM. When the parameter is set to Enabled, you can add one or more threshold rules to the policy. The options are:

- Enabled
- Disabled (default)

escalation (defined by specific policy)

(isSeverityEscalationEnabled)

The escalation (defined by specific policy) parameter specifies whether to automatically escalate the severity of an alarm based on the specific alarm policy. This parameter is configurable when the automatic severity alterations parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

Frequency

(frequencyThreshold)

The Frequency parameter specifies how many times in a 24-hour period that an alarm needs to occur before the severity level is escalated or de-escalated based on the Severity parameter. The range is 1 to 100 000. There is no default. You must configure the parameter.

Group Tag

(groupTag)

The Group Tag parameter specifies a name for an alarm or group of alarms. The range is 0 to 15 alphanumeric characters. The default is N/A.

Use the parameter to create a common name for the same type of alarms. For example, if you gave all ospf class alarms the Group Tag name “OSPF”, you could then generate a list of only OSPF alarms, by sorting them using the OSPF group tag.

History Enabled

(historyEnabled)

The History Enabled parameter specifies whether an entry should occur in the log each time a policy is applied to change the severity level of an alarm. The options are:

- Enabled (default)
- Disabled

implicit severity demotion

(isSeverityImplicitDemotionEnabled)

The implicit severity demotion parameter specifies whether to automatically demote the severity of the alarm based on the specific alarm policy. The parameter is configurable when the automatic severity alterations parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

implicit severity promotion

(isSeverityImplicitPromotionEnabled)

The implicit severity promotion parameter specifies whether to automatically promote the severity of the alarm based on the specific alarm policy. This parameter is not configurable if the automatic severity alterations parameter is set to Disabled. The options are:

- Enabled (default)
- Disabled

Initial Severity Assignment

(autoAssignedSeverity)

The Initial Severity Assignment parameter specifies the severity level of the alarm when it is first raised. The default value is based on the specific alarm that you are viewing. The options are:

- cleared
- indeterminate
- info
- condition
- warning
- minor
- major
- critical

Interval

(collectionInterval)

The Interval parameter specifies the amount of time that alarms are collected. The default value is based on the specific alarm that you are viewing. The options are:

- | | |
|----------------------|-----------------------|
| • 10 minutes | • 2 hours, 15 minutes |
| • 15 minutes | • 2 hours, 30 minutes |
| • 30 minutes | • 2 hours, 45 minutes |
| • 45 minutes | • 3 hours |
| • 1 hour | • 6 hours |
| • 1 hour, 15 minutes | • 9 hours |
| • 1 hour, 30 minutes | • 12 hours |
| • 1 hour, 45 minutes | • 24 hours |
| • 2 hours | |

Log On Change

(logOnChange)

The Log On Change parameter specifies whether to log an event and store the alarm in the historical alarm database when an alarm property changes, for example, when an alarm is acknowledged. The options are:

- Enabled
- Disabled (default)

Log On Deletion

(logOnDeletion)

The Log On Deletion parameter specifies whether to log an event and store the alarm in the historical alarm database when an alarm is deleted. Alcatel-Lucent recommends that you specify the Enabled option, otherwise there is no record of the alarm after it is deleted. The options are:

- Enabled (default)
- Disabled

manual

(manualDeletionRule)

The manual parameter specifies when an operator can manually remove an alarm. When this parameter is set to disabled, operators cannot manually remove alarms. The options are:

- disabled
- when cleared
- when acknowledged
- when cleared and acknowledged
- when cleared or acknowledged
- always (default)

manual severity alterations

(isSeverityManuallyAlterable)

The manual severity alterations parameter specifies whether operators can manually change the severity of alarms. The parameter is configurable when the Severity Alterable parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

Max 24hr Partition Log Size (records)

(maxDailySize)

The Max 24hr Partition Log Size (records) parameter specifies the maximum number of alarm history records in an alarm history partition. The 5620 SAM stores alarm history records in partitions that correspond to 24h periods. Each day, at midnight UTC, or when the number of alarm history records in the current partition reaches the parameter value, the 5620 SAM deletes the oldest partition and creates a new partition. The range is 2000 to 100 000. The default is 50 000.

Object Type

The Object Type parameter specifies the type of object that is to be associated with an alarm policy. You can list and choose an object type by clicking on the Select button.

Order

(order)

The Order parameter specifies the numeric sequence of attributes listed in the Additional Text field on the Alarm Info form and the dynamic alarm list. The range is 0 to 65 535.

Overwrite existing

(overwrite)

The Overwrite existing parameter specifies whether existing text in the Additional Text field on the Alarm Info form is overwritten. If the parameter is disabled, new information is appended to the existing text. The options are:

- Enabled
- Disabled (default)

Reason for change

The Reason for change parameter specifies the justification for editing an existing note to an alarm. The options are:

- unspecified (default)
- unknown
- comment
- clarification
- update
- confirmation
- correction
- dispute

Severity

(associatedSeverity)

The Severity parameter specifies which severity level an alarm should be escalated or de-escalated to, if the alarm exceeds the threshold value set by the Frequency parameter. Table 154-3 describes the parameter options.

Table 154-3 Severity parameter

Option	Option description
unspecified (default)	No severity level is assigned.
cleared	The alarm, regardless of the previous state, is cleared and is no longer current. Typically, a cleared alarm is removed from the list of active alarms to the history log.
indeterminate	The 5620 SAM uses internal rules to determine the severity level of the alarm. For example, when a disk full alarm is raised, the alarm is indeterminate while the 5620 SAM determines whether the alarm should be minor, major, or critical, depending on the remaining disk capacity. When an alarm has its severity changed to indeterminate based on existing rules, the 5620 SAM reverts the alarm severity back to its initial rule.

(1 of 2)

Option	Option description
info	The alarm reports information only and does not signify a fault condition.
condition	—
warning	The reporting device detected a condition that could potentially impede service, even though no significant service disruption has occurred. The problem should be investigated to determine whether further action is required before the condition escalates.
minor	The event or condition reported is caused by a fault, which is not currently affecting essential network operation. The problem should be investigated to determine whether corrective action is required to prevent a more serious service-affecting condition.
major	The event or condition reported is causing a degradation of service and corrective action should be taken as soon as possible. For example, a major alarm may be raised if the capacity of a managed object is affected, which may result in degradation or interruption of service.
critical	A severe service-affecting fault has occurred, and corrective action should be taken immediately. For example, the failure of a managed object may result in a significant disruption or complete loss of service due to a device failure.

(2 of 2)

Severity Alterable

(isSeverityAlterable)

The Severity Alterable parameter specifies whether to allow automatic changes to severity based on individual alarm policies or manual changes to the severity based on operator actions. The options are:

- Enabled (default)
- Disabled

severity demotion

(isSeverityManualDemotionEnabled)

The severity demotion parameter specifies whether to allow an operator to decrease the severity of an alarm. The parameter is configurable when the manual severity alterations parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

severity promotion

(isSeverityManualPromotionEnabled)

The severity promotion parameter specifies whether to allow an operator to increase the severity of an alarm. The parameter is configurable when the manual severity alterations parameter is set to Enabled. The options are:

- Enabled (default)
- Disabled

Squelch

(isSquelched)

The Squelch parameter specifies whether every instance of the specific alarm is ignored. This allows for event suppression. When the parameter is enabled, the alarm is not displayed on the client GUI and any OSS system listening on the JMS event channel do not receive notification of the alarm. The options are:

- Enabled
- Disabled (default)

155 –Discovery Manager parameters

155.1 Discovery Manager parameters 155-2

155.1 Discovery Manager parameters

This chapter describes the parameters on the Discovery Manager form and child forms.

Administrative State

See the [Administrative State](#) parameter in section 161.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 161.1.

Description

See the [Description](#) parameter in section 161.1.

Displayed Name

See the [Displayed Name](#) parameter in section 161.1.

Element Manager System Name

(**displayName**)

The Element Manager System Name parameter specifies a name for the created Element Manager System. Only the characters a-z, A-Z, 0-9, and _ are allowed in the name. The range is 0 to 64 characters.

Group Name

(**topologyGroupPointer**)

The Group Name parameter specifies the topology group into which newly discovered Network Elements are placed. Click on the Select button to list and choose a topology group.

Host Name

(**hostName**)

The Host Name parameter specifies the host name of the server. The range is 1 to 80 characters.

ID

(**id**)

The ID parameter specifies a unique ID for a discovery rule. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 5000. The default is 0.

Ignore Timestamps

The Ignore Timestamps parameter specifies whether entries with unchanged last change timestamps are processed. The options are:

- Enabled
- Disabled (default)

IP Address

(ipAddress)

The IP Address parameter specifies a unique identifier for a network element in standard IP address format. The format of the IP address is IPv4 or IPv6, depending on the setting of the [Management Protocol](#) parameter.

Last Active Management IP

(activeManagementIp)

The Last Active Management IP parameter specifies the last active management IP address for a device. If the device is unmanaged and then later remanaged again, the 5620 SAM attempts to use this address to rediscover the device unless the [Use Original Management IP](#) parameter is enabled.

Management Protocol

(ipAddressType)

The Management Protocol parameter specifies the format of the IP addresses that are specified for discovery purposes. The options are:

- IPv4 (default)
- IPv6

Mask Bits

(maskBits)

The Mask Bits parameter specifies the mask bits for a general IP range to discover a subnet. You can discover a subnet by specifying a general IP address and setting a portion of the network mask bits to 0. For example, when you set the IP address to 192.168.24.0 and set the network mask bits to 24, all devices in subnet 192.168.24 are discovered. The range is 24 to 32. The default value is 32.

OLC State

(olcState)

The OLC State parameter specifies whether an object or service is in-service or maintenance to filter alarms in the Alarms Window. Alarms are generated for objects and services regardless of the OLC State parameter setting. The parameter setting is not sent to the objects or services.

You can set the OLC state for the following objects and services:

- network element
- card slot
- daughter card
- port
- composite service
- service
- site
- LAG
- SAPs (L2 access interfaces and L3 access interfaces)

See the chapter 26 in the *5620 SAM User Guide* for more information about the OLC.

Table 155-1 describes the options.

Table 155-1 OLC State parameter

Option	Option description	Default
Maintenance	For objects and services that are in maintenance	The default is Maintenance for services. The default value for objects can be specified in the discovery rules.
In Service	For objects and services that are in service	The default is In Service for objects. The default value for services can be specified using the nms-server.xml file.

Password

(password)

The Password parameter specifies the password that is used to connect to the Element Manager System server. The password is not visible outside of the SAM server. The range is 0 to 32 characters.

Read Policy ID

(readMediationPolicyId)

Click on the Select button to choose a Read Policy for the discovery rule, or click on the View button to display the selected policy.

Server IP Address

(ipAddress)

The Server IP Address parameter specifies the IP address of the Element Manager System server. The default is 0.0.0.0.

Server Port Number

(portNumber)

The Server Port Number parameter specifies the port number used to connect to the Element Manager System server. The range is 1 to 65 535. The default is 12 800.

Server Type

(type)

The Server Type parameter specifies the server type. The options are:

- Element Manager (default)
- Unknown

Usage

(usage)

The Usage parameter specifies how a rule is used as a search filter to discover network elements. For example, one rule element may specify that a subnet be included and therefore discovered, while another rule element may specify that specific IP addresses in the subnet be excluded and therefore not discovered. Table 155-2 describes the parameter options.

Table 155-2 Usage parameter

Option	Option description	Dependencies
Include (default)	Specifies that the discovery rule is used to find elements that meet the search criteria	—
Exclude	Specifies that the discovery rule is used to filter out elements that meet the search criteria	

Use Original Management IP

(useOriginalDiscoveryIp)

The Use Original Management IP parameter specifies that the original discovery IP address is retained as the management IP address for a device if the device is placed in an unmanaged state and then later remanaged again by the 5620 SAM. Table 155-3 describes the parameter options.

Table 155-3 Use Original Management IP parameter

Option	Option description
Disable (default)	The 5620 SAM retains the Last Active Management IP parameter value as the device management IP address after the device is un-managed and then re-managed.

(1 of 2)

Option	Option description
Enable	The 5620 SAM retains the Use Original Management IP parameter value as the device management IP address after the device is un-managed and then re-managed.

(2 of 2)

User Name

(userName)

The User Name parameter specifies the user name that is used to connect to the Element Manger System server. The range is 0 to 50 characters.

Write Policy ID

(writeMediationPolicyId)

Click on the Select button to choose a Write Policy for the discovery rule, or click on the View button to display the selected policy.

156 –Generic NE Manager parameters

156.1 Generic NE Manager parameters 156-2

156.1 Generic NE Manager parameters

This chapter describes the parameters on the Generic NE Manager form and child forms.

Additional Text

(additionalText)

The Additional Text parameter specifies additional information about the alarm, such as troubleshooting information, that is displayed in the Additional Text field on the alarm information form. The range is 0 to 300 characters. The default is Source Trap OID `${trapOid}`, where Source Trap OID is literal text and `${trapOid}` is a scripting function that returns the SNMP trap OID. The parameter is configurable when the [Use Default Additional Text](#) parameter is disabled.

The parameter value can contain the following:

- literal text
- one or more scripting functions
- a combination of literal text and scripting functions

A scripting function obtains information about the SNMP trap event, such as the trap source identifier. The following scripting functions are supported:

- `${trapOid}`—returns the SNMP trap OID
- `${getVarValue(n)}`—returns varbind value *n* from the SNMP trap PDU, where *n* is a number; the lowest value is 1, which represents the first varbind that follows the trap OID varbind
- `${routerId}`—returns the SNMP trap source IP address

For example, varbind 3 in an SNMP trap contains the LSP index, and the parameter value is the following:

```
Alarm source: ${routerId}, LSP_${getVarValue(3)}
```

When LSP 159 on generic NE 192.168.3.14 goes down, the following text is generated and displayed in the Additional Text field on the alarm information form:

Alarm source: 192.168.3.14, LSP_159



Note 1 — The `getVarValue` function returns an empty string if the specified varbind is not present in the trap.

Note 2 — The 5620 SAM limits the text generated by a scripting function in this parameter to 4000 characters.

Note 3 — If you use the 5620 SAM Script Manager or another velocity-based tool to create a function, you must do the following:

- Define a variable called `D` using the following statement at the beginning of the script:
`#set (D = '$')`
- Substitute `${D}` for the `$` in each script function statement; for example, `${trapOid}` becomes `${D}{trapOid}`.

Administrative State

(adminState)

The Administrative State parameter specifies the administrative state of the alarm mapping. The options are:

- Up (default)
- Down

Alarm Name

(alarmName)

The Alarm Name parameter specifies a general name for the alarm that the 5620 SAM raises when it receives the trap specified by the [Trap OID](#) parameter. The parameter is configurable when the [Specify Transform Function](#) parameter is disabled. The options are:

- GNE Communication Alarm (default)
- GNE Processing Error Alarm
- GNE Environmental Alarm
- GNE Quality Of Service Alarm
- GNE Equipment Alarm
- GNE Service Alarm
- GNE Transport Alarm
- GNE System Alarm

Using the [FDN Extension](#) parameter, you can add static text and varbind values from the trap PDU to dynamically generate a more specific or more descriptive alarm name.

Answer

(confirmPromptAnswer)

The Answer parameter specifies the answer the 5620 SAM provides to the CLI of a generic NE when a login confirmation prompt is encountered. This parameter applies only if the [Enable Confirm Prompt](#) parameter is enabled. The parameter is specified as a string of up to 255 characters. The answer string should be typed to match exactly the response expected by the CLI of the generic NE.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [161.1](#).

Catalogue Name

Table [156-1](#) lists where to find information about the Catalogue Name parameter.

Table 156-1 Catalogue Name parameter

Parameter	See
Catalogue Name for existing alarm catalogue	Catalogue Name parameter in this section
Catalogue Name for new alarm catalog	Catalogue Name parameter in this section

Catalogue Name

(alarmCatalogue)

The Catalogue Name parameter specifies the name of the alarm catalogue to associate with the generic NE profile. Click on the Select button to choose an alarm catalogue.

Catalogue Name

(catalogueName)

The Catalogue Name parameter specifies the name of the alarm catalogue. The range is 1 to 32 characters. There is no default.

Chassis MAC Object ID

(macObjectId)

The Chassis MAC Object ID parameter specifies the SNMP System MAC Object ID for this product profile. The range is 0 to 255 characters. There is no default.

CLI Supported

(isCliSupported)

Selecting the check box for this parameter enables the CLI Profile and CLI Second Level Login tab buttons on the Generic NE Profile (Create) form. The default is enabled.



Note — The CLI Profile and CLI Second Level Login tab buttons may be disabled for GNEs that do not support CLI.

Command Prompt

(commandPrompt)

The Command Prompt parameter specifies the command prompt that is used to manage the generic NE using the CLI. Regular expressions can be used. The range is 1 to 255 characters. The default is:

```
[\\n\\r][ \\t]?[A-Za-z0-9]*[A-Za-z0-9_-]*(>|#[ \\t])*
```

See the specific device documentation for the appropriate CLI information.

See <http://www.regularexpression.org> for more information about regular expressions.

Description

See the [Description](#) parameter in section [161.1](#).

Default Element Manager URL

(defaultEmUrl)

The Default Element Manager URL parameter specifies the default URL of the generic NE for network element management. You can specify the IP address as a variable in the URL using the following value:

```
%IP%
```

Default External EMS

(defaultExternalEms)

This parameter is used to specify the Installation Path for the External Application to be launched. The path is compatible with Windows, Linux, and Solaris path formats where the client is installed. The installation path must be located where the client is installed. The default is 0 and the maximum is 500 characters.



Note — As this field is stored on the 5620 SAM server, the path of the EMS/craft terminal installed will be the same for all GUI workstations and delegate servers.

Default Out Value

(defaultValue)

The Default Out Value parameter specifies the default value that the transform function assigns to the alarm property specified by the [Out Value Type](#) parameter. The parameter is configurable when the [Specify Default Out Value](#) parameter is set to true. Click on the Select button to choose a default value. The selectable values depend on the [Out Value Type](#) setting.

Disable Paging Command

(disablePagingCommand)

The Disable Paging Command parameter specifies the CLI command to disable paging on the device. The range is 0 to 100 characters. A value of 0 means that the device does not support paging.

See the specific device documentation for the appropriate CLI information.

Enable Confirm Prompt

(hasConfirmPrompt)

The Enable Confirm Prompt parameter specifies whether the CLI of a generic NE presents a confirmation prompt after successful user login. The parameter is disabled by default.

Enable Login Command

(writeAccessLoginCommand)

The Enable Login Command parameter specifies the command to enable the second-level login. This parameter is configurable if the Enable Second Login parameter is set to Enabled. The range is 1 to 255 characters.

See the specific device documentation for the appropriate CLI information.

Enable Login Prompt

(enablingWriteAccessLoginPrompt)

The Enable Login Prompt parameter specifies the write-access password prompt for the second-level login. This parameter is configurable if the Enable Second Login parameter is set to Enabled. The range is 1 to 255 characters. The default is:

```
[\\n\\r][Pp]assword(:)?[ \\t]*
```

See the specific device documentation for the appropriate CLI information.

This parameter is not a regular expression.

Enable Second Login

(twoStepsLogin)

The Enable Second Login parameter specifies whether the generic NE has a second-level of login for write access. The options are:

- Enabled
- Disabled (default)

Error Indicator

(errorIndicator)

The Error Indicator parameter specifies whether the errors in a command result are indicated. Regular expressions can be used. The default is:

```
[\\n\\r].*(ERROR|Error).*
```

See the specific device documentation for the appropriate CLI information.

See <http://www.regularexpression.org> for more information about regular expressions.

Execution Command Timeout (seconds)

(freezeDetectTime)

The Execution Command Timeout (seconds) parameter specifies the time before an execution command times out and is stopped. The range is 1 to 65 535. The default is 120.

External EMS

(externalEms)

The External EMS parameter is set to the value of the [Default External EMS](#) parameter after the GNE device is discovered.

FDN Extension

(fdnExtension)

The FDN Extension parameter specifies an extension that the 5620 SAM appends to the [Alarm Name](#) parameter value to more specifically or descriptively identify the alarm. The range is 0 to 300 characters. There is no default.

The parameter value can contain the following:

- literal text
- one or more scripting functions
- a combination of literal text and scripting functions

A scripting function obtains information about the SNMP trap event, such as the trap source identifier. Including one or more scripting functions enables one alarm mapping to generate differently named alarms of the same type.

The following scripting functions are supported:

- `${trapOid}`—returns the SNMP trap OID
- `${getVarValue(n)}`—returns varbind value *n* from the SNMP trap PDU, where *n* is a number; the lowest value is 1, which represents the first varbind that follows the trap OID varbind
- `${routerId}`—returns the SNMP trap source IP address

For example, if the [Alarm Name](#) parameter is set to GNE Transport Alarm and varbind 3 in the associated SNMP trap contains the LSP index, an FDN extension of `-LSP_${getVarValue(3)}` generates the following alarm name when LSP 14 goes down on a generic NE:

```
GneTransportAlarm-LSP_14
```



Note 1 — The `getVarValue` function returns an empty string if the specified varbind is not present in the trap.

Note 2 — The 5620 SAM limits the text generated by a scripting function in this parameter to 128 characters.

Note 3 — An FDN extension is displayed as part of the alarm name in the title bar of the alarm information form and in the Additional Text field on the form, but is not displayed as part of the alarm name in the 5620 SAM GUI Alarm Window.

Note 4 — If you use the 5620 SAM Script Manager or another velocity-based tool to create a function, you must do the following:

- Define a variable called `D` using the following statement at the beginning of the script:
`#set (D = '$')`
- Substitute `${D}` for the `$` in each script function statement; for example, `${trapOid}` becomes `${D}{trapOid}`.

Full Node Resync on Max Trap Gap

(fullNodeResyncOnMaxTrapGap)

The Full Node Resync on Max Trap Gap parameter specifies whether a full NE resynchronization is performed if the number of lost SNMP traps exceeds the number specified in the [Maximum Trap Gap](#) parameter. The options are:

- Disabled (default)
- Enabled

Generic NE Type

(productName)

The Generic NE Type parameter specifies a unique network element type for this generic NE profile. The range is 1 to 80 characters.

Generic NE Category

(category)

The Generic NE Category parameter specifies the GNE category name as well as the associated topology map icon and equipment tree icons for a GNE profile.

ID

See the [ID](#) parameter in section [161.1](#).

Idle Session Warning Message

(idleSessionWarningMsg)

The Idle Session Warning Message parameter specifies whether an idle session message is ignored if the session becomes idle. The options are:

- Enabled
- Disabled (default)

In Value

(id)

The In Value parameter specifies the varbind value that the transform function converts to the value specified by the [Out Value](#) parameter. The range is –100 000 to 100 000. The default is 0.

In Value Type

(typeInValue)

The In Value Type parameter specifies the type of varbind value that the transform function is to receive. The parameter is not configurable. The default is Integer.

Login Prompt Optional

(isLoginPromptOptional)

The Login Prompt Optional parameter specifies whether the login prompt is optional. The options are:

- Enabled (default)
- Disabled

Login Timeout (seconds)

(loginTimeout)

The Login Timeout (seconds) parameter specifies the time before a login command times out and is stopped. The range is 1 to 65 535. The default is 10.

Max Number Of Sessions

(maxNumSessions)

The Max Number Of Sessions parameter indicates the maximum number of concurrent Telnet sessions that the generic NE can accept. The range is 1 to 300. The default is 1.

Minimum Time Interval Between Full Node Resyncs (seconds)

(minTimeIntervalBetweenFullNodeResyncs)

The Minimum Time Interval Between Full Node Resyncs (seconds) parameter specifies the minimum amount of time, in seconds, that the 5620 SAM waits between successive NE resynchronizations in response to SNMP trap losses. The parameter is configurable when the [Full Node Resync on Max Trap Gap](#) parameter is enabled. The range is 600 to 86 400. The default is 600.

Maximum Trap Gap

(maxTrapGap)

The Maximum Trap Gap parameter specifies the maximum number SNMP traps that are lost before the 5620 SAM performs a full NE resynchronization. The range is 1 to 1000. The default is 200.

Out Value

(value)

The Out Value parameter specifies the value that the transform function assigns to the alarm property specified by the [Out Value Type](#) parameter. Click on the Select button to choose a value. The selectable values depend on the [Out Value Type](#) setting.

Out Value Type

(typeOutValue)

The Out Value Type parameter specifies the type of value to which the [In Value Type](#) value is converted. The options are:

- Alarm Name (default)
- Probable Cause
- Severity

Pre Login Prompt

(preLoginPrompt)

The Pre Login Prompt parameter specifies any pre-login messages. Regular expressions can be used. The range is 0 to 255 characters.

See the <http://www.regularexpression.org> for more information about regular expressions.

Probable Cause

(probableCause)

The Probable Cause parameter specifies the probable cause of the alarm. The parameter is configurable when the [Specify Transform Function](#) parameter is disabled. Click on the Select button to choose a probable cause.

Prompt

(confirmPrompt)

The Prompt parameter specifies the login confirmation prompt issued by the CLI of a generic NE. This parameter applies only if the [Enable Confirm Prompt](#) parameter is enabled. The parameter is specified as a string of up to 255 characters. The prompt string should be typed exactly as it appears in CLI of the generic NE.

Read Login Prompt

(readLoginPrompt)

The Read Login Prompt parameter specifies the read-access login prompt. Regular expressions can be used. The range is 1 to 255. The default is:

```
[\\n\\r][IL]ogin(:)?[ \\t]*
```

See the specific device documentation for more information.

See <http://www.regularexpression.org> for more information about regular expressions.

Read Password Prompt

(readPasswordPrompt)

The Read Password Prompt parameter specifies the read-access password prompt. Regular expressions can be used. The range is 1 to 255 characters. The default is:

```
[\\n\\r][Pp]assword(:)?[ \\t]*
```

See the specific device documentation for more information.

See <http://www.regularexpression.org> for more information about regular expressions.

Reset Command

(resetCommand)

The Reset Command parameter specifies the command to return to the root of the CLI command tree. The range is 1 to 100 characters.

Script ID

(trapConfigScriptPointer)

The Script ID parameter specifies the name of the script that enables trap forwarding to the 5620 SAM. The 5620 SAM runs this script on the generic NE when it tries to manage the generic NE. Click on the Select button to choose a script.

Script ID

(trapDeConfigScriptPointer)

The Script ID parameter specifies the name of the script that disables trap forwarding to the 5620 SAM. The 5620 SAM runs this script on the generic NE when it tries to unmanage or delete the generic NE. Click on the Select button to choose a script.

Severity

(severity)

The Severity parameter specifies the severity of the alarm that the 5620 SAM raises when it receives the trap specified by the [Trap OID](#) parameter. The parameter is configurable when the [Specify Transform Function](#) parameter is disabled. The options are:

- indeterminate (default)
- info
- condition
- warning
- minor
- major
- critical

Specify Default Out Value

(specifyDefaultOutValue)

The Specify Default Out Value parameter specifies whether the transform function assigns a default value to the alarm property specified by the [Out Value Type](#) parameter when the received varbind value is not associated with a value pair in the transform function. The options are:

- disabled (default)
- enabled

Specify Transform Function

(useTransformFnAlarmName)

The Specify Transform Function parameter specifies whether a transform function is to be used to create the Alarm Name value. The options are:

- disabled (default)
- enabled

Specify Transform Function

(useTransformFnProbableCause)

The Specify Transform Function parameter specifies whether a transform function is to be used to define the Probable Cause value. The options are:

- disabled (default)
- enabled

Specify Transform Function

(useTransformFnSeverity)

The Specify Transform Function parameter specifies whether a transform function is to be used to define the Severity value. The options are:

- disabled (default)
- enabled

Supports Trap Restoration Logs

(supportsTrapRestorationLogs)

The Supports Trap Restoration Logs parameter specifies whether the generic NEs associated with this profile support the use of SNMP trap restoration logs for restoring lost traps. The parameter is configurable when the [Supports Trap Sequence Number](#) parameter is enabled. The options are:

- Disabled (default)
- Enabled

Supports Trap Sequence Number

(supportsTrapSeqNumber)

The Supports Trap Sequence Number parameter specifies whether the generic NEs associated with this profile support SNMP trap sequence numbering. The options are:

- Disabled (default)
- Enabled



Caution — The 5620 SAM supports trap sequencing only for devices that increment the trap ID value by 1. Do not enable the parameter if the generic NE increments the trap ID value by anything other than 1.

Sys Object ID

(sysObjectId)

The Sys Object ID parameter specifies a unique SNMP sys object ID for this generic NE profile. The sys object ID can be specific to a product or to a product family using a wildcard character (*). The range is 0 to 255 characters. The default is:

.1.3.6.1.4.1.

Telnet Port

(telnetPort)

The Telnet Port parameter specifies the maximum number of concurrent Telnet sessions that the generic NE can accept or run. The range is 1 to 65535. The default is 23.

Transform Function Name

(transformFnName)

The Transform Function Name parameter specifies a name for the transform function. The range is 1 to 32 characters. There is no default.

Trap Name

(trapName)

The Trap Name parameter specifies an optional name for the trap. The range is 0 to 128 characters. There is no default.

Trap OID

(trapOid)

The Trap OID parameter specifies the SNMP OID of the trap that triggers the alarm. Specify a dot-separated numeric OID in the form *.n.n.n. . .*. The range is 2 to 128 characters. There is no default.

Use Default Additional Text

The Use Default Additional Text parameter specifies whether the alarm contains only the default additional text. When the parameter is enabled, the [Additional Text](#) parameter is set to the default value and cannot be configured. The options are:

- Enabled (default)
- Disabled

Varbind Position

(alarmNameVarBindIdx)

The Varbind Position parameter specifies which varbind in an SNMP trap PDU is associated with the Alarm Name transform function. The parameter is configurable when the [Specify Transform Function](#) parameter is enabled. The range is 1 to 99. The default is 1.

Varbind Position

(probableCauseVarBindIdx)

The Varbind Position parameter specifies which varbind in an SNMP trap PDU is associated with the Probable Cause transform function. The parameter is configurable when the [Specify Transform Function](#) parameter is enabled. The range is 1 to 99. The default is 1.

Varbind Position

(severityVarBindIdx)

The Varbind Position parameter specifies which varbind in an SNMP trap PDU is associated with the Severity transform function. The parameter is configurable when the [Specify Transform Function](#) parameter is enabled. The range is 1 to 99. The default is 1.

Varbind Transform Function

(transformFnAlarmNamePointer)

The Specify Transform Function parameter specifies which transform function is to be used to define the Alarm Name value. Click on the Select button to choose a transform function.

Varbind Transform Function

(transformFnProbableCausePointer)

The Specify Transform Function parameter specifies which transform function is to be used to define the Probable Cause value. Click on the Select button to choose a transform function.

Varbind Transform Function

(transformFnSeverityPointer)

The Specify Transform Function parameter specifies which transform function is to be used to define the Severity value. Click on the Select button to choose a transform function.

Version

(versionId)

The Version parameter specifies a version number for the alarm catalogue. The 5620 SAM does not increment the parameter value; a 5620 SAM operator must update the value manually, as required for version control. The range is 1 to 10000. The default is 1.

Write Login Prompt

(writeLoginPrompt)

The Write Login Prompt parameter specifies the write-access login prompt. Regular expressions can be used. The range is 1 to 255 characters. The default is:

```
[\\n\\r][IL]ogin(:)?[ \\t]*
```

See the specific device documentation for more information.

See <http://www.regularexpression.org> for more information about regular expressions.

Write Password Prompt

(writePasswordPrompt)

The Write Password Prompt parameter specifies the write-access password prompt. Regular expressions can be used. The range is 1 to 255. The default is:

```
[\\n\\r][Pp]assword(:)?[ \\t]*
```

See the specific device documentation for more information.

See <http://www.regularexpression.org> for more information about regular expressions.

157 –Mediation parameters

157.1 Mediation parameters 157-2

157.1 Mediation parameters

This chapter describes the parameters on the Poller Manager form and child forms.

Administrative State

See the [Administrative State](#) parameter in section 161.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 161.1.

Communication Protocol

(cliCommunicationProtocol)

The Communication Protocol parameter specifies the protocol that is used to connect to the device using the CLI. The options are:

- Telnet (default)
- SSH2

Community String

(community)

The Community String parameter specifies the name of the community shared between the network manager and a managed element. This parameter is configurable when the Security Model parameter is set to SNMP v2c. The range is 0 to 32 characters. The default is private.

Connect Timeout (sec)

(ftpReadTimeout)

The Connect Timeout parameter specifies the timeout period for the FTP connection. The range is 0 to 120 seconds. The default is 10.

Description

(description)

The Description parameter specifies a description for the policy. The range is 0 to 255 characters.

Discovery Rule Scan Interval

(topologyScanInterval)

The Discovery Rule Scan Interval parameter specifies how often the 5620 SAM rescans the network according to existing discovery rules. The options are:

- 5 minutes
- 15 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 1 hour, 15 minutes
- 1 hour, 30 minutes (default)
- 1 hour, 45 minutes
- 2 hours
- 2 hours, 15 minutes
- 2 hours, 30 minutes
- 2 hours, 45 minutes
- 3 hours
- 4 hours
- 8 hours
- 12 hours
- 24 hours
- 48 hours

Displayed Name

(displayedName)

The Displayed Name parameter specifies a name for the policy. The range is 0 to 80 characters.

File Transfer Type

(fileTransferType)

The File Transfer Type parameter specifies the protocol that is used for file transfers between the managed device and the 5620 SAM. Secure file transfer uses SCP and is supported on the following devices.

- 7210 SAS-D-6F-4T ETR
- 7210 SAS-M 24F
- 7210 SAS-M 24F 2XFP
- 7210 SAS-M 24F 2XFP ETR
- 7210 SAS-X 24F 2XFP
- 7450 ESS
- 7705 SAR
- 7710 SR
- 7750 SR
- OS 6250M
- OS 6250SME
- OS 6400
- OS 6850
- OS 6850E
- OS 6855
- OS 9600
- OS 9700
- OS 9700E
- OS 9800
- OS 9800E

The options are:

- FTP (default)
- Secure
- TFTP

When you choose the Secure option, node database backup and restores, software upgrades, and accounting statistics are transferred securely.



Note — If the parameter is set to Secure, the [Communication Protocol](#) parameter must be set to SSH2. The [User Name](#) and [User Password](#) parameters must be the user name and password of the SSH server.

Network Element Type

(neType)

The Network Element Type parameter specifies the type of NE to which the event notification policy applies. There is no default. The options are:

- Alcatel-Lucent 1830 PSS
- Alcatel-Lucent 5780 DSC
- Alcatel-Lucent 7210 SAS-E
- Alcatel-Lucent 7210 SAS-M24F
- Alcatel-Lucent 7210 SAS-M24F2XFP
- Alcatel-Lucent 7210 SAS-M24F2XFP [ETR]
- Alcatel-Lucent 7210 SAS-X24F2XFP
- Alcatel-Lucent 7250 SAS
- Alcatel-Lucent 7250 SAS-ES
- Alcatel-Lucent 7250 SAS-ESA
- Alcatel-Lucent 7450 ESS
- Alcatel-Lucent 7701 CPAA
- Alcatel-Lucent 7705 SAR
- Alcatel-Lucent 7710 SR
- Alcatel-Lucent 7750 SR
- Alcatel-Lucent 7750 SR MG
- Alcatel-Lucent 9471 MME
- Alcatel-Lucent 9xxx eNodeB
- Alcatel-Lucent 9500 MPR
- Alcatel-Lucent OS 6250
- Alcatel-Lucent OS 6400
- Alcatel-Lucent OS 6850
- Alcatel-Lucent OS 6850E
- Alcatel-Lucent OS 6855
- Alcatel-Lucent OS 9600
- Alcatel-Lucent OS 9700
- Alcatel-Lucent OS 9800
- Alcatel-Lucent OS 9700E
- Alcatel-Lucent OS 9800E
- Generic NE
- Telco

Number of Varbind per PDU

(numberOfVarPerPdu)

The Number of Varbind per PDU parameter specifies the maximum number of variable bindings, or varbinds, in the SNMP PDUs associated with the MIB entry policy. The parameter is used to adjust the PDU size with respect to the network MTU size. The range is 20 to 200. The default is 100.



Caution — Changing the parameter value may affect the time required for subsequent NE resynchronizations and degrade 5620 SAM server performance. Do not change the parameter value from the default without contacting Alcatel-Lucent technical support.

Ping Command Timeout (seconds)

(maxOSCommandExecutionTimeSeconds)

The Ping Command Timeout (seconds) parameter specifies how much time should be allowed to elapse before a timeout alarm is generated. The range is 1 to 30. The default is 3.

Ping Interval (minutes)

(pingScheduleMinutes)

The Ping Interval (minutes) parameter specifies how many minutes should elapse before a ping is attempted. The range is 0 to 10 000. The default is 2.

Ping Interval (seconds)

(pingScheduleSeconds)

The Ping Interval (seconds) parameter specifies how many seconds should elapse before a ping is attempted. The range is 0 to 59. The default value is 0.

Policy ID

(id)

The Policy ID parameter specifies a unique ID for the policy. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 65 535. The default is 0.

Polling Admin State

(administrativeState)

The Polling Admin State parameter specifies if the MISB is periodically resynchronized. When the Polling Admin State parameter value is set to up, periodic polling occurs according to the “[Polling Interval](#)” parameter setting. When the Polling Admin State parameter value is set to down, periodic polling is not executed. The options are:

- Up (default)
- Down

Polling Interval

(pollingInterval)

The Polling Interval parameter specifies how often MIB elements of discovered and managed devices are polled for changes. When changes are detected, the 5620 SAM rereads the MIB element and updates the database. The default for the 7210 SAS-E, 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7701 CPAA, and 7705 SAR is Disabled. The default for other devices depends on the type of MIB element. When this parameter is disabled, regular synchronization between NEs and the database does not occur. The options are:

- Disabled
- 5 minutes
- 15 minutes
- 30 minutes
- 45 minutes
- 1 hour
- 1 hour, 15 minutes
- 1 hour, 30 minutes
- 1 hour, 45 minutes
- 2 hours
- 2 hours, 15 minutes
- 2 hours, 30 minutes
- 2 hours, 45 minutes
- 3 hours
- 4 hours
- 8 hours
- 12 hours
- 24 hours
- 48 hours

Polling Synchronization Time

(pollingSyncTime)

See the [Polling Synchronization Time](#) parameter in section 161.1.

Port

(snmpPort)

The Port parameter specifies the port that is used for SNMP management. Use the default port 161 for all managed NEs, except the 9471 MME, which requires port 8001.

Read Timeout (sec)

(ftpReadTimeout)

The Read Timeout parameter specifies the read timeout period for the FTP connection. The range is 0 to 600 seconds. The default is 50.

Retry

(snmpRetry)

The Retry parameter specifies the number of retries for SNMP polling or deployment requests between the 5620 SAM and the managed devices. When a request is made, either polling or deployment, from the 5620 SAM to the managed device, and a response is not received from the managed device, the parameter determines the number of retries of the same request. A response may not be received because of network errors with UDP, or because the timeout (ms) parameter value is exceeded. The range is 0 to 4. The default is 1.

Schedule Enabled

(pingScheduleEnabled)

The Schedule Enabled parameter specifies whether pings should occur, based on the Ping Interval (minutes) and Ping Interval (seconds) parameters. The options are:

- Enabled
- Disabled (default)

You must enable scheduling for the default ping policy to be performed. When scheduling is not enabled, and a managed device is not reachable, management connection alarms may not be raised.

For example, if there is no standby CPM or in-band management IP address, a ping policy should be created that has the parameter disabled. This allows an inactive ping policy to be applied during discovery rule creation for the in-band management interface ping and standby CPM ping. This ensures those non-existent interfaces are not pinged. In this example, ping policy with the parameter enabled are created and applied during discovery rule creation for an out-of-band interface, since the interface exists and can be pinged.

Security Model

(securityModel)

The Security Model parameter specifies which version of SNMP should be used, depending on your network security requirements. Table 157-1 describes the parameter options.

Table 157-1 Security Model parameter

Option	Option description	Dependencies
SNMP v1	Version v1 of SNMP is used for authentication.	The Community String parameter must match that of the managed NE.
SNMP v2c (default)	Version 2c of SNMP is used for authentication.	
SNMP v3 (USM)	Version 3 of SNMP is used for authentication.	Choose a user by clicking on the Select button.

SSH2 Server Port

(sshCommunicationPort)

The SSH2 Server Port parameter specifies the port of the secure SSH2 server that is contacted by the 5620 SAM. This parameter is configurable when the [Communication Protocol](#) parameter is set to SSH2. The default is 22.

Timeout (milliseconds)

(snmpTimeout)

The Timeout (milliseconds) parameter specifies the SNMP timeout value for polling or deployment requests between the 5620 SAM and the managed devices. When the request is sent, and no response is received within the Timeout value set, then another request is sent if the Retry parameter value is greater than 1. The range is 200 to 40 000. The default is 10 000.

User Name

(userName)

The User Name parameter specifies the CLI user name. On CLE devices, such as the 7250 SAS and Telco devices, the [User Name](#), [User Password](#), and Confirm User Password parameters are used to allow CLI access on the managed device.

The range is unlimited. The default depends on the type of managed device. Contact your Alcatel-Lucent support representative for more information.

User Password

(cliPassword)

The User Password parameter specifies the CLI password for the user. On CLE devices, such as the 7250 SAS and Telco devices, the [User Name](#), [User Password](#), and Confirm User Password parameters are used to allow CLI access on the managed device.

The value that you enter for the User Password parameter must also be entered for the Confirm Password parameter value. The range is 0 to 80 characters. The default depends on the type of managed device. Contact your Alcatel-Lucent support representative for more information.

158 –NE Self Config Policy Manager parameters

158.1 NE Self Config Policy Manager parameters 158-2

158.1 NE Self Config Policy Manager parameters

This chapter describes the parameters on the NE Self Config Policy Manager form.

Checkpoints Before

(checkPoints)

The Checkpoints Before parameter specifies the steps of the self configuration process flow that requires confirmation before proceeding. You can choose one or more options. All options are enabled by default. The options are:

- (2) SW Upgrade
- (3) Configuration Deployment
- (4) Administrative Enable

Name

(displayName)

The Name parameter specifies the displayed name of the self-configuration policy. The range is 0 to 80. There is no default.

Process Flow

(processFlow)

The Process Flow parameter specifies the actions performed by the 5620 SAM when self configuration of an eNodeB starts. You can choose one or more of the available options. All options are enabled by default. The options are:

- (1) Auto Start
- (2) SW Upgrade
- (3) Configuration Deployment
- (4) Administrative Enable

159 –RAN License Manager parameters

159.1 RAN License Manager parameters 159-2

159.1 RAN License Manager parameters

This chapter describes the parameters on the RAN License Manager form and child forms.

Email Recipient Address

The Email Recipient Address parameter specifies the email addresses that will receive notifications of RAN license violations and threshold events. Multiple email addresses can be listed and separated by the ; character. The range is 0 to 80. There is no default.

First Expiration Threshold (days)

The First Expiration Threshold (days) parameter specifies first threshold of entitlement expiry for triggering RAN license notification. The 5620 SAM raises a minor alarm when the number of days remaining on an entitlement crosses the threshold specified by this parameter. The range is 0 to 365. The default is 90.

First Usage Threshold (%)

The First Usage Threshold (%) parameter specifies the first percentage threshold of entitlement token consumption for triggering RAN license notification. The 5620 SAM raises a minor alarm when RAN license token consumption crosses the threshold specified by this parameter. The range is 0 to 100. The default is 75.

Report File Format

The Report File Format parameter specifies the file format of exported RAN license reports. The options are:

- HTML (default)
- CSV

Second Usage Threshold (%)

The Second Usage Threshold (%) parameter specifies the second threshold of entitlement token consumption for triggering RAN license notification. The 5620 SAM raises a major alarm when RAN license token consumption crosses the threshold specified by this parameter. The range is 0 to 100. The default is 90.

Second Expiration Threshold (days)

The Second Expiration Threshold (days) parameter specifies second threshold of entitlement expiry for triggering RAN license notification. The 5620 SAM raises a major alarm when the number of days remaining on an entitlement crosses the threshold specified by this parameter. The range is 0 to 365. The default is 30.

160 –Pre-Provisioned NE Manager parameters

160.1 Pre-Provisioned NE Manager parameters 160-2

160.1 Pre-Provisioned NE Manager parameters

This chapter describes the parameters on the Pre-Provisioned NE Manager form and child forms.

Active Management IP

(**mgmtIpAddress**)

The Active Management IP parameter specifies the expected active management IP address of the pre-provisioned eNodeB. The default is 0.0.0.0.

Chassis Type

(**chassisType**)

The Chassis Type parameter specifies the chassis type of the eNodeB. There is no default. The options are:

- 9412 D2U E-NODEB FDD
- 9412 D2U E-NODEB TDD
- 9926 D2U E-NODEB FDD
- 9926 D2U E-NODEB TDD

Hardware Identifier

(**hardwareIdentifier**)

The Hardware Identifier parameter specifies the unique identifier for the node. The range is 0 to 256. There is no default.

Network Element ID

(**identifier**)

The Network Element ID parameter specifies the identifier of the pre-provisioned NE. The range is 1 to 64. There is no default.

Network Element Version

(**nodeVersion**)

The Network Element Version parameter specifies the version of the eNodeB. There is no default. The options are:

- 1.1.0
- 2.0.0
- 2.1.0
- 3.0.0
- 3.9.0
- 4.0.0

161 –Common Administration menu parameters

161.1 Common Administration menu parameters 161-2

161.1 Common Administration menu parameters

This chapter describes the parameters that are common to the Administration menu forms and child forms.

Accounting Port

(**accountingPort**)

The Accounting Port parameter specifies the accounting port of the RADIUS server that is contacted. This parameter is configurable on the 7710 SR, 7450 ESS, and 7750 SR. The range is 1 to 65 535. The default is 1813.

Address

(**address**)

The Address parameter specifies the IP address of the TACACS+ or RADIUS server. Each RADIUS or TACACS+ server must have its own unique IP address. There is no default IP address displayed. You must configure the parameter.

Administrative State

(**administrativeState**)

The Administrative State parameter specifies whether an object is administratively enabled. The default depends on the object type. For example, for RADIUS servers, the default is Up. For logging and performance statistics log policies, the default is Down. The options are:

- Up
- Down

Authentication Port

(**port**)

The Authentication Port parameter specifies the TCP port of the RADIUS server that is contacted. The range is 1 to 65 535. The default is 1812.

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

CoA Only

(coaOnly)

The CoA Only parameter specifies whether a RADIUS server entry in a subscriber authentication policy is used only for CoA messages. The options are:

- Enabled
- Disabled (default)

Configuration Mode

(configurationMode)

The Configuration Mode parameter specifies the mode in which the global policy is configured and determines whether the policy can be distributed to the network elements. Table 161-1 describes the parameter options.

Table 161-1 Configuration Mode parameter

Option	Option description	Dependencies
Draft (default)	The policy is not reviewed or approved for distribution to network elements. The policy can be synchronized.	Cannot be distributed
Released	The policy is reviewed and approved for distribution to network elements. Releasing a global policy does not distribute the policy to existing local definitions for management access filters and CPM IP filters. For all other policies, the policy is distributed when released. The policy can be synchronized.	Can be distributed

Confirm Password

The Confirm Password parameter specifies the password for a user of the system for confirmation purposes. Passwords must use at least one numerical character, one special character, an upper-case character, and a lower-case character, and cannot be the same as the user account name. The range is 8 to 100 characters. The parameter value must match the User Password parameter.

Description

(description)

The Description parameter specifies the description of an object. Table 161-2 describes the parameter ranges and defaults for different object types.

Table 161-2 Description parameter

Object	Range (characters)	Default
Database File Policy	0 to 80	—

(1 of 2)

Object	Range (characters)	Default
Generic NE alarm catalogue	0 to 128	—
NE DoS protection policy	0 to 80	—
OmniSwitch RADIUS policy	0 to 80	—
OmniSwitch TACACS+ policy	0 to 80	—
Scope of command profile	0 to 256	—
Scope of command role	0 to 1000	—
Span of control	0 to 1000	—
Span of control profile	0 to 256	—
User	0 to 80	—
User group	0 to 80	user group

(2 of 2)

Displayed Name

(displayedName)

The Displayed Name parameter specifies a name for the created object. The range is 0 to 32, 1 to 32, 1 to 31, or 0 to 80 characters, depending on the form.



Note — You cannot use the colon symbol in a policy or key chain name. The 5620 SAM uses colons as separators for the object full name.

Distribution Mode

(distributionMode)

The Distribution Mode parameter specifies whether the local policy is synchronized with the associated global policy. Table 161-3 describes the parameter options.

Table 161-3 Distribution Mode parameter

Option	Option description	Dependencies
Sync With Global (default)	The local policy is synchronized with the global policy at all times. The local instance cannot be modified.	—
Local Edit Only	You can modify the local instance only which affects the associated network element. Changes to the global policy do not affect the local policy unless a synchronization operation is manually performed.	—

Enable Accounting

(isAccountingEnabled)

The Enable Accounting parameter specifies whether to enable accounting on the RADIUS or TACACS+ server. Accounting is used to track how often users log into a RADIUS or TACACS+ server for authorization purposes. Accounting must be enabled on your RADIUS or TACACS+ server before setting this parameter to true. The options are:

- true
- false (default)

Enable Authorization

(isAuthorizationEnabled)

The Enable Authorization parameter specifies whether to enable authorization for site users. Setting this parameter to true requires users to authenticate themselves to a RADIUS or TACACS+ server before being granted access to the site (router). The options are:

- true
- false (default)

Enable User Template

(templateUsedByTacplus)

The Enable User Template parameter specifies whether to enable predefined user templates for policies.

- true
- false (default)

Exit On Reject

(authExitOnReject)

The Exit On Reject parameter specifies whether the next method in the password authentication order is attempted when a password authentication method attempt is rejected. When this parameter is enabled and one of the authentication methods configured in the authentication order sends a reject, the next method in the order is not attempted. The options are:

- Enabled
- Disabled (default)

ID

(id)

The ID parameter specifies a unique ID for the created object. The parameter is configurable when the [Auto-Assign ID](#) parameter is disabled. The range is 1 to 65 535. The default is 0, which means that the parameter is not configured.

IP Address

(aaasIpAddress)

The IP Address parameter specifies the IP address or DNS host name of the primary RADIUS or TACACS+ server. An IP address or host name is required when you create a server. The default is 0.0.0.0.

IP Address 2

(aaasIpAddress2)

The IP Address 2 parameter specifies the IP address or DNS host name of an optional backup RADIUS or TACACS+ server. An IP address or host name is required when you create a server.

Password

(password)

The Password parameter specifies the password for a user of the system for confirmation purposes. Passwords must use at least one numerical character, one special character, an upper-case character, and a lower-case character, and cannot be the same as the user account name. The range is 8 to 100 characters. The parameter value must match the Confirm Password parameter.

Polling Synchronization Time

(pollingSyncTime)

The Polling Synchronization Time parameter specifies the polling synchronization start time from which the polling intervals are calculated in hh:mm format based on a 24-hour clock. When the server restarts, the next appropriate collection interval is calculated and polling restarts for all enabled MIBs. The default is 00:00.

Port

(port)

The Port parameter specifies the TCP port of the RADIUS server that is contacted. The range is 1 to 65 535. The default is 1812.

Protocol

(protocol)

The Protocol parameter specifies which protocol to use as a match filter. Table [161-4](#) describes the parameter options.

Table 161-4 Protocol parameter

Options			
NONE	MERIT_INP	RVD	GMTP
HOPOPT	SEP	IPPC	IFMP
ICMP	3PC	any distributed file system (68)	PNNI
IGMP	IDPR	SAT_MON	PIM
GGP	XTP	VISA	ARIS
IP	DDP	IPCV	SCPS
ST	IDPR_CMTP	CPNX	QNX
TCP	TP++	CPHB	A/N Active Networks (107)
CBT	IL	WSN	IPComp
EGP	IPv6	PVP	SNP
IGP	SDRP	BR_SAT_MON	Compaq_Peer
BBN_RCC_MON	IPv6Route	SUN_ND	IPX_in_IP
NVP_II	IPv6Frag	WB_MON	VRRP
PUP	IDRP	WB_EXPAK	PGM
ARGUS	RSVP	ISO_IP	any 0-hop protocol (114)
EMCON	GRE	VMTP	L2TP
XNET	MHRP	SECURE_VMTP	DDX
CHAOS	BNA	VINES	IATP
UDP	ESP	TTP	STP
MUX	AH	NSFNET_IGP	SRP
DCN_MEAS	I_NLSP	DGP	UTI
HMP	SWIPE	TCF	SMP
PRM	NARP	EIGRP	SM
XNS_IDP	MOBILE	OSPFIGP	PTP
TRUNK_1	TLSP	Sprite_RPC	ISIS
TRUNK_2	SKIP	LARP	FIRE
LEAF_1	IPv6_ICMP	MTP	CRTP
LEAF_2	IPv6_Noxt	AX.25	CRUDP
RDP	IPv6_Opts	IPIP	SSCOPMCE
IRTP	any host internal protocol (61)	MICP	IPLT
ISO_TP4	CFTP	SCC_SP	SPS
NETBLT	any local network (63)	ETHERIP	PIPE
MFE_NSP	SAT_EXPAK	ENCAP	SCTP

(1 of 2)

Options			
RSVP_E2E_IGNORE	KRYPTOLAN	any private encryption scheme (99)	FC
IPv6_ICMP	IPv6_No_Nxt	IPv6_Opts	—

(2 of 2)

Protocol Name

(aaasProtocol)

The Protocol Name parameter specifies the protocol type for this policy. The options are:

- RADIUS (default)
- TACACS+

Retry Attempts

(retryAttempts)

The Retry Attempts parameter specifies the maximum number of times an attempt is made to contact the RADIUS server to perform authorization. The range is 1 to 10. The default is 3.

Secret Name

(secret)

The Secret Name parameter specifies a secret value that must match the secret value on the RADIUS or TACACS+ server. Table 161-5 describes the parameter ranges and defaults for different NE releases.

Table 161-5 Secret Name parameter

NE release	Range (characters)	Default
8.0 R3 and earlier	1 to 20	—
8.0 R4 and later	1 to 128	—

Single Connection

(singleConnection)

The Single Connection parameter specifies whether to use a single connection to the TACACS+ server. This allows a single connection to the TACACS+ server to stay up, instead of setting up a new connection for each authentication event. When a single connection is used, all Telnet, SSH, or FTP sessions use the connection. The options are:

- Enabled
- Disabled (default)

Source Address

(sourceAddress)

The Source Address parameter specifies the IP address of the RADIUS or TACACS+ server. The default is 0.0.0.0.

If this object is configured with the address of the router interface, the RADIUS client uses it while making a request to the server. If the address is not configured or is not the address of the one of interfaces, the source address is based on the address of the RADIUS server. If the server address is in-band, the client uses the system IP address. If it is out-of-band, the source address is the address of the management interface.

Source IP

(sourceIpAddress)

The Source IP parameter specifies the IP address of the requester. Specify an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format.

Source IP Mask

(sourceIpAddressMask)

The Source IP Mask parameter specifies the mask bits to use when you specify a general IP range with the Source IP parameter to discover a subnet. Packets matching the specified IP mask are permitted or denied, based on the option chosen by the Action parameter. The range is 0 to 32 for an IPv4 address, or 0 to 128 for an IPv6 address. The default is 0.

Time Out

(aaasTimeOut)

The Time Out parameter specifies the timeout period for server replies to authentication requests. The range is 1 to 30. The default is 2.

Timeout (seconds)

(timeoutSeconds)

The Timeout (seconds) parameter specifies how many seconds the managed device waits for a response from the RADIUS or TACACS+ server. The range is 1 to 90. The default is 3. The default is 5 for the Timeout (seconds) parameter assigned to subscriber authentication policies.

Equipment navigation tree parameters

- 162 – Device parameters
- 163 – CCAG parameters
- 164 – TWAMP parameters
- 165 – IGH parameters
- 166 – ISA-AA Group parameters
- 167 – ISA-IPsec Group parameters
- 168 – ISA-LNS Group parameters
- 169 – ISA-NAT Group parameters
- 170 – ISA-Video Group parameters
- 171 – LAG parameters
- 172 – Shelf parameters
- 173 – APS Groups parameters
- 174 – Card Slot parameters
- 175 – Daughter Card and Daughter Card Slot parameters
- 176 – Bundles parameters
- 177 – Port parameters

- 178 – HSMDA Egress Secondary Shaper parameters
- 179 – Channel parameters
- 180 – Gateway parameters
- 181 – ISA-MG Group parameters
- 182 – Common equipment navigation tree parameters

162 –Device parameters

162.1 Device parameters 162-2

162.1 Device parameters

This chapter describes the parameters on a device properties form, the child forms, and the forms opened using device contextual menu options.

Active Management IP

(**activeManagementIp**)

The Active Management IP parameter specifies the preferred management method used for the device. Table 162-1 describes the parameter options.

Table 162-1 Active Management IP parameter

Option	Option description
Out Of Band (default)	Specifies that management traffic should use the device management port IP address. Out-of-band management means that traffic is sent on the control plane, separate from customer traffic.
In Band	Specifies that management traffic should use the system IP address discovered for the device, or the L3 management interface (if configured). If the Enable L3 Management Interface parameter is enabled, management traffic is directed to the L3 management interface. In-band management means that traffic is sent on the data plane using the customer forwarding path, but is distinguished from customer data using a VRF table.

Active Time-out (minutes)

(**activeTimeout**)

The Active Time-out (minutes) parameter specifies, in m, how long Cflowd samples an active flow before terminating the flow. The range is 1 to 600. The default is 30.

Administrative State

(**administrativeState**)

See the [Administrative State](#) parameter in section 182.1.

Administrative Status

(**adminStatus**)

The Administrative Status parameter specifies whether LLDP is operationally enabled on the system. This is a system-wide configuration and overrides the individual port administrative status. The options are:

- Enabled
- Disabled (default)

Admission Control

(admissionControl)

The Admission Control parameter specifies whether 4QAM throughput can be exceeded to allow the provisioning of additional E1s on a 9500 MPR. This allows a high number of E1s to be transmitted while maintaining adaptive modulation for Ethernet traffic. When Admission Control parameter is enabled, 4QAM throughput cannot be exceed. If the parameter value is set to disabled, 4QAM throughput can be exceeded. The options are:

- Enabled (default)
- Disabled

Aggregation Type

(aggregation)

The Aggregation Type parameter specifies the type of aggregation scheme to export. The parameter is configurable when the [Version](#) parameter is set to version-8. Table [162-2](#) describes the parameter options.

Table 162-2 Aggregation Type parameter

Raw	Flows are not aggregated, but sent to the collector in a V5 record.
Destination Prefix	Flows are aggregated based on the destination prefix and mask, destination AS, and egress interface.
Protocol Port	Flows are aggregated based on the IP protocol type, source port number, and destination port number.
Source Destination Prefix	Flows are aggregated based on the source prefix and mask, destination prefix and mask, source and destination ASs, ingress interface, and egress interface.
Source Prefix	Flows are aggregated based on the source prefix and mask, source AS, and ingress interface.
Matrix	Flows are aggregated based on the source and destination AS, and ingress and egress interfaces.

ATM OAM Loopback Location ID

(atmOamLoopbackLocationId)

The ATM OAM Loopback Location ID parameter specifies the 16 octets that identifies the system loopback location ID as required by the ATM OAM loopback capability. Invalid values include an ATM OAM Loopback Location ID where the first octet is: 00, FF, or 6A. A valid ATM OAM Loopback Location ID requires the first octet to be: 01 or 03. Other values are not accepted. The minimum is 0 and the maximum is 47. The default is 01:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00.

ATM OAM Loopback Period

(atmOamLoopbackPeriod)

The ATM OAM Loopback Period parameter specifies how the number of times the loopback cell is transmitted on the ATM interface to verify its connection to an endpoint on a virtual circuit. You can enable ATM loopbacks for IES and VPRN SAPs on a 7750 SR interface. The range is 0 to 40. The default is 10.

Autonomous System

(asInfo)

The Autonomous System parameter specifies whether the AS information that Cflowd sends for analysis is from the originating AS or peer AS. The options are:

- Origin (default)
- Peer

Auto Revert to Preferred

(isMgmtIpAutoRevertive)

The Auto Revert to Preferred parameter specifies which management method to revert to when the original device returns to an active state after a switchover. Table [162-3](#) describes the parameter options.

Table 162-3 Auto Revert to Preferred parameter

Option	Option description	Dependencies
Enabled	Specifies that the device reverts to the management method configured in the Management IP Selection parameter when the device returns to an active state	Use only when the Management IP Selection parameter is set to Out Of Band Preferred or In Band Preferred
Disabled (default)	Specifies that no attempt to revert to the management method configured in the Management IP Selection parameter is attempted when the device returns to an active state	If the Active Management IP parameter is set to Out Of Band Only or In Band Only and the Auto Revert to Preferred parameter is set to Disabled, a loss of network visibility can occur if in-band management fails.



Note — If there is a communication outage on the preferred management IP address, the 5620 SAM switches to the redundant (non-preferred selection).

If the Auto Revert to Preferred parameter is enabled, the 5620 SAM periodically checks for connectivity on the preferred management IP address. If the communication outage persists, the 5620 SAM continues issuing periodic SNMP reachability alarms to alert the operator that the preferred management IP address is still unreachable. This scenario could give the appearance that the NE is down, when in fact the NE is still managed through the non-preferred management IP address.

Bridge Type

(bridgeType)

The Bridge Type parameter specifies the encap type of 9500 MPR Ethernet ports. The options are:

- 802.1D (default)
- 802.1Q

Cache Size

(cacheSize)

The Cache Size parameter specifies the maximum number of active flows in the flow cache table. The range is 1000 to 131 072. The default is 65 536.

CFLOWD State

(cflowdStatus)

The CFLOWD State parameter specifies whether Cflowd is active. The options are:

- Disabled (default)
- Enabled

Description

The Description parameter specifies a description for the object. The range is 0 to 80 characters. There is no default.

DNS Domain

(sbiDnsDomain)

This parameter specifies the domain name that is used to perform DNS address resolution. There is no default.

Egress

(egressFrameBased)

The Egress parameter specifies whether frame-based accounting is enabled for egress traffic on all of the ports. The options are:

- true
- false (default)

Enable L3 Management Interface

(isL3MgmtItfEnabled)

The Enable L3 Management Interface parameter specifies whether [L3 Management Interface](#) is used for NE management. The options are:

- true
- false (default)

Fast Transmission Interval (Seconds)

(messageFastTx)

The Fast Transmission Interval (Seconds) parameter specifies the interval at which LLDP frames are transmitted on behalf of this LLDP agent during a fast transmission period (for example, when a new neighbor is detected). The range is 1 to 3600. The default is 1.

Group Name

(groupName)

The Group Name parameter specifies the name of the operational group. The range is 1 to 32 characters. There is no default.

Hold Down Time

(holdDownTime)

The Hold Down Time parameter specifies the number of seconds to wait before notifying clients who are monitoring this group when its operational status transitions from up to down. The range is 0 to 3600. The default is 0.

Hold Up Time

(holdUpTime)

The Hold Up Time parameter specifies the number of seconds to wait before notifying clients who are monitoring this group when its operational status transitions from down to up. The range is 0 to 3600. The default is 4.

Host Address

The Host Address parameter specifies the Cflowd collector host address. Specify an IPv4 address in dotted-decimal format

Ignore Timestamps

The Ignore Timestamps parameter specifies whether entries with unchanged last change timestamps are processed. The options are:

- Enabled
- Disabled (default)

In-Active Time-out (seconds)

(inActiveTimeout)

The In-Active Time-out (seconds) parameter specifies how long, in s, Cflowd waits for a matching flow packet before it considers the flow inactive and terminates it. The range is 10 to 600. The default is 15.

Ingress

(ingressFrameBased)

The Ingress parameter specifies whether frame-based accounting is enabled for ingress traffic on all of the ports. The options are:

- true
- false (default)

IP Address

(ipAddress)

The IP Address parameter specifies the current management IP address for a network element. The format of the IP address is either IPv4 or IPv6.

IP Address

(sasUplinkAAddress)

The IP Address parameter specifies an IP address for the 7210 SAS primary uplink port that is used during boot up. A value of 0.0.0.0 indicates that the 7210 SAS uses DHCP to obtain an IP address. The default is 0.0.0.0.

IP Address

(sasUplinkBAddress)

The IP Address parameter specifies an IP address for the 7210 SAS secondary uplink that is used during boot up. A value of 0.0.0.0 indicates that the 7210 SAS uses DHCP to obtain an IP address. The default is 0.0.0.0.

Interface Ip Address

(interfaceIpAddr)

The Interface Ip Address parameter specifies the IP address of the interface used for the SRLG. The default is 0.0.0.0.

L3 Management Interface

(inBandL3ManagementIf)

The L3 Management Interface parameter specifies an optional L3 interface IP address for in-band device management. This parameter is set, by default, to the discovery IP address if the discovery IP address is not the [Management IP Address](#) or the [System IP Address](#). The operator can use this parameter to specify an alternate in-band management interface, if required.

L4 Load Balancing

(l4LoadBalancing)

The L4 Load Balancing parameter specifies whether the device performs system-wide load TCP and UDP load balancing. If enabled, the device includes the L4 source and destination port fields in the hashing calculation for a TCP or UDP packet.

- enabled
- disabled (default)

LACP System Priority

(sysLacpSystemPriority)

The LACP System Priority parameter specifies the priority for link aggregation on the device. The range is 1 to 65 535. The default is 32 768.

Latitude (degrees)

(latitudeInDegrees)

The latitude parameter specifies the latitude in degrees of the NE. The range is -90.0 to 90.0 degrees. The default is 0.0.

LI Local Save Allowed

(liLocalSaveAdmin)

The LI Local Save Allowed parameter specifies whether lawful interception configuration is saved locally. If the information is saved locally it is subject to local regulations. When LI Local Saved parameter is enabled, 5620 SAM periodically performs a save. If the parameter value is set to false, the LI information must be reconfigured after a system reboot. The options are:

- True
- False (default)

Location

(location)

The Location parameter specifies the physical location of the device. The range is N/A, or 0 to 80. The default is N/A.

Use the parameter to indicate a physical location for the device. This is useful when generating inventories of network devices.

Longitude (degrees)

(longitudeInDegrees)

The longitude parameter specifies the longitude in degrees of the NE. The range is -180.0 to 180.0 degrees. The default is 0.0.

Management IP Address

(outOfBandAddress)

The Management IP Address parameter specifies the IP address of the NE management port. The address can be IPv4 or IPv6 format.

Management IP Selection

(mgmtIpRule)

The Management IP Selection parameter specifies the management method to be used if there is a switchover. The Active Management IP parameter must be set to In Band or Out Of Band. Table 162-4 describes the parameter options.

Table 162-4 Management IP Selection parameter

Option	Option description
Out Of Band Preferred	Specifies that out-of-band management is available for the device as the preferred management method if there is a switchover
Out Of Band Only (default)	Specifies that only out-of-band management is available for the device and that no attempt is made to use in-band management if there is a switchover
In Band Only	Specifies that only in-band management is available for the device and that no attempt is made to use out-of-band management if there is a switchover
In Band Preferred	Specifies that in-band management is available for the device as the preferred management method if there is a switchover

To avoid a communications outage between the 5620 SAM and managed NEs, users should configure the Management IP Selection parameter, the [Primary Route Preference](#) parameter, and the [Secondary Route Preference](#) parameter, following the combinations of settings outlined in Table 162-5.

Table 162-5 Management and notification parameter setting combinations

If Management IP Selection parameter is set to...	...Primary Route Preference parameter should be set to...	...and Secondary Route Preference parameter should be set to...
Out Of Band Preferred	Out Of Band	In Band
Out Of Band Only	Out Of Band	None
In Band Only	In Band	None
In Band Preferred	In Band	Out Of Band

Mask

(sasUplinkAMask)

The Mask parameter specifies the subnet mask length for the primary uplink IP address when the IP prefix is specified in CIDR format. The parameter indicates the number of bits that are used for the network portion of the IP address; the rest of the IP address is used to determine the host portion of the IP address. The range is 0 to 32. The default is 0.

Mask

(sasUplinkBMask)

The Mask parameter specifies the subnet mask length for the secondary uplink IP address when the IP prefix is specified in CIDR format. The parameter indicates the number of bits that are used for the network portion of the IP address; the rest of the IP address is used to determine the host portion of the IP address. The range is 0 to 32. The default is 0.

Mask

(uplinkRouteMask)

The Mask parameter specifies the subnet mask length for the route destination IP address when the IP prefix is specified in CIDR format. The mask length parameter indicates the number of bits used for the network portion of the IP address; the remainder of the IP address is used to determine the host portion of the IP address. The range is 0 to 32. The default is 0.

Maximum Consecutive Transmissions

(txCreditMax)

The Maximum Consecutive Transmissions parameter specifies the maximum number of consecutive LLDP PDUs that can be transmitted at any time. The range is 1 to 100. The default is 5.

MEP Id

(id)

The MEP Id parameter specifies the starting MEP ID for automatic MEP ID assignment on an NE. When the parameter is configured and a MEP is created on the NE, the NE assigns the lowest unused value above the parameter value as the MEP ID. The range is 0 to 8191. The default is 0, which means that the parameter is not configured.

Next Hop

(uplinkRouteNextHop)

The Next Hop parameter specifies the next hop IPv4 address that is used to reach the route destination address. Specify an IP address in dotted-decimal format. The default is 0.0.0.0

Notification Interval (Seconds)

(notificationInterval)

The Notification Interval (Seconds) parameter specifies the time interval that must elapse before a notification about a local system MIB change is generated. The range is 5 to 3600. The default is 5.

Number of Tries for Down State

(atmOamRetryDown)

The Number of Tries for Down State parameter specifies the number of times that the loopback attempts transmission on the ATM interface if it does not receive a response. If a response is not received and consecutive retry-down commands also result in failure, the endpoint raises an alarm. The range is 0 to 10. The default is 4.

Number of Tries for Up State

(atmOamRetryUp)

The Number of Tries for Up State parameter specifies the number of times that the loopback attempts transmission on the ATM interface after a response is received. If a response is received and consecutive retry-up commands also result in failure, the endpoint displays an up state. The range is 0 to 10. The default is 2.

Over Flow (percent)

(overflow)

The Over Flow (percent) parameter specifies the percentage of flow cache entries that Cflowd removes when the number of cache entries exceeds the [Cache Size](#) value.

PDUs in Fast Transmission

(messageFastTxInit)

The PDUs in Fast Transmission parameter specifies the number of PDUs to transmit during a fast transmission period. The range is 1 to 8. The default is 4.

Persistent SNMP Indices

(persistentSnmpIndices)

The Persistent SNMP Indices parameter specifies whether persistent SNMP indices are configured on the managed devices. The options are:

- true (default)
- false



Caution — The 5620 SAM requires persistent SNMP indices to save running configurations on managed devices. If persistence is not enabled, there is database inconsistencies and the 5620 SAM is not able to discover managed devices. You should set the parameter to true if persistency has been turned off on the managed device. You cannot set the parameter to false using 5620 SAM. The 5620 SAM cannot properly manage a device with SNMP index inconsistencies.

Physical Impedance

(physicalImpedance)

The Physical Impedance parameter specifies the impedance for all 9500 MPR E1 ports. The options are:

- Unbalance 75 Ohm (default)
- Balance 120 Ohm

Port Number

The Port Number parameter specifies the Cflowd collector UDP port. The range is 1 to 65 535. The default is 2055.

Primary DNS

(sbiPrimaryDns)

The Primary DNS parameter specifies the primary DNS server that is used for DNS name resolution.

Primary Route Preference

(primaryRoutePreference)

The Primary Route Preference parameter specifies the primary routing preference for SNMP notifications and syslog messages. Table 162-6 describes the parameter options.

Table 162-6 Primary Route Preference parameter

Option	Option description	Dependencies
In Band	The logging utility attempts to use the base routing context to send SNMP notifications and syslog messages to remote destinations.	If the remote destination is not reachable via the routing context specified by the Primary Route Preference parameter, the logging utility attempts to connect to the remote destination using the secondary routing preference, as specified by the Secondary Route Preference parameter.
Out Of Band (default)	The Logging utility attempts to use the management routing context to send SNMP notifications and syslog messages to remote destinations.	

QoS Classification

(inFlowClassificationMode)

The QoS Classification parameter specifies the type of IP header information that the 9500 MPR uses to assign traffic to the QoS queues. The options are:

- Disabled (default)
- 802.1p
- DiffServ

Redundant Synchronization Mode

(**redundantSynchronizationMode**)

The Redundant Synchronization Mode parameter specifies when redundant devices should be resynchronized, based on changes to configuration on the devices. Table 162-7 describes the parameter options.

Table 162-7 Redundant Synchronization Mode parameter

Option	Option description
None (default)	Specifies that no resynchronization is performed for redundant devices when one of the device configurations changes.
Configuration File Change	Specifies that resynchronization is performed for redundant devices when the configuration file of one of the devices changes.
Boot Environment Change	Specifies that resynchronization is performed for redundant devices when the BOF file of one of the devices changes.

Re-Init Delay (Seconds)

(**reinitDelay**)

The Re-Init Delay (Seconds) parameter specifies the time interval that must elapse before the current status of a port is reinitialized after a status change. The range is 1 to 10. The default is 2.

Resource Group ID

The Resource Group ID parameter specifies the group to which the NE is assigned for the management of 5620 SAM system resources.



Caution — Changing the Resource Group ID parameter setting has serious consequences. Do not configure the parameter without first contacting your Alcatel-Lucent technical-support representative.

Route Destination

(**uplinkRouteDestination**)

The Route Destination parameter specifies a static route to the image and configuration files in dotted-decimal format for an IPv4 address. The default is 0.0.0.0.

Router ID

(routerId)

The Router ID parameter specifies the routing instance as the IP address of the managed router. The router ID uniquely identifies the device within an autonomous system and is used by OSPF and BGP in the routing table manager instance. This is an IPv4 address in dotted-decimal format.

Sample Rate

(sampleRate)

The Sample Rate parameter specifies the rate at which Cflowd samples packets. Cflowd samples one packet out of every N packets, where N is the parameter value. For example, a value of 100 specifies that one of every 100 packets is to be sampled, and a value of 1 means that all packets are to be sampled. The range is 1 to 10 000. The default is 1000.

Scheduled Polling

(resyncState)

The Scheduled Polling parameter specifies whether polling is enabled for the device. Polling policies are configured under the Poller Policies menu, using the Base Polling Interval and the Discovery Rule Scan Interval parameters. The options are:

- Enabled (default)
- Disabled

Secondary DNS

(sbiSecondaryDns)

The Secondary DNS parameter specifies the secondary DNS server for DNS name resolution. The secondary DNS server is used only if the primary DNS server does not respond.

Secondary Route Preference

(secondaryRoutePreference)

The Secondary Route Preference parameter specifies the secondary routing preference for SNMP notifications and syslog messages. The routing context specified by this parameter is attempted if the remote destination is not reachable using the primary routing preference, as specified by the [Primary Route Preference](#) parameter. Table [162-8](#) describes the parameter options.

Table 162-8 Secondary Route Preference parameter

Option	Option description	Dependencies
In Band (default)	The logging utility attempts to use the base routing context to send SNMP notifications and syslog messages to remote destinations.	If the remote destination is not reachable via the routing context specified by the Primary Route Preference parameter or the Secondary Route Preference parameter, the log utility does not send SNMP notifications and syslog messages to the remote destination.
Out Of Band	The logging utility attempts to use the management routing context to send SNMP notifications and syslog messages to remote destinations.	
None	The logging utility does not attempt to send SNMP notifications and syslog messages to remote destinations.	

Separate LI Administration

(liSeparateAdmin)

The Separate LI Administration parameter specifies whether a node can be configured to separate normal system administrative tasks from tasks of the LI user. When the parameter value is set to true, there is an administrative separation and the LI user is the only entity who can grant LI permissions to any other user. System administrators without LI privileges cannot modify, create, or view any LI-specific configurations. The node must be rebooted to activate the separate mode. The options are:

- True
- False (default)

In the separate mode, the anonymity of the mirror source object is protected. After source criteria is attached to the LI source, the following applies:

- In SAP configurations, only the modifications that stop the flow of LI data while the customer receives data is blocked.
- In filter configurations, if a filter entry is attached to the LI source, modifications and deletion of both the filter and the filter entry are either blocked or permitted, based on the value configured for the [LI Filter Lock](#) parameter. For devices at NE releases prior to 8.0 R7, modifications and deletion of both the filter and the filter entry are blocked.

Slot

The Slot parameter specifies the location on the managed device where the router or switch writes the DHCP persistence file, which tracks all the information learned through DHCP snooping. When this information is written to the compact flash on the managed device, the learned information is retained across reboots.

Use the Select button to choose a flash file location on the appropriate card slot. Click on the OK button to select the card slot. The card slot ID and flash ID are populated on the form.

You can use the Layer 2 and Layer 3 parameters to save the DHCP information to different flash devices, or the same device.

SSH Session

Click on the SSH Session button to start an SSH-secured Telnet session with the device. SSH must be enabled on the device for this option to be available. Only SSH2 is supported on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7450 ESS, 7750 SR, 7250 SAS, and generic NEs. The devices require preconfiguration before an SSH session can be established using SSH2. See the chapter [15](#) for more information about configuring SSH2.

System ID (Loopback Ip Address)

(systemAddress)

The System ID parameter specifies the loopback IP address for the system, also known as the system IP address. When the system IP address is used to discover the device, the management connection is in-band and there must be a route from the 5620 SAM to the port on which the system IP address is configured. The system ID is associated with the network entity (such as a specific router), not a specific interface. The system ID preserves connectivity when routing reconvergence is possible. If an interface fails or is removed, the system ID is used as the router identifier.

The address can be specified in the following formats:

- IPv4 (with 32 bit subnet mask)
- IPv6 (with 128 bit subnet mask)

The system ID is associated automatically during configuration of the following entities:

- termination points for service tunnels
- hops when you configure MPLS paths and LSPs
- addresses on a target router for BGP and LDP peering

System IP Address

(inBandSystemAddress)

The System IP Address parameter specifies the loopback IP address for the system (also known as the system ID). The system IP address is used for in-band device management. There must be a route from the 5620 SAM to the port on which the system IP address is configured. The system IP address is associated with the network entity (such as a specific router), but not a specific interface.

The system IP address preserves connectivity when routing reconvergence is possible. If an interface fails or is removed, the system IP address is used as the router identifier.

The system IP address can be specified in the following formats:

- IPv4 (with 32 bit subnet mask)
- IPv6 (with 128 bit subnet mask)

Telnet Session

See the [Telnet Session button](#) parameter in section [182.1](#).

Template Re-transmit (seconds)

The Template Re-transmit (seconds) parameter specifies how often, in s, Cflowd sends Cflowd template definitions to collectors. The parameter is configurable when the [Version](#) parameter is set to version-9 or version-10. The range is 10 to 600. The default is 600.

Template Type

(type)

The Template Type parameter specifies which set of templates Cflowd sends to the collector. The parameter is configurable when the [Version](#) parameter is set to version-9 or version-10. The choices are:

- Basic (default)
- MPLS-lp

Template Type

(type)

The Template Type parameter specifies which set of templates Cflowd sends to the collector. The parameter is configurable when the [Version](#) parameter is set to version-9.

Tertiary DNS

(sbiTertiaryDns)

The Tertiary DNS parameter specifies the tertiary DNS server for DNS name resolution. The tertiary DNS server is used only if the primary DNS server and the secondary DNS server do not respond.

Transmission Delay (Seconds)

(txDelay)

The Transmission Delay (Seconds) parameter specifies the minimum time interval between successive LLDP PDU transmissions. The transmit delay is less than or equal to the multiplication of transmit interval and 0.25 (transmit interval * 0.25). The range is 1 to 8192. The default is 2.

Transmission Interval (Seconds)

(messageTxInterval)

The Transmission Interval (Seconds) parameter specifies the transmit interval between LLDP PDUs. The range is 5 to 32768. The default is 30.

Transmission Multiplier

(messageTxHoldMultiplier)

The Transmission Multiplier parameter specifies the transmit hold multiplier value, which is used to calculate the Time To Live TLV. The Time To Live is a multiple of the Transmission Interval (Seconds) parameter value and the Transmission Multiplier parameter value. The range 2 to 10. The default is 4.

Uplink

(uplinkName)

The Uplink parameter specifies the 7210 SAS uplink for which you need to configure route parameters. The options are:

- A (default)
- B

Vendor-Specific ICMP Extensions

The Vendor-Specific ICMP Extensions parameter specifies whether vendor-specific ICMP functionality is enabled on the 7705 SAR. The options are:

- Enabled
- Disabled (default)

Version

(version)

The Version parameter specifies the Cflowd version of the collector. The options are:

- version-5
- version-8
- version-9
- version-10

View Shelf

Click on the View Shelf button to open the Equipment Window - Display form for a graphical representation of the equipment in the shelf.

VLAN ID

(sasUplinkAVlan)

The VLAN ID parameter specifies the VLAN ID that is assigned to the 7210 SAS uplink A port. The range is -1 to 4094. The default is 0.

VLAN ID

(sasUplinkBVlan)

The VLAN ID parameter specifies the VLAN ID that is assigned to the 7210 SAS uplink B port. The range is -1 to 4094. The default is 0.

VPLS Mode

(vplsServiceMode)

The VPLS Mode parameter specifies the VPLS mode of a 7250 SAS-ES or 7250 SAS-ESA device. Table 162-9 lists the parameter options.

Table 162-9 VPLS Mode parameter

Option	Description
Disabled (default)	Specifies that the device supports only VLAN services.
Qualified	Supported for Releases 2.0 to 3.0 R3.1 Specifies that the device supports VPLS SAPs with encapsulation. A device in this mode uses a port and an encapsulation value to identify a VPLS SAP. Multiple services can use the same port if they have different encapsulation values.
Unqualified	Supported for Releases 2.0 to 3.0 R3.1 Specifies that the device does not support VPLS SAPs with encapsulation. A VPLS SAP uses an entire port that cannot be shared with another service.
Enabled	Supported for Release 3.0 R4 and later Specifies that the device supports VPLS. You cannot use the 5620 SAM to set the parameter to Disabled after you set the parameter to Enabled.

163 –CCAG parameters

163.1 CCAG parameters 163-2

163.1 CCAG parameters

This chapter describes the parameters on the CCAG property form, the child forms, and the forms opened from other contextual menu options for CCAGs.

Access Adapt QoS

(accessAdaptQos)

The Access Adapt QoS parameter specifies how the CCAG SAP queue and virtual scheduler buffering rate parameters are adapted over multiple active CCAs. The options are:

- Link
- Distribute (default)

When you choose Link, the CCAG creates the SAP queues and virtual schedulers on each CCA with the actual parameters specified in the path table.

When you choose Distribute, each CCA receives a portion of the parameters specified in the path table.

Administrative State

See the [Administrative State](#) parameter in section 182.1.

CCAG ID

(ccagId)

The CCAG ID parameter specifies a unique identifier for the CCAG. The CCAG ID is identical for all members of a CCAG. The CCAG ID creates an association between a VSM-CCA and a CCAG. The range is 1 to 8. There is no default.

CCA Rate (kbps)

(ccaRate)

The CCA Rate parameter specifies the maximum forwarding rate for each CCA member within the CCAG. The range is –1 to 100 000 000. The default is –1.

CCA Rate Enabled

(ccaRateEnabled)

The CCA Rate Enabled parameter is used in conjunction with CCA Rate to set a CCA Rate or disable it, defaulting CCA Rate to –1. By default the CCA Rate Enabled parameter is disabled.

CC ID

(ccId)

The CC ID parameter specifies a unique identifier for the CC within the CCAG. The range is 1 to 4094. The default is 0, which means that the parameter is not set.

Description

See the [Description](#) parameter in section 182.1.

Egress Reserved CBS (%)

See the [Committed Burst Size \(%\)](#) parameter in section 48.1.

Ingress Reserved CBS (%)

See the [Committed Burst Size \(%\)](#) parameter in section 48.1.

MTU (octets)

(mtuValue)

The MTU (octets) parameter specifies the default MTU size for the CCAG path. When the parameter is set to 0, the MTU is calculated internally. The default value is 1518.

Path Rate (Kb/s)

(pathRate)

The Path Rate specifies the bandwidth rate limitation for this path on each member CCA in the CCAG. The range is –1 to 100 000 000. The default is –1.

Path Rate Enabled

(pathRateEnabled)

The Path Rate Enabled parameter is used in conjunction with Path Rate to set a path Rate or disable it, defaulting Path Rate to –1. By default, Path Rate Enabled is disabled.

Path Rate Option

(pathRateOption)

The Path Rate Option parameter specifies whether the Path Rate is defined as an aggregate path rate for all CCAs in the CCAG or as a path rate for an individual CCA. The options are:

- Aggregate (default)
- CCA

Path Weight (%)

(pathWeight)

The Path Weight parameter specifies the scheduling percentage for this path. It is applied to all CCAs in the CCAG membership list for this path. The range is 1 to 100. The default is 50.

164 –TWAMP parameters

164.1 TWAMP parameters 164-2

164.1 TWAMP parameters

This chapter describes the parameters associated with implementing the Two-Way Active Measurement Protocol on a server.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled.

The options are:

- Enabled
- Disabled (default)

Administrative Status

(twampAdminState)

The Administrative Status (twampAdminState) parameter specifies if the TWAMP server is administratively enabled or disabled. The options are:

- Enabled
- Disabled (default)

Conn Idle Time Periodic Threshold (seconds)

The Conn Idle Time Periodic Threshold (Seconds) parameter specifies the configurable threshold for the elapsed time, in seconds, for a TWAMP message to be received on this control connection. When the value of this parameter exceeds the value configured for [Inactivity Timeout \(Seconds\)](#), the connection will be closed.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Conn Session Count Periodic Threshold

The Conn Session Count Periodic Threshold parameter specifies the configurable threshold for the number of test sessions conducted by the TWAMP server, for the connection specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Conn Test Packets Rx Periodic Threshold

The Conn Test Packets Rx Periodic Threshold parameter specifies the configurable threshold for the number of TWAMP test packets received by the TWAMP server, for the connection specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Conn Test Packets Tx Periodic Threshold

The Conn Test Packets Tx Periodic Threshold parameter specifies the configurable threshold for the number of TWAMP test packets sent by the TWAMP server, for the connection specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Conn Test Sess Completed Periodic Threshold

The Conn Test Sess Completed Periodic Threshold parameter specifies the configurable threshold for the number of test sessions completed by the TWAMP server, for the connection specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Conn Test Sess Rejected Periodic Threshold

The Conn Test Sess Rejected Periodic Threshold parameter specifies the configurable threshold for the number of test sessions rejected by the TWAMP server, for the connection specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Description

(description)

The Description parameter specifies the description for the TWAMP prefix identified by the index values. The range is 0 to 80 characters.

Inactivity Timeout (Seconds)

(twampInactTimeout)

The Inactivity Timeout (Seconds) (twampInactTimeout) parameter specifies the system-wide inactivity timeout for each TWAMP server control connection. The range is 60 to 3600. The default is 900.

Maximum Connections

(twampMaxConnections)

The Maximum Connections (twampMaxConnections) parameter specifies the system-wide maximum number of concurrent TWAMP server control connections. The range is 0 to 64. The default is 32.

Maximum Sessions

(twampMaxSessions)

The Maximum Sessions (twampMaxSessions) parameter specifies the system-wide maximum number of concurrent TWAMP server test sessions. The range is 0 to 128. The default is 32.

Maximum # Connections

(prefixMaxConnections)

The Maximum # Connections parameter specifies the maximum number of concurrent TWAMP control connections allowed for the TWAMP prefix identified by the index values. In addition, the number of concurrent TWAMP control connections for this prefix is limited by the system maximum.

The range is 0 to 64. The default is 32.

Maximum # Sessions

(prefixMaxSessions)

The Maximum # Sessions parameter specifies the maximum number of concurrent TWAMP test sessions allowed for the TWAMP prefix identified by the index values. In addition, the number of concurrent TWAMP test sessions for this prefix is limited by the system maximum for the [Maximum Sessions](#) parameter.

The range is 0 to 128. The default is 32.

Prefix Address

(prefixAddr)

The Prefix Address parameter specifies the IPv4 or IPv6 Twamp Server Prefix address that is to be matched against a TWAMP client address.

Specify an IPv4 address in dotted-decimal format, or, if IPv6 is enabled, an IPv6 address in colon-hexadecimal format. The default is 0.0.0.0, which means that the parameter is not configured.

Prefix Length

(PrefixLen)

The Prefix Length parameter specifies the number of bits to match when comparing a TWAMP client address in an incoming message to the [Prefix Address](#). Best-fit is used when matching a TWAMP client's IP address against the set of configured prefixes. For example, suppose the Server configuration has the prefix 138.120.0.0/16, and the second prefix is 138.120.214.0/24. The TWAMP client address 138.120.214.52 matches the second server prefix.

The range is 0 to 128. The default is 32.

Retention Time (hours)

(retentionInterval)

The Retention Time (hours) parameter specifies the time, in hours, that the 5620 SAM database stores the statistics associated with a statistics policy.

The range for a performance or server performance statistics policy is 1 to 8760.

The range for an accounting statistics policy is configurable. The minimum is 1. The maximum is $24 \times$ the [Accounting Statistic Data Retention Period \(Days\)](#) value, which is initially specified during 5620 SAM database installation and is configurable using the 5620 SAM Database Manager form.

The default for policy types other than those associated with a TWAMP server is 24.

The default for a statistics policy associated with a TWAMP server is 20.

Srv Pfx Conn Count Periodic Threshold

The Srv Pfx Conn Count Periodic Threshold parameter specifies the configurable threshold for the number of control connections currently managed by the TWAMP server, for the prefix specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Srv Pfx Conns Rejected Periodic Threshold

The Srv Pfx Conns Rejected Periodic Threshold parameter specifies the configurable threshold for the number of control connection requests which have been rejected by the TWAMP server, for the prefix specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Srv Pfx Session Count Periodic Threshold

The Srv Pfx Session Count Periodic Threshold parameter specifies the configurable threshold for the number of currently in-progress TWAMP test sessions, for the prefix specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Srv Pfx Test Packets Rx Periodic Threshold

The Srv Pfx Test Packets Rx Periodic Threshold parameter specifies the configurable threshold for the number of TWAMP test packets received by the TWAMP server.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Srv Pfx Test Packets Tx Periodic Threshold

The Srv Pfx Test Packets Tx Periodic Threshold parameter specifies the configurable threshold for the number of TWAMP test packets sent by the TWAMP server.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Srv Pfx Test Sess Abort Periodic Threshold

The Srv Pfx Test Sess Abort Periodic Threshold parameter specifies the configurable threshold for the number of test sessions aborted by the TWAMP server, for the prefix specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Srv Pfx Test Sess Completed Periodic Threshold

The Srv Pfx Test Sess Completed Periodic Threshold parameter specifies the configurable threshold for the number of test sessions completed by the TWAMP server, for the prefix specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Srv Pfx Test Sess Rejected Periodic Threshold

The Srv Pfx Test Sess Rejected Periodic Threshold parameter specifies the configurable threshold for the number of test sessions rejected by the TWAMP server, for the prefix specified by the index values.

The range is 0 to 9 223 372 036 854 775 807. The default is 0.

Threshold Reporting State

(thresholdReportingState)

The Threshold Reporting State parameter specifies whether to generate threshold alarms when the number of log entries exceeds the Max Log Records parameter value. The options are:

- Up (default)
- Down

165 –IGH parameters

165.1 IGH parameters 165-2

165.1 IGH parameters

This chapter describes the parameters on the IGH forms.

Administrative State

(administrativeState)

The Administrative State (administrativeState) parameter specifies whether the IGH is administratively enabled. The options are:

- Down (default)
- Up

CLI Name

(portName)

The CLI Name parameter specifies the name of the port. The name can be up to 252 characters. The name is the same as port name displayed on node cli.

IGH ID

(ighId)

The IGH ID parameter specifies the row index of the IGH. The range is 0 to 100. The default is 0.

Minimum Active Link Threshold

(threshold)

The Minimum Active Link Threshold parameter specifies the minimum number of links that must be active before the Administrative State parameter can be set to Up. The range is 1 to 8. The default is 1.

166 –ISA-AA Group parameters

166.1 ISA-AA Group parameters 166-2

166.1 ISA-AA Group parameters

This chapter describes the parameters on the ISA-AA Group property form, the child forms, and the forms opened from other contextual menu options for ISA-AA groups.

AA Stats Type

(aaStatsType)

The AA Stats Type parameter specifies the type of object for per-subscriber statistics collection. Table 166-1 describes the parameter options:

Table 166-1 AA Stats Type parameter options

Option	Dependencies
AA Application (default)	—
AA Application Group	Supported for custom AA accounting policy only
AA Protocol	—

AA Subscriber Name

(displayName)

The AA Subscriber Name parameter specifies the name of the subscriber for which to enable special-study statistics collection. The range is 1 to 32 characters. There is no default.

AA Subscriber Type

(aaSubType)

The AA Subscriber Type parameter specifies the AA subscriber type. The options are:

- None (default)
- SAP
- Spoke SDP Binding
- Transit

Administrative State

See the [Administrative State](#) parameter in section 182.1.

Buffer Utilization High Water Mark

(egressFromSubWaSBfHiWmk)

The Buffer Utilization High Water Mark parameter in the Egress From-Subscriber tab specifies the high watermark percentage threshold for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool for each ISA. When a buffer pool is not in the overload state and the weighted average shared buffer utilization for an ISA is greater than or equal to the specified buffer utilization high watermark, the ISA from-subscriber buffer pool enters an overload state and a warning alarm is raised. The range is -1 to 100. The default is -1. The value of -1 specifies the maximum possible threshold and prevents the NE from raising overload warning alarms.

Buffer Utilization High Water Mark

(egressToSubWaSBfHiWmk)

The Buffer Utilization High Water Mark parameter in the Egress To-Subscriber tab specifies the high watermark percentage threshold for the weighted average utilization of the shared buffer space in the to-subscriber buffer pool for each ISA. When a buffer pool is not in the overload state and the weighted average shared buffer utilization for an ISA is greater than or equal to the specified buffer utilization high watermark, the ISA to-subscriber buffer pool enters an overload state and a warning alarm is raised. The range is -1 to 100. The default is -1. The value of -1 specifies the maximum possible threshold and prevents the NE from raising overload warning alarms.

Buffer Utilization Low Water Mark

(egressFromSubWaSBfLoWmk)

The Buffer Utilization Low Water Mark parameter in the Egress From-Subscriber tab specifies the low watermark for the weighted average utilization of the shared buffer space in the from-subscriber buffer pool. When a buffer pool is in an overloaded state and the weighted average shared buffer utilization for an ISA is less than or equal to buffer utilization low water mark, the ISA from-subscriber buffer pool leaves the overload state and the warning alarm that indicates the overload state is cleared. The value of the Buffer Utilization Low Water Mark parameter must be lower than the specified value of the [Buffer Utilization High Water Mark](#) parameter. The range is 0 to 99. The default is 0.

Buffer Utilization Low Water Mark

(egressToSubWaSBfLoWmk)

The Buffer Utilization Low Water Mark parameter in the Egress To-Subscriber tab specifies the low watermark for the weighted average utilization of the shared buffer space in the to-subscriber buffer pool. When a buffer pool is in an overloaded state and the weighted average shared buffer utilization for an ISA is less than or equal to buffer utilization low water mark, the ISA to-subscriber buffer pool leaves the overload state and the warning alarm that indicates the overload state is cleared. The value of the Buffer Utilization Low Water Mark parameter must be lower than the specified value of the [Buffer Utilization High Water Mark](#) parameter. The range is 0 to 99. The default is 0.

Capacity Cost High Threshold

(capCostHighThres)

The Capacity Cost High Threshold parameter specifies the high threshold of the capacity cost for the ISA-AA group. The range is 0 to 4 294 967 295. The default is 4 294 967 295. For more information, see the [Capacity Cost](#) parameter in section [90.1](#).

Capacity Cost Low Threshold

(capCostLowThres)

The Capacity Cost Low Threshold parameter specifies the low threshold of the capacity cost for the ISA-AA group. The range is 0 to 4 294 967 295. The default is 0. For more information, see the [Capacity Cost](#) parameter in section [90.1](#).

Collector Port

The Collector Port parameter specifies the UDP port of the AA Cflowd collector. The range is 1 to 65 535. The default is 4739.

Description

See the [Description](#) parameter in section [182.1](#).

Reserved CBS (%)

(egressFromSubReservedCbs)

The Reserved CBS (%) parameter in the Egress From-Subscriber tab specifies the percentage of the buffer pool that is reserved for high priority traffic for subscriber to network traffic egressing towards the ISA-AA MDA. The range is -1 to 100. The default is -1. The value of -1 specifies that the reserved CBS is calculated as the sum of the CBS requested by the entities that use this pool.

Reserved CBS (%)

(egressToSubReservedCbs)

The Reserved CBS (%) parameter in the Egress To-Subscriber tab specifies the percentage of the buffer pool that is reserved for high priority traffic for all traffic egressing from the ISA-AA MDA. The range is -1 to 100. The default is -1. The value of -1 specifies that the reserved CBS is calculated as the sum of the CBS requested by the entities that use this pool.

Forwarding Class Name

(fcName)

The Forwarding Class Name parameter specifies the divertable forwarding class for the group. The options are:

- be (default)
- l2
- af
- ef
- hi
- ll
- nc

Group Number

(groupNumber)

The Group Number parameter specifies the identifier assigned to the group of ISA-AA MDAs. The range is 1 to 255.

Host Address

The Host Address parameter specifies the Cflowd collector host address. Specify an IPv4 address in dotted-decimal format

ISA-AA MDA Role

(aaMdaRole)

The ISA-AA MDA Role parameter specifies the role of the selected MDA. The options are:

- Primary (default)
- Backup

Operation Upon Failure

(failToMode)

The Operation Upon Failure parameter specifies whether traffic is permitted or denied when there is an operation upon failure of the group. The options are:

- Fail To Wire (default, traffic is permitted)
- Fail To Open

Overload Cut-Through

(overloadCutThru)

The Overload Cut-Through parameter specifies whether overload cut-through is enabled within an ISA-AA group. The options are:

- Disabled (default)
- Enabled

Override ASO Characteristic Name

(ovrdAsoName)

The Override ASO Characteristic Name parameter specifies the name of a characteristic that a subscriber can choose. The range is 1 to 32.

Override ASO Characteristic Value

(asoCharacteristicValue)

The Override ASO Characteristic Value parameter specifies the override characteristic value for the application profile characteristic that is used by the application assurance subscriber. The range is 1 to 32. There is no default.

Partition ID

(partitionId)

The Partition ID parameter specifies how many partitions are defined for each ISA-AA group. Up to 128 partitions are allowed per ISA-AA group for AA deployments with VPN customization. The range is 1 to 65 535. The default is 0.

Partitions

(partitionEnabled)

The Partitions parameter specifies whether partitions are enabled or disabled within an ISA-AA group. When the value is set to Enabled, partitions can be created on the ISA-AA group. The options are:

- Disabled (default)
- Enabled

Performance Administrative State

(rtpPerformanceAdminStatus)

The RTP Performance Administrative State parameter specifies whether AA RTP Performance Cflowd sampling is enabled. The options are:

- Down (default)
- Up

Performance Administrative State

(performanceAdminStatus)

The TCP Performance Administrative State parameter specifies whether AA TCP Performance Cflowd sampling is enabled. The options are:

- Down (default)
- Up

Sample Flow Rate

(rtpFlowRate)

The RTP Performance Sample Rate parameter specifies the rate at which AA Performance Cflowd samples packets to evaluate RTP performance. Cflowd samples one packet out of every N packets, where N is the parameter value. For example, a value of 100 specifies that one of every 100 packets is to be sampled, and a value of 1 means that all packets are to be sampled. The range is 1 to 10 000. The default is 1000.

Sample Flow Rate

(flowRate)

The TCP Performance Sample Rate parameter specifies the rate at which AA Performance Cflowd samples packets to evaluate TCP performance. Cflowd samples one packet out of every N packets, where N is the parameter value. For example, a value of 100 specifies that one of every 100 packets is to be sampled, and a value of 1 means that all packets are to be sampled. The range is 1 to 10 000. The default is 1000.

Sampling Rate

(volumeRate)

The Sample Rate parameter specifies the rate at which AA Cflowd samples packets. Cflowd samples one packet out of every N packets, where N is the parameter value. For example, a value of 100 specifies that one of every 100 packets is to be sampled, and a value of 1 means that all packets are to be sampled. The range is 0 to 10 000. The default is 1000.

Subscriber Scale

(subScale)

The Subscriber Scale parameter specifies a set of scaling limits that are applied to an ISA-AA group. The scaling limit determines the maximum number of AA subscribers per ISA and the corresponding policies that can be applied. The parameter is configurable only during ISA-AA group creation. The options are:

- Residential (default)
- VPN

Template Re-transmit

The Template Re-transmit parameter specifies how often, in s, AA Cflowd sends Cflowd template definitions to collectors. The range is 10 to 600. The default is 600.

Transit Subscriber Name

(transitSubscriberName)

The Transit Subscriber Name parameter specifies the name of the transit IP subscriber for which to enable special-study statistics collection. The range is 1 to 32 characters. There is no default.

Version

(collectorVersion)

The Version parameter specifies the Cflowd version that AA uses. The parameter is set to 10 and cannot be configured.

Volume Administrative State

(volumeAdminStatus)

The Volume Administrative State parameter specifies whether flow sampling is enabled for the ISA-AA group. The options are:

- Down (default)
- Up

167 –ISA-IPsec Group parameters

167.1 ISA-IPsec Group parameters 167-2

167.1 ISA-IPsec Group parameters

This chapter describes the parameters on the IPsec Group form, the child forms, and the forms opened from other contextual menu options for ISA-IPsec groups.

Administrative State

See the [Administrative State](#) parameter in section [182.1](#).

Description

See the [Description](#) parameter in section [182.1](#).

Group Number

(groupNumber)

The Group Number parameter specifies the identifier assigned to the group of IPsec MDAs. The range is 1 to 4. There is no default.

For 7750 SR and 7450 ESS version 9.0 and later NEs, the range for the Group Number parameter is 1 to 16.

168 —ISA-LNS Group parameters

168.1 ISA-LNS Group parameters 168-2

168.1 ISA-LNS Group parameters

This chapter describes the parameters on the ISA-LNS Group form, the child forms, and the forms opened from other contextual menu options for ISA-LNS groups.

Administrative State

See [Administrative State](#) in section 182.1.

Description

See [Description](#) in section 182.1.

Group Number

(groupNumber)

The Group Number parameter specifies the identifier assigned to the group of ISA broadband application MDAs. The range is 1 to 4. There is no default.

169 –ISA-NAT Group parameters

169.1 ISA-NAT Group parameters 169-2

169.1 ISA-NAT Group parameters

This chapter describes the parameters on the ISA-NAT Group property form, the child forms, and the forms opened from other contextual menu options for ISA-NAT groups.

Active MDA Limit

(activeMdaLimit)

The Active MDA Limit parameter specifies the maximum number of active MDAs in the ISA-NAT group. The range is 0 to 6. The default is 0, which means that the parameter is not configured.

Administrative State

See the [Administrative State](#) parameter in section 182.1.

Description

See the [Description](#) parameter in section 182.1.

Group Number

(groupNumber)

The Group Number parameter specifies the identifier of the ISA-NAT group. The range is 1 to 4. There is no default.

Reservation Count

(reservationCount)

The Reservation Count parameter specifies, for each MDA in the NAT-ISA group, the number of reserved sessions. A reserved session is exempt from subscriber session limits. The range is 0 to 4 195 303. The default is 0.

Session Watermark High

(sessionWatermarkHi)

The Session Watermark High parameter specifies the percentage of used sessions on an MDA in the ISA-NAT group above which the 5620 SAM raises an alarm. The alarm clears when the session usage on each MDA drops below the [Session Watermark Low](#) value. The parameter value must be higher than the [Session Watermark Low](#) value, unless both parameters are set to 0. The range is 0 to 100. The default is 0.

Session Watermark Low

(sessionWatermarkLo)

The Session Low Watermark parameter specifies the percentage of used sessions on an MDA in the ISA-NAT group below which the 5620 SAM clears an alarm raised for session usage that exceeds the [Session Watermark High](#) value on an MDA. The parameter value must be lower than the [Session Watermark High](#) value, unless both parameters are set to 0. The range is 0 to 99. The default is 0.

170 –ISA-Video Group parameters

170.1 ISA-Video Group parameters 170-2

170.1 ISA-Video Group parameters

This chapter describes the parameters to configure video services parameters related to the functionality provided by the ISA-Video module.

Address Type

(ipAddressType)

The Address Type parameter specifies the type of IP address that is assigned to the video interface. The options are:

- IPv4 (default)

Ad Insert Server

(adServerState)

The Ad Insert Server parameter specifies whether an ADI server is enabled on the video group. The options are:

- Enabled
- Disabled (default)

Administrative State

(administrativeState)

The Administrative State parameter specifies whether the video interface is administratively enabled. The options are:

- Up (default)
- Down

ADI Administrative Status

(adiState)

The ADI Administrative Status parameter specifies whether the ADI server is enabled on the video group. The options are:

- Enabled
- Disabled (default)

ADI Zone Multicast Address

(zoneGrpAddr)

The ADI Zone Multicast Address parameter specifies the IP multicast group IP address for downstream ADI. Specify an IPv4 address. There is no default.

ADI Zone Unicast Source Address

(zoneSrcAddr)

The ADI Zone Unicast Source Address parameter specifies the unicast source IP address. Specify an IPv4 address. There is no default.

Analyzer

(analyzer)

The Analyzer parameter specifies whether the VQM analyzer is enabled or disabled on the video group. The options are:

- Enabled
- Disabled

Associated Multicast Service ID

(mcastSvcId)

The Associated Multicast Service ID parameter specifies the multicast service to be used for sending replies in the multicast service instance. In situations where multicast and unicast are carried in separate service instances, the value of this object should be set on the unicast video interface to form an association with the multicast service. The default value should be the service ID of the service where this Video Interface is located. The range is 0 to 2147483647. The default is 0.

Description

(description)

The Description parameter specifies a description for the video group, video interface, or ADI channel. If the description is for a video group, it may be up to 255 characters long. If the description is for a video interface or an ADI channel, it may be up to 80 characters long.

Fast Channel Change Server

(fccServerState)

The Fast Channel Change Server parameter specifies whether the FCC server is enabled on the video group. The options are:

- Enabled
- Disabled (default)

Gateway Address

(gatewayAddr)

The Gateway Address parameter specifies the gateway IP address for the video Interface within the VPLS service. Specify an IPv4 address. There is no default.

Group Number

(groupNumber)

The Group Number parameter specifies the group number of this video group. The range is 1 to 4. There is no default.

IP Address

(ipAddress)

The IP address parameter specifies the IP address of the video interface. Specify an IPv4 address. There is no default.

Local Retransmission Server

(localRtServerState)

The Local Retransmission Server parameter specifies whether a local RT server is enabled. It indicates whether to process the retransmission requests from the client. The options are:

- Enabled
- Disabled (default)

Multicast Channel IP Address

(grpAddr)

The Multicast Channel IP Address specifies the IP address of the multicast group. Specify an IPv4 address. There is no default.

Name

(displayName)

The Name parameter specifies a unique administrative name for the channel or video interface. The range is 1 to 32 characters.

Prefix Length

(ipAddressPrefixLength)

The Prefix Length parameter specifies the length of the IP netmask for the video interface address. The range is 1 to 32. The default is 32.

Reserve Retransmission Bandwidth (Mbps)

(resvRet)

The Reserve Retransmission Bandwidth (Mbps) parameter specifies a reserved amount of egress retransmission bandwidth for all ISAs in the video group. The range is 0 to 10 500 Mb/s. The default is 0.

If the amount of egress bandwidth is less than the parameter value, FCC requests are discarded and only RET requests are processed.

RT Client Address

(rtClientAddr)

The RT Client Address parameter specifies the IP address for the RT client in the video interface within the service. The RT client IP address is the originating address used for communication with upstream RT servers. If no RT client address is assigned, the RT client is operationally down, since the RT client configuration is incomplete. For a VPLS service, the RT client address cannot be the same as an existing address for the video interface, but it must be an address within a video interface subnet. For IES and VPRN services, the RT client address can be the same as an existing address for the video interface or an address within a video interface subnet. Specify an IPv4 address.

SCTE 30 Control Address

(scteCtrAddr)

The SCTE 30 Control Address parameter specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (scte30) ad control streams. This address should be in the same subnet as the IP address assigned to the video interface. The values of the SCTE 30 Control Address and [SCTE 30 Data Address](#) parameters must be set together in the same SNMP request PDU or else the set request fails with an inconsistent value error. Specify an IPv4 address.

SCTE 30 Data Address

(scteDataAddr)

The SCTE 30 Data Address parameter specifies the local IP address to which ad servers send Society of Cable Telecommunications Engineers 30 (scte30) ad data streams. This address should be in the same subnet as the IP address assigned to the video interface. The values of the [SCTE 30 Data Address](#) and [SCTE 30 Control Address](#) parameters must be set together in the same SNMP request PDU or else the set request fails with an inconsistent value error. Specify an IPv4 address.

SCTE 35 Action

(scte35Fwd)

The SCTE 35 Action parameter specifies whether the SCTE 35 messages are forwarded in the downstream. The options are:

- Forward (default)
- Drop

Server Address

(serverAddr)

The Server Address parameter specifies the IP multicast group address of the ADI SCTE server. Specify an IPv4 address. There is no default.

Stream Selection

(streamSelection)

The Stream Selection parameter specifies whether stream selection is enabled or disabled on the video group. The options are:

- Enabled
- Disabled

Unicast Source IP Address

(srcAddr)

The Unicast Source IP Address specifies the source IP address for which this entry contains information. Specify an IPv4 address. There is no default.

171 –LAG parameters

171.1 LAG parameters 171-2

171.1 LAG parameters

This chapter describes the parameters on the LAG property form, the child forms, and the forms opened from other contextual menu options for LAGs.

Active Sub-Group Selection Criteria

(lacpSelCrit)

The Active Sub-Group Selection Criteria parameter specifies the criterion for selecting the active LAG subgroup. Table 171-1 describes the parameter options.

Table 171-1 Active Sub-Group Selection Criteria parameter

Option	Option description	Dependencies
Highest_Count (default)	The subgroup with the highest number of eligible link members is the active group. An eligible member is a LAG link that can potentially become active since it is operational and has not been disabled by a remote system (on which standby link signaling is not supported).	—
Highest_Weight	The subgroup with the highest aggregate weight is the active group.	—
Best_Port	The subgroup with the highest-priority port is the active group.	—

Actor Administration Key

Table 171-2 lists where to find more information about the Actor Administration Key parameter.

Table 171-2 Actor Administration Key parameter

Parameter	See
Actor Administration Key for an OmniSwitch	Actor Administration Key parameter in this section
Actor Administration Key for non-OmniSwitch nodes	Actor Administration Key parameter in this section

Actor Administration Key

(actorAdminKey)

The Actor Administration Key parameter specifies a unique value to identify the channel group on each port that is configured to use LACP. This parameter is configurable when the Auto-Generate parameter is disabled. The range is 1 to 65 535.

Actor Administration Key

(actorAdminKey)

The Actor Administration Key parameter specifies a unique value used to identify a dynamic LAG. The range is 0 to 65 535. The default is 0.

Actor System ID

(actorSystemId)

The Actor System ID parameter specifies the MAC address of a dynamic LAG. Specify a MAC address in the format xx-xx-xx-xx-xx-xx. The default is 00-00-00-00-00-00.

Actor System Priority

(actorSystemPriority)

The Actor System Priority parameter specifies the priority of a dynamic LAG in relation to other dynamic LAGs. The range is 0 to 65 535. The default is 0.

Administrative State

(administrativeState)

See the [Administrative State](#) parameter in section 182.1.

Admin Key

(portActorAdminKey)

The Admin Key parameter species an actor administrative key for a port, which allows the port to join a dynamic LAG. The range is 0 to 65 535. The default is 0.

Admin Key

(portPartnerAdminKey)

The Admin Key parameter species the administrative key for a port of a LAGs remote partner. The range is 0 to 65 535. The default is 0.

Admin Port

(portPartnerAdminPort)

The Admin Port parameter specifies the administrative status of a partner port. The range is 0 to 65 535. The default is 0.

Admin Port Priority

(portPartnerAdminPortPriority)

The Admin Port Priority parameter specifies the priority of a partner port. The range is 0 to 255. The default is 0.

Admin State

(actorAdminState)

The Admin State parameter specifies the system administrative state of a dynamic LAG actor port on the local switch. The options correspond to bits in the actor state octet in the LACPDU frames sent by the port. Table 171-3 describes the parameter options.

Table 171-3 Admin State parameter

Option	Option Description	Default Value
Active	When this option is enabled, the dynamic LAG is able to exchange LACPDU frames.	Enabled
Aggregate	When this option is enabled, the system considers this port to be a potential candidate for aggregation. If this option is not enabled, the system considers the port to be individual (it can only operate as a single link).	Enabled
Collect	When this option is enabled, incoming LACPDU frames are collected from the individual ports that make up the dynamic LAG.	Value set by the system
Default	When this option is enabled, it indicates that the actor port is using the defaulted partner information administratively configured for the partner.	Value set by the system
Distribute	When this option is enabled, the distribution of outgoing frames on the port is disabled.	Value set by the system
Expire	When this option is enabled, the actor port cannot receive LACPDU frames.	Value set by the system
Synchronize	When this option is enabled, the port is allocated to the correct dynamic LAG. If this option is disabled, the port is not allocated to the correct dynamic LAG.	Value set by the system
Timeout	When this option is enabled a short timeout is used for LACPDU frames. When this option is disabled, a long timeout is used for LACPDU frames.	Enabled

Admin State

(partnerAdminState)

The Admin State parameter specifies the system administrative state of a dynamic LAG partner port on the remote switch. The options correspond to bits in the partner state octet in the LACPDU frame. Table 171-4 describes the parameter options.

Table 171-4 Admin State parameter

Option	Option Description	Default Value
Active	When this option is enabled, the dynamic LAG is able to exchange LACPDU frames.	Enabled
Aggregate	When this option is enabled, the system considers this port to be a potential candidate for aggregation. If this option is not enabled, the system considers the port to be individual (it can only operate as a single link).	Enabled
Collect	When this option is enabled, incoming LACPDU frames are collected from the individual ports that make up the dynamic LAG.	Value set by the system
Default	When this option is enabled, it indicates that the actor port is using the defaulted partner information administratively configured for the partner.	Value set by the system
Distribute	When this option is enabled, the distribution of outgoing frames on the port is disabled.	Value set by the system
Expire	When this option is enabled, the actor port cannot receive LACPDU frames.	Value set by the system
Synchronize	When this option is enabled, the port is allocated to the correct dynamic LAG. If this option is disabled, the port is not allocated to the correct dynamic LAG.	Disabled
Timeout	When this option is enabled a short timeout is used for LACPDU frames. When this option is disabled, a long timeout is used for LACPDU frames.	Enabled

Admin System Id

(portPartnerAdminSystemId)

The Admin System Id parameter specifies the partner administrative system ID (MAC address) for a dynamic LAG port. Specify a MAC address in the format xx-xx-xx-xx-xx-xx. The default is 00-00-00-00-00-00.

Admin System Priority

(portPartnerAdminSystemPriority)

The Admin System Priority parameter specifies the partner system priority for a dynamic LAG port. The range is 0 to 255. The default is 0.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 182.1.

Auto-Generate

The Auto Generate parameter specifies whether to automatically configure an Actor Administration Key parameter. The options are:

- Enabled (default)
- Disabled

Automatic VLAN Binding

(vlanAutoBind)

The Automatic VLAN Binding parameter specifies whether an L2 network interface is created on a network LAG. The L2 network interface is bound to VLAN services on the switch. The options are:

- Enabled (default)
- Disabled

Table 171-5 describes the behavior of network LAGs for Standard and Stacked VLANs.

Table 171-5 Automatic VLAN Binding parameter

Type of VLAN	Behavior	General
Standard	The 5620 SAM cannot identify network LAGs that can be used for Standard VLAN network interfaces. Configure the network LAGs that you need to use before configuring Standard VLANs. Network LAGs that have the Automatic VLAN Binding parameter enabled can be identified by the 5620 SAM for use by Standard VLANs.	All network LAGs with the Automatic VLAN Binding parameter enabled is used as network ports for all VLANs.
Stacked	The 5620 SAM can identify network LAGs that can be used for Stacked VLAN network interfaces. Although it is not necessary to enable the Automatic VLAN Binding parameter on network LAGs in order for the 5620 SAM to identify the LAG for use by Stacked VLANs, it is recommended. When you switch an access LAG to a network LAG and the Automatic VLAN Binding parameter is enabled, a VLAN binding is automatically created between the LAG and all of the Stacked VLANs on the switch.	If you do not need a network LAG to be used by VLANs, disable the Automatic VLAN Binding parameter.

Class

(portClass)

The Class parameter specifies the class of the LAG member's ports. The options are:

- Fast Ethernet
- Gigabit Ethernet
- 10G Ethernet
- SONET
- Virtual Port
- SONET Channel
- Variable Speed Ethernet
- VSM Ethernet
- TDM
- Radio
- 100 Gigabit Ethernet
- WDM
- Serial
- Voice



Note — Available options depend on compatibility when the [Show Only Compatible Ports](#) parameter is enabled.

Configured Address

See the [Configured MAC](#) parameter in section [182.1](#).

Description

See the [Description](#) parameter in section [182.1](#).

Dynamic Cost

(dynamicCosting)

The Dynamic Cost parameter specifies whether to enable the LACP and OSPF costing for a LAG, based on the available aggregated, operational bandwidth. The parameter is used to calculate path cost.

Table [171-6](#) describes the parameter options.

Table 171-6 Dynamic Cost parameter

Option	Option description	Dependencies
Enabled	Specifies that when the number of active links is greater than the value set in the Port Threshold parameter, the path cost is dynamically calculated. The calculation occurs when there is a change in the number of active links, regardless of the specified port threshold action. If the port-threshold is met and dynamic cost is set, the path cost is dynamically recalculated. If OSPF auto-cost is not configured, the cost configured on the OSPF metric determines the cost when the number of links available exceeds the configured LAG threshold value. The configured threshold action determines whether the LAG is advertised.	—
Disabled (default)	Specifies that when dynamic-cost and OSPF auto-cost are not configured, the cost configured on the OSPF metric determines the cost advertised when the number of links available exceed the configured LAG threshold value. The Port Threshold Action parameter setting determines whether the LAG is advertised. If OSPF auto-cost is configured, the cost is based on the total number of configured links. This cost remains static provided the number of links that are up exceeds the LAG threshold value. The configured threshold action determines whether and at what cost the LAG is advertised.	

Path cost is dynamically calculated based on interface bandwidth. The cost advertised is inversely proportional to the number of links available when the number of links that are up exceeds the configured LAG threshold value. The configured threshold action determines if and at what cost the LAG is advertised.

For example, assume a physical link in OSPF has an associated cost of 100, and the LAG consists of four physical links. The cost associated with the logical link is 25 (one quarter for each physical link). If one link fails, the cost is automatically adjusted to 33 (one-third for each physical link).

Enable Per Forwarding Path Ingress Queue

(perFpIngQueuing)

The Enable Per Forwarding Path Ingress Queue parameter allows optimization of queue allocation for SAPs on an access mode LAG within an SHG. This allows the allocation of only one queuing set per ingress forwarding path. When the parameter is enabled, per-forwarding-path ingress queuing is enabled instead of per-link ingress queuing. The default is false. This parameter is configurable in VPLS on a 7450 ESS or 7750 SR. The options are:

- disabled (default)
- enabled

The following usage rules apply:

- The LAG must be in access mode.
- The parameter is not applicable if the LAG mode is changed from access to network.

- The parameter setting can be changed provided no port members exist in the LAG.
- The parameter setting can be changed if the SAPs reference the LAG.
- The parameter is not applicable if the LAG port type is set to HSMDA.

Encap Type

See the [Encap Type](#) parameter in section [182.1](#).

Hold Time (100s of milliseconds)

(lacpHoldTimeDown)

The Hold Time (100s of milliseconds) parameter specifies the delay between the detection of a LAG being down (all active ports are down) and reporting the detection. The range is 0 to 50. The default is 0.

The parameter is configurable on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, and 7750 SR.

L2Uplink

(isl2UplinkMode)

See the [L2Uplink](#) parameter in section [14.1](#).

LACP Mode

(lacpMode)

The LACP Mode parameter specifies whether the LACP is active or passive. The parameter is used for aggregated Ethernet interfaces only. One end of the LAG group must be configured as active for the LACP to work. The options are:

- active
- passive (default)

LACP System ID

(lagSystemId)

The LACP System ID parameter specifies a 6-octet MAC address that is used as a unique identifier for the system that contains this router. The default is 00-00-00-00-00-00, which indicates that the Actor System ID will be used.

LACP System Priority

(lagSystemPriority)

The LACP System Priority parameter specifies the priority value associated with the Actor's System ID. The default is -1, which specifies the priority is taken from the Actor's System Priority.

LACP System Priority

(sysLacpSystemPriority)

The LACP System Priority parameter specifies the LACP system priority on aggregated Ethernet interfaces. The range is 1 to 65 535, where 1 is the highest priority. The default is 1.

LACP Transmit Interval

(lacpTransmitInterval)

The LACP Transmit Interval parameter specifies the speed of the transmission. The options are:

- Slow
- Fast (default)

LACP Transmit Standby

(lacpXmitStdby)

The LACP Transmit Standby parameter specifies whether LACP message transmission on standby links is enabled. By default, links that are members of a LAG and are in standby mode still receive and transmit LACP messages. The disabling of LACP message transmission on standby links adversely affects switchover times and should only be done to ensure interworking with systems that do not support standby link signaling. The options are:

- Enabled (default)
- Disabled

The parameter is configurable on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7710 SR, and 7750 SR.

LAG ID

(lagId)

The LAG ID parameter specifies a unique identifier for the LAG. You can configure the parameter for LAGs when the [Auto-Assign ID](#) parameter is set to disabled.

The LAG ID is identical for all members of a LAG. The LAG ID creates an association between a logical IP interface and a LAG. An IP interface can be associated with a port or the system loopback address.

Table [171-7](#) lists the ranges for different devices.

Table 171-7 LAG ID ranges by device

NE device	LAG ID range
Multiple-slot 7450 ESS and 7750 SR	1 to 200
7450 ESS-1, 7750 SR-1, and the 7710 SR	1 to 64
All OmniSwitch variants	0 to 31
7210 SAS-E	1 to 6
7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR]	1 to 12

Mode

See the [Mode](#) parameter in section 182.1.

Name

(lagName)

The Name parameter specifies a name for a static or dynamic LAG. The name can be an alphanumeric string up to 256 characters. Spaces must be contained within quotes.

Partner Administration Key

(partnerAdminKey)

The Partner Administrative Key parameter specifies the administrative key for a dynamic LAG's remote partner. The range is 0 to 65 535. The default is 0.

Partner System ID

(partnerSystemId)

The Partner System ID parameter specifies the MAC address of the remote LAG to which the local switch's dynamic LAG is attached. Specify a MAC address in the format xx-xx-xx-xx-xx-xx. The default is 00-00-00-00-00-00.

Partner System Priority

(partnerSystemPriority)

The Partner System Priority parameter specifies the priority of the partner LAG to which the local switch's LAG is attached. The range is 0 to 65 535. The default is 0.

Port Threshold

(portThreshold)

The Port Threshold parameter specifies the number of operational links that can fall below the configured threshold level. The range is 0 to 7. The default is 0, which indicates that the link is operationally down when all links are down.

Port Threshold Action

(portThresholdAction)

The Port Threshold Action parameter specifies the action taken when the number of operational links falls below the configured port threshold. Depending on the path cost value that is calculated, this parameter determines whether the LAG is advertised. Table 171-8 describes the parameter options.

Table 171-8 Port Threshold Action parameter

Option	Option description	Dependencies
down (default)	Specifies that dynamic costing is disabled, indicating that the LAG is not advertised. When the number of links that are up in a LAG is less than the configured threshold, the LAG is operationally down. For example, assume that a LAG consists of eight physical links, the threshold is set to four, and dynamic costing is not configured. If the number of operational links drops below four, the link is operationally down until the number of operational links is at least four.	—
Dynamic Cost	Specifies that dynamic costing is enabled, indicating that the LAG is advertised. When the number of links available in a LAG is less than the configured threshold, the LAG uses the dynamic cost, which allows other nodes to adjust their routing tables according to the revised costs. When the threshold is not exceeded, a fixed metric for all operational links is advertised.	

Port Type

(lagPortType)

The Port Type parameter specifies the port member type for the LAG. The options are:

- standard (default)
- hsmdda

A LAG cannot contain both standard and hsmdda port members. It can only contain one or the other. The LAGs added to the MC-LAG must also have the same member port type.

If the Port Type parameter in a LAG must be altered at some point, the LAG should not have any members associated with it.

Priority

(priority)

The Priority parameter specifies the Actor System Priority for the LAG member. Table 171-9 describes the range and defaults.

Table 171-9 Priority parameter

NE type	Range	Default
OmniSwitch	0 to 255	0
Non-OmniSwitch	1 to 65 535	32768

QoS Adaptation

(adaptQoS)

The QoS Adaptation parameter specifies the CCAG SAP queue and virtual scheduler buffering and rate parameters are adapted over multiple active CCAs. Table 171-10 describes the parameter options.

Table 171-10 QoS Adaptation parameter

Option	Option description	Dependencies
Distribute (default)	CCAG SAP queues and schedulers on each CCA receives a portion of the defined parameters in the QoS and scheduler policies. The portion is decided on an IOM basis, with the ratio determined by the number of active CCA members on the IOM relative to the total number of active members within the CCAG. The following equation may be used to determine the actual ratio: $\text{IOM-parameter-value} = (\text{IOM-active-CCA} / \text{total-active-CCA}) * \text{policy-parameter-value}$	—
Link	CCAG creates the SAP queues and virtual schedulers on each CCA with the actual parameters defined in the QoS and scheduler policies. This mode is useful when conversation hashing places all or most traffic over a single CCA.	

Show Only Compatible Ports

The Show Only Compatible Port Numbers parameter specifies whether to filter the list of ports presented, by determining whether the ports can be configured as LAGs.

The options are:

- Enabled (default)
- Disabled

When the parameter is enabled, several checks are performed. Which of the following checks are performed depends on the type of NE:

- the port mode is network
- the port cannot be a mobile port
- the port cannot be POS

- the port cannot belong to another LAG
- there cannot be more than eight ports in a LAG
- the port cannot be bound to a Layer 3 interface
- the ports must have the same speed
- the port must be set to full duplex and auto negotiation must be turned off

Size

(lagSize)

The Size parameter specifies the maximum number of links allowed in a LAG. The options are:

- 2 (default)
- 4
- 8

Slave to Partner

(lacpSelCritSlaveToPartner)

The Slave to Partner parameter specifies whether all ports in a LAG that are signaled as standby by the partner should be considered as eligible members for active selection. An eligible member is a LAG member link that can potentially become active, since it is operational and has not been disabled by a remote system (on which standby link signaling is not supported). The default is disabled.

The parameter is configurable on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7450 ESS, 7710 SR, and 7750 SR.

Standby Signalling

(standbySignalling)

The Standby Signalling parameter specifies whether LACP configuration is available on a LAG. Table 171-11 describes the options for this parameter.

Table 171-11 Standby Signalling parameter

Option	Parameter description	Dependencies
LACP (default)	LACP configuration is enabled on the LAG.	—
Power Off	LACP configuration is disabled on the LAG.	Active Sub-Group Selection Criteria parameter must be set to Best_Port.

Sub-Group ID

(subGroupId)

The Sub-Group ID parameter specifies a unique identifier for the LAG subgroup. The range is 1 to 8. The default is 1. Table 171-12 describes additional options for this parameter.

Table 171-12 Sub-Group ID parameter

Option	Parameter description	Dependencies
auto_mda	Ports that belong to the same MDA are assigned the same subgroup ID.	—
auto-iom	Ports that belong to the same IOM are assigned the same subgroup ID.	—

System Id

(portActorSystemId)

The System Id parameter specifies the system ID (MAC address) for the local port associated with a dynamic LAG. Specify a MAC address in the format xx-xx-xx-xx-xx-xx. The default is 00-00-00-00-00-00.

System Priority

(portActorSystemPriority)

The System Priority parameter specifies the system priority of the port that belongs to the dynamic LAG. The range is 0 to 255. The default is 0.

Type

(lagType)

The Type parameter specifies the type of LAG that you need to create. The options are:

- Static (default)
- Dynamic

View the newly created interface

The View the newly created interface parameter specifies that the Properties form for the newly created LAG opens when you close the configuration form.

172 –Shelf parameters

172.1 Shelf parameters 172-2

172.1 Shelf parameters

This chapter describes the parameters on the Shelf form, and the child forms launched from the right-click contextual menu options for shelves.

Activation

(packageCommand)

The Activation parameter specifies whether software that is stored in the standby bank of the compact flash card becomes the committed software during a reboot of the 9500 MPR. This can result in an upgrade or downgrade of the 9500 MPR, depending on the version of software in the standby bank. Table 172-1 describes the parameter options.

Table 172-1 Activation parameter

Option	Description	Dependencies
None	Displays the operational state of the software banks.	—
Activation	Activates the software stored in the standby bank. The 9500 MPR reboots using the software stored in the standby bank. The standby bank becomes the committed bank and the former committed bank becomes the standby bank.	The reboot occurs only when the software in the standby bank differs from the software in the committed bank.
Forced Activation	Activates the software stored in the standby bank. The 9500 MPR reboots using the software stored in the standby bank. The standby bank becomes the committed bank and the former committed bank becomes the standby bank.	The reboot occurs even when the software in the standby bank is the same as the software in the committed bank.

Active Timeout

(activateTimeout)

The Active Timeout parameter specifies the time delay before the certified directory is copied to the working directory. The parameter is configurable only when you set the [Command to Apply](#) parameter to copy certified to working. The range is 0 to 900. The default is 0.

Administrative Mode

(adminMode)

The Administrative Mode parameter specifies the administrative chassis mode of the device. The administrative chassis mode becomes the operational chassis mode when the minimum IOM card requirements are met. Table 172-2 describes the parameter options.

Table 172-2 Administrative Mode parameter

Option	Description	Dependencies
A (default)	Specifies chassis mode A	<p>Supported on the:</p> <ul style="list-style-type: none"> 7450 ESS-4, 7450 ESS-6, 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 7750 SR-7 and 7750 SR-12 <p>At least one of the following card types must be provisioned:</p> <ul style="list-style-type: none"> 2 x 10-Gig MDA IOM 2 x 10-Gig MDA IOM Card, B 2 x 10-Gig MDA IOM 2 (7750 SR only) 2 x 10-Gig MDA Oversubscribed IOM (7450 ESS only) 2 x XP MDA IOM 3
B	Specifies chassis mode B	<p>Supported on the:</p> <ul style="list-style-type: none"> 7450 ESS-4, 7450 ESS-6, 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 7750 SR-7 and 7750 SR-12 <p>At least one of the following card types must be provisioned:</p> <ul style="list-style-type: none"> 2 x 10-Gig MDA IOM Card, B 2 x 10-Gig MDA IOM 2 (7750 SR only) 2 x 10-Gig MDA Oversubscribed IOM (7450 ESS only) 2 x XP MDA IOM 3
C	Specifies chassis mode C	<p>Supported on the:</p> <ul style="list-style-type: none"> 7750 SR-7 and 7750 SR-12 <p>At least one of the following card type must be provisioned:</p> <ul style="list-style-type: none"> 2 x 10-Gig MDA IOM 2 (7750 SR only) 2 x XP MDA IOM 3
D	Specifies chassis mode D	<p>Supported on the:</p> <ul style="list-style-type: none"> 7450 ESS 7750 MG 7750 SR-7 7750 SR-12 <p>The following card type must be provisioned in all card slots:</p> <ul style="list-style-type: none"> 2 x XP MDA IOM 3 <p>The following card type must be provisioned for the 7750 MG:</p> <ul style="list-style-type: none"> ISM Mobile Card

Administrative State

Table 172-3 lists where to find more information about the Administrative State parameter.

Table 172-3 Administrative State parameter

Parameter	See
Administrative State for shelf objects	Administrative State parameter in this section

(1 of 2)

Parameter	See
Administrative State for BITS	Administrative State parameter in this section
Administrative State for external timing reference	Administrative State parameter in this section
Administrative State for first timing reference	Administrative State parameter in this section
Administrative State for PTP	Administrative State parameter in this section
Administrative State for PTP clock	Administrative State parameter in this section
Administrative State for PTP peer	Administrative State parameter in this section
Administrative State for second timing reference	Administrative State parameter in this section

(2 of 2)

Administrative State

See the [Administrative State](#) parameter in section 182.1.

Administrative State

(bitsAdministrativeState)

The Administrative State parameter specifies whether the BITS clock is administratively enabled. The options are:

- Up
- Down (default)

Administrative State

(clockAdminState)

The Administrative State parameter specifies whether the PTP is administratively enabled. For a master, this determines whether or not clock information should be sent to the nodes. For a slave, this determines whether or not clock information should be received from the configured master. The options are:

- Enabled
- Disabled (default)

Administrative State

(externalInIfAdminStatus)

The Administrative State parameter specifies whether the external input timing reference is administratively enabled on the 7705 SAR. The options are:

- Up
- Down (default)

Administrative State

(firstTimingReferenceAdministrativeState)

The Administrative State parameter specifies whether the first timing reference is administratively enabled. The options are:

- Up
- Down (default)

Administrative State

(peerAdminState)

The Administrative State parameter specifies whether PTP communication can be established with the corresponding master. The options are:

- Enabled (default)
- Disabled

Administrative State

(ptpAdministrativeState)

The Administrative State parameter specifies whether the PTP clock is administratively enabled. The options are:

- Up
- Down (default)

Administrative State

(secondTimingReferenceAdministrativeState)

The Administrative State parameter specifies whether the second timing reference is administratively enabled. The options are:

- Up
- Down (default)

Alarm Clear Message

(externalAlarmClearMessage)

The Alarm Clear Message parameter allows you to customize the message that is displayed when a dry contact alarm is cleared. A text string of up to 64 characters may be entered. The default is N/A.

Alarm Severity

(externalAlarmSeverity)

The Alarm Severity parameter specifies the level of severity that is assigned to an external alarm condition. The options are:

- major (default)
- critical
- info

Alarm Trigger Message

(externalAlarmTriggerMessage)

The Alarm Trigger Message parameter allows you to customize the message that is displayed when a dry contact alarm is raised. A text string of up to 64 characters may be entered. The default is N/A.

Analog Threshold (mV)

(analogThreshold)

The Analog Threshold parameter specifies the input voltage threshold for all analog inputs associated with an auxiliary alarm definition. The parameter is specified in millivolts (mV). The range is 0 to 75000. The default is 0.

Announce Interval

(announceInterval)

The Announce Interval parameter specifies the expected interval, in seconds, between the receipt of announce messages. The range is 0 to 3. The default is 1.

Announce Receive Timeout

(announceRxTimeout)

The Announce Receive Timeout parameter specifies the number of announce timeouts that must occur before communication messages with a master clock are considered lost and the master clock is considered unavailable. The range is 2 to 10. The default is 3.

Clock ID

(clockId)

The Clock ID parameter specifies an IEEE 1588 PTP clock identifier. The range is 1 to 2. The default is 1.

Clock MDA

(clockHwPointer)

The Clock MDA parameter specifies the source MDA for an IEEE 1588 PTP clock. Only Ethernet v2 MDAs are supported. An MDA can be used as a source for only one clock. A single MDA cannot act as a source for multiple clocks.

Clock Priority 1

(clockGMPriority1)

The Clock Priority 1 parameter specifies a precedence hint used to determine a master clock for the PTP domain. The range is 0 to 255. The default is 255.

Clock Priority 2

(clockGMPriority2)

The Clock Priority 2 parameter specifies the a precedence hint used to determine a master clock for the PTP domain. The range is 0 to 255. The default is 255.

Clock Slave Only

(clockSlave)

The Clock Slave Only parameter specifies whether an IEEE 1588 PTP clock is slaved to a master clock. The parameter can be configured only if the [Clock Type](#) parameter is set to Ordinary. The default is True.

Clock Type

(clockType)

The Clock Type parameter specifies the type of the IEEE 1588 PTP clock. Table [172-4](#) describes the parameter options.

Table 172-4 Clock Type parameter

Option	Description	Dependencies
Boundary	A boundary clock is specified for a transmission component like an Ethernet switch.	—
Ordinary (default)	An ordinary clock is specified for an end node.	—

Command to Apply

(versionMngt)

The Command to Apply parameter allows you to manage the OmniSwitch running configuration. Table 172-5 describes the parameter options.



Note — If a switch is running from the certified directory, you cannot save any changes made in the running configuration. If the switch reboots, the changes made to switch parameters are lost. In order to save running configuration changes, the switch must be running from the working directory.

Table 172-5 Command to Apply parameter

Option	Description	Dependencies
No command applied (default)	Software management commands are not issued.	—
Certify and Synchro	Copies the working directory version of the software on the primary CMM to the certified directory on the primary CMM. This option also synchronizes the files between the primary and secondary CMMs by overwriting the contents of the secondary CMM certified directory with the contents of the primary CMM certified directory. This option updates all switches in an OS 6850, OS 6850E, or OS 6400 stack with the primary CMM files.	Choose this option only when the contents of the working directory have been verified as the best version of the CMM files. This option does not work when the switch is running from the certified directory.
Certify	Copies the working directory version of the software on the primary CMM to the certified directory on the primary CMM.	Choose this option only when the contents of the working directory have been verified as the best version of the CMM files. This option does not work when the switch is running from the certified directory.
Flash Synchro	Copies the certified directory version of the primary CMM software to the certified directory of the secondary CMM. This option is used to synchronize the certified directories of the primary and secondary CMMs. The two CMMs must be synchronized in case a fail over occurs. This option updates all switches in an OS 6850, OS 6850E, or OS 6400 stack with the primary CMM files.	—
Copy certified to working	Copies the contents of the primary CMM certified directory to the working directory of the primary CMM. The files in the working directory are overwritten by the contents of the certified directory.	—
Reload from working	Immediately reboots the primary CMM from the working directory. CMM fail over does not take place during this reboot, which causes a loss of switch functionality during the reboot. In addition, all network interfaces reboot, including the secondary CMM. This option synchronizes the working directories of all the switches in an OS 6850 , OS 6850E, or OS 6400 stack with the working directory of the primary CMM switch.	—

Control Status

(controlledStatus)

This parameter specifies the external Control Status of the User Interface Panel port. The options are:

- Release (default)
- Operate
- Raman APR

Control Type

(controlType)

This parameter specifies the external Control Type of the User Interface Panel port. The range is from 0 to 56 characters.

Connected To

(connectedTo)

This parameter specifies the Amplifier Card that the User Interface Panel port is connected to.

CPU Threshold (%)

(cpuThreshold)

The CPU Threshold (%) parameter specifies the CPU usage threshold. CPU usage refers to the total amount of CPU processor capacity currently being used by the switch applications. The default is 80. The range is 0 to 100.

Delayed Activation Timer

(delayedActivateTimer)

The Delayed Activation Timer parameter specifies the time delay before executing the reload from working directory option. The parameter is configurable only when you set the [Command to Apply](#) parameter to reload from working directory. The range is 0 to 4 294 967 295 seconds. The default is 0.

Description

See the [Description](#) parameter in section [182.1](#).

Domain

(domain)

The Domain parameter specifies the PTP device domain. A domain consists of one 7705 SAR or multiple PTP 7705 SARs communicating with each other. A PTP domain defines the scope of PTP message communication, state, operations, data sets and time scale. A domain is configured since it is possible that a deployment could require the two PTP instances within a single 7705 SAR to be configured with different domain values. The range is 0 to 127. The default is 0.

Dynamic Peers

(clockDynamicPeers)

The Dynamic Peers parameter specifies whether dynamic PTP peer discovery is enabled for a PTP clock. Dynamic discovery is supported only for boundary and master clocks. The default is False.

The Dynamic Peers parameter is supported only when the [PTP Profile](#) parameter is set to IEEE1588-2008.

First Timing Reference Input

(firstTimingReferenceInput)

The First Timing Reference Input parameter specifies first timing reference input type to the BITS clock. The options are:

- BITS (default)
- Reference One (default for 7710 SR)
- Reference Two
- external (default for 7705 SAR)
- PTP

First Timing Reference Interface Type

(firstTimingRefBitsInterfaceType)

The First Timing Reference Interface Type parameter specifies first timing reference input type to the BITS clock. The default is T1 ESF.

First Timing Reference PTP Clock

(firstTimingReferenceSrcPtpClock)

The First Timing Reference PTP Clock parameter specifies the clock ID of an IEEE 1588 PTP clock for the first timing reference input. The range is 0 to 2. The default is 0.

Force Mode

(forceMode)

The Force Mode parameter specifies whether to force a change in the chassis mode set by the [Administrative Mode](#) parameter even if the installed IOM cards are not compatible with the configured chassis mode. The operational chassis mode is only changed if the installed IOM card is compatible with the specified administrative chassis mode. If the Force Mode parameter is enabled, all cards in the chassis that do not support the new chassis mode are taken offline. The parameter is disabled by default.

Fourth Timing Reference Input

(fourthTimingReferenceInput)

The Fourth Timing Reference Input parameter specifies fourth timing reference input type to the clock. The options are:

- BITS
- Reference One
- Reference Two
- PTP (default)

ID

(id)

The ID parameter specifies a unique numerical identifier for an auxiliary alarm definition. The range is 1 to 2147483647. The parameter is set to auto-assign by default.

Impedance Type

(externalInputImpedanceType)

The Impedance Type specifies the input impedance value of the external input timing interface on the 7705 SAR. The options are:

- High Impedance (default)
- 75 ohm
- 50 ohm

Input 1

(inputOne)

The Input 1 parameter specifies the CLI name of an auxiliary alarm resource.

Input 2

(inputTwo)

The Input 2 parameter specifies the CLI name of an auxiliary alarm resource.

Input 3

(inputThree)

The Input 3 parameter specifies the CLI name of an auxiliary alarm resource.

Input 4

(inputFour)

The Input 4 parameter specifies the CLI name of an auxiliary alarm resource.

Input 5

(inputFive)

The Input 5 parameter specifies the CLI name of an auxiliary alarm resource.

Input 6

(inputSix)

The Input 6 parameter specifies the CLI name of an auxiliary alarm resource.

Input 7

(inputSeven)

The Input 7 parameter specifies the CLI name of an auxiliary alarm resource.

Input 8

(inputEight)

The Input 8 parameter specifies the CLI name of an auxiliary alarm resource.

Input Administrative State

(bitsAdministrativeState)

The Input Administrative State parameter specifies whether external BITS timing reference is input to the 7450 ESS, 7710 SR, 7750 SR or 7750 SR-c4. The options are:

- Up
- Down (default)

Input Type

(externalInIfType)

The Input Type parameter specifies the interface type of the external input timing reference on the 7705 SAR. The options are:

- 2048Khz-G703 (default)
- 5 Mhz
- 10 Mhz

Interface Name

Click on the Select button beside the Interface Name parameter and select a timing reference.

Interface Type

(bitsInterfaceType)

The Interface Type parameter specifies the BITS interface type. The options are:

- T1 ESF (default)
- T1 SF
- E1 PCM30CRC
- E1 PCM31CRC
- 2048Khz-G703



Note — The 2048Khz-G703 option is available only for the 7705 SAR 18, version 4.0 R3 and later.

Log Event

(logEvent)

The Log Event parameter specifies whether an auxiliary alarm event generates an event in a log file. The parameter is enabled by default.

Master 1 Address

(masterOneIpAddress)

The Master 1 Address specifies the IP address of the PTP master clock to which PTP communications can be established. A second PTP master clock is defined using the [Master 2 Address](#) parameter. Specify an IPv4 address in dotted-decimal format.

Master 2 Address

(masterTwoIpAddress)

The Master 2 Address specifies the IP address of the second PTP master clock to which PTP communications can be established. The other PTP master clock is defined using the [Master 1 Address](#) parameter. Specify an IPv4 address in dotted-decimal format.

Memory Threshold (%)

(memoryThreshold)

The Memory Threshold (%) parameter specifies the memory usage threshold. Memory usage refers to the total amount of RAM currently being used by the switch applications. The default is 80. The range is 0 to 100.

Mixed Mode State on Chassis Enabled

(mixedMode)

The Mixed Mode State on Chassis Enabled parameter specifies when:

- 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 devices support the functionality of the 7750 SR IOM3-XPs and associated MDA-XPs or IMMs.
- IPv6 functionality is supported on a 7750 SR-7 or 7750 SR-12 device set to chassis mode B.

When the parameter is enabled for 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 devices and the [Capability](#) parameter is enabled, the IOM3-XPs and associated MDAs and IMMs function as 7750 SR cards and the 7450 ESS supports:

- base IPv6 routing
- access to VPRN services
- full-scale IP, including BGP support
- ATM and frame relay VLLs

When the parameter is enabled for a 7750 SR-7 or 7750 SR-12 device and the [Administrative Mode](#) parameter is set to B, IPv6 is supported without having to upgrade the entire chassis to support a new level. However all IPv6 interfaces are restricted to ports on the 7750 IOM3-XPs or IMMs.

When the parameter is disabled, the 7450 ESS is configured for legacy mode and the IOM3-XPs and associated MDAs and IMMs function as 7450 ESS cards. In addition, the 7750 SR-7 and 7750 SR-12 devices will not support IPv6 functionality in chassis mode B.

Monitored Status

(enableStatus)

The Monitored Status parameter specifies whether an alarm is raised on the 5620 SAM if an external alarm condition is detected. The options are:

- Enable (default)
- Disable

Name

(dryContactName)

The Name parameter specifies a name for the dry contact sensor. The range is 0 to 16 characters. The default is 0, which does not specify a name is specified for the dry contact sensor.

Network Type

(clockNetworkType)

The Network Type parameter specifies the network type of the IEEE 1588 PTP clock. The options are:

- SDH (default)
- SONET

Operation

(analogOperation)

The Operation parameter specifies whether analog inputs for an auxiliary alarm become active when the detected voltage is greater than or less than the threshold specified by the [Analog Threshold \(mV\)](#) parameter. The options are:

- Not Monitored (default)
- Greater Than
- Less Than

Output Administrative State

(bitsOutputState)

The Output Administrative State parameter specifies whether external BITS timing reference is output to the 7450 ESS, 7710 SR, 7750 SR or 7750 SR-c4. The options are:

- Up
- Down (default)

Output Line Length

(bitslineLength)

The Output Line Length parameter specifies the distance, in feet, between the NE and the office clock for DS1 interface type. This parameter is not applicable for BITS E1 interface type. The options are:

- | | |
|-----------------------------|---------------------|
| • Length 0 to 110 (default) | • Length 330 to 440 |
| • Length Not Applicable | • Length 440 to 550 |
| • Length 110 to 220 | • Length 550 to 660 |
| • Length 220 to 330 | |

Output Type

(externalOutIfType)

The Output Type parameter specifies the interface type of the external output timing reference on the 7705 SAR and 9500 MPR. The options for the 7705 SAR are:

- 2048Khz-G703 (default)
- 5 Mhz
- 10 Mhz

The options for the 9500 MPR are:

- None (default)
- 2048Khz-G703
- 5 Mhz
- 10 Mhz
- 1024 KHz (supported on ETSI 3.0.0 only)

Peer ID

(peerId)

The Peer ID parameter specifies the identity of the IEEE 1588 PTP peer. The range is 1 to 2. The default is 1.

Peer IP Address

(peerIpAddress)

The Peer IP Address parameter specifies the IP address of the IEEE 1588 PTP peer. Specify an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

Peer Priority

(peerPriority)

The Peer Priority parameter specifies the priority of the IEEE 1588 PTP peer. The range is 1 to 255. The default is 128.

Polarity

(polarity)

The Polarity parameter specifies the state of external contact sensors that are used to indicate an alarm condition. Table 172-6 describes the parameter options.

Table 172-6 Polarity parameter

Option	Description	Dependencies
Normally Opened	An open circuit indicates normal operation of the external device. A closed circuit indicates an alarm condition.	—
Normally Closed	A closed circuit indicates normal operation of the external device. An open circuit indicates an alarm condition.	—

Port or Channel Name

Click on the Select button beside the Port or Channel Name parameter and select a timing reference.

Primary Multicast Bandwidth (mbps)

(primaryPerMcastPlaneLimit)

The Primary Multicast Bandwidth (mbps) parameter specifies the multicast traffic rate limit supported on each switch fabric multicast plane when there is only one switch fabric card. The value of this parameter must be greater than or equal to the [Secondary Multicast Bandwidth \(mbps\)](#) parameter value. The range is 1 to 2000. The default is 2000.

Primary Multicast Bandwidth for Dual-SFM Mode (mbps)

(primaryPerMcastDualPlaneLimit)

The Primary Multicast Bandwidth for Dual-SFM Mode (mbps) parameter specifies the multicast traffic rate limit supported on each switch fabric multicast plane when there is more than one switch fabric card. The value of this parameter must be greater than or equal to the [Secondary Multicast Bandwidth for Dual-SFM Mode \(mbps\)](#) parameter value. The range is 1 to 2000. The default is 2000.

Primary Reference Type

(primaryTimingReferenceType)

The Primary Reference Type parameter specifies the primary timing source for the 9500 MPR. The options are:

- Free Run Local Oscillator (default)
- E1/T1 Port
- Sync-In Port
- Radio Port
- Ethernet Port
- None
- STM Port

PTP Profile

(clockProfile)

The PTP Profile parameter specifies the PTP profile for a PTP clock. Table [172-7](#) lists the parameter options.

Table 172-7 PTP Profile parameter

Option	Description	Dependencies
IEEE1588-2008 (default)	A profile defined by the Institute of Electrical and Electronics Engineers (IEEE). This profile is defined in accordance with the IEEE 1588-2008 standard.	—
ITUTelecomFreq	A profile defined by the International Telecommunication Union (ITU). This profile is targeted towards frequency synchronization, as required for operating GSM base stations, UMTS Node Bs, WiMax-FDD base stations, etc.	—

Quality Level Override

This parameter specifies the quality level used for SETS input selection. This value overrides any value received by the SSM process of that reference. Table 172-8 lists the Quality Level Override parameters.

Table 172-8 Quality Level Override parameters

Parameter	Description	Options
Quality Level Override (firstTimingReferenceQualityLevel)	Specifies the quality level used for the first timing reference for SETs input selection.	<ul style="list-style-type: none"> • None • Prs • Stu • St2 • Tnc • St3e • St3 • Prc • Ssua • Ssub • Sec • Eec1 • Eec2
Quality Level Override (secondTimingReferenceQualityLevel)	Specifies the quality level used for the second timing reference for SETs input selection.	
Quality Level Override (bitsQualityLevel)	Specifies the quality level used for the reference for SETs input selection.	
Quality Level Override (ptpQualityLevel)	Specifies the quality level used for the reference for SETs input selection.	

Quality Level Reference

(qualityLevel)

The Quality Level Reference parameter specifies whether the quality level is considered for system timing reference and BITS output timing reference. When this parameter is set to Enabled, SSM encoding is enabled for timing reference selection. The options are:

- Disabled (default)
- Enabled

Reference Input Mode

(revertive)

Table 172-9 lists where to find information about the Reference Input Mode (revertive) parameter.

Table 172-9 Reference Input Mode (revertive) parameter

Parameter	See the
Reference Input Mode (revertive) for 9500 MPR	Reference Input Mode (revertive) parameter in this section
Reference Input Mode (revertive) for devices other than the 9500 MPR	Reference Input Mode (revertive) parameter in this section

Reference Input Mode (revertive)

(revertive)

The Reference Input Mode parameter specifies whether the 9500 MPR reverts to the timing source specified by the [Primary Reference Type](#) parameter when the timing source returns to service after a failure. The options are:

- true (default)
- false

Reference Input Mode (revertive)

(revertive)

The Reference Input Mode parameter specifies whether the input mode of the timing reference is revertive. The options are:

- false (default)
- true

Role

(role)

The role parameter specifies the state of the timing status. The options are:

- Master (default)
- Slave

Rx Threshold (%)

(rxThreshold)

The Rx Threshold (%) parameter specifies the maximum percentage of total bandwidth allowed for incoming traffic on the switch. The total bandwidth is defined as the Ethernet port capacity of all network interface modules currently operating in the switch. The default is 80. The range is 0 to 100.

Sampling Interval (seconds)

(samplingInterval)

The Sampling Interval (seconds) parameter specifies the sampling interval between health statistics checks. The sampling interval is the time interval between polls of the consumable resources of the switch to see if it is performing within set thresholds. The options are:

- 1
- 2
- 3
- 4
- 5 (default)
- 6
- 10
- 12
- 15
- 20
- 30

Second Timing Reference Input

(secondTimingReferenceInput)

The Second Timing Reference Input parameter specifies second timing reference input type to the BITS clock. The options are:

- BITS
- Reference One (default)
- Reference Two
- external
- PTP

Second Timing Reference Interface Type

(secondTimingRefBitsInterfaceType)

The Second Timing Reference Interface Type parameter specifies second timing reference input type to the BITS clock. The default is T1 ESF.

Second Timing Reference PTP Clock

(secondTimingReferenceSrcPtpClock)

The Second Timing Reference PTP Clock parameter specifies the clock ID of an IEEE 1588 PTP clock for the second timing reference input. The range is 0 to 2. The default is 0.

Secondary Multicast Bandwidth (mbps)

(secondaryPerMcastPlaneLimit)

The Secondary Multicast Bandwidth (mbps) parameter specifies the rate limit for secondary multicast traffic for each switch fabric multicast plane when there is only one switch fabric card. The value of this parameter must be less than or equal to the [Primary Multicast Bandwidth \(mbps\)](#) parameter value. The range is 1 to 2000. The default is 1800.

Secondary Multicast Bandwidth for Dual-SFM Mode (mbps)

(secondaryPerMcastDualPlaneLimit)

The Secondary Multicast Bandwidth for Dual-SFM Mode (mbps) parameter specifies the rate limit for secondary multicast traffic for each switch fabric multicast plane when there is more than one switch fabric card. The value of this parameter must be less than or equal to the [Primary Multicast Bandwidth for Dual-SFM Mode \(mbps\)](#) parameter value. The range is 1 to 2000. The default is 1800.

Secondary Reference Type

(secondaryTimingReferenceType)

The Secondary Reference Type parameter specifies the secondary timing source for the 9500 MPR. The options are:

- None (default)
- Free Run Local Oscillator
- E1/T1 Port
- Sync-In Port
- Radio Port
- Ethernet Port
- STM Port

Severity

(severity)

The Severity parameter specifies the severity level raised for an auxiliary alarm. The options are:

- Critical
- Major (default)
- Minor
- Warning

Status

(status)

The Status parameter specifies the timing synchronization role of the 9500 MPR shelf. Table [172-10](#) describes the parameter options.

Table 172-10 Status parameter

Option	Description
Master (default)	The shelf generates the timing signal that it sends to other shelves.
Slave	The shelf does not generate the timing signal that it sends to other shelves.

SSM

(saBit)

The SSM parameter specifies which saBit to use for conveying SSM information when the interface type is E1. The range is 4 to 8. The default is 8.

Sync Interval

(syncInterval)

The Sync Interval parameter specifies the interval between the receipt of synchronization messages. The range is -7 to -6. The default is -6.

Sync In Port

(syncInPort)

The Sync In Port parameter specifies the 9500 MPR timing synchronization port that receives the timing signal. The options are:

- Not Used (default)
- 1024 KHz (ETSI only)
- 2.048 MHz
- 5 MHz
- 10 MHz

Sync Out Port

(syncOutPort)

The Sync Out Port parameter specifies the 9500 MPR timing synchronization port that sends the timing signal to other shelves. The options are:

- Not Used (default)
- 1.024 MHz (ETSI only)
- 2.048 MHz
- 5 MHz
- 10 MHz

System Quality Level

(systemQualityLevel)

The System Quality Level parameter, which is not configurable (read-only), specifies the quality level of synchronization status messages for downstream network elements. A number of standardized quality levels are available to convey to a downstream clock. The options are:

- None
- Prs
- Stu (default)
- St2
- Tnc
- St3e
- St3
- Smc
- St4
- Prc
- Ssua
- Ssub
- Sec
- Eec1
- Eec2

Temperature Threshold

(temperatureThreshold)

The Temperature Threshold parameter specifies the chassis temperature threshold. The chassis temperature threshold is the maximum operating temperature allowed within the chassis before a trap is sent. The default is 60. The range is 0 to 100.

Temperature Threshold Unit

(temperatureThresholdUnit)

The Temperature Threshold Unit parameter specifies the temperature units used to display the chassis temperature. The options are:

- Celsius (default)
- Fahrenheit

Third Timing Reference Input

(thirdTimingReferenceInput)

The Third Timing Reference Input parameter specifies third timing reference input type to the BITS clock. The options are:

- BITS
- Reference One
- Reference Two (default)
- external
- PTP

The third timing reference is not supported on the 7710 SR and 7705 SAR.

Trigger Rule

(triggerRule)

The Trigger Rule parameter specifies whether an auxiliary alarm is triggered as a result of any single input becoming active, or as a result of all inputs becoming active. The options are:

- Any Input (default)
- All Inputs

TxRx Threshold (%)

(txRxThreshold)

The TxRx Threshold (%) parameter specifies the maximum percentage of total bandwidth allowed for all incoming and outgoing traffic. The total bandwidth is defined as the Ethernet port capacity for all the network interface modules. The default is 80. The range is 0 to 100.

Type

(firstTimingReferenceType)

The Type parameter specifies the type of reference for the first timing reference. The options are:

- Port or Channel
- Network Interface

Type

(secondTimingReferenceType)

The Type parameter specifies the type of reference for the second timing reference. The options are:

- Port or Channel
- Network Interface

When you set the [Type](#) parameter to Network Interface, the 7705 SAR is configured as a client for IEEE 1588 PTP.

Update Chassis Relays

(chassisRelays)

The Update Chassis Relays parameter specifies whether an auxiliary alarm event updates chassis indicator LEDs and relay settings. The parameter is enabled by default.

Wait to Restore Time (Min):**(waitToRestoreMin)**

The Wait to Restore Time (Min): parameter specifies the amount of time in minutes to wait before restoring timing synchronization. The default is 5. The range is 0 to 12, in increments of 1. This parameter can be configured in conjunction with the [Wait to Restore Time \(Secs\):](#) parameter.

Wait to Restore Time (Secs):**(waitToRestoreSec)**

The Wait to Restore Time (Secs): parameter specifies the amount of time in seconds to wait before restoring timing synchronization. This parameter can be configured in conjunction with the [Wait to Restore Time \(Min\):](#) The options are:

- 0 (default)
- 10
- 20
- 30
- 40
- 50

173 –APS Groups parameters

173.1 APS Groups parameters 173-2

173.1 APS Groups parameters

This chapter describes the parameters on the SC APS Group creation form, the MC APS Group creation form, and child forms.

Administrative State

See the [Administrative State](#) parameter in section 112.1.

Advertise Interval (100s of milliseconds)

(multiChassisAdvertiseInterval)

The Advertise Interval (100s of milliseconds) parameter specifies how often the protection and working channels of neighbor devices in a MC APS group send messages to each other to indicate that they are operationally up. The range is 10 to 650 in 100s of ms. The default is 10.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 112.1.

Channel Role

(apsChannelRole)

The Channel Role parameter indicates whether the APS channel is working or protection. The options are:

- Working
- Protection

Command Switch

(commandSwitch)

The Command Switch parameter specifies the operational state of APS. This parameter allows you to perform protection switch actions. Table 173-1 describes the options.

Table 173-1 Command Switch parameter

Option	Option Description
No Cmd	Indicates that no command is issued to the APS channel
Clear (default)	Clears all switches for the specified channel
Lockout of Protection	Disables use of the protection channel Because this option has the highest priority, a failed working channel that switches to the protection channel switches back to the working channel even if the channel has a fault condition.

(1 of 2)

Option	Option Description
Forced Switch of Working to Protection	Forces a high-priority switch of traffic on the specified working channel to the protection channel, unless a request of equal or higher priority is in effect This option is overridden by a Lockout of Protection command or the detection of a signal fault on the protection line. If the working channel traffic is already on the protection channel, no action occurs.
Forced Switch of Protection to Working	Forces a high-priority switch of traffic on the specified protection channel to the working channel, unless a request of equal or higher priority is in effect If the protection channel traffic is already on the working channel, no action occurs.
Manual Switch of Working to Protection	Allows the user to manually switch traffic on the specified working channel to the protection channel, unless a request of equal or higher priority is in effect If the working channel traffic is already on the protection channel, no action occurs.
Manual Switch of Protection to Working	Allows the user to manually switch the traffic on the specified protection channel to the working channel, unless a request of equal or higher priority is in effect If the protection channel traffic is already on the working channel, no action occurs.
Exercise	Exercises the protection channel by sending an exercise request message over the protection line to the far-end device and expecting a reverse request message in return No switch is performed during the exercise routine. This option is only supported in bidirectional mode on 1+1 architecture.

(2 of 2)

Description

See the [Description](#) parameter in section 112.1.

Direction

(direction)

The Direction parameter specifies the direction for APS. The options are:

- bidirectional
- unidirectional
- uni1plus1

Group Number

(groupNumber)

The Group Number parameter specifies the group number for the APS group. The range is 1 to 64 for a single seven-slot or twelve-slot 7750 SR. The range is 1 to 16 for a single one-slot 7750 SR. There is no default.

Hold Time (100s of milliseconds)

(multiChassisHoldTime)

The Hold Time (100s of milliseconds) parameter specifies the maximum time that a peer device in a MC APS group waits between successive update messages from its neighbor before considering that the MC signaling link is operationally down. The range is 10 to 650 in 100s of ms. The default is 30.

Hold Time for Line Signal Degradation (100s of milliseconds)

(holdTimeApslSignalDegrade)

The Hold Time for Line Signal Degradation (100s of milliseconds) parameter specifies hold-down timers to debounce signal degrade conditions. The parameter is configurable on a 7750 SR-c4 or 7750 SR-c12 when the [Direction](#) parameter is set to uni1plus1. The range is 0 to 100. The default is 0.

Hold Time for Line Signal Failure (100s of milliseconds)

(holdTimeApslSignalFail)

The Hold Time for Line Signal Failure (100s of milliseconds) parameter specifies hold-down timers to debounce signal failure conditions. The parameter is configurable on a 7750 SR-c4 or 7750 SR-c12 when the [Direction](#) parameter is set to uni1plus1. The range is 0 to 100. The default is 0.

Network Interface

Table [173-2](#) lists where to find more information about the Network Interface parameter.

Table 173-2 Network Interface parameter

Parameter	See
Network Interface for first MC APS group member	Network Interface parameter in this section
Network Interface for second MC APS group member	Network Interface parameter in this section

Network Interface

(interfaceAddressHigh)

The Network Interface parameter specifies the interface of the second MC APS group member. Click on the Select button to list and choose an interface. The interface must be a numbered IPv4 interface. The default is the NE system interface.

Network Interface

(interfaceAddressLow)

The Network Interface parameter specifies the interface of the first MC APS group member. Click on the Select button to list and choose an interface. The interface must be a numbered IPv4 interface. The default is the NE system interface.

RDI Alarm Generation

(rdiAlarmGeneration)

The RDI Alarm Generation parameter specifies how RDI alarms are generated. The parameter is configurable on a 7750 SR-c4 or 7750 SR-c12 when the [Direction](#) parameter is set to uni1plus1. The options are:

- Circuit (default)
- Suppress

Reversion Mode

(revertMode)

The Reversion Mode parameter specifies whether the APS configuration is revertive. In non-revertive switching, a switch to the protection channel is maintained even after the working line has recovered from a failure or the manual switch has been cleared. In revertive switching, the traffic is switched back to the working channel after the working line has recovered from a failure or the manual switch has been cleared. The options are:

- nonrevertive (default)
- revertive

Wait To Restore (seconds)

(waitToRestore)

The Wait To Restore (seconds) parameter specifies the wait-to-restore period in seconds for revertive switching. After clearing a condition that necessitated an automatic switch, the wait-to-restore period must elapse before traffic reverts to the working channel. The parameter is enabled when the [Reversion Mode](#) parameter is set to revertive. The range is 0 and 60 to 3600 s. The default is 300 s.

A change in the value of the Wait To Restore (seconds) parameter takes effect at the next initiation of the wait-to-restore period. A change in the value does not modify the length of a wait-to-restore period that is currently active.

174 –Card Slot parameters

174.1 Card Slot parameters 174-2

174.1 Card Slot parameters

This chapter describes the parameters on the Card Slot form, and the child forms launched from the right-click contextual menu options for card slots.

Administrative

The Administrative parameter is used to differentiate between an OS 6850 and OS 6850E NE for card slot configuration purposes at the administrative level. The options are:

- OS 6850 (default)
- OS 6850E

Administrative State

See the [Administrative State](#) parameter in section [182.1](#).

Assigned Card Type

(assignedChildType)

The Assigned Card type parameter specifies the card type to be configured for the card slot. The options depend on the settings of the Supported Card Types and Allowed Card Types parameters. You can configure the card for the slot when the Supported Card Types and Allowed Card Types parameters are set to the same value.

- 400g CPM/Switch Fabric
- 400g CPM/Switch Fabric 2
- 2 x 10-Gig MDA IOM
- 250g CPM/Switch Fabric 3
- 500g CPM/Switch Fabric 3
- 2 x 10-Gig MDA IOM Card, B
- 2 x 10-Gig MDA IOM 2
- 2 x 10-Gig MDA Oversubscribed IOM
- 2 x XP MDA IOM 3
- 7705 IOM
- 2-Port Gig Ethernet MDA with SyncE
- 4-Port 10GE XFP IMM
- 8-Port 10GE XFP IMM
- 5-Port 10GE XFP IMM
- 7750 SR-c12 IOM-XP
- OS9600-CMM
- OS9700-CMM
- OS 9700E-CMM
- 24-Port Gig Ethernet FX
- 2-Port 10 Gig Ethernet XFP
- 24-Port Fast Ethernet Metro(24 TX, 2 Dual TX/FX)
- 24-Port Fast Ethernet SME(24 TX, 2 Dual TX/FX)
- 24-Port PoE Gig Ethernet SME(24 TX, 2 Dual TX/FX)
- 8-Port Fast Ethernet Metro (8 TX, 2 Dual TX/FX)
- 24-Port Fast Ethernet SME(24 TX, 2 Dual TX/FX) with DC Power Supply
- 12-Port 10GE SF IMM
- 6 x EM
- 24-Port Gig Ethernet TX
- 7750-SRc4 CFM-C4-XP
- VSM Cross Connect Adapter
- 16 x Channelized DS1/E1 ASAP
- 14-Port Gig Ethernet (12 TX (4PoE), 2FX)
- 10-Port Gig Ethernet (8 FX, 2 TX)
- 24-Port Gig Ethernet (22 FX, 2 TX/FX, 2 FX/STK)
- 24-Port Gig Ethernet (20 TX (4 PoE), 4 TX/FX, 4 Dual TX/FX)
- 24-Port Gig Ethernet (22 FX, 2 TX/FX)
- OS9800-CMM
- OS 9800E-CMM
- 12g 7710 IOM
- 100g CPM/Switch Fabric
- 1 x 10-Gig MDA IOM
- 200g CPM/Switch Fabric
- 200g CPM/Switch Fabric 2
- 80g CPM/Switch Fabric 2
- 7705 1g CSM
- 48-Port GIGE SFP IMM
- 48-Port GIGE TX IMM
- CORE-ENH
- CORE-B
- 32 x E1
- 2 x DS3
- 32 x DS1
- 16 x E1 ASAP
- 4+4 x Ethernet (EAS)
- 2+2 x Ethernet (EAS)
- 1-Port OC768 OTU3 Long Reach DWDM Tunable IMM
- 1 x Radio Modem
- 1-Port 100GE CFP IMM
- 7750 SRc12 CFM-XP
- Auxiliary Alarm
- 7750-SRc4 IOM-C4-XP
- VSM Cross Connet Adapter Extended Performance
- 32 x Channelized DS1/E1 ASAP
- 500g CPM/Switch Fabric 4
- 1 Tb CPM/Switch Fabric 4

Capability

(cardCapability)

The Capability parameter specifies whether the cards on the 7450 ESS-6v, 7450 ESS-7, and 7450 ESS-12 function as 7450 ESS cards, or 7750 SR IOM3-XP's and associated MDA-XP's or IMMs.

When the Capability parameter and the [Mixed Mode State on Chassis Enabled](#) parameter are both enabled, the IOM3-XP's and associated MDAs and IMMs function as 7750 SR cards.

When the Capability parameter is not enabled, the IOM3-XP's and associated MDAs and IMMs function as 7450 ESS cards.

Combo Port

(comboPort)

The Combo Port parameter specifies whether an RJ45 10/100/1000BaseT or 100/1000baseX SFP combination port is configurable. The parameter is configurable only on an OS 6250 SME. The options are:

- disable (default)
- enable

Command Action

(commandAction)

The Command Action parameter allows you to configure hardware-related operations on an OS 6850, OS 6850E, OS 6400, or OS 6250 switch stack. Table [174-1](#) describes the parameter options.

Table 174-1 Command action parameter

Option	Description	Dependencies
Not Significant	A command is not issued.	—
Clear Slot (default)	Clears the current saved slot information for a switch in an OS 6850, OS 6850E, OS 6400, or OS 6250 stacked configuration. When the saved slot information is cleared, the corresponding switch is automatically assigned a unique slot number after a reboot.	—
Reload	Reboots the OS 6850, OS 6850E, OS 6400, or OS 6250 switch	When the OS 6850, OS 6850E, OS 6400, or OS 6250 switch is the primary CMM in a stack, it will no longer be primary. Instead, it will be secondary in a two-switch stack and idle in a stack consisting of three or more switches.

Commands

See the [Commands](#) parameter in section 182.1.

Enable Power Capacitor Detection

(capacitorDetect)

The Enable Power Capacitor Detection parameter specifies whether to enable or disable the capacitor detection method for an OmniSwitch. The options are:

- true (default)
- false

The capacitor detection method should only be enabled if there are legacy IP phones that are attached to the corresponding slot which is not compatible with IEEE specification 802.3af. Contact your Alcatel-Lucent technical support representative to find out which Alcatel-Lucent IP phone models need capacitor detection enabled.

Enable Priority Disconnect

(priorityDisconnect)

The Enable Priority Disconnect parameter specifies whether to enable or disable the priority disconnect function on all ports in a specified slot of an OS 6400, OS 6850, or OS 6850E. Priority disconnect is used by the system software to determine whether an incoming PD is granted or denied power when the PoE power resource cannot support an additional device. The options are:

- true (default)
- false

Maximum Power (Watts)

(maxPower)

The Maximum Power (Watts) parameter specifies the maximum amount of inline power, in watts, that is allocated to all PoE ports in a slot. The range is 37 to 390. The default is 37.

Operational

The Operational parameter is used to differentiate between an OS 6850 and OS 6850E NE for card slot configuration purposes at the operational level. The options are:

- OS 6850 (default)
- OS 6850E

Pool Mode

(poolMode)

The Pool Mode parameter specifies whether named pools can be created for an MDA. The Pool Mode parameter can be enabled and disabled at any time. When the Named Pool is in service the system no longer creates default pools per port, instead a set of pools that can be used by all queues and are not explicitly mapped to a named pool is used. The options are:

- In service
- Out of Service

Port Maximum Power (MilliWatts)

(portMaximumPower)

The Port Maximum Power (MilliWatts) parameter specifies the maximum amount of inline power, in milliwatts, that is allocated to an individual PoE port in a slot. The range is 3000 to 16000. The default is 3000.

Power State

(adminStatus)

The Power State parameter specifies whether to disable or enable power on all PoE ports in a slot. The options are:

- On (default)
- Off

Protection Type

(cardProtectionType)

The Protection Type parameter specifies the type of protection scheme used by the 9500 MPR card. Table 174-2 describes the parameter options.

Table 174-2 Protection Type parameter

Card Type	Option	Description
1 x Radio Modem	No Protection (default)	Main card is not protected by a spare card.
	1 + 1 FD	Packets from the active card are transmitted simultaneously by two ODUs. Each ODU transmits on a different frequency. Packets are received by two ODUs. The active card selects and processes the best signal.
	1 + 1 HSB	Packets from the active card are transmitted simultaneously by two ODUs. Each ODU transmits on the same frequency. Packets are received by two ODUs. The active card selects and processes the best signal.

(1 of 2)

Card Type	Option	Description
32 x DS1/E1	No Protection (default)	Main card is not protected by a spare card.
	1 + 1 EPS	When the switch detects a failure in the active card, the standby card becomes active.

(2 of 2)

Reserved CBS Max (%)

(wredResvCbsMax)

The Reserved CBS Max (%) parameter specifies the maximum buffer size for the queue. The range is 0.01 to 99.99. The default is 25.00. The parameter value must be the same as the [Reserved CBS Min \(%\)](#) value.

Reserved CBS Min (%)

(wredResvCbsMin)

The Reserved CBS Min (%) parameter specifies the minimum buffer size for the queue. The range is 0.00 to 99.99. The default is 25.00. The parameter value must be the same as the [Reserved CBS Max \(%\)](#) value.

Restoration Criteria

See the [Restoration Criteria](#) parameter in section [182.1](#).

Saved Slot NI Number

(savedSlotNINumber)

The Saved Slot NI Number parameter sets the saved slot number for OS 6850, OS 6850E, OS 6855, OS 6400, or OS 6250 switches in a stacked configuration. The saved slot number is the slot position for the switch after a reboot. The range is 1 to 8, except for the OS 6855 U24X, which is 1 to 4, and the OS 6250M, which is 1 to 2. The default is 1.

Shutdown IOM for Memory Parity Errors

(failOnError)

The Shutdown IOM for Memory Parity Errors parameter specifies if a IOM card will be forcefully shutdown when the error threshold on the card is reached.

This parameter can only be configured on 7705 SAR-ME, 7450 ESS, and 7750 SR nodes.

Slot Priority

(slotPriority)

The Slot Priority parameter specifies an inline power priority level for a slot of an OS 6850, OS 6850E, or OS 6400. If the power supply of a stack is down, the order that slots are disabled is based on a priority assigned to the PoE ports on the slot. Table 174-3 describes the parameter options.

Table 174-3 Slot Priority parameter

Option	Description	Dependencies
Low (default)	Intended for slots that have low-priority devices attached. If there is a power problem, inline power to low-priority ports is interrupted first.	—
High	Intended for slots that have important, but not mission-critical devices attached. If there is a power problem, inline power to high-priority ports is assigned second priority.	—
Critical	Intended for slots that have mission-critical devices attached. If there is a power problem, inline power to critical ports is maintained as long as possible.	—

Stacking Action

(stackingAction)

The Stacking Action parameter specifies the stacking configuration for OS 6855 U24X and OS 6250 NEs. The options are:

- Stackable (default)
- Standalone



Note — For the stacking configuration of OS 6855 U24X NEs, when the value of this parameter is set to Standalone, the “[Saved Slot NI Number](#)” parameter value cannot be changed.

Temperature Threshold (Celsius)

(temperatureThreshold)

The Temperature Threshold (Celsius) parameter sets the CPU warning temperature threshold for an OmniSwitch. The range is 16 to 94. The default is 0.

Type

(powerSrcType)

This parameter indicates the power source type for a card slot of the 2+2 x Ethernet (EAS) card on 9500 MPR (ETSI 2.1) NEs. The options are:

- QMA (default)
- PoE
- Disabled

175 – Daughter Card and Daughter Card Slot parameters

175.1 Daughter Card and Daughter Card Slot parameters 175-2

175.1 Daughter Card and Daughter Card Slot parameters

This chapter describes the parameters on the Daughter Card and Daughter Card Slot forms and child forms.

Administrative State

See the [Administrative State](#) parameter in section [182.1](#).

Administrative State

(wredAdminState)

The Administrative State parameter specifies the administrative state of egress WRED queue support on an IOM3 or IMM card. When up, any WRED queue control attribute may be executed on the IOM3 or IMM card, and an egress QoS policy with [Use WRED Queue](#) enabled can apply to a SAP on the IOM3 or IMM card. Also, an egress queue group template policy with the [Use WRED Queue](#) parameter enabled can apply to a port on the IOM3 or IMM card. When the Administrative State is down, egress WRED queue support is disabled on the IOM3 or IMM card. The Administrative State parameter options are:

- Up
- Down (default)

Assigned Daughter Card Type

(assignedChildType)

The Assigned Daughter Card Type parameter specifies the daughter card type to be configured for the daughter card slot. The options depend on the settings of the unconfigurable Equipped Daughter Card Type and Supported Daughter Card Types parameters. You can configure the daughter card for the slot when the unconfigurable Supported Daughter Card Types parameter and the configurable [Assigned Card Type](#) parameter have the same value. The supported daughter cards vary for each managed device.

Assigned MCM Card Type

The Assigned MCM Card Type parameter specifies the MDA carrier module type to be configured for the daughter card slot. The options depend on the settings of the unconfigurable Supported Daughter Card Types and Allowed Daughter Card Types parameters. You can configure the parameter when the In MDA Carrier Module Slot parameter is enabled.

Buffer Allocation Max (%)

(wredBufAllocMax)

The Buffer Allocation Max (%) parameter specifies the maximum value of hardware buffer space that is used by the egress queue. The range is 0.01 to 99.99. The default is 25.00. The parameter value must be the same as the [Buffer Allocation Min \(%\)](#) value.

Buffer Allocation Min (%)

(wredBufAllocMin)

The Buffer Allocation Min (%) parameter specifies the minimum value of hardware buffer space that is used by the egress queue. The range is 0.00 to 99.99. The default is 25.00. The parameter value must be the same as the [Buffer Allocation Max \(%\)](#) value.

Channel ID

(channelId)

The Channel ID parameter specifies the identifier for the Channel Group. The identifier must be unique across the device. The range is 1 to 64. The default is 0, which means that the parameter is not configured.

Clock Mode

(clock)

The Clock Mode parameter specifies the source of the clock signal for the CES module. Table [175-1](#) lists the parameter options.

Table 175-1 Clock Mode parameter

Option	Option description
adaptive	The TDM bitstream from the master CES module supplies the clock signal.
backplane	The CES module uses a clock signal from the neighboring CES module. The neighboring CES module receives its clock signal from an external oscillator.
External backplane port 1 backup	The clock signal from an external device that is connected to port 1 is the primary clock source, and the clock signal from the neighboring CES module acts as a backup clock source when the primary clock source is not available.
external port 1	The CES module uses a clock signal from an external device that is connected to port 1.
local	The on-card oscillator supplies the clock signal.
loopback (default)	The master CES module loops back the receive (Rx) clock signal and uses it as the transmit clock signal.
backplane backup external port 1	The clock signal from the neighboring CES module is the primary clock source, and the clock signal from an external device that is connected to port 1 acts as a backup clock source when the primary clock source is not available.

Clock Mode

(clockMode)

The Clock Mode parameter specifies the source of the clock signal for the MDA. The options are:

- Adaptive
- Differential
- Not Applicable (default)

Companding Law

(voiceCompanding)

The Companding Law parameter sets the companding law for a 7705 SAR six port E&M daughter card. The default is muLaw.

Differential Timestamp Frequency

(diffTimestampFrequency)

The Differential Timestamp Frequency parameter specifies the timestamp frequency, in kHz, of the differential clock on the MDA. The options are:

- 0 (default when clock mode is not differential)
- 19440
- 77760
- 103680 (default when clock mode is differential)

The Differential Timestamp Frequency parameter can be configured only when the [Clock Mode](#) parameter is set to Differential and no ports are configured on the MDA. If ports are configured, you must shut down the MDA.

Gateway IP Address

(gatewayIpAddress)

The Gateway IP Address parameter specifies the IP address that the CES module uses as a default gateway. The default is the [IP Address](#) parameter value.

In MDA Carrier Module Slot

(inMCM)

The In MDA Carrier Module Slot parameter specifies whether the daughter card slot on the 7710 SR allows the configuration of MDAs that are also supported on the 7750 SR. The default is disabled.

IP Address

(ipAddress)

The IP Address parameter specifies the IP address for the CES module. The default is 192.168.0.4 for the CES module in slot 4 and 192.168.0.4 for the CES module in slot 5.

Mask

(mask)

The Mask parameter specifies the subnet mask that is applied to the [IP Address](#) parameter value to create a unique IP identifier for the CES module. The range is 0 to 32. The default is 24.

Mode

(mode)

The Mode parameter specifies the type of line that is connected to the CES module. The options are:

- E1 (default)
- T1

Packet Byte Offset

(packetByteOffset)

The Packet Byte Offset parameter specifies (in bytes) the per-packet offset for a queue. A positive number adds bytes. A negative number removes bytes. The range is -64 to +32. The default is 0.

Reserved CBS %

See the [Reserved CBS%](#) parameter in section [182.1](#).

Signalling Type

(voiceSigType)

The Signalling Type parameter sets the voice signalling type for a 7705 SAR six port E&M daughter card. The default is Type 1.

Synchronous Ethernet

(syncE)

The Synchronous Ethernet parameter specifies whether the MDA maintains synchronous Ethernet communication on all of its ports. The options are:

- True
- False (default)

Threshold High Burst Increase

(mdaEgrHsmdaThrshHighBurstIncrease)

The Threshold High Burst Increase parameter specifies the incremental number of bytes above the low burst limit to be used as the high burst threshold for the aggregate rate of the queues pertaining to the high burst threshold in the queue group. The range is -1 to 65536. The default is -1.

Threshold Low Burst Multiplier

(mdaEgrHsmdaThrshlowBurstMultiplier)

The Threshold Low Burst Multiplier parameter specifies the bytes per megabit/second of rate multiplier for the aggregate rate of the queues pertaining to the low burst threshold in the queue group. The range is -1 and 1 to 65536. The default is -1.

Use WRED Queue

(wredQueue)

The Use WRED Queue parameter specifies whether to alter the generic buffer pool association of the queue to allow queue specific WRED slopes. The options are:

- Enabled
- Disabled (default)

176 –Bundles parameters

176.1 Bundles parameters 176-2

176.1 Bundles parameters

This chapter describes the parameters for the forms and child forms launched from the right-click contextual menu options of the Bundles object.

Ack Timer

(**mlfrAckTimer**)

The Ack Timer parameter specifies the amount of time, in seconds, that the FR bundle T_ACK timer waits for a response to a message before it attempts to retransmit the message on the bundle link. The range is 1 to 10. The default is 4.

Administrative State

See the [Administrative State](#) parameter in section 182.1.

ATM Interface Cell Format

(**atmInterfaceCellFormat**)

See the [ATM Interface Cell Format](#) parameter in section 182.1.

ATM Minimum VPI Value

(**atmInterfaceMinimumVPIValue**)

The ATM Minimum VPI Value parameter specifies the minimum VPI value that can be used on the ATM interface for a VPC for the IMA group bundle. When the ATM Interface Cell Format parameter is set to UNI, the range is 0 to 255. When the ATM Interface Cell Format parameter is set to NNI, the range is 0 to 4095. The default is 0.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 182.1.

Bundle ID

(**bundleId**)

The Bundle ID parameter specifies a unique identifier for the multi-link bundle. The Bundle ID is identical for all members of a bundle. Table 176-1 describes the parameter options. The default is 0.

Table 176-1 Bundle ID parameter

Option	Supported for
1 to 8	7710 SR, on the 8 X ATM DS1/E1 CMA
1 to 10	7705 SAR, Releases 1.0 and 1.1

(1 of 2)

Option	Supported for
1 to 16	7705 SAR, Release 2.0 or later
1 to 32	7705 SAR, Release 2.1 or later on the 2 x Channelized OC3/STM1 ASAP SFP daughter card
1 to 56	7750 SR and 7710 SR, on the following MDAs: <ul style="list-style-type: none"> • 1 x OC12 Deep Channel • 4 x OC3 Deep Channel • 4 x DS3/E3 Deep Channel • 12 x DS3/E3 Deep Channel • 8 x DS1/E1 Channel CMA (7710 SR)
1 to 112	7750 SR and 7710 SR, on the 4 x Channelized DS3/E3 ASAP MDA
1 to 128	7750 SR and 7710 SR on all supported channelized ASAP MDAs
1 to 256	7750 SR and 7710 SR, on the following MDAs: <ul style="list-style-type: none"> • 4 x Channelized OC3 ASAP • 1 x Channelized OC12 ASAP • 12 x Channelized DS3/E3 ASAP
1 to 336	7710 SR and 7750 SR, on a 1 x Channelized OC12 ASAP MDA

(2 of 2)

Bundle MRRU (bytes)

(bundleMRRU)

The Bundle MRRU parameter specifies the maximum frame size that can be reconstructed from multi-link fragments. The range is 1500 to 9206. The default is 1524. Table 176-2 describes the ranges for the 7705 SAR.

Table 176-2 Bundle MRRU ranges on the 7705 SAR

Device	Range
7705 SAR, Release 1.0 or later	1500 to 1572
7705 SAR, Release 2.1	1500 to 2088

Bundle Number

(bundleNumber)

The Bundle Number parameter specifies the bundle number for the APS bundle. There is no default. Table 176-3 describes the ranges by device.

Table 176-3 Bundle number ranges

Device	APS bundle range
7710 SR	1 to 256

(1 of 2)

Device	APS bundle range
7750 SR	1 to 2000

(2 of 2)

Bundle Type

(bundleType)

The Bundle Type parameter specifies the type of multilink bundle that is created on a channelized ASAP MDA. The options are:

- IMA Group
- PPP

Class Count

(mlpppClassCount)

The Class Count parameter specifies the number of classes in a MC MLPPP bundle. The range is 0 to 4. The default is 0. When the parameter is set to 0, MC MLPPP is disabled.

Clock Source

(channelClockSource)

The Clock Source parameter specifies whether the DS3 timing source for transmitted data is the internal clock or a clock recovered from the receive data stream for the line. The options are:

- Loop Timed
- Node Timed (default)

Configured MAC

See the [Configured MAC](#) parameter in section [182.1](#).

Daughter Card CLI Name

(daughterCardDisplayedName)

The Daughter Card CLI Name parameter specifies the CLI name of the daughter card on which the APS working and protection bundle reside. Click on the Select button to list and choose a daughter card.

Description

See the [Description](#) parameter in section [182.1](#).

DDM Event Suppression

See the [DDM Event Suppression](#) parameter in section 182.1.

Encap Type

See the [Encap Type](#) parameter in section 182.1.

End Point Class ID

(mlpppEndPointIdClass)

The End Point Class ID parameter specifies the class of service that is transmitted over the MC MLPPP bundle. The options are:

- IP Address
- IEEE 802.1q (default)

End Point ID

(mlpppEndPointId)

The End Point ID parameter specifies the IPv4 address of the endpoint class in dotted-decimal format. The [End Point ID](#) parameter is configurable when the [End Point Class ID](#) parameter is set to IP Address. The default is 0.0.0.0.

Error Threshold

(dceLmiErrorThreshold)

See the [Error Threshold](#) parameter in section 182.1.

Error Threshold

(dteLmiErrorThreshold)

See the [Error Threshold](#) parameter in section 182.1.

First Network Element

(nodeIdLow)

The First Network Element parameter specifies the near-end device in the MC APS bundle.

Fragment Threshold (bytes)

(fragmentThreshold)

The Fragment Threshold (bytes) parameter specifies the maximum length of a fragment transmitted across a multi-link bundle. The range is 128 to 512. The default is 128. Setting the parameter to 0 specifies that the range for MLPPP bundles is unlimited.

Full Enquiry Interval

(**dteLmiFullEnquiryInterval**)

See the [Full Enquiry Interval](#) parameter in section 182.1.

Hello Retry Count

(**mlfrHelloRetryCount**)

The Hello Retry Count parameter specifies the number of times that the FR bundle N_RETRY counter attempts to retransmit on a bundle link before it raises an error. The range is 1 to 5. The default is 2.

Hello Timer

(**mlfrHelloTimer**)

The Hello Timer parameter specifies how often, in seconds, the FR bundle T_HELLO timer sends a HELLO message. The FR bundle also uses the parameter value to delay the retransmission of an ADD_LINK message when it receives an unexpected response to the message. The range is 1 to 180. The default is 10.

IMA Version

(**imaVersion**)

The IMA Version parameter specifies the ATM Forum IMA Specification Version that is used in the multilink IMA group bundle. The options are:

- 1.1 (default)
- 1.0

Link Activation Timer

(**linkActivationTimer**)

The Link Activation Timer parameter specifies how much time, in milliseconds, is needed for a member link of an IMA group to stabilize after an alarm is raised, before the member link is re-activated. The range is 1 to 30 000. The default is 10 000.

Link Deactivation Timer

(**linkDeactivationTimer**)

The Link Deactivation Timer parameter specifies how much time, in milliseconds, must elapse before a member link of an IMA group is deactivated after an alarm is raised. The range is 1 to 30 000. The default is 2000.

Link Fragmentation and Interleaving

(bundleLFI)

The Link Fragmentation and Interleaving parameter specifies LFI on the multilink bundle. LFI interleaves high-priority traffic within a stream of fragmented lower-priority traffic. LFI helps avoid excessive delays to high-priority, delay-sensitive traffic over a low-speed link. The options are:

- Enabled
- Disabled (default)

You are not required to use all timeslots when you configure a multilink bundle with LFI. There is a restriction of one member for a multilink bundle with LFI. Multilink bundles without LFI support up to 8 members.

LMI Mode

(mode)

See the [LMI Mode](#) parameter in section 182.1.

LMI Type

(frDlcmiState)

See the [LMI Type](#) parameter in section 182.1.

Magic Number

(mlpppMagicNumber)

The Magic Number parameter specifies whether a bundle detects a loopback scenario on member links and takes looped back member links out of service. The options are:

- Enabled
- Disabled (default)

The parameter is supported only on channelized 7750 SR ASAP MDAs.

Maximum Links

(maximumLinks)

The Maximum Links parameter specifies the maximum number of links that is used to determine the maximum configurable bandwidth for the IMA group. The range is 1 to 8. The default is 8.

The following formula determines the maximum configurable ATM bandwidth:

$$(\text{number of links}) \times (M-1)/M \times (2048/2049) \times \text{primary member link speed}$$

where

M is the IMA frame size

primary member link speed is either E1 (1920 kbps) or DS1 (1539 kbps); E1 is used for an IMA group that has no members

MCFR Egress Qos Profile

(frf12EgressQOSProfPointer)

See the [MCFR Egress QoS Profile](#) parameter in section [182.1](#).

MCFR Ingress Qos Profile

(mlfrIngressQOSProfPointer)

The MCFR Ingress QoS Profile specifies the profile to be used by an FRF.12 link with UNI/NNI fragmentation enabled. Click on the Select button to choose a profile from the list of MCFR ingress QoS profiles.

Minimum Links

(minimumLinks)

The Minimum Links parameter specifies the minimum number of links that must be active in order for a multilink bundle to be active. If the number of active links drop below the value specified by this parameter, the bundle becomes operationally down. The range is 1 to 8. The default is 1.

Monitored Events

(dceLmiMonitoredEvents)

See the [Monitored Events](#) parameter in section [182.1](#).

Monitored Events

(dteLmiMonitoredEvents)

See the [Monitored Events](#) parameter in section [182.1](#).

MTU

(bytes)

See the [MTU \(bytes\)](#) parameter in section [182.1](#).

Polling Interval (seconds)

(dceLmiPollingInterval)

See the [Polling Interval \(seconds\)](#) parameter in section 182.1.

Polling Interval (seconds)

(dteLmiPollingInterval)

See the [Polling Interval \(seconds\)](#) parameter in section 182.1.

Protection Type

(bundleProtectedType)

The Protection Type parameter specifies the multi-link bundle is a working or protection channel. The options are:

- Working (default)
- Protecting

Red Diff Delay (milliseconds)

(redDiffDelay)

The Red Diff Delay (milliseconds) parameter specifies the maximum acceptable differential delay for individual circuits within a multi-link bundle. If the differential delay exceeds the value set by this parameter, a BundleRedDiffExceeded alarms is raised. For PPP bundles, the range is 0 to 25. For IMA bundles, the range is 0 to 50. The default is 0.

For IMA bundles on the 16-port DS1/E1 daughter card on the 7705 SAR, Release 2.0 or earlier, the range is 0 to 75. For IMA bundles on the 16-port DS1/E1 daughter card on the 7705 SAR, Release 2.1 or later, the range is 2 to 50. For IMA bundles on the 7705 SAR 2-port channelized OC3/STM1 daughter card, the range is 2 to 50.

Red Diff Delay Action

(redDiffDelayAction)

The Red Diff Delay Action parameter specifies the action taken if the differential delay exceeds the threshold configured in the Red Diff Delay (milliseconds) parameter. Table 176-4 lists the parameter options.

Table 176-4 Red Diff Delay Action parameter

Option	Option description	Dependencies
None (default)	Specifies that no action is taken.	—
Down	Specifies that the bundle be put into an operationally down state.	

Second Network Element

(nodeIdHigh)

The Second Network Element parameter specifies the far-end device in the MC APS bundle.

Short Sequence

(shortSequence)

The Short Sequence parameter specifies that the multilink bundle should use short sequence (12 bit) numbers instead of the standard long sequence (24 bits) number. The options are:

- Enabled
- Disabled (default)

Show Only Compatible Channels

The Show Only Compatible Channels parameter specifies whether to filter the list of channels presented, by determining whether the channels can be configured as members of a multilink bundle. The options are:

- Enabled (default)
- Disabled

Test Member

(testMember)

The Test Member parameter specifies the IMA group member link that is used to verify link connectivity for the IMA group bundle. Click on the Select button to list and choose an IMA group member.

Test Pattern

(testPattern)

The Test Pattern parameter specifies the transmit test pattern in an IMA group loopback operation. The range is 0 to 255. The default is 0.

Time Slots

See the [Time Slots](#) parameter in section [182.1](#).

Yellow Diff Delay (milliseconds)

(yellowDiffDelay)

The Yellow Diff Delay (milliseconds) parameter specifies the yellow warning threshold for the differential delay for the circuits within a multilink bundle. If the differential delay exceeds the value configured for this parameter, a BundleYellowDiffExceeded alarm is raised. The range is 0 to 25. The default is 0.

177 –Port parameters

177.1 Port parameters 177-2

177.1 Port parameters

This chapter describes the parameters on the Port property form, and the child forms launched from the right-click contextual menu options for ports.

This chapter also describes the parameters on the APS Group property form, and child forms, launched from the right-click contextual menu options for APS groups.

Accounting Enabled

See the [Accounting Enabled](#) parameter in section [182.1](#).

Activation

(activation)

This parameter specifies the loopback status of a 9500 MPR DS1, ES1 or Radio port. The options are:

- Not Active (default)
- Active

Administrative State

Table [177-1](#) lists where to find information about the Administrative State parameter.

Table 177-1 Administrative State

Parameter	See
Administrative State for a port	Administrative State parameter in section 182.1
Administrative State for 802.3ah EFM OAM	Administrative State parameter in this section

Administrative State

(dot3OamAdminState)

The Administrative State parameter specifies the administrative state of the 802.3ah protocol on the selected port. The parameter is configurable when the [Tunneling](#) parameter is disabled. The options are:

- Disabled (default)
- Enabled

When the Administrative State parameter is set to Enabled and the Operational Status is Operational, the Peer Information panel appears on the 802.3ah form.

Administrative Status

(portCfgAdminStatus)

The Administrative Status parameter specifies the LLDP PDU transmission and reception characteristics for the port. Table 177-2 lists the parameter options.

Table 177-2 Administrative Status parameter

Option	Option description	Dependencies
Tx Only	Transmission of local LLDP information only is enabled.	—
Rx Only	Reception of remote LLDP information only is enabled.	—
Tx and Rx	Both transmission and reception of LLDP information are enabled.	Default for the OmniSwitch
Disabled	Both transmission and reception of LLDP information are disabled.	Default for non-OmniSwitch NEs

Advertised Capability

(addressedCapability)

The Advertised Capability parameter specifies the capabilities that a 9500 MPR Ethernet port advertises to other NEs. You can select the check box beside each capability to be advertised. By default, all capabilities are disabled. Table 177-3 describes the options.

Table 177-3 Advertised Capability parameter

Option	Dependencies
100 Mb/s - Full-Duplex	When the Auto-Negotiate parameter is set to true, one or more modes can be selected at the same time. When the Auto-Negotiate parameter is set to false, only one mode at a time can be selected and 1000 Mb/s - Full-Duplex is not supported.
100 Mb/s - Half-Duplex	
10 Mb/s - Full-Duplex	
10 Mb/s - Half-Duplex	
1000 Mb/s - Full-Duplex	
Flow Control	Cannot be selected unless at least one full duplex mode is selected

Aggregate Rate Limit (kbps)

(egressAggRateLimit)

The Aggregate Rate Limit (kbps) parameter specifies the maximum total rate of all egress queues for the access interface. You must select the Assign Aggregate Rate Limit check box before you configure the Aggregate Rate Limit (kbps) parameter. When the parameter is set to a value greater than 0, you cannot specify an egress scheduler. When you specify -1, the rate is unlimited or 1 to 40 000 000.

AIS Signal Type

(mprSignalType)

The Alarm Indication Signal Type parameter for the 2-port DS3 card on the 9500 MPR ANSI is configurable at the port level. The options are:

- allOnes (default)
- blueSignal

Applicant Mode

(applicantMode)

The Applicant Mode parameter specifies the applicant mode of an MVRP configuration on an OmniSwitch port. The options are:

- Participant
- Non-participant
- Active (default)

Async Mapping

(asyncMapping)

The Async Mapping parameter specifies whether the port supports asynchronous mapping of the payload inside the OTU. The options are:

- enabled
- disabled (default)

Authenticate

(mobilePortAuthenticate)

The Authenticate parameter specifies whether authentication is active on a mobile port. The parameter is configurable when the [Enable Port Mobility](#) parameter is set to Enable. When this Authenticate parameter is enabled on a mobile port, the port participates in a Layer 2 authentication process that restricts switch access at the VLAN level. The options are:

- Enable Auth VLAN
- Not Applicable
- Disable (default)
- Enable 802.1x

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section [182.1](#).

Automatic VLAN Binding

(vlanAutoBind)

The Automatic VLAN Binding parameter specifies whether an L2 network interface is created on a network port. The L2 network interface is bound to VLAN services on the switch. The options are:

- Enabled (default)
- Disabled

Table [177-4](#) describes the behavior of network ports for Standard and Stacked VLANs.

Table 177-4 Automatic VLAN Binding parameter

Type of VLAN	Behavior	General
Standard	The 5620 SAM cannot identify network ports that can be used for Standard VLAN network interfaces. Configure the network ports that you need to use before configuring Standard VLANs. Network ports that have the Automatic VLAN Binding parameter enabled can be identified by the 5620 SAM for use by Standard VLANs.	All network ports with the Automatic VLAN Binding parameter enabled are used as network ports for all VLANs.
Stacked	The 5620 SAM can identify network ports that can be used for Stacked VLAN network interfaces. Although it is not necessary to enable the Automatic VLAN Binding parameter on network ports in order for the 5620 SAM to identify the port for use by Stacked VLANs, it is recommended. When you switch an access port to a network port and the Automatic VLAN Binding parameter is enabled, a VLAN binding is automatically created between the port and all of the Stacked VLANs on the switch.	If you do not need a network port to be used by VLANs, disable the Automatic VLAN Binding parameter. If you need to add a network port to a network LAG, disable the Automatic VLAN Binding parameter.

Auto-negotiate

(autoNegotiate)

The Auto-negotiate parameter specifies whether to automatically negotiate the Speed and Duplex parameters. Table [177-5](#) lists the parameter options.

Table 177-5 Auto-negotiate parameter

Option	Option description
True	The link Speed and Duplex parameters are automatically negotiated with the far-end link or port. All speed and duplex information is advertised.
False (default value, except for OmniSwitch ports)	The Speed and Duplex parameter values for the link are used, based on the Speed and Duplex parameter settings.

(1 of 2)

Option	Option description
Limited	The current Speed and Duplex parameter settings are advertised, and the parameters are negotiated with the far-end link. This option is not supported for the 9500 MPR.

(2 of 2)

Backpressure

(backpressure)

The Backpressure parameter specifies whether backpressure is used. The parameter setting applies only when the Duplex parameter is set to Half Duplex. The options are:

- Disabled (default)
- Enabled

BER Signal Degradation Threshold

(bitErrorRateSdThreshold)

The BER Signal Degradation Threshold parameter specifies the threshold for the line signal degradation BER. The line signal (b2) interleaved parity BER is continuously measured. If the BER exceeds the degradation threshold, an alarm is raised. The range is 3 to 9. The default is 6.

BER Signal Failure Threshold

(bitErrorRateSfThreshold)

The BER Signal Failure Threshold parameter specifies the threshold for line signal failures. The line signal (b2) interleaved parity BER is continuously measured. If the BER exceeds the failure threshold, an alarm is raised and the link is set to operationally down. The range is 3 to 6. The default is 3.

Bind Type

(bindType)

An ERP type NNI-SVLAN binding should be created before establishing an ERP ring on that SVLANNNI Binding.

A VLAN Stacking Network Interface (NNI) can participate in an ERP ring. However, an NNI is created through an association of a port with an SVLAN. Both STP and ERP cannot control the same VLAN-port association (VPA). By default, the NNI to SVLAN association is controlled by STP.

To include an NNI in an ERP ring, specify ERP control at the time the NNI association is configured. This is done using the `erp` parameter of the `ethernet-service vlan nni` command. For example:

```
ethernet-service vlan 1001 nni 1/1 erp
```

```
ethernet-service svlan 1001 nni 1/2 erp
```

The above commands configure ports 1/1 and 1/2 as NNI ports for SVLAN 1001 with ERP control over the VPA. Note that the SVLAN specified must already exist in the switch configuration. The options are:

- STP (default)
- ERP

Broadcast Limit (kbps)

(broadcastLimit)

The Broadcast Limit (kbps) parameter specifies the received broadcast traffic limit. Limiting broadcast and multicast traffic helps to protect the switch from massive amounts of traffic. The range is -1 to 102 400. A value of -1 specifies that there is no broadcast limit. A value of 0 specifies that all broadcast traffic is blocked.

Broadcast Limit (Pkts/s)

(broadcastLimitInPkt)

The Broadcast Limit (Pkts/s) parameter specifies the received broadcast and multicast traffic limit. Limiting broadcast and multicast traffic helps to protect the switch from massive amounts of traffic. The range is -1, or 0 to 262 143. A value of -1 specifies that there is no broadcast limit. A value of 0 specifies that all broadcast and multicast packets are blocked.

Cable Length

(cableLength)

The Cable Length parameter specifies the cable length for the T1 or E1 line that is connected to the port. Table 177-6 lists the parameter options.

Table 177-6 Cable Length parameter

Option	Description	Dependencies
Cable length 0..133ft (Short) (default)	The cable length is between 0 and 133 ft.	The Mode parameter for the CES module is set to E1.
120 ohm high return loss on E1	Specifies a termination impedance of 120 ohms at high return loss on the E1 line	The Mode parameter for the CES module is set to E1.
120 ohm normal return loss on E1	Specifies a termination impedance of 120 ohms at normal return loss on the E1 line	The Mode parameter for the CES module is set to E1.
75 ohm high return loss on E1	Specifies a termination impedance of 75 ohms at high return loss on the E1 line	The Mode parameter for the CES module is set to E1.
75 ohm normal return loss on E1	Specifies a termination impedance of 75 ohms at normal return loss on the E1 line	The Mode parameter for the CES module is set to E1.
Rx gain 20 dB, Tx attenuation -7.5 dB (Long)	Specifies a receive gain of 20 dB and a -7.5 dB transmit attenuation	The Mode parameter for the CES module is set to T1.

(1 of 2)

Option	Description	Dependencies
Rx gain 20 dB, Tx attenuation -15 dB (Long)	Specifies a receive gain of 20 dB and a -15 dB transmit attenuation	The Mode parameter for the CES module is set to T1.
Rx gain 20 dB, Tx attenuation -22.5 dB (Long)	Specifies a receive gain of 20 dB and a -22.5 dB transmit attenuation	The Mode parameter for the CES module is set to T1.
Rx gain 26 dB, Tx attenuation -7.5 dB (Long)	Specifies a receive gain of 26 dB and a -7.5 dB transmit attenuation	The Mode parameter for the CES module is set to T1.
Rx gain 26 dB, Tx attenuation -15 dB (Long)	Specifies a receive gain of 26 dB and a -15 dB transmit attenuation	The Mode parameter for the CES module is set to T1.
Rx gain 26 dB, Tx attenuation -22.5 dB (Long)	Specifies a receive gain of 26 dB and a -22.5 dB transmit attenuation	The Mode parameter for the CES module is set to T1.
Rx gain 32 dB, Tx attenuation -7.5 dB (Long)	Specifies a receive gain of 32 dB and a -7.5 dB transmit attenuation	The Mode parameter for the CES module is set to T1.
Rx gain 32 dB, Tx attenuation -15 dB (Long)	Specifies a receive gain of 32 dB and a -15 dB transmit attenuation	The Mode parameter for the CES module is set to T1.
Rx gain 32 dB, Tx attenuation -22.5 dB (Long)	Specifies a receive gain of 32 dB and a -22.5 dB transmit attenuation	The Mode parameter for the CES module is set to T1.

(2 of 2)

CFM LoopBack Mode

(cfmlbMode)

The CFM LoopBack Mode parameter specifies the priority level of CFM loopback reply messages for an Ethernet port. Table 177-7 lists the parameter options.

Table 177-7 CFM LoopBack Mode parameter

Option	Description
Disabled (default)	CFM loopback message processing is not enabled on the port.
Priority-Low	CFM loopback reply messages have low priority.
Priority-High	CFM loopback reply messages have high priority.

The CFM LoopBack Mode parameter is configurable only on 7705 SAR (version 4.0 R1 or later) daughter cards. The parameter can only be configured on one port per daughter card. The parameter can be configured on ports in Access or Network mode.

Channel

(dwdmChannel)

The Channel parameter allows the user to “tune” or configure/select at which wavelength frequency the transponder transmits. The ITU channel values are 17 to 61 in unit increments, and 175 to 605, in increments of 10. The default is 0. The wavelength can be modified without resetting the MDA. Table 177-8 lists the configurable wavelengths.

Table 177-8 “Tunable” DWDM Wavelengths

C- Band					
100 Ghz Grid			50 GHz Grid		
nm	THz	ITU channel	nm	THz	ITU channel
1528.77	196.10	61	1529.16	196.05	605
1529.55	196.00	60	1529.94	195.95	595
1530.33	195.90	59	1530.72	195.85	585
1531.12	195.80	58	1531.51	195.75	575
1531.90	195.70	57	1532.29	195.65	565
1532.68	195.60	56	1533.07	195.55	555
1533.47	195.50	55	1533.86	195.45	545
1534.25	195.40	54	1534.64	195.35	535
1535.04	195.30	53	1535.43	195.25	525
1535.82	195.20	52	1536.22	195.15	515
1536.61	195.10	51	1537.00	195.05	505
1537.40	195.00	50	1537.79	194.95	495
1538.19	194.90	49	1538.58	194.85	485
1538.98	194.80	48	1539.37	194.75	475
1539.77	194.70	47	1540.16	194.65	465
1540.56	194.60	46	1540.95	194.55	455
1541.35	194.50	45	1541.75	194.45	445
1542.14	194.40	44	1542.54	194.35	435
1542.94	194.30	43	1543.33	194.25	425
1543.73	194.20	42	1544.13	194.15	415
1544.53	194.10	41	1544.92	194.05	405
1545.32	194.00	40	1545.72	193.95	395
1546.12	193.90	39	1546.52	193.85	385
1546.92	193.80	38	1547.32	193.75	375
1547.72	193.70	37	1548.11	193.65	365
1548.51	193.60	36	1548.91	193.55	355
1549.32	193.50	35	1549.72	193.45	345
1550.12	193.40	34	1550.52	193.35	335
1550.92	193.30	33	1551.32	193.25	325
1551.72	193.20	32	1552.12	193.15	315
1552.52	193.10	31	1552.93	193.05	305
1553.33	193.00	30	1553.73	192.95	295
1554.13	192.90	29	1554.54	192.85	285

(1 of 2)

C- Band					
100 Ghz Grid			50 GHz Grid		
nm	THz	ITU channel	nm	THz	ITU channel
1554.94	192.80	28	1555.34	192.75	275
1555.75	192.70	27	1556.15	192.65	265
1556.55	192.60	26	1556.96	192.55	255
1557.36	192.50	25	1557.77	192.45	245
1558.17	192.40	24	1558.58	192.35	235
1558.98	192.30	23	1559.39	192.25	225
1559.79	192.20	22	1560.20	192.15	215
1560.61	192.10	21	1561.01	192.05	205
1561.42	192.00	20	1561.83	191.95	195
1562.23	191.90	19	1562.64	191.85	185
1563.05	191.80	18	1563.45	191.75	175
1563.86	191.70	17			

(2 of 2)

Channel Number

(channelNumber)

The Channel Number parameter indicates the channel number for an APS channel in an APS group. Table 177-9 lists the parameter options.

Table 177-9 Channel Number parameter

Option	Description
1	Specifies the APS working channel
0	Specifies the APS protection channel

Clock Source

(clockSource)

The Clock Source parameter specifies whether the timing source for transmitted data is the internal clock (node timed), a clock recovered from the receive data stream for the line (loop timed), or the internal clock on a 7705 SAR daughter card (free run). Table 177-10 lists the parameter options.

Table 177-10 Clock Source parameter

For	Options
OC-192	Loop Timed (default) Node Timed
OC-48	
1 X 10-Gig with the XGig Mode parameter configured for WAN	
8-port Channelized DS1/E1 CMA	
4-port DS3/E3 CMA	
8-port 10/100TX Ethernet CMA	
1-port GIGE CMA	
2-port OC-3/12c/STM1/4 CMA-SFP	
8-port T1/E1 ATM CMA	
1-port Channelized OC-3/STM-1 CES CMA	
1-port GIGE CMA-XP SFP	
5-port GIGE CMA-XP SFP	
Channelized OC-12	
Channelized OC-12	
Channelized DS3	
OC-12	Node Timed
OC-3	
DS3 channel on the 2-port OC3/STM1 channelized ASAP SFP daughter card (7705 SAR, Release 2.1 or later)	Loop Timed (default) Free Run

Collect Accounting Statistics

(accountingOn)

The Collect Accounting Statistics parameter specifies whether the collection of accounting statistics on the port is enabled. The options are:

- Enabled (default)
- Disabled

Commands

See the “[Commands](#)”, “[Commands](#)”, and “[Commands](#)” parameters in chapter [182](#).

Configured Alarms

The Configured Alarms parameter specifies the alarms that are monitored by the interface. Table [177-11](#) lists the configurable OTU alarms.

Table 177-11 Configured Alarms (cfgAlarms): OTU Alarms

Configurable OTU Alarms	
OTU Backward Defect Indication	OTU Bit Error Rate Signal Degrade
OTU Bit Error Rate Signal Fail	OTU Alarm Indication Signal
Loss of Multi-frame	Loss of OTU Framing
Loss of Signal	Loss of Clock
ODU Alarm Indication Signal	Uncorrectable FEC errors
FEC Rx/Tx Mode Mismatch	FEC Signal Degrade
FEC Signal Failure	OTU Backward Incoming Alignment Error
OTU Incoming Alignment Error	OTU Trace ID Mismatch
PM Trace ID Mismatch	OPU PSI Payload Type Mismatch
OPU PSI Trace Mismatch	PM Backward Defect Indication
ODU Locked	ODU Open Connection Indication

Table 177-12 lists the configurable Wave Tracker alarms.

Table 177-12 Configured Alarms (cfgAlarms): Wave Tracker Alarms

Configurable Wave Tracker Alarms	
Power Control Low limit reached	Power Control High limit reached
Power Control Degrade	Power Control Failure
Encoder Degrade	Encoder Failure

Table 177-13 lists the configurable Optical Amplifier alarms.

Table 177-13 Configured Alarms (ampcfgAlarms): Optical Amplifier Alarms

Configurable Optical Amplifier Alarms	
Amplifier Module communication failure	Amplifier Loss of output power
Amplifier Loss of input optical power	Amplifier Module Case temperature low
Amplifier Module Case temperature high	Amplifier Pump temperature
Amplifier Pump over-current	—

Table 177-14 lists the configurable Optical Tunable Dispersion Compensation Module alarms.

Table 177-14 Configured Alarms (tdcmcfgAlarms): Optical Tunable Dispersion Compensation Module Alarms

Configurable Optical Tunable Dispersion Compensation Module Alarms	
Tdcm module communication failure	Tdcm EEPROM invalid
Tdcm thermal control temperature limit	Tdcm thermal control unlocked
Tdcm module temperature low	Tdcm module temperature high
Tdcm not ready	—

Configured Data Rate (Gb/s)

(lanDataRate)

The Configured Data Rate parameter specifies the data rate to use when configuring the port for an OTU encapsulated 10GE-LAN signal. The values are 11.049 Gb/s, which configures the port to transmit and receive an 11.049 Gb/s synchronous signal (with no fixed stuffing bytes in the frame), and 11.096 Gb/s which configures the port to transmit and receive an 11.096 Gb/s signal (with fixed stuffing bytes in the frame). The default value is 11.049 Gb/s.

Configured MAC

See the [Configured MAC](#) parameter in section [182.1](#).

Control Mode

(algorithmMode)

The Control Mode parameter specifies the dispersion algorithm mode used for the port. The options are:

- Automatic (default)
- Manual

Controlled Port Control

(paeAuthControlledPortControl)

The Controlled Port Control parameter specifies the control values for the type of 802.1X authentication for the port. The options are:

- Force Unauthorized
- Auto
- Force Authorized (default)

Critical Event Notify

(dot3OamCriticalEventEnable)

The Critical Event Notify parameter, if the value is set to true, specifies that the local OAM entity should attempt to indicate a critical event via the OAMPDU flags to its peer OAM entity when a critical event occurs. The options are:

- True (default)
- False

Db Loss

(dbLoss)

The Db Loss parameter specifies the number of decibels the transmission signal decreases over time. This parameter is configurable when the [Line Buildout](#) parameter is set to Long on a DS1 interface. The options are:

- 0 dB (default)
- -7.5 dB
- -15.0 dB
- -22.5 dB

DDM Event Suppression

(ddmEventSuppression)

The DDM Event Suppression parameter specifies whether the NE is blocked from sending DDM-specific notifications to the 5620 SAM when digital diagnostics monitoring thresholds are exceeded on ports on SFP and XFP optical modular transceivers. The thresholds for SFPs and XFPs are programmed by the transceiver manufacturer. The options are:

- Enabled
- Disabled (default)

Default 802.1p

(qosPortDefault8021p)

The Default 802.1p parameter specifies the default 802.1p value that is inserted into packets received on untrusted ports. The range is 0 to 7. The default is 0.

Default Classification

(qosPortDefaultClassification)

The Default Classification parameter specifies the type of packet that is used to classify traffic on the port. The options are:

- b802.1p
- TOS (default)
- DSCP

Default DSCP

(qosPortDefaultDSCP)

The Default DSCP parameter specifies the default DSCP value that is inserted in packets received on untrusted ports. The range 0 to 63. The default is 0.

Default VLAN Enable

(defaultVlanEnable)

The Default VLAN Enable parameter specifies whether a mobile port forwards or drops the configured default VLAN traffic that does not match any VLAN rules. The parameter is configurable when the [Enable Port Mobility](#) parameter is set to Enable. When the parameter is enabled, non-matching traffic is carried on the configured default VLAN for the port. When the parameter is disabled, non-matching traffic is dropped. The options are:

- Enable
- Disable
- Not Applicable (default)

Default VLAN Restore

(defaultVlanRestore)

The Default VLAN Restore parameter specifies whether a mobile port retains or drops a dynamic VPA when the traffic on the port that triggered the VLAN assignment ages out. When the parameter is enabled, the VPA is dropped. When the parameter is disabled, the VPA is retained. The parameter is configurable when the [Enable Port Mobility](#) parameter is set to Enable. The options are:

- Enable
- Disable
- Not Applicable (default)

Description

See the [Description](#) parameter in section [182.1](#).

Destination MAC Address

(destMACAddress)

This parameter specifies the destination MAC address of the test frames of an advanced loopback test on an OmniSwitch port. Specify a unicast MAC address in the form xx-xx-xx-xx-xx-xx.

Destination String

(destString)

The Destination String parameter specifies the intermediate destination id to be used for matching subscribers hosts with a virtual port. The range is a string of up to 32 characters. There is no default.

Detect Remote Faults

(remoteFaultDetection)

The Detect Remote Faults parameter specifies whether remote fault detection is enabled on the port. When remote fault detection is enabled, the local device indicates link down on the port if the remote peer device detects link down. The options are:

- Disabled (default)
- Enabled

Detection

(mdiMdxCrossoverDetection)

The Detection parameter specifies the type of crossover detection for the port. When the parameter is set to Auto, you can interconnect any combination of MDI/MDIX ports using either a crossover or straight-through type of cable without distinction. The options are:

- Auto (default)
- MDI
- MDIX

Dispersion

(dispersion)

The Dispersion parameter specifies the dispersion rate (in ps/nm) of the tunable dispersion compensation module. The range is –1200 to 1200. The default is 0.

Dot1 Q Acceptable Frames

(dot1qAcceptableFrameTypes)

The Dot1 Q Acceptable Frames parameter specifies whether an OmniSwitch Ethernet port should accept all traffic (tagged and untagged) or only tagged traffic. The options are:

- Admit All (default)
- Only VLAN Tagged

Dot1 Q Ethertype

(dot1qEtype)

The Dot1 Q Ethertype parameter specifies the Ethertype expected when the Encap Type parameter is set to Dot1 Q. The range is 1536 to 65 535. The default is 33 024.

Down When Looped

(downWhenLooped)

The Down When Looped parameter specifies whether physical loop detection for the Ethernet port is enabled or disabled. When enabled, the port periodically sends out keep-alive PDUs with an EtherType of 0x9000. If the port receives a keep-alive that it transmitted, then the port's State (on the States tab) is set to Link Down, if it was previously up. The port is not move back to the Link Up state for a period of time, as defined by the [Retry Timeout \(Sec\)](#) parameter. Instead, it continues to periodically send out keep-alive PDUs. Every time the port receives a keep-alive PDU it sent while a loop has been detected, it resets the time period that it remains down, as defined by the [Retry Timeout \(Sec\)](#) parameter.

The options are:

- Disabled (default)
- Enabled

Duplex

(duplex)

The Duplex parameter specifies the duplex communication type for an Ethernet port. Table [177-15](#) describes the parameter options.

Table 177-15 Duplex parameter

Option	Description	Dependencies
Full Duplex (default)	Specifies that both ends of the communication link can send and receive signals at the same time	Cannot choose this option if the Auto-negotiate parameter is set to enabled. The Ethernet port must support multiple duplex modes. OmniSwitch 1 Gigabit and 10 Gigabit fiber ports only support full duplex.
Half Duplex	Specifies that the signals on the communication link can only flow in one direction at a time	
Auto	Specifies that the switch advertises all available duplex modes during auto-negotiation	This mode is available only on the OmniSwitch. This is the default mode for copper Ethernet ports.

Dying Gasp Notify

(dot3OamDyingGaspEnable)

This parameter specifies whether or not the specified port or range of ports will propagate local event notifications to the remote peer. The options are:

- True (default)
- False



Note 1 – To see this alarm in the 5620 SAM, the NE must be managed with a "public" community string, since this alarm has a pre-defined community string of "public".

Note 2 – If the Backup/Primary power supply fails, a major alarm will be raised. This alarm will be sent only to the first two SNMP stations or management system configured on the switch.

The "Loopback0" address should not be used for the source IP address field for the NE.

Egress Max-Burst

(egressMaxBurst)

The Egress Max-Burst parameter specifies the rate at which traffic leaves the network. The range is 32 to 16 384. The default is –1. You can only configure this parameter when the [Egress Rate \(Kbps\)](#) parameter is set to a value other than –1.

Egress Percentage of Rate (%)

(mdaEgrNamedPoolPolicy)

The Egress Percentage of Rate (%) parameter defines a percentage value that changes the amount of buffers used by an egress port. Changing the port's active bandwidth artificially lowers or increases the buffers managed by one egress port and gives them to other egress ports on the same MDA. This parameter does not change the actual bandwidth available on the port. The egress Percentage of Rate value is multiplied by the egress active bandwidth of the port. For example an Egress Percentage of Rate value of 150% results in an increased value of 50% (1.5 x rate). A value of 50% causes the active bandwidth to be reduced by 50%. A value of 100 restores the egress active rate to a normal value. The range is 1 to 1000. The default is 100.

Egress Percentage of Rate (%)

(portEgrPoolPercentageRate)

The Egress Percentage of Rate (%) parameter specifies the port buffer allocation rate that limits the active bandwidth for the egress port. The range is 0 to 1000. The default is 100.

Egress Rate (Kbps)

(egressRate)

The Egress Rate (Kbps) parameter specifies the maximum rate of traffic that can leave the port. The range varies depending on the NE type. A value of –1 indicates that the limit on the egress rate is the full physical limit of the port.

Egress Scheduler Mode

(egressSchedulerMode)

The Egress Scheduler Mode parameter specifies the egress scheduler mode for network and access ports. The options for a network port are:

- Profile (default)
- Four-Priority

The Egress Scheduler Mode parameter for network ports is only configurable on the 7705 SAR, Release 3.0 or later.

The Egress Scheduler Mode parameter for access ports is only configurable on the 7210 SAS-X, Release 3.0 R3 or later. The options for an access port are:

- FC based (default)
- SAP based

Enable Multicast Limit Mode

(enableMulticastLimitMode)

The Enable Multicast Limit Mode parameter specifies whether the maximum flood rate for multicast traffic is allowed on an OmniSwitch Ethernet port. The options are:

- True
- False (default)

Enable Port Mobility

(enablePortMobility)

The Enable Port Mobility parameter specifies whether the mobile status of an OmniSwitch Ethernet port is enabled. When the parameter is enabled, the port is eligible for dynamic VLAN assignment. The options are:

- true
- false (default)

Encap Type

See the [Encap Type](#) parameter in section [182.1](#).

Errored Frame Window (dsec)

(dot3OamErrFrameWindow)

The Errored Frame Window parameter specifies the amount of time (in 100ms increments) over which the threshold is defined. The range is 10 to 600. The default is 10.

Errored Frame Period Window (frames)

(dot3OamErrFramePeriodWindow)

The Errored Frame Period Window parameter specifies the number of frames over which the threshold is defined. The default value of the window is the number of minimum size Ethernet frames that can be received over the physical layer in one second. The range is 20000 to 1200000000. The default is 20000.

Errored Frame Seconds Summary Window (dsec)

(dot3OamErrFrameSecsSummaryWindow)

The Errored Frame Seconds Summary Window parameter specifies the amount of time (in 100 ms intervals) over which the threshold is defined. The range is 100 to 9000. The default is 600.

Ethernet Down Reason

A read-only Ethernet Down Reason parameter on the port configuration form indicates that the two ports are down because of the No Service Port. The No Service Port applies only to BOF which is configured using CLI. The 7210 SAS-Mx (24SFP 2x10GXFP) node is unable to support all ports when the 2x10G MDA is equipped. Two ports have to be dedicated as No Service Ports. By default the node will assume two ports as No Service Ports. The check-box is read-only.

Expected Payload Type (hex)

(psiPayloadTypeExp)

The Expected Payload Type (hex) parameter specifies the expected received payload type value of the PSI of the OPU overhead. The value is a two-character hexadecimal number. The default is 00.

Expected Rx Bytes

The Expected Rx Bytes parameters specify the expected type of receiver (Rx) Trail Trace Identifier (TTI) in the OTU. The parameters appear only when the [Expected Rx Mode](#) parameter is set to Bytes.

The value is a hexadecimal number. Table [177-16](#) lists the Expected Rx Bytes parameters.

Table 177-16 Expected Rx Bytes parameters

Parameter	Specifies the TTI for
Expected Rx Bytes (pmTtiExp)	PM
Expected Rx Bytes (smTtiExp)	SM
Expected Rx Bytes (psiTtiExp)	PSI

Expected Rx Mode

The Expected Rx Mode parameters specify the expected type of TTI in the OTU overhead. Table 177-17 lists the Expected Rx Mode parameters.

Table 177-17 Expected Rx Mode parameters

Parameter	Specifies the TTI for	Options
Expected Rx Mode (pmTtiExpMode)	PM	<ul style="list-style-type: none"> Auto (default) String Bytes
Expected Rx Mode (smTtiExpMode)	SM	
Expected Rx Mode (psiTtiExpMode)	PSI	

Expected Rx String

The Expected Rx String parameters specify the expected receiver (Rx) TTI in the OTU overhead. The parameters are only configurable when the [Expected Rx Mode](#) parameter is set to String.

The value is 0 to 192 bytes. Table 177-18 lists the Expected Rx String parameters.

Table 177-18 Expected Rx String parameters

Parameter	Specifies the TTI for
Expected Rx String (pmTtiExp)	PM
Expected Rx String (smTtiExp)	SM
Expected Rx String (psiTtiExp)	PSI

The auto-populated default sequence is the name of the NE, the IOM number, the MDA slot number, the port number, and the DWDM channel number.

First Network Element

(nodeIdLow)

The First Network Element parameter specifies the near-end device in the MC APS group.

FEC Mode

(fecMode)

This parameter specifies whether to enable the FEC encoder/decoder and which encoder/decoder mode to use when enabled. The options are:

- Disabled
- G.709
- Enhanced (default)

Flow

(flowControl)

The Flow parameter specifies the flow control mode for the port. Table 177-19 lists the parameter options.

Table 177-19 Flow parameter

Option	Description
Disabled (default)	Specifies that flow control for the port is disabled
Enabled	Specifies that flow control for the port is enabled
Auto-negotiate	Specifies that the flow control is enabled only if it is in use at the far end

Forbid IGMP Snooping

(forbidIgmpSnooping)

The Forbid IGMP Snooping parameter specifies whether IGMP snooping occurs on the current port. The options are:

- Disabled (default)
- Enabled

Forward All Multicast Traffic

(forwardAllMulticast)

The Forward All Multicast Traffic parameter specifies whether all multicast traffic is forwarded to the current port. The options are:

- Disabled (default)
- Enabled

Frame-Based Accounting

(schedulerPolicyFrameBasedAccnt)

The Frame-Based Accounting parameter specifies whether to use frame-based accounting or packet-based accounting. Frame-based accounting uses the inter-frame gap and instructions to calculate overhead.

Frames Delay (ms)

(l1PingFramesDelay)

The Frames Delay parameter specifies the delay (in ms) between two frames transmitted during an L1-ping. The range is 10 to 1000. The default is 1000.

Framing

(framing)

The Framing parameter specifies what type of framing a port uses. The options are:

- SONET (default)
- SDH

Hold Time (s)

(dot3OamHoldTime)

The Hold Time parameter specifies the number of seconds the 802.3ah efm-oam protocol should wait after the Operational Status transitions from operational to a non-operational state before reverting back to the operational state. The range is 5 to 120. The default is 5.

Hold Time Down

Table 177-20 lists where to find information about the Hold Time Down parameter.

Table 177-20 Hold Time Down parameter

Parameter	See
Hold Time Down for an interface	Hold Time Down (seconds) parameter in this section
Hold Time Down for an interface or SONET link	Hold Time Down (100s of ms) parameter in this section

Hold Time Down (100s of ms)

(holdTimeDown)

The Hold Time Down (100s of ms) parameter specifies how long an interface or SONET link is not advertised as down to the rest of the system. This prevents reporting excessive interface transitions. This occurs by not advertising subsequent transitions of the interface to upper layer protocols until the configured timer has expired. The range is 0 to 100 in 100s of ms. The default is 0. When the parameter is set to 0, down-link transitions are immediately reported to upper layer protocols.

Hold Time Down (seconds)

(holdTimeDown)

The Hold Time Down (seconds) parameter specifies the time, in s, that an interface is not advertised as down when the interface changes from an up to a down state. The range is 0 to 50. The default is 0, which means that down-link transitions are immediately reported to upper-layer protocols.

Hold Time Up

Table 177-21 lists where to find information about the Hold Time Up parameter.

Table 177-21 Hold Time Up parameter

Parameter	See the
Hold Time Up for an interface	Hold Time Up (seconds) parameter in this section
Hold Time Up for an interface or SONET link	Hold Time Up (100s of ms) parameter in this section

Hold Time Up (100s of ms)

(holdTimeUp)

The Hold Time Up (100s of ms) parameter specifies the SONET link up dampening timers. This prevents reporting excessive interface transitions. This occurs by not advertising subsequent transitions of the interface to upper layer protocols until the configured timer has expired. The range is 0 to 100 in 100s of ms. The range is 5 to 100 in 100s of ms on the 2 x Channelized OC3/STM1 ASAP MDA on the 7705 SAR. The default is 5 (500 ms). When the parameter is set to 0, up-link transitions are immediately reported to upper layer protocols.

Hold Time Up (seconds)

(holdTimeUp)

The Hold Time Up (seconds) parameter specifies the number of seconds an interface is not advertised as up when an interface transitions from a down to an up state. This parameter allows for event damping, which prevents the excessive advertising of interface state changes. The range is 0 to 50. The default is 0, which means that up-link transitions are immediately reported to upper-layer protocols.

Host String

(hostString)

The Host String parameter specifies the intermediate destination id to match on for host matching purposes. The string can be up to 32 characters in length.

Ignore BPDU

(mobilePortIgnoreBPDU)

The Ignore BPDU parameter specifies whether BPDU ignore is active on a mobile port. The parameter is configurable when the [Enable Port Mobility](#) parameter is set to Enable. When Ignore BPDU is disabled, switch ports that send or receive spanning tree BPDUs are not eligible for mobile port dynamic VLAN assignment. When Ignore BPDU is enabled, BPDUs are ignored on the switch port and port traffic is subject to VLAN rules in the same manner as it is for non-BPDU mobile ports. Alcatel-Lucent recommends that you do not enable the Ignore BPDU parameter. If you enable the Ignore BPDU parameter, network loops may not be detected or the switch may experience connectivity problems. The options are:

- Enable
- Disable
- Not Applicable (default)

Ingress Filtering

(mobilePortIngFiltering)

The Ingress Filtering parameter specifies whether ingress filtering is enabled. The parameter is configurable when the [Enable Port Mobility](#) parameter is set to Enable. When ingress filtering is enabled and the VPM check fails, all ingress packets are silently dropped. Ingress filtering is enabled for all non-mobile ports. When ingress filtering is disabled and the VPM check fails, ingress VLAN packets are sent to the CPU for software VLAN classification. Ingress filtering is disabled for all mobile ports. The options are:

- True
- False (default)

Ingress Percentage of Rate (%)

(mdaIngrNamedPoolPolicy)

The Ingress Percentage of Rate (%) parameter defines a percentage value that changes the amount of buffers used by an ingress port. Changing the port's active bandwidth artificially lowers or increases the buffers managed by one ingress port and gives them to other ingress ports on the same MDA. This parameter does not change the actual bandwidth available on the port. The Ingress Percentage of Rate

value is multiplied by the ingress active bandwidth of the port. For example an Ingress Percentage of Rate value of 150% results in an increased value of 50% (1.5 x rate). A value of 50% causes the active bandwidth to be reduced by 50%. A value of 100 restores the ingress active rate to a normal value. The range is 1 to 1000. The default is 100.

Ingress Percentage of Rate (%)

(portIngrPoolPercentageRate)

The Ingress Percentage of Rate (%) parameter specifies the port buffer allocation rate that limits the active bandwidth for the ingress port. The range is 0 to 1000. The default is 100.

Ingress Rate (Mbps)

(ingressRate)

The Ingress Rate (Mbps) parameter specifies the maximum rate of traffic that can ingress the port. The range is -1 to 10 000. A value of -1 indicates that the limit on the ingress rate is the physical limit of the port.

Initialize

(paePortInitialize)

The Initialize parameter specifies whether the port begins to initialize 802.1X support. The options are:

- true
- false (default)

When you set the parameter to true, after initialization is performed, the parameter reverts to the false option.

Inter-Frame Gap (bytes)

(interFrameGap)

The Inter-Frame Gap (bytes) parameter specifies the minimum idle time between the end of one frame transmission and the beginning of the next frame transmission. The parameter only applies to OmniSwitch Gigabit Ethernet ports. The range is 9 to 12 bytes. The default value is 12 bytes.

IP Source Filtering

(dhcpSnoopingPortIpSourceFiltering)

The IP Source Filtering parameter specifies whether DHCP snooping port traffic is restricted to only packets that contain the client source MAC address and IP address. The DHCP snooping binding table is used to verify the client information for the port that is enabled for IP source filtering. The options are:

- Disabled (default)
- Enabled

J0 Byte

The J0 Byte parameter specifies a numeric value for a SONET section trace. This value is inserted at the source and is checked against the value expected by the receiver. The parameter is configurable when the [Framing](#) parameter is set to SONET and the [SONET Section Trace Mode](#) parameter is set to Byte. The range is a hexadecimal number from 00 to FF. The default is 01.

J0 String

(j0String)

The J0 String parameter specifies a text string that identifies a SONET section trace. The parameter is configurable when the [Framing](#) parameter is set to SONET and the [SONET Section Trace Mode](#) parameter is set to String. The range is 0 to 16 characters. There is no default.

Join Timer

(joinTimer)

The Join Timer parameter specifies (in milliseconds) the interval between MVRP PDU transmit opportunities on an OmniSwitch port. The range is 250 to 1073741773. The default is 600.

Keep Alive Interval (Sec)

(keepAliveInterval)

The Keep Alive Interval (Sec) parameter specifies the number of seconds between each keep-alive PDU transmission. The range is 1 to 120. The default is 10.

L2Uplink

(isl2UplinkMode)

See the [L2Uplink](#) parameter in section [14.1](#).

Leave All Timer

(leaveAllTimer)

The Leave All Timer parameter specifies (in milliseconds) the interval between Leave All messages generated by an OmniSwitch port. The range is 750 to 2147483647. The default is 30000.

Leave Timer

(leaveTimer)

The Leave Timer parameter specifies (in milliseconds) the amount of time an OmniSwitch port waits in the Leave state before changing to the Unregistered state. The range is 750 to 2147483647. The default is 1800.

Line Buildout

(lineBuildout)

The Line Buildout parameter specifies the cable length for physical DS1 interfaces. Table 177-22 lists the parameter options.

Table 177-22 Line Buildout parameter

Option	Option description
Long	Specifies the line buildout for cable lengths over 655 ft (199.644 m).
Short (default)	Specifies the line buildout for cable lengths up to 655 ft (199.644 m).

Line Code

(lineCode)

The Line Code parameter specifies the line coding for 7250 SAS E1 and T1 CES ports and 9500 MPR T1 ports. Table 177-23 lists the parameter options. You cannot configure this parameter on a 9500 MPR T1 port if the [Signal Mode](#) parameter is disabled.

Table 177-23 Line Code parameter

Option	Option description	Dependencies
AMI	The port uses AMI coding.	—
B8ZS (default for T1 ports)	The port uses B8ZS coding.	—
hdb3 (default for E1 ports)	The port uses hdb3 coding.	Does not apply to 9500 MPR T1 ports.

Line Impedance

(lineImpedance)

The Line Impedance parameter specifies the termination impedance for TDM ports. This parameter is configurable when the [Port Type](#) or [Mode](#) parameter is set to E1. Table 177-24 lists the parameter options.

Table 177-24 Line Impedance parameter

Option	Option description
75 ohm normal return loss on E1	Specifies a termination impedance of 75 Ω at normal return loss on the E1 line.
75 ohm high return loss on E1	Specifies a termination impedance of 75 Ω at high return loss on the E1 line.
120 ohm normal return loss on E1	Specifies a termination impedance of 120 Ω at normal return loss on the E1 line.
120 ohm high return loss on E1 (default)	Specifies a termination impedance of 120 Ω at high return loss on the E1 line.

Not all of the values that are listed in n Table 177-24 are supported by all TDM ports.

Line Length

(mprLineLength)

The Line Length parameter specifies the line length, in feet, for the T1 line that is connected to the DS1 port or for lines connected to the DS3 port. The range is 0 to 655 for the DS1 port and 0 to 450 for the DS3 port. The default is 20. You can only figure this parameter when the [Signal Mode](#) parameter is not disabled.

Line Length

(lineLength)

The Line Length parameter specifies the line length, in feet, for the T1 line that is connected to the DS1 port. This parameter is configurable when the [Line Buildout](#) parameter is set to Short. Table 177-25 lists the parameter options.

Table 177-25 Line Length parameter

Option	Description	Dependencies
Line length 0..133ft (Short) (default)	The line length is between 0 and 133 ft.	—
Line length 134..266ft (Short)	The line length is between 134 and 266 ft.	—
Line length 267..399ft (Short)	The line length is between 267 and 399 ft.	—
Line length 400..533ft (Short)	The line length is between 400 and 533 ft.	—
Line length 534..655ft (Short)	The line length is between 534 and 655 ft.	—

LLDP TLVs

(portCfgTLVsTxEnable)

The LLDP TLVs parameter specifies whether a TLV is transmitted on the port. By default, none of the options are enabled. A check mark beside the LLDP TLV option enables the TLV to be transmitted. The options are:

- System Capabilities TLV
- System Description TLV
- System Name TLV
- Port Description TLV

Load Balance Algorithm

(loadBalanceAlgorithm)

See the [Load Balance Algorithm](#) parameter in section 182.1.

Loopback

Table 177-26 lists where to find information about the Loopback parameter.

Table 177-26 Loopback parameter

Parameter	See
Loopback for SONET, SDH, and TDM classes	Loopback parameter in this section
Loopback for CES port	Loopback parameter in this section

Loopback

(loopback)

The Loopback parameter specifies the loopback mode for the CES port. Table 177-27 lists the parameter options.

Table 177-27 Loopback parameter

Option	Description	Dependencies
disabled (default)	Specifies that no loopback is configured for the CES port	—
external	Specifies that an external loopback connector is present on the current TDM port. In this condition, the CES module ignores false signaling and alarms in the loopback signal.	—
local	The bitstream that is derived from the received PSN packets is looped back.	The Clock Mode parameter for the daughter card slot must be set to adaptive.

(1 of 2)

Option	Description	Dependencies
remote	The bitstream received on the TDM port over the T1/E1 line is looped back to the T1/E1 line.	—

(2 of 2)

Loopback

(loopback)

The Loopback parameter specifies the loopback mode for SONET, SDH, and TDM classes. Table 177-28 lists the parameter options.

Table 177-28 Loopback parameter

Option	Option description	Dependencies
None (default)	—	—
Line	Specifies a line loopback mode for the associated port or channel. Line loopback loops the frames received on the corresponding port or channels back to the remote router. You must shut down the corresponding port or channel to enabled loopback.	
Internal	Specifies an internal loopback mode for the associated port or channel. Internal loopback loops the frames from the local router back to the framer.	
Remote	Specifies a remote loopback mode for the associated port or channel.	

MAC Address

(IpsL2MacAddress)

The MAC Address parameter specifies an authorized static MAC address for a port that belongs to a VLAN. The port must belong to a VLAN and have learned port security enabled on the port. There is no default.

Max Egress BW (kbps)

(qosPortMaxEgrBW)

The Max Egress BW (kbps) parameter specifies the maximum egress bandwidth for each of the eight class of service queues on the port. The range is 0 to 4 294 967 296. The default is 0.

Max Ingress BW (kbps)

(qosPortMaxIngBW)

The Max Ingress BW (kbps) parameter specifies the maximum ingress bandwidth for each of the eight class of service queues on the port. The range is 0 to 4 294 967 296. The default is 0.

Max Req

(paeAuthMaxReq)

The Max Req Period parameter specifies the maximum number of authentication requests to the authentication server, for example, a RADIUS server. The range is 1 to 10. The default is 2.

Maximum Power (milliwatt)

(powerMaximum)

The Maximum Power (milliwatt) parameter specifies the maximum amount of power that is available for peripheral devices attached to the port. The range is 3000 to 16 000. The default is 3000.

Maximum Rate (Mbps)

(schOvrMaxRate)

The Maximum Rate (Mbps) parameter specifies the value that overrides the configured explicit maximum frame-based bandwidth for the HSMDA scheduler policy. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value entered overrides the configured bandwidth of the HSMDA scheduler policy.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that all instances of the scheduler policy on the egress ports or ingress HSMDBAs are allowed at the available line rate.

Mode

Table 177-29 lists where to find information about the Mode parameter.

Table 177-29 Mode parameter

Parameter	See
Mode for a service	Mode parameter in section 182.1
Mode for 802.3ah EFM OAM	Mode parameter in this section
Mode for a hybrid Ethernet port	Mode parameter in this section

Mode

(dot3OamMode)

The Mode parameter specifies the 802.3ah EFM OAM port mode. The options are:

- Active (default)
- Passive

Ethernet ports in active mode initiate 802.3ah EFM OAM monitoring activities, such as putting a peer port into a loopback state. Ethernet ports in the passive mode wait for a peer to initiate 802.3ah EFM OAM activities.

Mode

(hybridMode)

The Mode parameter specifies the mode of operation of a hybrid (also known as combo) Ethernet port. Table 177-30 describes the parameter options.

Table 177-30 Hybrid Port Mode Parameter

Option	Description
Preferred Copper	Hybrid ports use the copper RJ-45 10/100/1000 port instead of the fiber MiniGBIC SFP port when both ports are enabled and have a valid link. If the copper port goes down, the switch automatically switches to the fiber MiniGBIC SFP port.
Forced Copper	Hybrid ports always use the copper RJ-45 10/100/1000 port instead of the equivalent fiber MiniGBIC SFP port.
Preferred Fiber (default)	Hybrid ports use the fiber MiniGBIC SFP port instead of the copper RJ-45 10/100/1000 port when both ports are enabled and have a valid link. If the fiber port goes down, the switch automatically switches to the copper RJ-45 port.
Forced Fiber	Hybrid ports always use the fiber MiniGBIC SFP port instead of the equivalent copper RJ-45 10/100/1000 port.

MTU (bytes)

See the [MTU \(bytes\)](#) parameter in section 182.1.

Multiplier (Intervals)

(dot3OamMultiplier)

The Multiplier (Intervals) parameter specifies the number of receive intervals that can pass before any OAMPDUs are received on a port until the EFM OAM negotiation process restarts.

Name

(virtualPortName)

The name parameter specifies a string of up to 32 characters that uniquely identifies a virtual port. There is no default.

Notifications

(portCfgNotifyEnable)

The Notifications parameter specifies whether the port can receive notifications of local system MIB changes. The options are:

- true
- false (default)

Notify

(dot3OamErrFrameEvNotifEnable)

The Notify parameter specifies whether the OAM entity should send an Event Notification OAMPDU when an Errored Frame Event occurs. The options are:

- true (default)
- false

Number of Frames

(l1PingFrames)

The Number of Frames parameter specifies the number of frames to be transmitted from the interface during an L1-ping. The range is 1 to 20. The default is 5.

ODU-TIM reaction

(pmTimReaction)

The ODU-TIM reaction parameter specifies whether a reaction should occur or not in the event of a PM trace identifier mismatch. The options are:

- None (default)
- Squelch-rx

Optical Transport Channel Unit

(otuEnable)

The Optical Transport Channel Unit parameter specifies whether to enable the OTU encapsulation type. When this parameter is set to Enabled, the Optical Transport Channel Unit tab is enabled. The options are

- Enabled
- Disabled (default)

OPU-PLM reaction

(psiPlmReaction)

The OPU-PLM reaction parameter specifies whether a reaction should occur or not in the event of a PSI payload type mismatch. The options are:

- None (default)
- Squelch-rx

OPU-TIM reaction

(psiTimReaction)

The OPU-TIM reaction parameter specifies whether a reaction should occur or not in the event of a PSI trace identifier mismatch. The options are:

- None (default)
- Squelch-rx

OTU-TIM reaction

(smTimReaction)

The OTU-TIM reaction parameter specifies whether a reaction should occur or not in the event of a SM trace identifier mismatch. The options are:

- None (default)
- Squelch-rx

Payload Type (hex)

(psiPayloadTypeTx)

The Payload Type (hex) parameter specifies the transmit payload type value of the PSI of the OPU overhead. The value is a two-character hexadecimal number. The default is 00.

Period Notify

(dot3OamErrFramePeriodEvNotifEnable)

The Period Notify parameter specifies whether the OAM entity should send an Event Notification OAMPDU when an Errored Frame Period Event occurs. The options are:

- true (default)
- false

Period Threshold (frames)

(dot3OamErrFramePeriodThreshold)

The Period Threshold parameter specifies the number of frame errors that must occur for a threshold crossing alarm to be triggered. The range is 1 to 4294967295. The default is 1.

Periodic Timer

(periodicTimer)

The Periodic Timer parameter specifies (in seconds) the interval between periodic events generation for an MVRP configuration on an OmniSwitch port. The range is 1 to 2147483647. The default is 1.

Periodic Transmission Status

(periodicTransmissionStatus)

The Periodic Transmission Status parameter specifies whether an OmniSwitch port is configured to transmit and receive MVRP data. The options are:

- Enabled
- Disabled (default)

Port Framing

(framing)

The Port Framing parameter specifies the type of framing on the attached T1 or E1 line. Table 177-31 lists the parameter options.

Table 177-31 Port Framing parameter

Option	Description	Dependencies
Unframed (default)	The CES module operates in unstructured mode.	—
E1 Framing (cas)	The CES module operates in structured mode. Timeslot 16 carries signaling information.	The Mode parameter for the CES module is set to E1.
E1 Framing (noncas)	The CES module operates in structured mode. Timeslot 16 carries data	The Mode parameter for the CES module is set to E1.
Superframe (cas)	Specifies the framing of 12 consecutive DS1 frames, and that timeslot 16 carries signaling information	The Mode parameter for the CES module is set to T1.
Superframe (noncas)	Specifies the framing of 12 consecutive DS1 frames, and timeslot 16 carries data	The Mode parameter for the CES module is set to T1.
Extended superframe (cas)	Specifies the framing of 24 consecutive DS1 frames, and that timeslot 16 carries signaling information	The Mode parameter for the CES module is set to T1.
Extended superframe (noncas)	Specifies the framing of 24 consecutive DS1 frames, and timeslot 16 carries data	The Mode parameter for the CES module is set to T1.

Port Type

(ds1PortType)

The Port Type parameter specifies whether the port is DS1 or E1. The options are:

- DS1
- E1

Port Usage

(portUsage)

The Port Usage parameter is displayed for ports 5, 6, 7 and 8 of the 4+4 x Ethernet (EAS) card slot. The options are:

- Empty (default)
- MPT
- SFP

Selecting MPT allows long-haul, or MPT-HL, configuration on the port and automatically sets the mode to Network and makes the port available as FE or GE-RJ45 Electrical. Radio-link and service configuration are not supported.

Additionally port-usage is present for port 5 under the core-enhanced card. It can be configured as Empty or SFP.

Selecting SFP on a port configures the mode as Access and makes the port available as GE-Optical.

The Port Usage parameter is displayed for ports 1, 2, 3 and 4 of the 2+2 x Ethernet (EAS) card slot. The options are:

- Empty (default)
- MPT-HC
- MPT-MC
- MPT-ACC (ANSI 3.0.0 only)

Power Priority

(powerPriority)

The Power Priority parameter specifies the priority of powered devices that are connected to a port. Power to low-priority powered devices is removed before power is supplied to high- or critical-priority devices during a power shortage. The options are:

- Critical
- High
- Low (default)

Power State

(adminStatus)

The Power State parameter specifies whether power is available to PD devices connected to a PoE port. The options are:

- Off
- On (default)

Protection Type

(**protectionType**)

The Protection Type parameter specifies the type of protection scheme used by the 9500 MPR port. Table 177-32 describes the parameter options.

Table 177-32 Protection Type parameter

Port Type	Option	Description
MPT or MD 300	No Protection (default)	Main port is not protected by a spare port.
	1 + 1 FD	Packets from the active port are transmitted simultaneously by two ODUs. Each ODU transmits on a different frequency. Packets are received by two ODUs. The active port selects and processes the best signal.
	1 + 1 HSB	Packets from the active port are transmitted simultaneously by two ODUs. Each ODU transmits on the same frequency. Packets are received by two ODUs. The active port selects and processes the best signal.

Q in Q Ethertype

(**qinqEtype**)

The Q in Q Ethertype parameter specifies the Ethertype expected when the Encap Type parameter is set to Q in Q. The range is 1536 to 65 535. The default is 33 024.

Queue 1 through Queue 8

The Queue 1 through Queue 8 parameters allow you to specify which egress queues on a port to monitor for the collection of forwarded packets statistics. Up to eight queues can be enabled for any port. However, only eight counters in total can be enabled for each 7210 SAS-E device. If no queues are enabled on a port, no accounting statistics are collected for that port.

These parameters are only applicable to the 7210 SAS-E.

Table 177-33 Queue 1 through Queue 8 parameters XML strings

Parameter	XML reference
Queue 1	portStatsQueue1PktsFWd

(1 of 2)

Parameter	XML reference
Queue 2	portStatsQueue2PktsFWd
Queue 3	portStatsQueue3PktsFWd
Queue 4	portStatsQueue4PktsFWd
Queue 5	portStatsQueue5PktsFWd
Queue 6	portStatsQueue6PktsFWd
Queue 7	portStatsQueue7PktsFWd
Queue 8	portStatsQueue8PktsFWd

(2 of 2)

The options are:

- Disabled (default)
- Enabled

Q0

(qosPortCOS0MaxBW)

The Q0 parameter specifies the maximum egress bandwidth for traffic in Q0. The range is 0 to 4 294 967 296. The default is 0. A value of 0 specifies best effort. A value of 4 294 967 296 specifies the maximum port speed.

Q0

(qosPortCOS0MinBW)

The Q0 parameter specifies the minimum egress bandwidth for traffic in Q0. The range is 0 to 4 294 967 296. The default is 0. A value of 0 specifies best effort. A value of 4 294 967 296 specifies the maximum port speed.

Q0

(qosPortLowPriorityWeight)

The Q0 parameter specifies the weight assigned to a port CoS egress queue. The range is 0 to 15. The default is 1.

Q1

(qosPortCOS1MaxBW)

See the [Q0](#) parameter in this section.

Q1

(qosPortCOS1MinBW)

See the [Q0](#) parameter in this section.

Q1

(qosPortMediumPriorityWeight)

See the [Q0](#) parameter in this section.

Q2

(qosPortCOS2MaxBW)

See the [Q0](#) parameter in this section.

Q2

(qosPortCOS2MinBW)

See the [Q0](#) parameter in this section.

Q2

(qosPortHighPriorityWeight)

See the [Q0](#) parameter in this section.

Q3

(qosPortCOS3MaxBW)

See the [Q0](#) parameter in this section.

Q3

(qosPortCOS3MinBW)

See the [Q0](#) parameter in this section.

Q3

(qosPortUrgentPriorityWeight)

See the [“Q0”](#) parameter in this section.

Q4

(qosPortCOS4MaxBW)

See the [Q0](#) parameter in this section.

Q4**(qosPortCOS4MinBW)**See the [Q0](#) parameter in this section.**Q4****(qosPortQ4PriorityWeight)**See the [Q0](#) parameter in this section.**Q5****(qosPortCOS5MaxBW)**See the [Q0](#) parameter in this section.**Q5****(qosPortCOS5MinBW)**See the [Q0](#) parameter in this section.**Q5****(qosPortQ5PriorityWeight)**See the [Q0](#) parameter in this section.**Q6****(qosPortCOS6MaxBW)**See the [Q0](#) parameter in this section.**Q6****(qosPortCOS6MinBW)**See the [Q0](#) parameter in this section.**Q6****(qosPortQ6PriorityWeight)**See the [Q0](#) parameter in this section.

Q7**(qosPortCOS7MaxBW)**

See the [Q0](#) parameter in this section.

Q7**(qosPortCOS7MinBW)**

See the [Q0](#) parameter in this section.

Q7**(qosPortQ7PriorityWeight)**

See the [Q0](#) parameter in this section.

QoS Status**(qosEnabled)**

The QoS Status parameter specifies whether QoS is enabled on the port. The options are:

- Enabled
- Disabled (default)

Quiet Period**(paeAuthQuietPeriod)**

The Quiet Period parameter specifies the quiet period for the device. The range is 1 to 3600 s. The default is 60 s.

Rate (Mbps)

Table [177-34](#) lists where to find information about the Rate (Mbps) parameter.

Table 177-34 Rate (Mbps) parameter

Parameter	See
Rate for Class 1	Rate (Mbps) parameter in this section
Rate for Class 2	Rate (Mbps) parameter in this section
Rate for Class 3	Rate (Mbps) parameter in this section
Rate for Class 4	Rate (Mbps) parameter in this section
Rate for Class 5	Rate (Mbps) parameter in this section
Rate for Class 6	Rate (Mbps) parameter in this section

(1 of 2)

Parameter	See
Rate for Class 7	Rate (Mbps) parameter in this section
Rate for Class 8	Rate (Mbps) parameter in this section
Rate for Group 1	Rate (Mbps) parameter in this section
Rate for Group 2	Rate (Mbps) parameter in this section

(2 of 2)

Rate (Mbps)

(schOvrClass1Rate)

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 1. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 1.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)

(schOvrClass2Rate)

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 2. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 2.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)

(schOvrClass3Rate)

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 3. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 3.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)**(schOvrClass4Rate)**

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 4. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 4.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)**(schOvrClass5Rate)**

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 5. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 5.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)**(schOvrClass6Rate)**

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 6. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 6.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)**(schOvrClass7Rate)**

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 7. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 7.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)

(schOvrClass8Rate)

The Rate (Mbps) parameter specifies the value that overrides the configured maximum rate allowed for scheduling Class 8. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value for this parameter overrides the configured rate allowed for scheduling Class 8.

The parameter is configurable when the Override option is enabled and the MAX option is disabled. MAX (-1) means that the limit is not enforced for the class.

Rate (Mbps)

(schOvrGrp1Rate)

The Rate (Mbps) parameter specifies the value that overrides the maximum rate allowed for the scheduling classes mapped to Group 1. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value entered overrides the configured rate allowed for scheduling classes mapped to group 1. MAX (-1) means that the bandwidth limitation is removed from Group 1.

Rate (Mbps)

(schOvrGrp2Rate)

The Rate (Mbps) parameter specifies the value that overrides the maximum rate allowed for the scheduling classes mapped to Group 2. The parameter is configurable when the Override option is enabled and the MAX option is disabled. The range is -2 to 100 000 (0 is not allowed). The default is no override (-2). When the Override option is enabled, the value entered overrides the configured rate allowed for scheduling classes mapped to group 2. MAX (-1) means that the bandwidth limitation is removed from Group 2.

Rate (kbps)

(portEgrShaperRate)

The Rate (kbps) parameter specifies the maximum shapers rate threshold. When a shapers rate limit is reached, scheduling for all queues associated with the shaper is stopped. When the rate drops below the threshold, the queues are placed back in the scheduler service lists. The range is -1 to 10 000. The default is MAX (-1).

Reauth Enabled

(paeAuthReAuthEnabled)

The Reauth Enabled parameter specifies whether to allow reauthentication requests. The options are:

- true
- false (default)

Reauth Period

(paeAuthReAuthPeriod)

The Reauth Period parameter specifies the time between reauthentication requests. The parameter is configurable when the Reauth Enabled parameter is set to true. The range is 1 to 9000 s. The default is 3600 s.

Reauthenticate Control

(paePortReauthenticate)

The Reauthenticate Control parameter specifies whether to reauthenticate the user. The options are:

- true
- false (default)

Received Remote Loopback Requests

(dot3OamLoopbackIgnoreRx)

The Received Remote Loopback Requests parameter specifies whether a port ignores or processes received 802.3ah EFM OAM loopback commands. The options are:

- Ignored (default)
- Processed

A port in loopback mode ignores all other traffic except 802.3ah EFM OAM traffic.

Receiver

These parameters specify the TTI in the received OPU overhead. The auto-populated default sequence is the name of the NE, the IOM number, the MDA slot number, the port number, and the DWDM channel number.

Table 177-35 lists the Receiver parameters.

Table 177-35 Receiver parameters

Parameter	Specifies the TTI for	Options
Receiver (pmTtiRx)	PM	0 to 192 bytes

(1 of 2)

Parameter	Specifies the TTI for	Options
Receiver (smTtiRx)	SM	0 to 192 bytes
Receiver (psiTtiRx)	Payload Structure Trail Trace Identifier (PSI-TTI)	0 to 192 bytes
Receiver (psiPayloadTypeRx)	PSI	0 to 254 bytes

(2 of 2)

Registration Mode

(registrationMode)

The Registration Mode parameter specifies the manner in which VLAN information is registered on an OmniSwitch port. Table 177-36 lists the parameter options.

Table 177-36 Registration Mode parameter

Option	Option Description
Normal (default)	The port accepts MVRP messages and participates in MVRP.
Fixed	The port accepts the initial MVRP registration and then ignores and additional MVRP information. All existing registrations on the port are retained.
Forbidden	The port does not register and does not participate in MVRP.

Report Alarms

(reportAlarmBits)

The Report Alarms parameter specifies the SONET alarms to monitor and report. A check mark beside the alarm option enables the alarm to be logged. Table 177-37 lists the parameter options.

Table 177-37 Report Alarms parameter

Option	Option Description	Default
Loss of Clock	Reports a clock loss which causes the operational state of the port to be shut down	Alarm monitored and reported
Line Remote Defect Indication	Reports line remote defect indication errors. LRDI errors are caused by a remote LOF, LOC, or LOS. When enabled, LRDI alarms are raised and cleared.	
BER Line Signal Failure	Reports line signal failure BER errors. Use the threshold command to set the error rates that, when exceeded, determine signal degradation and signal failure. When enabled, BER line signal failure alarms are raised and cleared.	
Section Loss of Frame	Reports section loss of frame errors. When enabled, SLOF alarms are raised and cleared.	
Section Loss of Signal	Reports a section loss of signal error on the transmit side. When enabled, SLOS alarms are raised and cleared.	
Line Alarm Indication Signal	Reports line alarm indication signal errors. When enabled, LAIS alarms are raised and cleared.	Alarm not monitored or reported
Section S1 Failure	Reports section synchronization failure as reported by the S1 byte. When enabled, SSLF alarms are raised and cleared.	
BER Line Signal Degradation	Reports line signal degradation BER (bit interleaved parity) errors. The parameter sets the threshold for the error rates that, when exceeded, determines signal degradation and signal failure. When enabled, line signal degradation BER alarms are raised and cleared.	
Line Error Condition	Reports a line error condition raised by the remote because of b1 errors received from this device. When enabled, line error conditions are raised but not cleared.	

Reserved CBS%

See the [Reserved CBS%](#) parameter in section 182.1.

Restoration Criteria

See the [“Restoration Criteria”](#), [“Restoration Criteria”](#), and [“Restoration Criteria”](#) parameters in chapter 182.

Restrict-Static-VLAN-Registration

(restrictStaticVlanRegistration)

The Restrict-Static-VLAN-Registration parameter specifies whether static VLAN registration is restricted for an MVRP configuration on a port. The parameter is disabled by default.

Restrict-Advertisement

(restricAdvertisement)

The Restrict-Advertisement parameter specifies whether VLAN advertisement is restricted for an MVRP configuration on a port. The parameter is disabled by default.

Restrict-Registration

(restrictRegistration)

The Restrict-Registration parameter specifies whether VLAN registration is restricted for an MVRP configuration on a port. The parameter is disabled by default.

Retry Timeout (Sec)

(retryTimeout)

The Retry Timeout (Sec) parameter specifies the minimum number of seconds the port should wait after detecting a loop before its State variable (displayed on the States tab) can be set to Link Up. A value of “No retry” specifies that the port should not be set to the Link Up state until the user manually disables and re-enables the port by setting the [Administrative State](#) parameter to Down and then to Up. The range is 0 to 160. The default is 120.

Rx Decision Threshold Voltage Adjustment

(rxdtvAdjust)

The Rx Decision Threshold Voltage Adjustment parameter specifies whether the receive decision threshold voltage adjustment feedback loop is enabled. The options are:

- enabled (default)
- disabled

SAP Id

(sapId)

This parameter specifies the SAP Id for an advanced loopback test on an OS 6250 NE port, where the value of the [Traffic Type](#) parameter is Outward. The range is 0 to 1024. The default is 0.

SD Threshold (10E-n bits received)

(sdThreshold)

The SD Threshold (10E-n bits received) parameter specifies the bit error rate (BER) threshold used to determine when to raise and clear Signal Degradation alarms (otuBerSd/fecSd). The value represents an error rate of 10E- <value>. The range is 5 through 9, and the default value is 7.

Seconds Summary Notify

(dot3OamErrFrameSecsEvNotifEnable)

The Seconds Summary Notify parameter specifies whether the local OAM entity should send an Event Notification OAMPDU when an Errored Frame Seconds Event occurs. The options are:

- true (default)
- false

Seconds Summary Threshold (framesec)

(dot3OamErrFrameSecsSummaryThreshold)

The Seconds Summary Threshold parameter specifies the number of errored frame seconds that must occur for a threshold crossing alarm to be triggered. The range is 1 to 900. The default is 1.

Second Network Element

(nodeIdHigh)

The Second Network Element parameter specifies the far-end device in the APS group container.

Server Timeout

(paeAuthServerTimeout)

The Server Timeout parameter specifies the timeout period for authentication requests from the authenticating server, for example, a RADIUS server. The range is 1 to 300 s. The default is 30 s.

Servicing Mode

(qosPortServicingMode)

The Servicing Mode parameter specifies whether the port uses strict priority or weighted fair queuing to service the port QoS queues. Table 177-38 describes the parameter options.

Table 177-38 Servicing Mode parameter

Option	Description
Default (default)	A strict priority method using eight priority queues. Lower priority traffic is dropped in the presence of higher priority traffic.
Strict Priority	A type of WFR that combines strict-priority queues and WRR queues. In Strict Priority scheduling, each CoS queue associated with the egress port is serviced in priority order from highest 7 to lowest 0. All traffic for a specific CoS is transmitted before the scheduler proceeds to the next highest priority queue.

(1 of 2)

Option	Description
WRR	All queues participate in a WRR scheme. Traffic is serviced from each queue based on the weight of the queue. Weighted Round Robin (WRR) scheduling services each CoS queue associated with the egress port in round robin order from highest priority to lowest priority. WRR provides a weighted access to the egress port bandwidth at the packet level. A configurable weight from 1 to 15 is assigned to each CoS queue.
DRR	All queues participate in a DRR scheme. Traffic is serviced from each queue based on the weight of the queue. The DRR scheduling algorithm maintains a quantum value that defines the total number of credits for each CoS queue and a credit counter that is decremented each time a byte is taken from the queue for transmission. The purpose of the credit counter is to track the use of bandwidth by a CoS queue relative to the amount of bandwidth that has been allocated to the queue.

(2 of 2)

The port servicing mode overrides the global default servicing mode that is configured with QoS global parameter settings. To reset the servicing mode for the port to the global default mode, choose the Default option.

Set Local Loopback

(dot3OamLoopbackLocalStatus)

The Set Local Loopback parameter specifies the local port loopback mode. The parameter is configurable when the Operational Status is Operational. You can specify the local loopback mode using this parameter even when the [Received Remote Loopback Requests](#) parameter is set to Ignored. This parameter overrides 802.3ah EFM OAM command messages. The options are:

- No Loopback (default)
- Local Loopback

This parameter has no effect unless the Loopback Status parameter is set to No Loopback.

Set Remote Loopback

(dot3Actions)

The Set Remote Loopback parameter specifies the peer loopback state. The parameter is configurable when the Operational Status is Operational. When you enable this parameter, the local port sends an initiating loopback OAMPDU to the peer port to set it to a loopback state. If the peer port is already in a loopback state, you can disable this parameter to send a terminating loopback OAMPDU to the peer port to take it out of a loopback state. The options are:

- Disable (default)
- Enable

SF Threshold (10E-n bits received)

(sfThreshold)

The SF Threshold (10E-n bits received) parameter specifies the bit error rate (BER) threshold used to determine when to raise and clear Signal Failure alarms (otuBerSf/fecSf). The value represents an error rate of 10E- <value>. The range is 3 through 6, and the default value is 5.

SF-SD Method

(sfsdMethod)

The SF-SD Method parameter specifies the method used to determine the Signal Failure and Signal Degradation alarms. The method values are BIP8, specifying that SM-BIP8 errors are used and FEC, specifying that FEC corrected bits are used. The default value is FEC.

Signal Mode

(mprFraming)

The Signal Mode parameter specifies the type of framing used for E1 and DS1 ports. Table 177-39 describes the options.

Table 177-39 Signal Mode parameter

Option	Option description	Dependencies
Disabled (default)	Framing is disabled	—
Unframed	The entire T1 or E1 frame is used to carry data.	—
Framed	The E1 is divided into 32 channels.	Only applies to E1 ports
Framed SF	A group of 12 24-channel frames, referred to as a super frame format.	Only applies to DS1 ports
Framed ESF	A group of 24 24-channel frames, referred to as an extended super frame format.	Only applies to DS1 ports

Single Fiber

(singleFiber)

The Single Fiber parameter specifies whether to enable gathering and redirection of IP packets from a single fiber on the RX port of a SONET or Ethernet port and redistribute packets to other interfaces through static routes or policy-based forwarding. The options are:

- true
- false (default)

Start L1-Ping

(l1PingStart)

This parameter is used to trigger an L1-Ping from the 5620 SAM. The options are:

- true
- false (default)

Status

(loopbackStatus)

This parameter specifies the status of an advanced loopback test on an OmniSwitch port. The options are:

- Config (default and not selectable)
- Start
- Stop

SONET Section Trace Mode

(sonetSectionTraceMode)

The SONET Section Trace Mode parameter specifies the section trace type in the SONET section header to interoperate with some older versions of ADMs or regenerators that require an incremental STM ID. Table 177-40 lists the parameter options.

Table 177-40 SONET Section Trace Mode parameter

Option	Option description	Dependencies
Byte (default)	00 to ff hexadecimal characters, as configured using the J0 String parameter	—
Increment-z0	Set to hexadecimal 01 and cannot be changed	
String	Up to 16 decimal characters, as configured using the J0 String parameter	

Source MAC Address

(sourceMACAddress)

This parameter specifies the source MAC address of the test frames of an advanced loopback test on an OmniSwitch port. Specify a unicast MAC address in the form XX-XX-XX-XX-XX-XX.

Speed

See the [Speed](#) parameter in section 182.1.

SSM Code-Type

(codeType)

The SSM Code-Type parameter specifies the encoding type for synchronous status messages. You can configure the parameter only on synchronous Ethernet MDAs. The options are:

- SDH (default)
- SONET

Status

(mvrpStatus)

The Status parameter specifies whether an MVRP configuration is enabled or disabled on an OmniSwitch port. The options are:

- Enabled
- Disabled (default)

Supplicant Timeout

(paeAuthSuppTimeout)

The Supplicant Timeout parameter specifies the timeout period for the authenticating device; for example, a RADIUS server. The range is 1 to 300 s. The default is 60 s.

Swap MAC Address

(swapMacAddr)

The Swap MAC Address parameter specifies whether MAC address swapping is enabled on an Ethernet port. The options are:

- false (default)
- true

The Swap MAC Address parameter is configurable only on 7705 SAR (version 4.0 R1 or later) daughter cards. The parameter can only be configured if the [Type](#) parameter is configured for the Line option. The parameter can be configured on network ports only.

Synchronous status messages

(ssm)

The Synchronous status messages parameter specifies whether synchronous status messages are enabled on the Ethernet port. The options are:

- false (default)
- true

You can configure the parameter only when the [Synchronous Ethernet](#) parameter is set to True.

Target Power

(targetPower)

The Target Power parameter specifies the average output power of the interface's transmitted optical signal. The range is -20 to -3 dBm. The default is -20 dBm.

This parameter appears only when the [Wave Tracker Power Control](#) parameter is enabled.

Test Name

(testName)

This parameter specifies the name of an advanced loopback test on an OmniSwitch port. The range is 1 to 32 characters. The default is 0.

Threshold (frames)

(dot3OamErrFrameThreshold)

The Threshold parameter specifies the number of frame errors that must occur for a threshold crossing alarm to be triggered. The range is 1 to 4294967295. The default is 1.

Time (seconds)

(portLoopbackTime)

The Time parameter specifies the loopback time, in seconds, of a timed loopback. The range is 0 to 84 600. The default is 0. A value of zero indicates an unlimited loopback time. For line loopbacks, the time must be a value other than zero.

Timeout Period (Days)

(activationTimeOutDays)

This parameter specifies the loopback timeout period in days of a 9500 MPR DS1, ES1 or Radio port. This parameter is configurable only if the [Activation](#) parameter value is set to Active. The maximum is 3 and the default is 0.

Timeout Period (Hrs)

(activationTimeOutHrs)

This parameter specifies the loopback timeout period in hours of a 9500 MPR DS1, ES1 or Radio port. This parameter is configurable only if the [Activation](#) parameter value is set to Active. The maximum is 23 and the default is 0.

Timeout Period (Mins)

(activationTimeOutMins)

This parameter specifies the loopback timeout period in minutes of a 9500 MPR DS1, ES1 or Radio port. This parameter is configurable only if the [Activation](#) parameter value is set to Active. The maximum is 59, and the default is 5.

Traffic Type

(trafficType)

This parameter specifies whether the traffic type of an advanced loopback test on an OmniSwitch port is ingress (inward) or egress (outward). The options are:

- Inward
- Outward (default)

Transmit Interval

(dot3OamInterval)

The Transmit Interval parameter specifies the amount of time, in 100-ms intervals for non-OmniSwitch NEs, and 1 second intervals for OmniSwitch NEs, between each periodic 802.3ah EFM OAMPDU that is transmitted and received. A lower value indicates that OAMPDUs are transmitted more frequently to the peer and that OAMPDUs must be received more frequently from the peer. For non-OmniSwitch NEs, the default is 10, which specifies that there is one second between the transmitted and received OAMPDUs; similarly the default is 1 second for OmniSwitch NEs. Table [177-41](#) lists the parameter options.

Table 177-41 Transmit Interval values

Device	Range	Default
Non-OmniSwitch	1 to 600-ms	10-ms
OmniSwitch	1 to 60 s	1 s

Transmit Management Address

(portCfgManAddrTxEnabled)

The Transmit Management Address parameter specifies whether the management address is transmitted. The options are:

- Disabled (default)
- Enabled

Transmitter Bytes

The Transmitter Bytes parameters specify the type of transmit (Tx) TTI in the OTU. These parameter appears only when the [Transmitter Mode](#) parameter is set to Bytes.

The value is a hexadecimal number. Table 177-42 lists the Transmitter Bytes parameters.

Table 177-42 Transmitter Bytes parameters

Parameter	Specifies the TTI for
Transmitter String (pmTtiTx)	PM
Transmitter String (smTtiTx)	SM
Transmitter String (psiTtiTx)	PSI

Transmitter Mode

The Transmitter Mode parameters specify the type of TTI in the OTU overhead. Table 177-43 lists the various Transmitter Mode parameters.

Table 177-43 Transmitter Mode parameters

Parameter	Specifies the TTI for	Options
Transmitter Mode (pmTtiTxMode)	PM	<ul style="list-style-type: none"> Auto (default) String Bytes
Transmitter Mode (smTtiTxMode)	SM	
Transmitter Mode (psiTtiTxMode)	PSI	

Transmitter String

These parameters allow specify the type of transmit TTI in the OTU overhead. These parameters are only configurable when the [Transmitter Mode](#) parameter is set to String.

The value is 0 to 192 bytes. Table 177-44 lists the Transmitter String parameters.

Table 177-44 Transmitter String parameters

Parameter	Specifies the TTI for
Transmitter String (pmTtiTx)	PM
Transmitter String (smTtiTx)	SM
Transmitter String (psiTtiTx)	PSI

The auto-populated default sequence is the name of the NE, the IOM number, the MDA slot number, the port number, and the DWDM channel number.

Trust Mode

(dhcpSnoopingPortTrustMode)

The Trust Mode parameter specifies the DHCP snooping trust mode for a port. Table 177-45 describes the options.

Table 177-45 Trust Mode parameter

Option	Option description	Dependencies
Client Only (default)	Allows only DHCP client-related traffic on the port. When this mode is active for the port, the port is considered an untrusted interface.	Trust mode only applies when DHCP snooping is enabled for the switch or for a VLAN. When DHCP snooping is enabled at the switch level, the trust mode applies to all switch ports. When DHCP snooping is enabled for a specific VLAN, the trust mode applies to only those ports that are associated with that VLAN.
Blocked	Blocks all DHCP traffic on the port. When this mode is active for the port, the port is considered an untrusted interface.	
Trusted	Allows all DHCP traffic on the port. The port is considered a trusted interface and behaves as if DHCP snooping was not enabled.	

Trusted

(qosPortTrusted)

The Trusted parameter specifies whether a port is trusted. All switch ports, by default, are not trusted, which means that the ports do not require incoming traffic packets to have their 802.1p or ToS/DSCP values set. When a port is not trusted, the 802.1p or ToS/DSCP bits in incoming packets are set to the default 802.1p or to DSCP values that are configured for the port.

Fixed ports that are configured for 802.1q are always trusted, regardless of QoS settings, and cannot be configured as untrusted. Mobile ports are also trusted, but they may or may not accept Q-tagged traffic. The options are:

- Yes
- No (default)

Tunneling

(dot3OamTunneling)

The Tunneling parameter specifies whether OAMPDUs are transparently passed through a port which is part of an Epipe service. The options are:

- Disabled (default)
- Enabled

You can enable this parameter when the [Administrative State](#) parameter is Disabled.

You may need to run 802.3ah OAMPDUs between devices which are located at each end of an Epipe service.

When you enable tunneling at both ends of an Epipe, the 802.3ah OAMPDUs that are received at one end of the Epipe are forwarded transparently through the Epipe. When you disable tunneling, OAMPDUs are dropped or processed locally, depending on the state of the 802.3ah protocol.

Tx DUS/DNU

(txDus)

The Tx DUS/DNU parameter specifies whether the QL value that is transmitted from the SSM channel of the SONET, SDH, or Synchronous Ethernet port is set to QL-DUS or QL-DNU. You can configure the parameter only on synchronous Ethernet MDAs, and on optical MDAs. The options are:

- true
- false (default)

Tx Period

(paeAuthTxPeriod)

The Tx Period parameter specifies the transmit period for the device. The range is 1 to 3600 s. The default is 30 s.

Type

Table [177-46](#) lists where to find information about the Type parameter.

Table 177-46 Type parameter

Parameter	See
Type for access group	Type parameter in this section
Type for channel framing	Type parameter in this section
Type for APS group	Type parameter in this section
Type for timed loopback on 7705 SAR Ethernet ports	Type parameter in this section

Type

(accessType)

The Type parameter specifies the type of access group to create. The options are:

- IP (default)
- MAC

Type

(ds3Type)

The Type parameter specifies the framing type for channels on the specified port. The options are:

- DS3 (default)
- E3

Type

(nodeCardinality)

The Type parameter specifies whether the working and protection channels of the APS group are located on a single device or on two independent devices. The options are:

- Single Chassis (default)
- Multi Chassis

Type

(portLoopback)

The Type parameter specifies the type of loopback of the Ethernet port of the 7705 SAR. The options are described in Table 177-47.

Table 177-47 Type parameter

Option	Description	Dependencies
None (default)	No loopback.	—
Line	Loops frames received on the corresponding port back towards the transmit direction.	Supported only on ports configured in network mode.
Internal	Loops frames from the local router back to the framer. This is also referred to as an equipment loopback. The transmit signal is looped back and received by the interface.	Supported only on ports configured in access mode.

VLAN

(vlan)

This parameter specifies the outer VLAN number of the test frames of an advanced loopback test on an OmniSwitch port. The range is 2 to 4094.

Wave Key1

(encodeKey1)

The Wave Key1 parameter specifies the first wavelength tracker identifier to be transmitted on the interface's optical signal. The range is 0 to 4096. The default is 0. Table 177-48 lists the wave key value ranges.

Table 177-48 Wave Key value ranges

ITU channel	Key 1 minimum	Key 1 maximum	Key 2 minimum	Key 2 maximum
17	1276	1290	1760	1774
18	1259	1273	1743	1757
19	1242	1256	1726	1740
20	1225	1239	1709	1723
21	528	542	1072	1086
22	511	525	1055	1069
23	494	508	1038	1052
24	477	491	1021	1035
25	1208	1222	1692	1706
26	460	474	1004	1018
27	443	457	987	1001
28	426	440	970	984
29	409	423	953	967
30	1191	1205	1675	1689
31	392	406	936	950
32	375	389	919	933
33	358	372	902	916
34	341	355	885	899
35	1174	1188	1658	1672
36	324	338	868	882
37	307	321	851	865
38	290	304	834	848
39	273	287	817	831
40	1157	1171	1641	1655
41	256	270	800	814
42	239	253	783	797
43	222	236	766	780
44	205	219	749	763
45	1140	1154	1624	1638
46	188	202	732	746
47	171	185	715	729
48	154	168	698	712

(1 of 3)

ITU channel	Key 1 minimum	Key 1 maximum	Key 2 minimum	Key 2 maximum
49	137	151	681	698
50	1123	1137	1607	1621
51	120	134	664	678
52	103	117	647	661
53	86	100	630	644
54	69	83	613	627
55	1106	1120	1590	1604
56	52	66	596	610
57	35	49	579	593
58	18	32	562	576
59	1	15	545	559
60	1089	1103	1573	1587
61	1548	1548	2032	2032
175	3553	3567	4065	4079
185	3536	3550	4048	4062
195	3519	3533	4031	4045
205	3502	3516	4014	4028
225	3823	3837	2287	2301
235	3806	3820	2270	2284
245	3789	3803	2253	2267
255	3485	3499	3997	4011
265	3772	3786	2236	2250
275	3755	3769	2219	2233
285	3738	3752	2202	2216
285	3840	3854	2304	2318
295	3721	3735	2185	2199
305	3468	3482	3980	3994
315	3704	3718	2168	2182
325	3687	3701	2151	2165
335	3670	3684	2134	2148
345	3653	3667	2117	2131
355	3451	3465	3963	3977
365	3636	3650	2100	2114
375	3619	3633	2083	2097
385	3602	3616	2066	2080
395	3585	3599	2049	2063

(2 of 3)

ITU channel	Key 1 minimum	Key 1 maximum	Key 2 minimum	Key 2 maximum
405	3434	3448	3946	3960
415	1548	1562	2032	2046
425	1531	1545	2015	2029
435	1514	1528	1998	2012
445	1497	1511	1981	1995
455	3908	3922	2372	2386
465	1480	1494	1964	1978
475	1463	1477	1947	1961
485	1446	1460	1930	1944
495	1429	1443	1913	1927
505	3891	3905	2355	2369
515	1412	1426	1895	1911
525	1395	1409	1879	1893
535	1378	1392	1862	1876
545	1361	1375	1845	1859
555	3874	3888	2338	2352
565	1344	1358	1828	1842
575	1327	1341	1811	1825
585	1310	1324	1794	1808
595	1293	1307	1777	1791
605	3857	3871	2321	2335

(3 of 3)

This parameter appears only when the [Wave Tracker Encode](#) parameter is enabled.

Wave Key2

(encodeKey2)

The Wave Key2 parameter specifies the second wavelength tracker identifier to be transmitted on the interface's optical signal. The range is 0 to 4079. The default is 0. See Table [177-48](#) for information about wave key value ranges.

This parameter appears only when the [Wave Tracker Encode](#) parameter is enabled.

Wave Tracker Encode

(waveTrackerEncode)

The Wave Tracker Encode parameter specifies whether wavelength tracker keys are encoded on the transmitted optical signal. The options are:

- enabled
- disabled (default)

Wave Tracker Power Control

(waveTrackerPowerControl)

The Wave Tracker Power Control parameter specifies whether the wavelength power control loop that maintains the interface's transmitted optical signal average output power is enabled. The options are:

- enabled
- disabled (default)

Weight in Group

Table 177-49 lists where to find information about the Weight in Group parameter.

Table 177-49 Weight in Group parameter

Parameter	See
Weight in Group for Class 1	Weight in Group parameter in this section
Weight in Group for Class 2	Weight in Group parameter in this section
Weight in Group for Class 3	Weight in Group parameter in this section
Weight in Group for Class 4	Weight in Group parameter in this section
Weight in Group for Class 5	Weight in Group parameter in this section
Weight in Group for Class 6	Weight in Group parameter in this section
Weight in Group for Class 7	Weight in Group parameter in this section
Weight in Group for Class 8	Weight in Group parameter in this section

Weight in Group

(schOvrClass1WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 1. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

Weight in Group

(schOvrClass2WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 2. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

Weight in Group

(schOvrClass3WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 3. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

Weight in Group

(schOvrClass4WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 4. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

Weight in Group

(schOvrClass5WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 5. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

Weight in Group

(schOvrClass6WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 6. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

Weight in Group

(schOvrClass7WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 7. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

Weight in Group

(schOvrClass8WtInGp)

The Weight in Group parameter specifies the value that overrides the configured weight of scheduling class 8. The parameter is configurable when the Override option is enabled and the Default option is disabled. The range is -2 to 100 (0 and -1 are not allowed). The default is 1. To configure the parameter for no override set the value to -2.

XGig Mode

(networkMode)

The XGig Mode parameter specifies whether the 10-Gbyte port is configured in LAN or WAN mode. When you configure the XGig Mode parameter on a port on a 10Gig Extended Performance MDA, the same value is applied to all other ports on the MDA. Table 177-50 describes the options.

Table 177-50 Xgig Mode parameter

Option	Option description	Dependencies
LAN (default)	When the port configured as LAN, SONET/SDH parameters cannot be configured.	—
WAN	When the port is configured as WAN, some SONET/SDH parameters are enabled, to reflect WAN requirements. The 5620 SAM automatically creates SONET-related objects when the XGig Mode parameter is set to WAN. When you set the XGig Mode parameter from WAN to LAN, the 5620 SAM removes the SONET-related objects. The 5620 SAM collects SONET-related statistics when the XGig Mode parameter is set to WAN.	SONET/SDH tabs appear on the properties form, but only a subset of parameters can be configured.

178 –HSMDA Egress Secondary Shaper parameters

178.1 HSMDA Egress Secondary Shaper parameters 178-2

178.1 HSMDA Egress Secondary Shaper parameters

This chapter describes the parameters on the HSMDA Egress Secondary Shaper form and child forms.

Class Burst Threshold (bytes)

Table 178-2 lists where to find information about the Class Monitor Threshold (Kbytes) parameter.

Table 178-1 Burst Threshold (bytes) parameter

Parameter	See
Class 1 Burst Threshold	Class 1 Burst Threshold (bytes) parameter in this section
Class 2 Burst Threshold	Class 2 Burst Threshold (bytes) parameter in this section
Class 3 Burst Threshold	Class 3 Burst Threshold (bytes) parameter in this section
Class 4 Burst Threshold	Class 4 Burst Threshold (bytes) parameter in this section
Class 5 Burst Threshold	Class 5 Burst Threshold (bytes) parameter in this section
Class 6 Burst Threshold	Class 6 Burst Threshold (bytes) parameter in this section
Class 7 Burst Threshold	Class 7 Burst Threshold (bytes) parameter in this section
Class 8 Burst Threshold	Class 8 Burst Threshold (bytes) parameter in this section

Class 1 Burst Threshold (bytes)

(portEgrShaperClass1BurstThresh)

The Class 1 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class 2 Burst Threshold (bytes)

(portEgrShaperClass2BurstThresh)

The Class 2 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class 3 Burst Threshold (bytes)

(portEgrShaperClass3BurstThresh)

The Class 3 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class 4 Burst Threshold (bytes)

(portEgrShaperClass4BurstThresh)

The Class 4 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class 5 Burst Threshold (bytes)

(portEgrShaperClass5BurstThresh)

The Class 5 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class 6 Burst Threshold (bytes)

(portEgrShaperClass6BurstThresh)

The Class 6 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class 7 Burst Threshold (bytes)

(portEgrShaperClass7BurstThresh)

The Class 7 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class 8 Burst Threshold (bytes)

(portEgrShaperClass8BurstThresh)

The Class 8 Burst Threshold (bytes) parameter specifies the explicit shaping burst size of the class. The range is -1 and 1 to 327 680, where -1 specifies the Default rate. The default is Default.

Class Monitor Threshold (Kbytes)

Table 178-2 lists where to find information about the Class Monitor Threshold (Kbytes) parameter.

Table 178-2 Monitor Threshold (Kbytes) parameter

Parameter	See
Class 1 Monitor Threshold	Class 1 Monitor Threshold (Kbytes) parameter in this section
Class 2 Monitor Threshold	Class 2 Monitor Threshold (Kbytes) parameter in this section

(1 of 2)

Parameter	See
Class 3 Monitor Threshold	Class 3 Monitor Threshold (Kbytes) parameter in this section
Class 4 Monitor Threshold	Class 4 Monitor Threshold (Kbytes) parameter in this section
Class 5 Monitor Threshold	Class 5 Monitor Threshold (Kbytes) parameter in this section
Class 6 Monitor Threshold	Class 6 Monitor Threshold (Kbytes) parameter in this section
Class 7 Monitor Threshold	Class 7 Monitor Threshold (Kbytes) parameter in this section
Class 8 Monitor Threshold	Class 8 Monitor Threshold (Kbytes) parameter in this section

(2 of 2)

Class 1 Monitor Threshold (Kbytes)

(portEgrShaperClass1Thresh)

The Class 1 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 1. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class 2 Monitor Threshold (Kbytes)

(portEgrShaperClass2Thresh)

The Class 2 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 2. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class 3 Monitor Threshold (Kbytes)

(portEgrShaperClass3Thresh)

The Class 3 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 3. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class 4 Monitor Threshold (Kbytes)

(portEgrShaperClass4Thresh)

The Class 4 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 4. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class 5 Monitor Threshold (Kbytes)

(portEgrShaperClass5Thresh)

The Class 5 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 5. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class 6 Monitor Threshold (Kbytes)

(portEgrShaperClass6Thresh)

The Class 6 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 6. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class 7 Monitor Threshold (Kbytes)

(portEgrShaperClass7Thresh)

The Class 7 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 7. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class 8 Monitor Threshold (Kbytes)

(portEgrShaperClass8Thresh)

The Class 8 Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the Class 8. The parameter is configurable when the associated Default check box is disabled. The range is -1 to 8190, where -1 specifies the Default rate. The default is Default.

Class Rate (kbps)

Table 178-3 lists where to find information about the Class Rate (Kbps) parameter.

Table 178-3 Class Rate (Kbps) parameter

Parameter	See
Class 1 Rate	Class 1 Rate (kbps) parameter in this section
Class 2 Rate	Class 2 Rate (kbps) parameter in this section
Class 3 Rate	Class 3 Rate (kbps) parameter in this section
Class 4 Rate	Class 4 Rate (kbps) parameter in this section
Class 5 Rate	Class 5 Rate (kbps) parameter in this section
Class 6 Rate	Class 6 Rate (kbps) parameter in this section
Class 7 Rate	Class 7 Rate (kbps) parameter in this section
Class 8 Rate	Class 8 Rate (kbps) parameter in this section

Class 1 Rate (kbps)**(portEgrShaperClass1Rate)**

The Class 1 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 1. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

Class 2 Rate (kbps)**(portEgrShaperClass2Rate)**

The Class 2 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 2. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

Class 3 Rate (kbps)**(portEgrShaperClass3Rate)**

The Class 3 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 3. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

Class 4 Rate (kbps)**(portEgrShaperClass4Rate)**

The Class 4 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 4. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

Class 5 Rate (kbps)**(portEgrShaperClass5Rate)**

The Class 5 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 5. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

Class 6 Rate (kbps)**(portEgrShaperClass6Rate)**

The Class 6 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 6. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

Class 7 Rate (kbps)

(portEgrShaperClass7Rate)

The Class 7 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 7. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

Class 8 Rate (kbps)

(portEgrShaperClass8Rate)

The Class 8 Rate (Kbps) parameter specifies the maximum rate allowed for the shaper's Class 8. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000 000, where -1 specifies the MAX rate. MAX means that the limit is not enforced for the class. The default is MAX.

High Burst Increase

(portEgrExpShaperHighBurstIncrease)

The High Burst Increase parameter specifies the incremental number of bytes above the low burst limit to be used as the high burst threshold for the aggregate rate of the classes pertaining to the high burst threshold in the expanded secondary shaper. The range is -1 to 65 528. The default is -1.

Low Burst Limit

(portEgrExpShaperLowBurstLimit)

The Low Burst Limit parameter specifies the number of bytes to be used as the low burst threshold for the aggregate rate of the classes pertaining to the low burst threshold in the expanded secondary shaper. The range is -1 and 1 to 327 680. The default is -1.

Low Burst Max Class

(hsm daLowBurstMaxClass)

The Low Burst Max Class parameter specifies which class should use the low priority burst threshold. All classes starting from 1, up to and including the class configured for this property use the low priority burst threshold. All classes greater than the value configured for this property, up to and including class 8, use the high priority burst threshold. The range is 1 to 8. The default is 8.

Monitor Threshold (Kbytes)

(portEgrShaperThresh)

The Monitor Threshold (Kbytes) parameter specifies the monitoring non-conformance burst threshold for the aggregate exp-secondary-shaper. The range is -1 to 8190. The default is -1.

Name

(displayName)

The Name parameter specifies a string of up to 32 characters that uniquely identifies a name for the HSMDA egress secondary shaper. You cannot include a colon in the HSMDA egress secondary shaper name.

Rate (Mbps)

(portEgrShaperRate)

The Rate (Mbps) parameter specifies the explicit maximum frame based bandwidth limit allowed for all the classes mapped to the egress secondary shaper. The parameter is configurable when it is enabled. The range is -1 and 1 to 10 000, where -1 specifies the MAX rate. MAX means that all the shaper's classes are allowed at the available line rate. The default is MAX.

179 –Channel parameters

179.1 Channel parameters 179-2

179.1 Channel parameters

This chapter describes the parameters on the Channel property form, and the child forms launched from the right-click contextual menu options for channels.

Accounting Enabled

See the [Accounting Enabled](#) parameter in section 182.1.

Administrative State

See the [Administrative State](#) parameter in section 182.1.

Administrative Status

(adminStatus)

The Administrative Status parameter specifies the status of the PVCC created for an ILMI link. The options are:

- Disabled (default)
- Enabled

ATM Interface Cell Format

(atmInterfaceCellFormat)

See the [ATM Interface Cell Format](#) in chapter 182.

ATM Minimum VPI Value

(atmInterfaceMinimumVPIValue)

The Minimum VPI Value parameter specifies the minimum VPI value that can be used on the ATM interface for a VPC. The range is 0 to 4095. The default is 0.

BER SF Link Down

(tdmequipment.DS0ChannelGroupSpecifics)

The BER SF Link Down parameter specifies the status of a PPP channel when BER SF is detected. When set to Enabled, the link is set to out of service when BER SF is detected. When set to Disabled, the link remains in-service when BER SF is detected. The options are:

- Disabled (default)
- Enabled

Bit Error Insertion Rate

(bitErrorInsertionRate)

The Bit Error Insertion Rate parameter specifies the line signal degradation BER and line signal failure thresholds. The options are:

- Disabled (default)
- 1
- 2
- 3
- 4
- 5
- 6
- 7

The line signal (b2) interleaved parity BER is continuously measured. An alarm is raised if the rate exceeds the degradation or failure threshold. If the failure threshold is exceeded, the link is set to operationally down.

C2 Byte (hex)

(c2Byte)

The C2 Byte (hex) parameter specifies the C2 byte value as a hexadecimal character or a decimal integer. The purpose of this byte is to communicate the payload type on a channel that is encapsulated by SONET framing. The range is 00 to FF (hexadecimal), or 0 to 255 (decimal). The default is CF (hexadecimal). When you specify 00 (hexadecimal), the parameter is reset to the default value.

Channel Framing

(channelFraming)

The Channel Framing parameter specifies the DS1/E1 or DS3/E3 framing for the associated port or channel. Table 179-1 lists the parameter options.

Table 179-1 Channel Framing parameter

For	Option	Option description
DS1 or E1	esf	Specifies extended super frame framing for the port
	sf	Specifies super frame framing for the port
	G.703 (not DS1)	Specifies G.703 framing for the channel
	G.704 no-CRC	Specifies G.704 framing without cyclical redundancy checking
	G.704 CRC	Specifies G.704 framing with cyclical redundancy checking
	DS1-unframed	Specifies an unstructured DS1 channel
DS3 or E3	c-bit	Specifies C-Bit framing for the port or channel
	m23	Specifies M23 framing for the port or channel
	G.751 (not DS3)	Specifies G.751 framing for the port or channel
	G.832 (not DS3)	Specifies G.832 framing for the port or channel

Channelized

(channelized)

The Channelized parameter specifies whether the service is channelized. The options are:

- None (default)
- DS1
- E1

Channel Type

(portChannelType)

The Channel Type parameter specifies the type of channel that is created on the port. The options are:

- SONET Sts3 (Sdh Stm1)
- SONET Sts1 (Sdh Au3)
- PDH Ds1
- PDH E1

Clock Source

(channelClockSource)

The Clock Source parameter specifies whether the timing source for transmitted data is the internal clock or a clock recovered from the receive data stream for the line. The options are:

- Loop Timed
- Node Timed (default)
- Adaptive

Collect Accounting Statistics

(accountingOn)

The Collect Accounting Statistics parameter specifies whether the collection of accounting statistics for the channel is enabled. The options are:

- enabled
- disabled (default)

Compression

(hdrCompression)

The Compression parameter specifies one or more types of header compression. Table [179-2](#) describes the parameter options:

Table 179-2 Compression parameter

Option	Description
Address Control Field Compression	Specifies whether to minimize the required backhaul bandwidth for DS1 and E1 channel groups in a PPP configuration by compressing the data link layer address and control fields of the frame. Because these fields typically contain constant values for point-to-point links, they can easily be compressed. The peer is informed whether the implementation can receive compressed fields.
Protocol Field Compression	Specifies whether to minimize the required backhaul bandwidth for DS1 and E1 channel groups in a PPP configuration by compressing the data link layer protocol field of the frame. When low-speed links are used and this parameter is enabled, bandwidth is conserved by sending as little redundant data as possible. If successfully negotiated, the ISO 3309 extension mechanism can be used to compress the protocol field of the data packet to one octet instead of two.

Configured MAC

See the [Configured MAC](#) parameter in section 182.1.

CRC

(crc)

The CRC parameter specifies the cyclic redundancy check on a channel. You can only configure a 16-bit CRC on an OC-3 channel. The default is 32 bit and cannot be changed when the encapsulation type is set to ATM. The options are:

- 16 bit
- 32 bit (default)

CRC Precision

(channelCRC)

The CRC Precision parameter specifies the cyclic redundancy check on a DS0 or DS3 channel. You can only configure a 16-bit CRC on a DS3 channel. The options are:

- 16 bit (default)
- 32 bit

Description

See the [Description](#) parameter in section 182.1.

Destination ECID

(destinationECID)

The Destination ECID parameter specifies the emulated circuit identifier of the destination peer for a specific CES circuit. The range is 0 to 65 535. The default is 0.

Destination IP Address

(destinationIpAddress)

The Destination IP Address parameter specifies the IP address of the destination peer for a specific CES circuit. Specify a unicast IP address in the dotted-decimal format. The default is 192.168.0.127.

Destination MAC Address

(destinationMacAddress)

The Destination MAC Address parameter specifies the MAC address of the destination peer for a specific CES circuit. Specify a unicast MAC address in the form *xx-xx-xx-xx-xx-xx*. The range is 00-00-00-00-00-00 to FF-FF-FF-FF-FF-FF. The default is 00-00-00-00-00-00.

Destination Port

(destinationPort)

The Destination Port parameter specifies the port number of the destination peer for a specific CES circuit. The range is 2000 to 65 535. The default is 2000.

Down Count

(downCount)

The Down Count parameter specifies the number of keepalive intervals that must pass without receiving a keepalive packet before the link is declared down. The nodes at the two endpoints of the cHDLC link should be provisioned with the same values. The range is 1 to 16. The default is 3.

Drop Count

(keepaliveDropCount)

The Drop Count parameter specifies the number of failed responses to an SDP echo request before the SDP changes to a down state. The range is 1 to 255.

Ds3 Channel Payload Type

The Ds3 Channel Payload Type parameter specifies the type of payload that is configured for the channel. The parameter appears only for OC3 or OC12 ASAP ports when the [Channel Type](#) parameter is set to SONET Sts1 (Sdh Au3) and the Sts1 Channel Payload Type parameter is set to PDH Ds3. The options are:

- None (default)
- DS1
- E1

Duration (seconds)

(bertDuration)

The Duration (seconds) parameter specifies the length of time for the BERT. The range is 0 s to 240 s.

Edit ATM button

Click on the Edit ATM button to configure the ATM Interface parameters for the channel.

Edit ILMI Link button

Click on the Edit ILMI Link button to configure the ILMI link parameters for the ATM interface.

Edit PPP button

Click on the Edit PPP button to configure the keep-alive Period and Drop Count parameters for the channel.

Egress Traffic Descriptor

(egress)

The Egress Traffic Descriptor parameter specifies the ATM traffic descriptor profile ID for the egress traffic of the ILMI link. Click on the Select button to choose a qualified ATM QoS policy to associate to the ILMI link. The range is 1 to 1000. The default is 1.

Encap Type

See the [Encap Type](#) parameter in section [182.1](#).

Equipment ID Code

(channelMDLEicString)

The Equipment ID Code parameter specifies the EIC of the MDL. The range is 0 to 10 characters. The default is N/A.

Error Threshold

(dceLmiErrorThreshold)

See the [Error Threshold](#) parameter in section [182.1](#).

Error Threshold

(dteLmiErrorThreshold)

See the [Error Threshold](#) parameter in section [182.1](#).

Facility ID Code

(channelMDLPfiString)

The Facility ID Code parameter specifies the Facility ID Code sent in the MDL path message. The range is 0 to 38 characters. The default is N/A.

Fragment Threshold

(frf12FragmentThreshold)

The Fragment Threshold parameter specifies the maximum length of a fragment transmitted across an FRF.12 link with UNI/NNI fragmentation enabled. The range is 128 to 512. The default is 128.

Frame ID Code

(channelMDLFicString)

The Frame ID Code parameter specifies the FIC of the MDL. The range is 0 to 10. The default is N/A.

Full Enquiry Interval

(dteLmiFullEnquiryInterval)

See the [Full Enquiry Interval](#) parameter in section [182.1](#).

Generator Number String

(channelMDLGenString)

The Generator Number String parameter specifies the number string sent in the MDL test signal message. The range is 0 to 38 characters. The default is N/A.

Idle Cycle Flags

(idleCycleFlags)

The Idle Cycle Flags parameter specifies the value that the DS0, DS1, or DS3 interface transmits during idle cycles. Table [179-3](#) lists the parameter options.

Table 179-3 Idle Cycle Flags parameter

Option	Option description	Dependencies
Flags	0x7E is used as the idle cycle flag	—
Ones	0xFF is used as the idle cycle flag	

ILMI Link VCI

(ilmiLinkVci)

The ILMI Link VCI parameter specifies the VCI of the ILMI link on the ATM interface being configured. The range is 1, 2, and 5 to 65 535. The default is 16.

ILMI Link VPI

(ilmiLinkVpi)

The ILMI Link VPI parameter specifies the PVC identifier (vpi) of the ILMI link on the ATM interface being configured. When the ATM Interface Cell Format parameter is set to UNI, the range is 0 to 255. When the ATM Interface Cell Format parameter is set to NNI, the range is 0 to 4095. The default is 0.

IME Type

(requestedImeType)

The IME Type parameter specifies whether the device that executes the ILMI protocol represents the user or network side of an ATM interface. The options are:

- User-side (default)
- Network-side

Ingress Traffic Descriptor

(ingress)

The Ingress Traffic Descriptor parameter specifies the ATM traffic descriptor profile ID for the ingress traffic of the ILMI link. Click on the Select button to choose a qualified ATM QoS policy to associate to the ILMI link. The range is 1 to 1000. The default is 1.

Interface ID

(interfaceId)

The Interface ID parameter specifies the identifier for the CES interface. The identifier must be unique across the device. The range is 1 to 30. The default is 0, which indicates that the parameter is not set.

Interface Mapping

(atmInterfaceMapping)

The Interface Mapping parameter specifies the ATM cell mapping into a DS3 channel of an ATM interface. Table [179-4](#) lists the parameter options.

Table 179-4 Interface Mapping parameter

Option	Description	Dependencies
Direct (default)	ATM direct mapping	—
PLCP	PLCP mapping	The Payload Type parameter of the channel must be set to Pdh Ds3

J1 String

(j1String)

The J1 String parameter specifies the insertion of a continuous J1 path trace at the source to check against the expected value of the receiver. The J1 string contains all zeros for a path that is not provisioned. The range is 1 to 64 characters.

Keep Alive (seconds)

The Keep Alive (seconds) parameter specifies the interval, in seconds, used to send periodic keepalive packets. The receiver process expects to receive a keepalive packet at every keepalive interval. The link is declared down if the receiver process does not receive a keepalive packet within the timeout interval. The link is declared up when the number of continual keepalive packets received equals the up-count. The nodes at the two endpoints of the cHDLC link should be provisioned with the same values. The range is 0 to 300. The default is 10.

Keep-Alive Polling Count

(keepAlivePollCount)

The Keep-Alive Polling Count parameter specifies how many consecutive polls must occur after an ILMI response message has not been received before connectivity is declared lost between peer IMEs. The range is 1 to 255. The default is 4.

Keep-Alive Polling Frequency (seconds)

(keepAlivePollFreq)

The Keep-Alive Polling Frequency (seconds) parameter specifies the frequency, in seconds, between polls for ILMI connectivity loss between peer IMEs. The range is 1 to 255. The default is 1.

Keep-Alive Test Frequency (seconds)

(keepAliveTestFreq)

The Keep-Alive Test Frequency (seconds) parameter specifies the frequency, in seconds, of tests for the reestablishment of connectivity after connectivity is lost between peer IMEs. The range is 1 to 255. The default is 5.

Link Identifier

(frf12linkIdentifierName)

The Link Identifier parameter specifies the identifier for the FR bundle. The no form of this parameter resets the value to null. The range is 0 to 50 characters.

LMI Mode

(mode)

See the [LMI Mode](#) parameter in section 182.1.

LMI Type

(frDlcmiState)

See the [LMI Type](#) parameter in section 182.1.

Load Balance Algorithm

(loadBalanceAlgorithm)

See the [Load Balance Algorithm](#) parameter in section 182.1.

Local Channel ID

(displayedLocalChannelId)

The Local Channel ID parameter specifies a channel number on the port according to the port structure. The range is 1 to 28. Table 179-5 lists the valid values for different channel types.

Table 179-5 Local Channel ID parameter

Channel type	Valid values						
	STS192	STS48	STS3	STS1	DS3	DS1	DS0
SONET clear channel	1	1	1	—	1	—	—
SONET sub-channel	—	—	1 to 4	1 to 3	1	1 to 28	1 to 24
TDM	—	—	—	—	1	1 to 28	1 to 24

Local ECID

(localECID)

The Local ECID parameter specifies an identifier for the local CES circuit. The range is 0 to 65 535. The default is 0.

Local Port

(localPort)

The Local Port parameter specifies the port number for the local CES circuit. The range is 2000 to 65 535. The default is 2000.

Location ID Code

(channelMDLLicString)

The Location ID Code parameter specifies the LIC of the MDL. The range is 1 to 11 characters. The default is N/A.

Loop Respond

(channelFEACLoopRespond)

The Loop respond parameter specifies whether the associated DS3 interface can respond to remote loop signals. The DS3 far-end alarm and control signal can be used to send alarm or status information from the far-end terminal back to the local terminal. DS3 loopbacks at the far-end terminal are initiated from the local terminal. The options are:

- false (default)
- true

Loopback

(channelLoopback)

The Loopback parameter specifies a loopback mode for SONET, SDH, and TDM classes. Table 179-6 lists the parameter options.

Table 179-6 Loopback parameter

Option	Option Description	Dependencies
Line	Specifies a line loopback mode for the associated port or channel. Line loopback loops frames received on the corresponding port or channels back to the remote device.	Click on the Shut Down button to shut down the corresponding port or channel to enable loopback.
Internal	Specifies an internal loopback mode for the associated port or channel. Internal loopback loops the frames from the local device back to the framer.	
Remote	Specifies a remote loopback mode for the associated port or channel. This mode is not available for SONET at the port level.	
FDL ANSI	Specifies an FDL line loopback according to ANSI T1.403.	
FDL Bellcore	Specifies an FDL line loopback according to Bellcore TR-TSY-000312.	
Payload ANSI	Specifies a payload loopback using ANSI signaling.	
None	—	—

Max Jitter Expected (ms)

(maxJitter)

The Max Jitter Expected parameter specifies, in milliseconds, the initial delay introduced by the jitter buffer. The jitter-buffer delay varies depending on congestion and processing delays in the network.

As packets traverse the PSN, the delay varies from packet to packet. To accommodate this packet latency variation, the CES module uses a jitter buffer. The CES module supports a jitter buffer that can be sized according to the maximum packet latency variation expected for the network. The flexible buffer size helps prevent buffer underrun and overrun conditions. The range is 2 to 200. The default is 200.

MCFR Egress QoS Profile

(frf12EgressQOSProfPointer)

See the [MCFR Egress QoS Profile](#) parameter in section 182.1.

MDL Message Type

(channelMDLMessageType)

The MDL Message Type parameter specifies the:

- transmission method of a message over a channelized interface
- line message data link for a DS3

Table 179-7 lists the parameter options for the MDL message type.

Table 179-7 MDL Message Type parameter

Option	Option description	Dependencies
Disabled (default)	No MDL messages are transmitted	—
Test Signal	Specifies the MDL test signal message that contains a generator number.	—
DS3 Path	Specifies the MDL DS3 path message that contains a facility identification code.	C-bit framing must be used.
Idle Signal	Specifies the MDL idle signal message that contains a port number.	—

Table 179-8 lists the parameter options for the MDL message types listed in Table 179-7. The default for all message options is N/A.

Table 179-8 MDL message options

Option	Option description	Range	Dependencies
Port Number String	Specifies the port ID code	0 to 38 characters	—
Generator Number String	Specifies the generator number to send in the MDL test signal message	0 to 38 characters	
Equipment ID Code	Specifies the equipment ID code	0 to 10 characters	
Location ID Code	Specifies the location ID code	0 to 11 characters	
Frame ID Code	Specifies the frame ID code	0 to 10 characters	
Unit ID Code	Specifies the unit ID code	0 to 6 characters	
Facility ID Code	Specifies the facility ID code	0 to 38 characters	

Mode

See the [Mode](#) parameter in section 182.1.

Mode

(frf12Mode)

The Mode parameter specifies whether a channel uses FRF.12 UNI/NNI fragmentation. The options are:

- Enabled
- Disabled (default)

Monitored Events

(dceLmiMonitoredEvents)

See the [Monitored Events](#) parameter in section 182.1.

Monitored Events

(dteLmiMonitoredEvents)

See the [Monitored Events](#) parameter in section 182.1.

MTU (bytes)

See the [MTU \(bytes\)](#) parameter in section 182.1.

Network Queue Policy Name

(queueId)

Click on the Select button to list and choose a network queue policy.

Pattern

(bertPattern)

The Pattern parameter specifies the pattern that is used by the Bit Error Insertion Rate parameter. Table 179-9 lists the parameter options.

Table 179-9 Pattern parameter

Option	Option description	Dependencies
None	Specifies no pattern.	—
Ones	Specifies a repeating, all-ones pattern.	
Zeros	Specifies a repeating, all-zeros pattern.	
Alternating	Specifies a repeating pattern of ones and zeroes.	
2^3	Specifies a pseudo-random repeating pattern that is 8 bits long.	
2^9	Specifies a pseudo-random repeating pattern that is 512 bits long.	
2^15	Specifies a pseudo-random repeating pattern that is 32768 bits long.	
2^20	Specifies a pseudo-random repeating pattern that is 1048576 bits long.	

Payload Scrambling Enabled

(isPayloadScramblingEnabled)

The Payload Scrambling enabled parameter specifies whether payload scrambling is enabled. Scrambling randomizes the pattern of 1s and 0s carried in a SONET frame. Scrambling meets the needs of physical layer protocols that rely on sufficient transitions between 1s and 0s to maintain clocking. The options are:

- true
- false (default)

Payload Type

(payloadType)

The Payload Type parameter specifies the type of payload configured for the channel. The options are:

- Sonet Vt15 (Sdh Tu11)
- Sonet Vt2 (Sdh Tu12)
- Pdh Ds1
- Pdh Ds3
- Pdh E1 (for SDH framing only)

- Pdh E3 (for SDH framing only)
- Sdh Tug3 (for SDH framing only)

Period

(keepalivePeriod)

The Period parameter specifies the keep-alive timer. A keep-alive message is sent every time this time expires. The range is 1 to 60 s. The default is 10 s.

Polling Interval (seconds)

(dceLmiPollingInterval)

See the [Polling Interval \(seconds\)](#) parameter in section [182.1](#).

Polling Interval (seconds)

(dteLmiPollingInterval)

See the [Polling Interval \(seconds\)](#) parameter in section [182.1](#).

Port Number String

(channelMDLPortString)

The Port Number String parameter specifies the port number string sent in the MDL idle signal message. The range is 0 to 38 characters. The default is N/A.

Priority

(priority)

The Priority parameter specifies the VLAN priority for the packets on the circuit. The range is 0 to 7. The default is 1.

Protocol

(protocol)

The Protocol parameter specifies the type of protocol that the CES interface uses when generating packets for the PSN. Table [179-10](#) lists the parameter options.

Table 179-10 Protocol parameter

Option	Description
satop	An IP header is inserted in the packet. SAToP can only be used when the CES interface is configured for unstructured mode.

(1 of 2)

Option	Description
metro ethernet	A minimum-size header is used for the packets. This is bandwidth-efficient but the packets are not routable. Supported on structured and unstructured CES interfaces.
cesopsn	CESoPSN (Circuit Emulation Service over Packet Switched Network) - an IP header is inserted in the packet. CESoPSN can only be used when the CES interface is configured for structured mode.

(2 of 2)

Protocol Version

(requestedVersion)

The Protocol Version parameter specifies the ILMI protocol version used on the ILMI link. The [Administrative Status](#) parameter must be set to Disabled before the version can be changed. The options are:

- 4.0 (default)
- 3.1

Report Alarms

(reportAlarmBits)

The Report Alarms parameter specifies the TDM and SONET/SDH channel alarms to monitor and report. A check mark beside the alarm option enables the alarm to be logged. Table [179-11](#) lists the parameter options. The default is disabled.

Table 179-11 Report Alarms parameter

For	Option	Option description	Dependencies
SONET or SDH	Path Alarm unequipped path error	Reports path unequipped signal errors.	—
	Path Payload Mismatch	Reports a path payload mismatch, which causes the channel to be operationally down. When enabled, PPLM traps are raised but not cleared.	
	Path Loss of Pointer	Reports path loss of pointer errors for each tributary. When enabled, PLOP traps are raised but not cleared.	
	Path remote B3 error	Reports a path error condition raised as a result of B3 errors received from the node. When enabled, PREI traps are raised but not cleared.	
	Path Remote Defect Indication	Reports path remote defect indication errors. When enabled, PRDI alarms are raised and cleared.	
	Path Alarm Indication Signal	Reports path alarm indication signal errors. When enabled, PAIS alarms are raised and cleared.	
TDM	Far end wants the read end to loopback	Reports looped packets errors.	
	Out of frame	Reports out-of-frame errors. When enabled, OOF alarms are not raised or cleared.	
	Alarm Indication Signal	Reports alarm indication signal errors. When enabled, AIS alarms are not raised or cleared.	
	Resource Availability Indicator	Reports resource availability indicator events. When enabled, RAI alarms are not raised or cleared.	
	Loss of Signal	Reports loss of signal errors. When enabled, LOS traps are not raised or cleared.	

Reserved CBS%

See the [Reserved CBS%](#) parameter in section 182.1.

Restore Keep-Alive Defaults

Click on the Restore Keep-Alive Defaults button to restore the default values of the keep-alive parameters for the ILMI link.

Respond to Remote Loop Signal

(remoteLoopRespondConfig)

The Respond to Remote Loop Signal parameter specifies whether a channel responds to remote loop signals. The options are:

- True
- False (default)

Samples Aggregation

(samplesAggregation)

The Samples Aggregation parameter specifies the number of samples to aggregate in each outgoing PDU. The range is 2 to 39. The default is 2.

Scramble

(scramble)

The Scramble parameter enables payload scrambling on channel groups. The Scramble parameter is supported if the [Encap Type](#) parameter is ATM. The default is true.

Signal Mode

(signalMode)

The Signal Mode parameter specifies the type of signalling associated with the channel. The options are:

- None (default)
- CAS

Speed

See the [Speed](#) parameter in section [182.1](#).

STs1 Channel Payload Type

The STs1 Channel Payload Type parameter specifies the type of payload that is configured for the channel. The options are:

- SONET VT15 (SDH Tu11)
- PDH Ds3 (default)

Subrate CSU Mode

(subrateCSUMode)

The Subrate CSU Mode parameter configures the CSU compatibility mode to interoperate with existing DS3 subrate standards. The Subrate CSU Mode parameter applies only to non-channelized DS3s. Table [179-12](#) lists the parameter options.

Table 179-12 Subrate CSU Mode parameter

Option	Option description	Dependencies
Not Used (Default)	Disables the subrate functionality for the DS3 channel	—
Digital Link	Enables the Digital-Link (Quick Eagle) CSU compatibility mode for the DS3 channel	

Subrate Range

(subrateRange)

The Subrate Range parameter specifies the subrate value for the associated DS3. The Subrate Range parameter applies only to non-channelized DS3s. You can configure the parameter when the [Subrate CSU Mode](#) is set to the Digital Link option. The range is 1 to 147 Kb/s. The default is 1.

Time Slots

See the [Time Slots](#) parameter in section [182.1](#).

Time Slots per DS0 Channel Group

The Time Slots per DS0 Channel Group parameter specifies the timeslots from the selected TDM port to be assigned to the channel group. The range is 1 to 24 for DS1 channel groups or 1 to 31 for E1 channel groups. If you choose the option '0' for this parameter, no DS0 channel group is created.

For DS1 channel types, the maximum timeslots allowed are 24 (TS1-TS24). For E1 channel types, the maximum timeslots allowed are 31 (TS2-TS32). Depending on the TDM port selected, the 5620 SAM automatically creates the DS0 channel groups with the appropriate type of time slots.

Unit ID Code

(channelMDLUnitString)

The Unit ID Code parameter specifies the UIC of the MDL. The range is 0 to 6 characters. The default is N/A.

Up Count

(upCount)

The Up Count parameter specifies the number of continual keepalive packets that must be received to declare the link up. The nodes at the two endpoints of the cHDLc link should be provisioned with the same values. The range is 1 to 3. The default is 1.

Vt15 Channel Payload Type

The Vt15 Channel Payload Type parameter specifies the type of payload that is configured for the channel. The parameter appears only for OC3 or OC12 ASAP ports when the [Channel Type](#) parameter is set to SONET Sts1 (Sdh Au3) and the Sts1 Channel Payload Type parameter is set to SONET VT15 (SDH Tu11). The only option is PDH Ds1.

180 –Gateway parameters

180.1 Gateway parameters 180-2

180.1 Gateway parameters

This chapter describes the parameters on the 7750 MG Network Element property form, the child forms, and the forms opened from other contextual menu options for routers.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether the SGW or PGW instance is administratively enabled. The options are:

- Up (default)
- Down

Dynamic PCC

(pccDynamicState)

The Dynamic PCC parameter specifies if the gateway uses PCC rules sent from the PCRF during the creation of dedicated bearers. The options are:

- Disabled (default)
- Enabled

EPC ID

(epcId)

The EPC ID parameter assigns a unique ID to the SGW or PGW instance. The range is 1 to 8. The default is 0.

Group ID

(groupId)

The Group ID parameter assigns a unique group ID to the SGW or PGW instance. The group ID consists of three digits from 0 to 9. There is no default value.

Node ID

(nodeId)

The Node ID parameter assigns a unique node ID to the SGW or PGW instance. The node ID consists of three digits from 0 to 9. There is no default value.

181 –ISA-MG Group parameters

181.1 ISA-MG Group parameters 181-2

181.1 ISA-MG Group parameters

This chapter describes the parameters on the ISA-MG Group form, the child forms, and the forms opened from other contextual menu options for ISA-MG groups.

Group ID

(groupNumber)

The Group ID parameter specifies the identifier assigned to the ISA-MG group. The range is 1 to 8. The default is 0.

Redundancy Type

(groupRedundancy)

The Redundancy Type parameter specifies the ISA-MG group redundancy type. When the parameter is set to No Redundancy, the cards in this group are unprotected. When the parameter is set to oneToOne, each card has one backup card.

In Release 8.0 R1, the Redundancy Type parameter is not supported for the 7750 MG ISM mobile cards. The 5620 SAM GUI displays the default, read-only, value No Redundancy and cannot be changed.

For demonstration purposes, you can use the CLI to configure one-to-one redundancy for an 7750 MG member. The 5620 SAM resynchronises and displays One-to-one for the Redundancy Type parameter. The field remains read-only in the 5620 SAM GUI.

182 –Common equipment navigation tree parameters

182.1 Common equipment navigation tree parameters 182-2

182.1 Common equipment navigation tree parameters

This chapter describes the parameters that are common to the equipment navigation tree forms, and the child forms launched from the right-click contextual menu options.

Access Weight

Table 182-1 describes where to find information about the Access Weight parameter.

Table 182-1 Access Weight

For	See
Egress weight allocation for hybrid port	Access Weight in this section
Ingress weight allocation for hybrid port	Access Weight in this section

Access Weight

(egressAccessWeight)

The Access Weight parameter specifies the percentage of the port egress queue buffers that are allocated to access interface traffic on the hybrid port. The parameter is configurable when the [Mode](#) parameter is set to Hybrid. The range is 0 to 100. The default is 50.

Access Weight

(ingressAccessWeight)

The Access Weight parameter specifies the percentage of the port ingress queue buffers that are allocated to access interface traffic on the hybrid port. The parameter is configurable when the [Mode](#) parameter is set to Hybrid. The range is 0 to 100. The default is 50.

Accounting Enabled

(accounting)

The Accounting Enabled parameter specifies whether to enable accounting for the port or channel. The options are:

- Enabled
- Disabled (default)

When the parameter is enabled, accounting and statistics data is collected in the appropriate records file, and made available to 5620 SAM.

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled. The options are:

- Up (default)
- Down

Administrative Status

(adminStatus)

The Administrative Status parameter specifies whether 802.3ah functionality is enabled or disabled on the device. The options are:

- Disabled (default)
- Enabled

ATM Interface Cell Format

(atmInterfaceCellFormat)

The ATM Interface Cell Format parameter specifies the interface cell format. The options are:

- UNI (default)
- NNI

Auto-Assign ID

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

Commands

(protectionSwitchCommands)

The Commands parameter allows you to manually modify the protection state of a 9500 MPR card. Table [182-2](#) describes the parameter options.

Table 182-2 Commands parameter

Main card option	Spare card option	Description	Dependencies
None (default)	None (default)	The main card is active and the spare card is in standby. The 9500 MPR switches automatically from the main card to the spare when a failure occurs on the main card. The switch causes the main card to go into standby and the spare card becomes active. The Restoration Criteria parameter value determines whether the main card becomes active again automatically when the fault clears.	—
	Manual	You can initiate a manual switch from the spare card to the main card.	<ul style="list-style-type: none"> The Restoration Criteria parameter on the spare card must be set to Not Revertive The manual command is the lowest priority option and is performed only if there are no alarms that can activate an automatic switch The manual command cannot be performed when the Lockout or Forced commands are active The manual command fails when the main card is performing an automatic switch request The manual command is not supported by spare radio modem cards
	Lockout	You can prevent a spare card from providing protection for the main card. The Lockout command option has the highest priority of any commands option.	<ul style="list-style-type: none"> When the spare card is active and the command is applied, a forced switch back to the main card occurs A lockout command can be performed when the card has active alarms The None command option option can be used to remove the Lockout option
Manual	None	You can initiate a manual switch from the main card to the spare card.	<ul style="list-style-type: none"> The manual command option is the lowest priority option and is performed only if there are no alarms that can activate an automatic switch The manual command option cannot be performed if the lockout or forced commands are already activated When the manual command option is active it is canceled by an incoming alarm
	Lockout	Same behavior as None and Lockout	—
	Manual	Same behavior as None and Manual	<ul style="list-style-type: none"> Applies to radio modem and 32 x DS1/E1 cards
Forced	None	You can initiate or terminate a forced switch from the main card to the spare card.	<ul style="list-style-type: none"> The forced command option has higher priority than an automatic switch operation A lockout command can be performed when the card has active alarms
	Manual	Same behavior as None and Manual	Applies to all card types
	Lockout	Same behavior as None and Lockout	—

Table [182-3](#) lists the command option priorities.

Table 182-3 Commands option priorities

Command	Priority
Lockout	1
Forced	2
Automatic switch	3
Manual	4

Commands

(radioProtectionSwitchCommands)

The Commands parameter allows you to manually modify the protection state of a 9500 MPR radio port at the receiver end. The options for the port on the main card are:

- None (default)
- Manual
- Forced

The options for the port on the spare card are:

- None (default)
- Manual
- Lockout

Commands

(txProtectionSwitchCommands)

The Commands parameter allows you to manually modify the protection state of a 9500 MPR radio port at the transmitter end. The options for the port on the main card are:

- None (default)
- Manual
- Forced

The options for the port on the spare card are:

- None (default)
- Manual
- Lockout

Configured MAC

(macAddress)

The Configured Address parameter specifies the unicast MAC address or base chassis Ethernet MAC address that is configured for ports, LAGs, or BCP-enabled SONET channels.

Default VLAN

(vlan)

The Default VLAN parameter specifies a default VLAN for the port. The range is 1 to 4092. The default is 1.

Description

(description)

The Description parameter specifies a description for the object. The range is 0 to 80 characters, except as specified in Table 182-4.

Table 182-4 Description parameter

Object	Range (characters)
Dry contact sensor for 7250 SAS-ESA or 7210 SAS-M/7210 SAS-E	0 to 64
Port	0 to 160

The dry contact sensor feature is supported in 7210 SAS-M/7210 SAS-E version 2.0 or later.

DDM Event Suppression

(ddmEventSuppression)

The DDM Event Suppression parameter specifies whether the 5620 SAM raises an alarm when digital diagnostics monitoring thresholds are exceeded on ports on SFP and XFP optical modular transceivers. The thresholds for SFPs and XFPs are programmed by the transceiver manufacturer. The options are:

- Enabled
- Disabled (default)

Encap Type

(encapType)

The Encap Type parameter specifies the encapsulation type for a service on a port or channel. The appropriate type must be configured on the terminating channel. When a port is configured for access or network mode, the encapsulation type must be specified to differentiate the services on the port or channel. Table 182-5 lists the parameter options.

The encapsulation type for the 16 x channelized DS1/E1 ASAP daughter card cannot be changed after the DS0 channel group has been configured. The channel group must be deleted and reconfigured to change the encapsulation type.

Table 182-5 Encap Type parameter

For	Option	Option description	Dependencies
Ethernet access ports	Dot1 Q	Supports multiple services on the port and a default MTU size of 1518 bytes. The outer encapsulation ID, which is used to differentiate services, is the VLAN ID in the IEEE 802.1Q header.	—
	Q in Q	Supports multiple services on the port or channel. The inner and outer encapsulation IDs, which are used to differentiate services, are the VLAN IDs in the IEEE 802.1Q header.	—
	Null	Supports a single service on the port and has a default MTU size of 1514 bytes	No tags or labels are carried on the frames, so only one service can be configured on the port
Ethernet network ports	Dot1 Q	Supports multiple services on the port and up to 9212 bytes for the MTU size	—
	Null	Supports a single service on the port	—
SONET/SDH network ports	PPP Auto	Support VLAN tagged frames, and these tagged frames are allowed into the SONET path.	—

(1 of 2)

For	Option	Option description	Dependencies
SONET, SDH, or TDM access ports or channels	BCP Null	Supports a single service on the POS port or channel. This option is used to bridge a service between two devices using PPP over SONET, SDH, or TDM. The encapsulation ID is always 0.	BCP is used on the SONET path as the network control protocol.
	BCP Dot1 Q	Supports multiple services on the port or channel. This option is used to bridge multiple services between two devices using PPP over SONET, SDH, or TDM. The outer encapsulation ID, which is used to differentiate services, is the VLAN ID in the IEEE 802.1Q header in the BCP-encapsulated frame.	—
	IPCP	Supports one IP service on the port or channel. This option is typically used for device interconnection using PPP.	ICPC is used as the network control protocol, instead of BCP. IPCP encapsulation cannot be configured on DS0 channel groups whose containing DS1/E1 channel is configured for either Unframed mode or Adaptive clock source.
	FR	Supports multiple services using the DLCI header	—
	ATM	Supports the encapsulation of ATM cells within SONET/SDH frames	—
	WAN Mirror	Supports mirroring of frame relay and POS ports. No link management protocol runs on these ports.	—
	Cisco HDLC	Supports Cisco HDLC data encapsulation on synchronous serial links using frame characters and checksums. You can only configure Cisco HDLC on IES SAPs.	—
	CEM	Supports SONET, SDH, and TDM circuit emulation services	—
LAGs	Null	Supports a single service on the POS port	—
	Dot 1Q	Supports multiple services on the port	—

(2 of 2)

Error Threshold

Table 182-6 lists where to find more information about the Error Threshold parameter.

Table 182-6 Error Threshold parameter

Parameter	See
Error Threshold for DCE LMI	Error Threshold parameter in this section
Error Threshold for DTE LMI	Error Threshold parameter in this section

Error Threshold

(dceLmiErrorThreshold)

The Error Threshold parameter specifies, for a DCE LMI, the number of errors necessary to place the Frame Relay LMI link operationally down. The parameter is configurable when the LMI Mode parameter is set to DCE. The range is 1 to 4. The default is 3.

Error Threshold

(dteLmiErrorThreshold)

The Error Threshold parameter specifies, for a DTE LMI, the number of errors necessary to place the Frame Relay LMI link operationally down. The parameter is configurable when the LMI Mode parameter is set to DTE. The range is 1 to 4. The default is 3.

Full Enquiry Interval

(dteLmiFullEnquiryInterval)

The Full Enquiry Interval parameter specifies the full status polling interval for the Frame Relay LMI link. For example, when the parameter is set to 10, ten exchanges are completed between the DTE and DCE before a full status report is expected. The parameter is configurable when the LMI Mode parameter is set to DTE. The range is 1 to 255. The default is 6. When the parameter is set to 1, the DTE always expects full status messages from the DCE.

LMI Mode

(mode)

The LMI Mode parameter specifies the mode of the interface configured for Frame Relay. The options are:

- DTE (default)
- DCE
- Bi-Directional

Bidirectional LMI on a FR NNI link allows FR networks to peer with one another. Each end of the FR link acts as both a DTE and DCE device. The LMI Mode parameter can be set to Bi-Directional when the [LMI Type](#) parameter is set to ANSI or ITU.

LMI Type

(frDlcmiState)

The LMI Type parameter specifies the type of interface configured for Frame Relay. The options are:

- none
- rev1
- ANSI (default for DS1 channels)
- ITU (default for E1 channels)

Set the parameter to none to disable Frame Relay LMI. Set the parameter to ITU to use ITU standard Q933 annex A LMI specification. Set the parameter to ANSI to use ANSI standard T1.167 annex D LMI specification. Set the parameter to rev1 to use Rev 1 version of the ANSI standard T1.167 annex D LMI specification.

Load Balance Algorithm

(loadBalanceAlgorithm)

The Load Balance Algorithm parameter specifies the load balancing algorithm used for the port or channel. Table 182-7 lists the parameter options.

Table 182-7 Load Balance Algorithm parameter

Option	Option description	Dependencies
Include L4	Includes Layer 4 source and destination port values in the hashing algorithm	—
Exclude L4	Excludes Layer 4 source and destination port values in the hashing algorithm	—
Default (default)	Inherits the global settings. The value is not applicable for ports that do not pass any traffic	Default for 7750 SR and 7450 ESS
unspecified (default)	—	Default for 7710 SR

Log-history

(clearLogs)

The Log-history parameter defines the global clear event logs control for 802.3ah OAM functionality.

- Default (default)
- Reset

MCFR Egress QoS Profile

(frf12EgressQOSProfPointer)

The MCFR Egress QoS Profile specifies the profile to be used by an FRF.12 link with UNI/NNI fragmentation enabled. Click on the Select button to choose a profile from the list of MCFR egress QoS profiles.

Mode

(mode)

The Mode parameter specifies the mode for a port. Table 182-8 lists the parameter options.

Table 182-8 Mode parameter

For	Option	Option description
Ethernet SONET clear channel SONET channelized TDM channel LAGs L2 Uplink	Access	Specifies the port or channel for service access. An access port or channel is used for customer-facing traffic on which services are configured. SAPs can only use an access port or channel. When a port or channel is configured for access mode, the appropriate Encapsulation Type parameter must be specified to differentiate the services on the port or channel. If you change the access mode to hybrid mode and SAPs are configured, you can migrate the SAPs. See Procedure 17-3 for more information.
Ethernet SONET clear channel LAGs	Network	Configures the port or channel for transport network use. The network port or channel participates in the service provider transport or infrastructure network. For a 7250 SAS or Telco device, when you configure the mode as network, the ports are automatically made into uplinks for a VLAN and are added as tagged SAPs of the VLAN. When a port or channel is configured for Network mode, the Encap Type can be set to either Null or Dot1 Q.
Ethernet ports	Hybrid	Configures the port or channel for simultaneous service and transport network use. Hybrid ports do not support null encapsulation. The option is available only for ports in a Release 8.0 or later 7450 ESS, 7750 SR-7, 7750 SR-12, or 7750 SR-c12. The option is not available for the 7450 ESS-1 and 7750 SR-1 chassis types. If you change the access mode to hybrid mode and SAPs are configured, you can migrate the SAPs. See Procedure 17-3 for more information.

Monitored Events

Table 182-9 lists where to find more information about the Monitored Events parameter.

Table 182-9 Monitored Events parameter

Parameter	See
Monitored Events for DCE LMI	Monitored Events parameter in this section
Monitored Events for DTE LMI	Monitored Events parameter in this section

Monitored Events

(dceLmiMonitoredEvents)

The Monitored Events parameter specifies the event count for the Frame Relay LMI link. The event count is used to verify link integrity. When the number of events exceeds the configured value, the link is considered down, and is placed in an operationally down state. The parameter is configurable when the LMI Mode parameter is set to DCE. The range is 1 to 10. The default is 4. The parameter value must be larger than or equal to the Error Threshold parameter.

Monitored Events

(dteLmiMonitoredEvents)

The Monitored Events parameter specifies the event count for the Frame Relay LMI link. The event count is used to verify link integrity. When the number of events exceeds the configured value, the link is considered down, and is placed in an operationally down state. The parameter is configurable when the LMI Mode parameter is set to DCE. The range is 1 to 10. The default is 4. The parameter value must be larger than or equal to the Error Threshold parameter.

MTU (bytes)

(mtuValue)

The MTU (bytes) parameter specifies the default MTU size for a port. This is the size of the largest packet that can be sent or received on the physical interface — a port, SONET/SDH clear channel, or a TDM channel. The parameter is configured at the connection termination endpoint.

Service MTU values must be less than or equal to the service tunnel MTU. Service MTU values must be less than or equal to the access port MTU. The range is 512 to 4470 (512 to 2106 for the 7705 SAR). See the specific device documentation for more information about MTU size considerations.

Specifying a MTU value of 0 for the 7750 SR, 7710 SR, or 7705 SAR sets the MTU to the default value.

Table [182-10](#) lists the parameter options.

Table 182-10 MTU (bytes) parameter

For	Mode	Type	Default MTU size (bytes)
Ethernet port	Network	—	2106 (7705 SAR)
	Access	Null	1514
		Dot1 Q	1518
Fast Ethernet	Network	—	1514 2106 (7705 SAR)
Other Ethernet	Access	—	2106 (7705 SAR)
	Network	—	9212 2106 (7705 SAR)

(1 of 2)

For	Mode	Type	Default MTU size (bytes)
SONET/SDH clear channel	Access	BCP Null	1522
		BCP Dot1 Q	1526
		IPCP	1502
		FR	1578
		ATM	1524
		CEM	1578
	Network	PPP Auto	1578 2090 (7705 SAR)
TDM channel	Access	BCP Null	1518 2090 (7705 SAR)
		BCP Dot1 Q	1522
		IPCP	1502
		FR	1578
		ATM	1524 1524 (7705 SAR)
		CEM	1572 (7705 SAR)
	Network	PPP Auto	2090 (7705 SAR)
IMA bundles	—	—	2090 (7705 SAR)

(2 of 2)

The Ethernet port-level MTU parameter value indirectly defines the largest physical packet that the port can transmit or the far-end Ethernet port can receive. Packets received that are larger than the MTU are discarded. Packets that cannot be fragmented at egress and exceed the MTU are discarded.

The parameters specified for MTU configuration include the destination MAC address, source MAC address, Ethernet encapsulation type, length field, and the complete Ethernet payload. SONET channels use the MTU value to define the largest point-to-point payload that a SONET frame can contain. A major difference between channel and Ethernet physical MTU values is in what overhead is considered part of the framing method and what overhead is considered to be part of the application using the frame.

The MTU value is associated with the [Mode](#) and [Encap Type](#) parameter values for a port. If you change one of these values for a port, the 5620 SAM adjusts the port MTU value to a default value. You can configure the 5620 SAM to retain the current MTU value for ports rather than revert to the default. See “[MTU size and port configuration](#)” in chapter 17 for more information.

Multiple PDU Count

(multiplePduCount)

The Multiple PDU Count parameter is used to set the number of PDUs that will be sent when OAM needs to send multiple event notification PDUs. The range is 1 to 10. The default is 3.

Network Weight

Table 182-11 describes where to find information about the Network Weight parameter.

Table 182-11 Network Weight

For	See
Egress weight allocation for hybrid port	Network Weight in this section
Ingress weight allocation for hybrid port	Network Weight in this section

Network Weight

(egressNetworkWeight)

The Network Weight parameter specifies the percentage of the port egress queue buffers that are allocated to network interface traffic on the hybrid port. The parameter is configurable when the [Mode](#) parameter is set to Hybrid. The range is 0 to 100. The default is 50.

Network Weight

(ingressNetworkWeight)

The Network Weight parameter specifies the percentage of the port ingress queue buffers that are allocated to network interface traffic on the hybrid port. The parameter is configurable when the [Mode](#) parameter is set to Hybrid. The range is 0 to 100. The default is 50.

OLC State

(olcState)

The OLC State parameter specifies whether an object or service is in-service or maintenance to filter alarms in the Alarms Window. Alarms are generated for objects and services regardless of the OLC State parameter setting. The parameter setting is not sent to the objects or services.

You can set the OLC state for the following objects and services:

- network element
- card slot
- daughter card
- port
- composite service
- service
- site
- LAG
- SAPs (L2 access interfaces and L3 access interfaces)

See the chapter 26 in the *5620 SAM User Guide* for more information about the OLC.

Table 182-12 describes the options.

Table 182-12 OLC State parameter

Option	Option description	Default
Maintenance	For objects and services that are in maintenance	The default is Maintenance for services. The default value for objects can be specified in the discovery rules.
In Service	For objects and services that are in service	The default is In Service for objects. The default value for services can be specified using the nms-server.xml file.

Polling Interval

Table 182-13 lists where to find more information about the Polling Interval parameter.

Table 182-13 Polling Interval parameter

Parameter	See
Polling Interval for DCE LMI	Polling Interval (seconds) parameter in this section
Polling Interval for DTE LMI	Polling Interval (seconds) parameter in this section

Polling Interval (seconds)

(dceLmiPollingInterval)

The Polling Interval (seconds) parameter specifies, in seconds, how often the Frame Relay DCE LMI link checks for a keepalive response from the DTE. The parameter is configurable when the LMI Mode parameter is set to DCE. The range is 5 to 30. The default is 15.

Polling Interval (seconds)

(dteLmiPollingInterval)

The Polling Interval (seconds) parameter specifies, in seconds, how often the Frame Relay DTE LMI link sends out a keepalive response request to the DCE. The parameter is configurable when the LMI Mode parameter is set to DTE. The range is 5 to 30. The default is 10.

Reserved CBS%

(reservedCbs)

The Reserved CBS% parameter specifies the percentage of buffer space that is reserved for committed traffic. The range is 0 to 100, or Default. The default is -1, which specifies that the pool size should be computed as a fair weight between all pools.

Restoration Criteria

(**protectionRestorationCriteria**)

The Restoration Criteria parameter specifies whether an active card that has failed automatically becomes active again when the failure is corrected. The options are:

- Revertive (default)
- Not Revertive

Restoration Criteria

(**radioProtectionRestorationCriteria**)

The Restoration Criteria parameter specifies whether an active radio card, at the receiver end, that has failed automatically becomes active again when the failure is corrected. The options are:

- Revertive (default)
- Not Revertive

Restoration Criteria

(**txProtectionRestorationCriteria**)

The Restoration Criteria parameter specifies whether an active radio card, at the transmitter end, that has failed automatically becomes active again when the failure is corrected. The options are:

- Revertive (default)
- Not Revertive

Speed

(**speed**)

The Speed parameter specifies the speed of the port or channel. To change the port speed on a SONET/SDH port the port must be administratively shut down and all channels must be removed, when the port speed is changed the default channel configuration is recreated. Table [182-14](#) lists the parameter options.

Table 182-14 Speed parameter

For	Option	Option description	Dependencies
SONET Ethernet TDM	Line Rate	Port speed at the full capacity of the equipment	Cannot choose this option if the Auto-negotiate parameter is set to enabled.
SONET	OC3	Port speed for an OC-3 MDA	
	OC12	Port speed of an OC-12 MDA. The speed can be OC-3 or OC-12. Each port can have a different speed.	
	OC48	Port speed for an OC-48 MDA	
	OC192	Port speed for an OC-192 MDA	
	OC 768	Port speed for an OC-768 MDA	
Ethernet	10	Port speed of a Fast Ethernet (100Base-T), Gigabit Ethernet (1000Base-T), or 10 Gigabit Ethernet (10GBase-X) port in Mb/s. You cannot configure the speed for LAG ports. Ports in a LAG are set at 100. Max100 and Max1000 set the maximum port speed to 100Mbps and 1000 Mbs respectively.	
	100		
	1000		
	10000		
	Auto Speed		
	Max100		
	Max1000		
TDM	56 kbit/s	—	
	64 kbit/s	Port speed for an OC-12 MDA that carries SONET STS-1 sub-channels. The sub-channel connection termination point is a TDM DS0 that operates at 64 kb/s.	

Telnet Session button

Click on the Telnet Session button to open a Telnet session with the route. You can use the Telnet session to communicate directly with the managed objects.

Statistics

(clearStats)

The Statistics parameter defines the global clear statistics control for 802.3ah OAM functionality. The options are:

- Default (default)
- Reset

Time Slots

(timeSlotBits)

The Time Slots parameter specifies the DS0 channel to be used for TDM channelized services. The range is TS1 to TS24. The Time Slots parameter specifies the time slots from the selected TDM port to be assigned to the channel group. Select from the Time Slots list which time slots from the frame to include in the channel group.

OSPF navigation tree parameters

183 — OSPF navigation tree parameters

183 –OSPF navigation tree parameters

183.1 OSPF navigation tree parameters 183-2

183.1 OSPF navigation tree parameters

The parameters that you can configure from the OSPF navigation tree and from the OSPF icon on the network navigation tree are the same. See the chapter [200](#) for descriptions of the parameters on the OSPF navigation tree, its child forms, and forms launched from other right-click contextual menu options.

IS-IS navigation tree parameters

184 — IS-IS navigation tree parameters

184 –IS-IS navigation tree parameters

184.1 IS-IS navigation tree parameters 184-2

184.1 IS-IS navigation tree parameters

The parameters that you can configure from the IS-IS navigation tree and from the IS-IS icon on the network navigation tree are the same. See the chapter [199](#) for descriptions of the parameters on the IS-IS navigation tree, its child forms, and forms launched from other right-click contextual menu options.

Routing navigation tree parameters

- 185 – NE parameters
- 186 – Routing Instance parameters
- 187 – Bridge Instance parameters
- 188 – Interface parameters
- 189 – BGP parameters
- 190 – IGMP parameters
- 191 – L2TP parameters
- 192 – LDP parameters
- 193 – MLD parameters
- 194 – MPLS parameters
- 195 – MSDP parameters
- 196 – PIM parameters
- 197 – RIP parameters
- 198 – RSVP parameters
- 199 – IS-IS parameters
- 200 – OSPF parameters

201 – Network Domain parameters

202 – Static Routes parameters

203 – Common network navigation tree parameters

185 –NE parameters

185.1 NE parameters 185-2

185.1 NE parameters

The configurable NE parameters in the Routing and Equipment navigation tree views are the same. See the chapter [162](#) for descriptions of the configurable parameters on the Network Element form and the forms opened using the NE contextual menu options.

186 –Routing Instance parameters

186.1 Routing Instance parameters 186-2

186.1 Routing Instance parameters

This chapter describes the parameters on the Routing Instance form, and the child forms launched from the right-click contextual menu options for routing instances.

Action

See the [Action](#) parameter in section 203.1.

Action

See the [Action](#) parameter in section 14.1.

Action

(dhcpSnoopingBindingDatabaseAction)

The Action parameter specifies the action performed on the DHCP snooping binding table information stored in the switch memory. Table 186-1 describes the parameter options.

Table 186-1 Action parameter

Options	Option description	Dependencies
No Action (default)	—	—
Purge	Clears all binding table entries in the switch memory	—
Renew	Populates the binding table stored in memory with the binding table contents stored in the dhcpBinding.db file in the /flash/switch directory	—

Address

(dsliteAddress)

The Address parameter specifies the Dual Stack Lite address. Specify an IPv6 address in colon-hexadecimal format. There is no default.

Administrative State

Table 186-2 describes where to find information about the Administrative State parameter.

Table 186-2 Administrative State parameter

Parameter	See
Administrative State for NAT address pool or NAT static port forwarding	Administrative State in this section

(1 of 2)

Parameter	See
Administrative State for other objects	Administrative State in section 203.1

(2 of 2)

Administrative State

(**administrativeState**)

See the [Administrative State](#) parameter in section 203.1.

Administrative State

(**adminState**)

The Administrative State parameter specifies the administrative state of the NAT address pool or static port forwarding function. The options are:

- Out Of Service (default)
- In Service

Admin Link Local Address

(**adminLinkLocalAddr**)

The Admin Link Local Address parameter specifies the IPv6 VRRP administration address to be used as the Link Local Address. The Link Local Address on the parent interface has to be configured as one of the backup addresses (on same subnet) for the IPv6 VRRP instance. It is enabled by setting the Admin Link Local Address and the IPv6 Allowed parameters to enabled.

Specify an IPv6 address in colon-hexadecimal format. There is no default.

Admin Link Local Address Preferred

(**adminLinkLclAddrPreferred**)

The Admin Link Local Address Preferred parameter specifies whether to use the Admin Link Local Address as the Link Local Address for the IPv6 VRRP instance. The options are:

- enabled
- disabled (default)

AFTR Address

(**ipv6AftrAddress**)

The AFTR Address parameter specifies the AFTR address of the DS Lite tunnel. This parameter is configurable when the [Type](#) parameter is set to a value of DS Lite. Specify an IPv6 address in colon-hexadecimal format. There is no default.

Aggregator

(aggregator)

The Aggregator parameter specifies the use of a BGP aggregator. The aggregator is the BGP router that initially aggregates the currently advertised route. The options are:

- True
- False (default)

Aggregator AS

(aggregatorAS)

The Aggregator AS parameter specifies a a number identifier for the BGP aggregator. The range is 0 to 4294967295. The default is 0.

Aggregator IP Address

(aggregatorIPAddress)

The Aggregator IP Address parameter specifies a BGP aggregator IP address. The default is 0.0.0.0.

Allow Directed Broadcasts

See the [Allow Directed Broadcasts](#) parameter in section [203.1](#).

Allow Send Force Renews

(allowSendForceRenews)

The Allow Send Force Renews parameter specifies whether the server is allowed to send a DHCP force renew message to DHCP clients. When the value is set to true, the server sends a force renew message to DHCP clients, when the server detects configuration changes that affect lease configuration. The client must renew their lease to receive the new parameter. The options are:

- True
- False (default)

As Set

(asSet)

The As Set parameter specifies the BGP generation of autonomous system set path information. The options are:

- True
- False (default)

Auto-Assign

(id)

The Auto-Assign parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

Autonomous Address Configuration

(autonomous)

The Autonomous Address Configuration parameter specifies whether the routing prefix is used for stateless auto configuration. The options are:

- true (default)
- false

Autonomous System

(autonomousSystemNumber)

The Autonomous System parameter specifies the AS number for the device. A device can only belong to one AS. An AS number is a globally unique number with an AS. This number is used to exchange exterior routing information with neighboring ASs and as an identifier of the AS itself. The range is 0 to 4294967295. The default is 0.

B4 Address

(ipv6B4Address)

The B4 Address parameter specifies the B4 address of the DS Lite tunnel. This parameter is configurable when the [Type](#) parameter is set to a value of DS Lite. Specify an IPv6 address in colon-hexadecimal format. There is no default.

Binding Database Mode

(dhcpSnoopingBinding)

The Binding Database Mode parameter specifies whether the DHCP snooping binding table is functional. The binding table is automatically enabled when DHCP snooping is enabled on the switch or a VLAN. This table is used by DHCP snooping to filter DHCP traffic that is received on untrusted ports. You cannot enable the binding table unless the DHCP snooping is enabled. The options are:

- Disabled (default)
- Enabled

Binding Persistency

(dhcpSnoopingBindingPersistencyStatus)

The Binding Persistency parameter is associated with the DHCP snooping binding persistency check status. When the parameter is enabled, the binding entries expiry depends solely on lease time. The default is disabled. Binding persistency is supported on OmniSwitch NEs for Release 6.4.2 or later.

BGP Enabled

(bgpEnabled)

The BGP Enabled parameter specifies whether BGP is enabled for the device. Table 186-3 describes the parameter options.

Table 186-3 BGP Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that BGP routing is enabled on the device	The Autonomous System parameter must be set from the Routing tab button on the Routing Instance form.
Disabled (default)	Specifies that BGP routing is disabled on the device	—

Broadcast

See the [Broadcast](#) parameter in section 203.1.

Broadcast Address Format

See the [Broadcast Address Format](#) parameter in section 203.1.

Bypass Option-82 Check

(dhcpSnoopingBypassOpt82Check)

The Bypass Option-82 Check parameter specifies whether DHCP packets ingressing on untrusted ports are checked for the presence of an Option-82 field. When the parameter is enabled, DHCP packets ingressing on untrusted ports are not checked, the Option-82 field is ignored, and all DHCP packets are processed. The parameter can only be configured when DHCP snooping is enabled globally for the switch or at the VLAN level. Disable this parameter to allow untrusted ports to receive and process DHCP packets that already contain the Option-82 data field. The options are:

- Disabled (default)
- Enabled

Cflowd Type

See the [Cflowd Type](#) parameter in section 203.1.

Circuit ID

See the [Circuit ID](#) parameter in section 14.1.

Class

See the [Class](#) parameter in section 203.1.

Confederation Autonomous System

([confederationAutonomousSystemNumber](#))

The Confederation Autonomous System parameter specifies a confederation ID to reduce the IBGP mesh inside an AS. The range is 0 to 4294967295. The default is 0.

An AS can be logically divided into smaller groupings called subconfederations. To create this division, you can use the parameter to assign the confederation ID. Each subconfederation has fully meshed IBGP and connections to other ASs outside of the confederation.

Configured Primary Status

([configPrimaryStatus](#))

The Configured Primary Status parameter specifies whether the IP interface is the primary interface for the VLAN. The options are:

- True
- False (default)

Copy To Option 43

([copy82](#))

The Copy To Option 43 parameter specifies whether the content of option 82 will be copied to option 43 when the option 82 field is stripped. The options are:

- False (default)
- True

Current Hop Limit

([currentHopLimit](#))

The Current Hop Limit parameter specifies the hop limit value that the interface includes in router advertisement messages. The interface informs the nodes on the subnet about the hop limit when it sends IPv6 packets. The range is 0 to 255. The default is 64. A value of zero means that the interface includes no hop limit value in a router advertisement message.

Days

(days)

The Days parameter specifies the number of days for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 3650. The default is 0.

Table 186-4 lists and describes the [Option](#) parameter values that require a time specification.

Table 186-4 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCP OFFER response, the DHCP server uses this option to specify the offered lease time.
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

Days

(leaseHoldTimeDay)

The Days parameter specifies the minimum number of days that a leased IPv6 prefix is valid. The range is 0 to 3650. The default is 0.

Days

(maxLeaseDay)

The Days parameter specifies the maximum number of days that a leased IP address is valid. The range is 0 to 3650. The default is 10.

Days

(minLeaseDay)

The Days parameter specifies the minimum number of days that a leased IP address is valid. The range is 0 to 3650. The default is 0.

Days

(preferredLifeTimeDay)

The Days parameter specifies the minimum number of days that an assigned IP prefix is valid. The range is 0 to 3650. The default is 0.

Days**(rebindTimerDay)**

The Days parameter specifies the number of days between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 14. The default is 0.

Days**(renewTimerDay)**

The Days parameter specifies the number of days between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 7. The default is 0.

Days**(validLifeTimeDay)**

The Days parameter specifies the minimum number of days that an assigned IP prefix is valid. The range is 0 to 3650. The default is 1.

Description

See the [Description](#) parameter in section [203.1](#).

DHCP Snooping Mode**(dhcpSnooping)**

The DHCP Snooping Mode parameter specifies whether DHCP snooping is enabled on the switch. You cannot enable DHCP snooping if the DHCP Option-82 feature is enabled, these two features are mutually exclusive. Table [186-5](#) describes the parameter options.

Table 186-5 DHCP Snooping Mode parameter

Option	Option description	Dependencies
Disabled (default)	—	—
Switch Level	Enables DHCP snooping at the switch level.	When DHCP snooping is enabled at the switch level, the MAC Address Verification , Option-82 Data Insertion , and Binding Database Mode parameters are also enabled. In addition, the trust mode for all ports is set to the DHCP client only mode. If DHCP snooping is enabled at the switch level, you cannot enable it per-VLAN.
VLAN Level	Enables DHCP snooping on a per-VLAN basis.	When DHCP snooping is enabled at the VLAN level, the VLAN Level MAC Address Verification and VLAN Level Option-82 Data Insertion parameters are enabled on the VLAN. If DHCP snooping is enabled per-VLAN you cannot enable it at the switch level.

Displayed Name

(displayedName)

The Displayed Name parameter specifies the name for the created object. The range is 1 to 32.

Dot1p

(dot1p)

The Dot1p parameter specifies the forwarding class-to-IEEE 802.1p mapping for 802.1Q or 802.1P encapsulated packets that egress the access interface which uses the access egress policy. When a packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the IEEE 802.1p value specified by the Dot1p parameter. The range is 0 to 7, or default. The default is default. Specifying 0 is equivalent to removing the explicit marking.

DSCP

(dscp)

The DSCP parameter specifies the DiffServ Code Point value to be used as the match criterion for mapping packets to a forwarding class and enqueueing priority. The mapping is applied to packets that ingress the access interface to which the access ingress policy is applied.

When a packet is marked with the value specified by the DSCP parameter, the packet is mapped to the forwarding class specified by the Forwarding Class parameter and the priority specified by the Priority parameter. Table 186-6 lists the parameter options.

Table 186-6 DSCP parameter

Options			
be (default)	ef	nc1	nc2
cp1	cp2	cp3	cp4
cp5	cp6	cp7	cp9
cp11	cp13	cp15	cp17
cp19	cp21	cp23	cp25
cp27	cp29	cp31	cp33
cp35	cp37	cp39	cp41
cp42	cp43	cp44	cp45
cp47	cp49	cp50	cp51
cp52	cp53	cp54	cp55
cp57	cp58	cp59	cp60
cp61	cp62	cp63	cs1

(1 of 2)

Options			
cs2	cs3	cs4	cs5
af11	af12	af13	af21
af22	af23	af31	af32
af33	af41	af42	af43

(2 of 2)

DS Lite

(dsliteAdminState)

The DS Lite parameter specifies whether or not DS Lite is enabled on the routing instance. The options are:

- In Service
- Out of Service (default)

Egress Filter ID

See the [Egress Filter ID](#) parameter in section 203.1.

Enable DHCP Relay

See the [Enable DHCP Relay](#) parameter in section 203.1.

Enable Forwarding

(enableForwarding)

The Enable Forwarding parameter specifies whether the forwarding of IP frames to other subnets is enabled. The options are:

- True
- False (default)

Encap Type

(encapsulationType)

The Encap Type parameter specifies the encapsulation type that is allowed on the interface. The options are:

- Ethernet2 (default)
- SNAP

Enforce Maximum Number Of Multicast Routes

(enforceMaxNumberOfMcastRoutes)

The Enforce Maximum Number Of Multicast Routes parameter specifies whether to enforce a maximum number of multicast routes on an interface when you configure routing properties for a service. The options are:

- Enabled
- Disabled (default)

End Address

(endAddress)

The End Address parameter specifies the last IP address for a range of IP addresses to be configured for a subnetwork. You must also set the [Start Address](#) parameter. The default is 0.0.0.0.

EUI-64

(isEui64Address)

The EUI-64 parameter specifies whether to use an EUI-64 address. The options are:

- Enabled
- Disabled (default)

Exclusive

(isExclusive)

The Exclusive parameter specifies whether to allow the creation of an IP address range reserved for IESs or VPLSs. This provides a mechanism to reserve one or more address ranges for services. When this parameter is enabled, the configured IP addresses and subnet masks are exclusively used for services and cannot be assigned to network ports. The options are:

- Enabled
- Disabled (default)

Exported Address Prefix

(exportAddrPrefix)

The Exported Address Prefix parameter specifies the IP address of the prefix to be exported. While the export prefix is configured and the poll is active, the system exports this prefix in the realm of the virtual router instance associated with this pool. To the NAT redundancy peer, the presence of this prefix is an indication that the Large Scale NAT function in this virtual router instance is active. Therefore, the export prefix of this system is the monitor prefix of the peer. The export prefix must be different from the monitor prefix. The default is 0.0.0.0.

Forwarding Address

(udpForwAddr)

The Forwarding Address parameter specifies the DHCP Relay forwarding address. Specify an IPv4 address in dotted-decimal format.

Forwarding Class

(forwardingClass)

The Forwarding Class parameter specifies the forwarding class value to be used as the match criterion for mapping packets that egress the access interface which uses the policy to a queue and Dot1p value. When a packet is marked with the forwarding class specified by the Forwarding Class parameter, the packet is mapped to the queue specified by the Queue ID parameter, and the Dot1p value specified by the dot1p parameter. The options are:

- be (default)
- l2
- af
- h2
- h1
- nc
- l1

Forwarding Delay (seconds)

(forwDelay)

The Forward Delay (seconds) parameter specifies the amount of time that a VLAN port remains in the listening and learning states while the port is transitioning to a forwarding state. When a topology change occurs, the forward delay value is also used to age all dynamically learned MAC addresses in the MAC address forwarding table. The range is 0 to 65535. The default is 3, for all OmniSwitch NEs, except for OS 9700E and OS 9800E NEs, where the default is 2.

Forwarding Option

(forwardOption)

The Forwarding Option parameter specifies the DHCP Relay forwarding mode. Table 186-7 describes the parameter options.

Table 186-7 Forwarding Option parameter

Options	Options description	Dependencies
Standard (default)	All DHCP packets are processed by a global relay service.	You must specify at least one DHCP server IP address to enable a BOOTP/DHCP relay service.
AVLAN Only	Only DHCP packets received on authenticated VLAN ports from non-authenticated clients are processed by the DHCP relay service.	—

(1 of 2)

Options	Options description	Dependencies
Per-Vlan Only	Only DHCP packets received from a specific VLAN are processed by the DHCP relay service. Each VLAN can have a separate DHCP relay service.	You must specify at least one DHCP server IP address for each VLAN that requests a BOOTP/DHCP relay service. The standard relay service is not available.

(2 of 2)

Free Addresses Minimum Threshold

(minFree)

The Free Addresses Minimum Threshold parameter specifies the minimum number of available IP addresses for a specific subnetwork. These IP addresses can be offered to DHCP clients belonging to the subnetwork. When the value is set to 0, there is no minimum specified. The range is 0 to 255. The default is 1.

High Watermark

(watermarkHigh)

The High Watermark parameter specifies the percentage of used NAT-pool port blocks above which the 5620 SAM raises an alarm. The alarm clears when the port usage drops below the [Low Watermark](#) value. The parameter value must be higher than the [Low Watermark](#) value, unless both parameters are set to 0. The range is 0 to 100. The default is 0.

Hold Time (seconds)

(holdTime)

The Hold Time (seconds) parameter specifies how many seconds label information learned from the alternate router should be kept after that peer goes down. It is only displayed and applicable when the Interface Type parameter is set to Secondary. This timer should be set to a value large enough for the network to detect the failure and complete the reconvergence process. The range is 1 to 65535. The default is 30.

Hours

(hours)

The Hours parameter specifies the number of hours for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 23. The default is 0.

Table [186-8](#) lists and describes the [Option](#) parameter values that require a time specification.

Table 186-8 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCPPOFFER response, the DHCP server uses this option to specify the offered lease time.
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

Hours

(leaseHoldTimeHour)

The Hour parameter specifies the minimum number of hours that a leased IPv6 prefix is valid. The range is 0 to 23. The default is 0.

Hours

(maxLeaseHour)

The Hour parameter specifies the maximum number of hours that a leased proxy IP address is valid. The range is 0 to 23. The default is 0.

Hours

(minLeaseHour)

The Hour parameter specifies the minimum number of hours that a leased proxy IP address is valid. The range is 0 to 23. The default is 0.

Hours

(preferredLifeTimeHour)

The Hours parameter specifies the minimum number of hours that an assigned IP prefix is valid. The range is 0 to 23. The default is 1.

Hours

(rebindTimerHour)

The Hours parameter specifies the number of hours between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 23. The default is 0.

Hours

(renewTimerHour)

The Hours parameter specifies the number of hours between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 23. The default is 0.

Hours

(validLifeTimeHour)

The Hours parameter specifies the minimum number of hours that an assigned IP prefix is valid. The range is 0 to 23. The default is 0.

IGMP Enabled

(igmpEnabled)

The IGMP Enabled parameter specifies whether IGMP is enabled for the device. Table 186-9 describes the parameter options.

Table 186-9 IGMP Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that IGMP is enabled on the device	—
Disabled (default)	Specifies that IGMP is disabled on the device	—

IGP Inhibit

See the [IGP Inhibit](#) parameter in section 203.1.

Infinite

The Infinite parameter specifies whether or not the static port forward will have an infinite lifetime. The options are:

- Enabled (default)
- Disabled

Ingress Filter ID

See the [Ingress Filter ID](#) parameter in section 203.1.

Inside IP Address

(ipAddress)

The Inside IP Address parameter specifies an L2-aware or destination IP address, or an internal static port forwarding IP address for NAT. Specify an IPv4 address in dotted-decimal format. There is no default.

Inside Port

(port)

The Inside Port parameter specifies the internal port value that NAT maps to the host packets. This parameter is configurable when the [Auto-Assign](#) parameter is disabled. The range is 1 to 1023. The default is 0, which means that the parameter is not configured.

Interface ID

(id)

The Interface ID parameter specifies a unique ID for the interface. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 65 535. The default is 0.

IP Address

See the [IP Address](#) parameter in section [203.1](#).

IP Address 1

(address1)

The IP Address parameter specifies an IP address for the Subnet Option in dotted-decimal format for an IPv4 address. The default is 0.0.0.0. IP Address 1 parameters is available when the [Type](#) parameter is set to IP Address

IP Address 2

(address2)

See the [IP Address 1](#) parameter in this section for more information.

IP Address 3

(address3)

See the [IP Address 1](#) parameter in this section for more information.

IP Address 4

(address4)

See the [IP Address 1](#) parameter in this section for more information.

IP Address Preferred

(ipAddrPreferred)

The IP Address Preferred parameter specifies whether to set the IPv6 address on the parent interface to be used as a backup address (on same subnet) for IPv6 VRRP. This parameter can only be configured during creation of the L3 interface. The options are:

- enabled
- disabled (default)

IP Address Prefix

(ipAddrPrefix)

The IP Address Prefix parameter specifies a matching clause to the route map. Routes are distributed if the destination network number address is permitted by the specified prefix list. There is no default.

IPv6 Address

(address)

The IP Address parameter specifies the IP address for the object. An IP address must be assigned to each IP interface. An IP address and a subnet mask create an IP prefix. The defined IP prefix must be unique within the context of the routing instance. The prefix must not overlap with other IP prefixes that are defined as local subnets on other IPv6 prefixes that exist on any local DHCPv6 servers in the same routing context within the device. Specify an IPv6 address in colon-hexadecimal format. There is no default

IPv6 Prefix

(prefix)

The IPv6 Prefix parameter specifies the IP prefix for router advertisement messages. The range is 0 to 128. The default is 32.

IS-IS Enabled

(isisEnabled)

The IS-IS Enabled parameter specifies whether IS-IS is configured for the device. The options are:

- Enabled
- Disabled (default)

When this parameter is enabled, IS-IS routing is enabled on the device.

L2TP Enabled

(l2tpEnabled)

The L2TP Enabled parameter specifies whether L2TP is enabled for the device. The options are:

- Enabled
- Disabled (default)

LDP Enabled

(ldpEnabled)

The LDP Enabled parameter specifies whether LDP is enabled for the device. Table 186-10 describes the parameter options.

Table 186-10 LDP Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that LDP is enabled on the device	The Enable MPLS parameter must be set to Enabled.
Disabled (default)	Specifies that LDP is disabled on the device	—

LDP Shortcut Enabled

(ldpShortcutEnabled)

The LDP Shortcut Enabled parameter allows the forwarding of IP packets to IGP-learned routes that use LDP LSPs. The parameter is configurable on the default routing instance of a Release 8.0 or later NE. When the parameter is enabled, a forwarded IP packet is given the label from the next hop in the route that corresponds to the FEC prefix in the destination address of the packet. The routing table then uses the shortcut next hop as the best route. If such an LDP FEC does not exist, then the routing table uses the regular next hop, and the packet is forwarded normally.

This function requires that an egress LER advertises and maintains a <label, FEC> binding for each IGP-learned route. It operates on the network interface that participates in IS-IS and OSPF routing. The options are:

- Enabled
- Disabled (default)

LDP Synchronization Timer

(ldpSyncTimer)

The LDP Synchronization Timer parameter specifies a time interval, in s, that is used for IGP-LDP synchronization after a failure. The timer starts when the LDP session FEC bindings are exchanged. When the timer expires, the link cost is restored and re-advertised. IGP announces a new best hop that LDP can use if the label binding for the neighbor FEC is available. The parameter is configurable when Enable is selected. The range is 0 to 1800 seconds. The default is 0.

Lifetime (seconds)

Table 186-11 lists where to find more information about the Lifetime (seconds) parameter.

Table 186-11 Lifetime (seconds) parameter

Parameter	See
Lifetime (seconds) for a router	Lifetime (seconds) parameter in this section
Lifetime (seconds) for a static port forward	Lifetime (seconds) parameter in this section

Lifetime (seconds)

(defaultLifetime)

The Lifetime (seconds) parameter specifies the router lifetime in seconds. The range is 0 or 4 to 9000. The default is 1800. A value of zero means that the router is not to be a default router.

Lifetime (seconds)

(defaultLifetime)

The Lifetime (seconds) parameter specifies the static port forward lifetime in seconds. This parameter is configurable when the [Infinite](#) parameter is disabled. The range is 60 to 86 400. The default is infinite.

Loopback Enabled

(loopbackEnabled)

The Loopback Enabled parameter specifies whether any ports are associated with the interface. If the Loopback Enabled parameter is selected, no ports are associated with the interface and the interface is in a loopback state. The options are:

- Enabled
- Disabled (default)

Low Watermark

(watermarkLow)

The Low Watermark parameter specifies the percentage of used NAT-pool port blocks below which the 5620 SAM clears an alarm raised for port usage that exceeds the [High Watermark](#) value. The parameter value must be lower than the [High Watermark](#) value, unless both parameters are set to 0. The range is 0 to 99. The default is 0.

Lsp Name

(lspName)

The LSP Name parameter specifies the name of the LSP used by the routing instance. At least one alphanumeric character is required. There is no default.

MAC Address

See the [MAC Address](#) parameter in section [203.1](#).

MAC Address Verification

(dhcpSnoopingMacAddrVerification)

The switch-level MAC Address Verification parameter specifies whether the source MAC address contained in DHCP packets coming into the switch is compared to the client hardware MAC address. If the MAC addresses do not match the DHCP packet is dropped. This parameter must be disabled before VLAN-level DHCP snooping can be enabled. When DHCP snooping is enabled at the switch level, this parameter is enabled by default. The options are:

- Disabled (default)
- Enabled

Managed Address Config

(managedAddrConfigFlag)

The Managed Address Config parameter sets the managed address configuration flag. This flag indicates that DHCPv6 is available for address configuration in addition to any address that has been autoconfigured using stateless address autoconfiguration. The options are:

- false (default)
- true

Max Interval (seconds)

(maxInterval)

The Max Interval (seconds) parameter specifies the maximum interval, in seconds, between router advertisement messages sent on the interface. The range is 4 to 1800. The default is 600.

Mask

(mask)

The Mask parameter specifies a BGP aggregate address with a network mask. The default is 0.

Mask Reply

See the [Mask Reply](#) parameter in section [203.1](#).

Maximum Declined Addresses Stored

(maxDeclined)

The Maximum Declined Addresses Stored parameter specifies the maximum number of declined IP address that can be stored. After the maximum is reached, the oldest declined IP address is moved back to the free IP address pool. The range is 0 to 4 294 967 295. The default is 64.

Maximum Hops

(maxHops)

The Maximum Hops parameter specifies the maximum number of hops a BOOTP/DHCP packet is allowed to travel until it reaches the destination DHCP server. If a packet contains a hop count equal to or greater than this parameter value, DHCP relay discards the packet. The maximum hops value only applies to DHCP relay and is ignored by other services. The range is 1 to 16. The default is 4.

Maximum Number of Equal Cost Routes

The Maximum Number of Equal Cost Routes parameter specifies the number of routes for path sharing. Table [186-12](#) describes the parameter options.

Table 186-12 Maximum Number of Equal Cost Routes parameter

Option	Option description	Dependencies
1 (default)	The maximum number of equal cost routes allowed on this routing table instance, expressed as a number. The default 1 means equal cost routing is not implemented. For example, setting the parameter to 2 means two equal cost routes are used for cost sharing.	Can only be used for routes learned with the same preference and protocol.
0 to 16		

Member AS

(memberAS)

The Member AS parameter specifies the AS number of the BGP confederation member. The range is 1 to 65 535. The default is 0, which specifies that the parameter is not configured.

You must configure the parameter to create a BGP confederation.

Min Interval (seconds)

(minInterval)

The Min Interval (seconds) parameter specifies, in seconds, the minimum interval between router advertisement messages sent on the interface. The range is 3 to 1350. The default is 200.

Minutes

(leaseHoldTimeMinute)

The Minutes parameter specifies the minimum number of minutes that a leased proxy IPv6 prefix is valid. The range is 0 to 59. The default is 0.

Minutes

(maxLeaseMinute)

The Minutes parameter specifies the maximum number of minutes that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

Minutes

(minLeaseMinute)

The Minutes parameter specifies the minimum number of minutes that a leased proxy IP address is valid. The range is 0 to 59. The default is 10.

Minutes

(minutes)

The Minutes parameter specifies the number of minutes for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 59. The default is 10.

Table [186-13](#) lists and describes the [Option](#) parameter values that require a time specification.

Table 186-13 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCP OFFER response, the DHCP server uses this option to specify the offered lease time.
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

Minutes

(offerMinute)

The Minutes parameter specifies the time, in minutes, that a DHCP client can consider an IP address before the offer is withdrawn. The range is 0 to 10. The default is 1.

Minutes

(preferredLifeTimeMinute)

The Minutes parameter specifies the minimum number of minutes that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

Minutes

(rebindTimerMinute)

The Minutes parameter specifies the number of minutes between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 59. The default is 48.

Minutes

(renewTimerMinute)

The Minutes parameter specifies the number of minutes between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 59. The default is 30.

Minutes

(validLifeTimeMinute)

The Minutes parameter specifies the minimum number of minutes that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

MLD Enabled

(mldEnabled)

The MLD Enabled parameter specifies whether MLD is configured for the device. The options are:

- Enabled
- Disabled (default)

Monitored Address Prefix

(monitoredPrefix)

The Monitored Address Prefix specifies the the IP address of the prefix to be monitored. While the monitor prefic is configured and the poll is active, the system monitors this prefix in the realm of the virtual router instance associated with this pool. The presence of this prefix is an indication that the NAT redundancy peer is active. The monitor prefix of this system is the export prefix of the peer. The monitor prefix must be different from the export prefix. The default is 0.0.0.0.

MPLS Enabled

(mplsEnabled)

The MPLS Enabled parameter specifies whether MPLS is enabled for the device. The options are:

- Enabled
- Disabled (default)

MSDP Enabled

(msdpEnabled)

The MSDP Enabled parameter specifies whether MSDP is configured for the device. The options are:

- Enabled
- Disabled (default)

MTU

(mtu)

The MTU parameter specifies the MTU size for nodes on the link. The range is 0 to 9212. The default is 1280. A value of zero means that the interface sends no MTU option information in router advertisements.

Name

See the [Name](#) parameter in section [203.1](#).

NAT Pool Type

(natPoolType)

The NAT Pool Type parameter specifies the type of NAT address pool that you are configuring. The options are:

- Large Scale (default)
- L2 Aware

Netbios Node Type

(netbiosNodetype)

The Netbios Node Type parameter specifies the order and method to resolve a Netbios name into an IP address. Table 186-14 lists the parameter options and the option numbers.

Table 186-14 Netbios parameter options

Option	Option Description
Unspecified	Unspecified
B	The DHCP server uses broadcast for name resolution and registration.
P	The DHCP server uses peer to peer for name resolution and registration.
M	The DHCP server uses a combination of broadcast and peer to peer. If broadcast cannot resolve the name, it uses peer to peer.
H	The DHCP server uses a combination of peer to peer and broadcast. If peer to peer cannot resolve the name, it uses broadcast.

Network Policy ID

See the [Network Policy ID](#) parameter in section 203.1.

Number

(optionNumber)

The Number parameter specifies a DHCP option number defined in RFC 2131. The parameter is configurable when the [Option](#) parameter is set to Custom Option. The range is 1 to 254. The default is 0, which means the parameter is not configured.

Number of Redirects

See the [Number of Redirects](#) parameter in section 203.1.

Number of TTL Expired

See the [Number of TTL Expired](#) parameter in section 203.1.

Number of Unreachables

See the [Number of Unreachables](#) parameter in section 203.1.

On-Link Determination

(onLink)

The On-Link Determination parameter specifies whether the routing prefix is used for on-link determination. The options are:

- true (default)
- false

Option

(option)

The Option parameter specifies the information that a DHCP client receives from the DHCP server. Depending on the parameter value, a DHCP client can receive network service or network configuration information. If no option is specified, a DHCP client is identified using the client MAC Address. The following options are available when you configure the parameter in a subnet:

- Custom Option (default)
- Default Routers
- Subnet Mask

The following options are available for IP address pools:

- Custom Option (default)
- DNS Name Servers
- Netbios Name Server
- Domain Name
- Lease Rebind Time
- Lease Renew Time
- Lease Time
- Netbios Name Server
- Netbios Node Type

You can specify a different DHCP option by setting the parameter to Custom Option and setting the [Number](#) parameter using a DHCP option number defined in RFC 2131.

Option-82 Data Insertion

(dhcpSnoopingOpt82DataInsertion)

The switch-level Option-82 Data Insertion parameter specifies whether the switch inserts Option-82 data into DHCP packets before forwarding them to the DHCP server. This parameter must be disabled before VLAN-level DHCP snooping can be enabled. When DHCP snooping is enabled at the switch level, this parameter is enabled by default. Table 186-15 describes the parameter options.

Table 186-15 Option-82 Data Insertion parameter

Options	Option description	Dependencies
Disabled (default)	The relay agent does not insert any information into the Option-82 field.	You cannot disable this parameter when the binding table functionality is enabled.
Enabled	The relay agent inserts the Option-82 field into DHCP packets before forwarding them to the DHCP server	When DHCP snooping is enabled at the switch level, switch-level Option-82 data insertion is enabled by default.

Option-82 Format Type

(dhcpOption82FormatType)

The Option-82 Format Type parameter specifies the type of information inserted into the Circuit ID and Remote ID subfields of the Option-82 field. Table 186-16 describes the parameter options.

Table 186-16 Option-82 Format Type parameter

Option	Option description	Dependencies
MAC Address (default)	The base MAC address of the switch.	The Option-82 Data Insertion parameter must be enabled. When entering a user string, quotes are required around ambiguous characters, such as hex characters and spaces, so they are interpreted as text.
System Name	The system name of the switch.	
User String	A user-defined string.	
Interface Alias	The alias configured for the interface	
Auto Interface Alias	The switch automatically generates the interface-alias in the following format: SystemName_slot_port	

Option-82 User String

(dhcpOption82StringValue)

The Option-82 User String parameter specifies a string value that is used to populate the Circuit ID and Remote ID subfields. Quotes are required around ambiguous characters, such as hex characters and spaces, so they are interpreted as text. The range is 0 to 63.

OSPFv2 Enabled

(ospfEnabled)

The OSPFv2 Enabled parameter specifies whether OSPFv2 is enabled on the device. The options are:

- Enabled
- Disabled (default)

OSPFv3 Enabled

(ospfv3Enabled)

The OSPFv3 Enabled parameter specifies whether OSPFv3 is enabled on the device. The options are:

- Enabled
- Disabled (default)

Other Stateful Config

(otherStatefulConfigFlag)

The Other Stateful Config parameter specifies whether DHCPv6lite is available for the autoconfiguration of other non-address information, such as DNS parameters or information about other servers in the network. The options are:

- false (default)
- true

Outside IP Address

(outIpAddress)

The Outside IP Address parameter specifies the static port forward outside address from the NAT pool. Specify an IPv4 address in dotted-decimal format. The default is 0, which means that the parameter is not configured and the value is auto-assigned by the node.

Outside Port

(outPort)

The Outside Port parameter specifies the external port value that NAT maps to the host packets. This parameter is configurable when the [Auto-Assign](#) parameter is disabled. The range is 1 to the Port Forward Range End defined on the NAT pool. The default is 0, which means that the parameter is not configured and the value is auto-assigned by the node.

P2MP ID

(p2mpId)

The P2MP ID parameter specifies an index for LDP-based tunneling. The range is 1 to 4 294 967 295 for a non-root NE, and 1 to 8 192 for a root NE. The default is 0.

Peer Address

(peerAddress)

The Peer Address parameter specifies the IP address of the redundant node. The default is 0.0.0.0.

PIM Enabled

(pimEnabled)

The PIM Enabled parameter specifies whether PIM is enabled for the device. Table [186-17](#) describes the parameter options.

Table 186-17 PIM Enabled parameter

Option	Option description	Dependencies
Enabled	Specifies that PIM is enabled on the device	—
Disabled (default)	Specifies that PIM is disabled on the device	—

Physical Address

See the [Physical Address](#) parameter in section [203.1](#).

Port Forward Range End

(portFwdRangeEnd)

The Port Forward Range End parameter specifies the end of the port range available for port forwarding. The start of the range is always equal to one. The range is 1023 to 65 535. The default is 1023.

Port Mode

(mode)

The Port Mode parameter specifies the mode of operation for the NAT address pool. This parameter is only configurable for Large Scale NAT Pool Type. The options are:

- Auto (default)
- NAPT

Pool Name

(displayedName)

The Pool Name parameter specifies the name of the IP address pool. The pool contains IP addresses. The range is 0 to 32. There is no default.

Port Reservation Type

(portReservationType)

The Port Reservation Type parameter specifies how the NAT ports are to be reserved. Table 186-18 describes the parameter options.

Table 186-18 Port Reservation Type parameter

Option	Description
Blocks (default)	The Port Reservation Value specifies into how many blocks the port range is to be divided.
Ports	The Port Reservation Value parameter specifies the number of ports in a port range.

Port Reservation Value

(portReservationValue)

The Port Reservation Value parameter specifies, with the [Port Reservation Type](#) parameter, how many blocks of ports NAT reserves for the address pool. See the [Port Reservation Type](#) parameter description for more information. The range is 1 to 2016. The default is 128.

Prefix Length

See the [Prefix Length](#) parameter in section 203.1.

Primary

See the [Primary](#) parameter in section 203.1.

Protocol

(protocol)

The Protocol parameter specifies the type of protocol packets to which the static port mapping applies. The options are:

- TCP (default)
- UDP

PXE Support

(pxeSupport)

The PXE Support parameter specifies if the relay agent supports PXE devices. The options are:

- Disabled (default)
- Enabled

Range End

(rangeEnd)

The Range End parameter specifies the end address of the NAT address pool range. Specify an IPv4 address in dotted-decimal format. There is no default.

Range Start

(rangeStart)

The Range Start parameter specifies the beginning address of the NAT address pool range. Specify an IPv4 address in dotted-decimal format. There is no default.

Reachable Time (milliseconds)

(reachableTime)

The Reachable Time (milliseconds) parameter specifies how long, in milliseconds, this router should be considered reachable by other nodes on the link after the router receives a reachability confirmation. The range is 0 to 3 600 000. The default is 0.

Redirects

See the [Redirects](#) parameter in section [203.1](#).

Redirects Time

See the [Redirects Time \(seconds\)](#) parameter in section [203.1](#).

Relay Agent Information Mode

(agentInformation)

The Relay Agent Information Mode parameter specifies whether the DHCP relay agent Option-82 feature is enabled on the switch. When the DHCP Option-82 feature is enabled, DHCP Snooping is not available. These two features are mutually exclusive. Table 186-19 describes the parameter options.

Table 186-19 Relay Agent Information Mode parameter

Option	Option description	Dependencies
Disabled (default)	—	—
Enabled	Communications between a DHCP client and a DHCP server are authenticated by the relay agent. The agent adds Option-82 data to the end of the options field in DHCP packets sent from a client to a DHCP server.	Option-82 is not available on a per-VLAN basis, DHCP traffic received on all ports is eligible for Option-82 data insertion when it is relayed by the agent. When the relay agent receives a DHCP packet that already contains the Option-82 field, it processes the packet based on the Relay Agent Information Policy parameter value configured for the switch.

Relay Agent Information Policy

(agentInformationPolicy)

The Relay Agent Information Policy parameter specifies how DHCP packets that contain an Option-82 field are handled by the relay service. Table 186-20 describes the parameter options.

Table 186-20 Relay Agent Information Policy parameter

Options	Options description	Dependencies
Drop (default)	DHCP packets that contain an Option-82 field are dropped.	The policy is applied to DHCP packets received on all switch ports. If a DHCP packet contains a gateway IP address that matches a local subnet address the policy is not applied and the packet is dropped. If the DHCP packet contains a non-zero value for the gateway IP address, the policy is not applied and the packet is forwarded to the DHCP server.
Keep	DHCP packets that contain an Option-82 field are relayed to the next destination unchanged.	
Replace	Option-82 information is replaced with local information and relayed to the next destination.	

Relay Service Description

(udpRelayDescription)

The Relay Service Description parameter provides a user-defined description to identify the not well-known port service. Quotes are required around ambiguous characters, such as hex characters and spaces, so they are interpreted as text. The name can be from 1 to 30 characters. There is no default.

Relay Service Port

(udpRelayPort)

The Relay Service Port parameter specifies service port numbers that are not well known. Do not specify port numbers that are already listed in the [UDP Relay Service](#) parameter drop-down menu. The range is 0 to 65 535.

Remote ID

See the [Remote ID](#) parameter in section [14.1](#).

Remote ID String

See the [Remote ID String](#) parameter in section [14.1](#).

Retransmit Time (milliseconds)

(retransmitTime)

The Retransmit Time (milliseconds) parameter specifies, in milliseconds, the frequency of neighbor solicitation messages that are sent on the interface. The range is 0 to 1 800 000. The default is 0.

RIP Enabled

(ripEnabled)

The RIP Enabled parameter specifies whether RIP is enabled on the device. The options are:

- Enabled
- Disabled (default)

Root Node

(isRootNode)

The Root Node parameter specifies the root node for an LDP tunnel interface. The options are:

- Enabled
- Disabled (default)

Router ID

See the [Router ID](#) parameter in section [203.1](#).

Seconds

(leaseHoldTimeSecond)

The Seconds parameter specifies the minimum number of seconds that a leased proxy IPv6 prefix is valid. The range is 0 to 59. The default is 0.

Seconds

(maxLeaseSecond)

The Seconds parameter specifies the maximum number of seconds that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

Seconds

(minLeaseSecond)

The Seconds parameter specifies the minimum number of seconds that a leased proxy IP address is valid. The range is 0 to 59. The default is 0.

Seconds

(offerSecond)

The Seconds parameter specifies the time, in seconds, during which a DHCP client can consider an IP address before the offer is withdrawn. The range is 0 to 59. The default is 0.

Seconds

(preferredLifeTimeSecond)

The Seconds parameter specifies the minimum number of seconds that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

Seconds

(rebindTimerSecond)

The Seconds parameter specifies the number of seconds between the IP prefix assignment and the client transition to the REBINDING state. The range is 0 to 59. The default is 0.

Seconds

(renewTimerSecond)

The Seconds parameter specifies the number of seconds between the IP prefix assignment and the client transition to the RENEWING state. The range is 0 to 59. The default is 0.

Seconds

(seconds)

The Seconds parameter specifies the number of seconds for a lease option. The parameter is configurable when the [Option](#) parameter is set to Lease Time, Lease Renew Time, or Lease Rebind Time. The range is 0 to 3650. The default is 0.

Table 186-21 lists and describes the [Option](#) parameter values that require a time specification.

Table 186-21 Option parameter values that require time specification

Value	Value description
Lease Time	This option is used in a DCHCPDISCOVER or DHCPREQUEST client request to request a lease time for the IP address. In a DHCP OFFER response, the DHCP server uses this option to specify the offered lease time.
Lease Renew Time	This option is used to specify the time interval between the address assignment and the client transition to the RENEWING state.
Lease Rebind Time	This option is used to specify the time interval between the address assignment and the client transition to the REBINDING state.

Seconds

(validLifeTimeSecond)

The Seconds parameter specifies the minimum number of seconds that an assigned IP prefix is valid. The range is 0 to 59. The default is 0.

Send Advertisement

(sendAdvertisement)

The Send Advertisement parameter specifies whether the interface sends routing advertisement messages. The options are:

- false (default)
- true

Sender Address

(senderAddress)

The Sender Address parameter specifies the IPv4 address of the NE that is the source of the multicast traffic. Although the default is 0.0.0.0, however, an IPv4 address must be configured in order to create an object.

Server Name

(displayName)

The Server Name parameter specifies a name for a local DHCP server instance. The range is 0 to 31 characters. There is no default.

Source Address Termination

(ipOrInterfaceIndex)

The Source Address Termination parameter specifies whether the source address used by the IP application to send unsolicited packets to a managed node is a user-specified IP address or the primary address of the L3 access interface (referred to on the Source Address form as Interface Index). The L3 interface must be created on the routing instance and the VPRN service for the router before the IP Address value can be set.

The options are:

- IP Address
- Interface Index

Source IP Address

(sourceIpAddr)

The Source IP Address parameter specifies the IP address used by the IP application to send unsolicited packets to a node, in dotted-decimal format for IPv4, or colon-hexadecimal format for IPv6. An IPv6 IP address is configurable when the following conditions are true:

- the Source Address Termination parameter is set to IP Address
- the [IPv6 Allowed](#) parameter is enabled for the L3 access interface for the router; see chapter 28 for information about enabling IPv6.
- the [IPv6 Allowed](#) parameter is enabled for the VPRN service; see chapter 73 for information about enabling IPv6.

Source IP Application

(sourceIpApplication)

The Source IP Application parameter specifies the application for which the source IP or interface index is specified. Table 186-22 describes the parameter options available depending on the [Source IP Address](#) parameter value.

Table 186-22 IP Source Application Parameter

Option	Dependencies
Telnet	Selectable when the Source IP Address is set to an IPv4 address.
FTP	
SSH	
RADIUS	
TACACS+	
SNMP Traps	
Syslog	
ICMP Ping	
Trace Route	
DNS	
SNTP	
NTP	
CFLOWD	
PTP	
Multicast Reporter	
Telnet IPv6	Selectable when the Source IP Address is set to an IPv6 address.
FTP IPv6	
RADIUS IPv6	
TACACS+ IPv6	
SNMP Traps IPv6	
Syslog IPv6	
ICMP Ping IPv6	
Trace Route IPv6	
DNS IPv6	

Start Address

(startAddress)

The Start Address parameter specifies the first IP address for a range of IP addresses to be configured for a subnetwork. You must also set the [End Address](#) parameter. The default is 0.0.0.0.

Steering Route Address Prefix

(steerRtrAddr)

The Steering Route Address Prefix parameter specifies the IP address of the steering route. The steering route is used in the realm of this virtual router instance as an indirect next-hop for all the traffic that must be routed to the Large Scale NAT function. The default is 0.0.0.0.

Strip Label

(stripLabel)

The Strip Label parameter specifies whether MPLS labels are stripped from packets that are received on the interface. The options are:

- True
- False (default)

This parameter is only configurable for L3 interfaces on 7450 ESS and 7750 SR single fiber mode SONET or Ethernet network ports on an IOM 3 or IMM.

Subnet Mask

See the “[Subnet Mask](#)” parameter in section [203.1](#).

Subscriber Limit

(subscriberLimit)

The Subscriber Limit parameter specifies the maximum number of subscribers per outside IP address. In case multiple port blocks per subscriber are used, the block size is typically small. All blocks assigned to a given subscriber belong to the same IP address. The subscriber limit guarantees that any subscriber can get a minimum number of ports. This parameter is only configurable for Large Scale NAT Pool Type. The range is 1 to 65 535. The default is 65 535.

Subscriber Prefix Length

(dsliteSubPrefixLen)

The DS Lite parameter specifies whether or not DS Lite is enabled on the routing instance. The options are:

- In service
- Out of service (default)

Summary Only

(summaryOnly)

The Summary Only parameter specifies the advertising suppression of aggregate routes to all neighbors. The options are:

- True
- False (default)

Synchronization Timeout (seconds)

(dhcpSnoopingBindingDatabaseSyncTimeout)

The Synchronization Timeout (seconds) parameter specifies how often the DHCP binding table information stored in memory is saved to a file on the switch. The range is 180 to 600. The default is 300.

Timeout

See the “[Timeout \(seconds\)](#)” parameter in section [203.1](#).

TTL Expired

See the “[TTL Expired](#)” parameter in section [203.1](#).

TTL Expired Time (seconds)

See the “[TTL Expired Time \(seconds\)](#)” parameter in section [203.1](#).

Tunnel; MTU (bytes)

(tunnelMtu)

The Tunnel; MTU (bytes) parameter specifies the Dual Stack Lite address. The range is 512 to 9212. The default is 1500.

Type

(ifType)

The Type parameter specifies whether this interface is a Multi-Homing Primary or Secondary interface. The options are:

- Primary
- Secondary

This parameter is only configurable when creating a multi-homing interface, and then only if the primary interface has not yet been configured. It is not available when editing an existing interface.

The default is Primary if no primary interface has been created yet, or Secondary if the primary interface has already been configured.

Type

(optionType)

The Type parameter specifies the format of the DHCP option that the DHCP server sends to the DHCP client. The options are:

- IP Address (default)
- ASCII String
- Hex String

Type

(subType)

The Type parameter specifies the subscriber type for which NAT static port forwarding will be configured. The options are:

- DS Lite
- Large Scale Network (default)

UDP Relay Service

(udpRelayService)

The UDP Relay Service parameter specifies whether UDP port relay is enabled for well-known UDP ports and user-defined service ports that are not well-known. Only use the Other option to specify service port numbers that are not well-known. The options are:

- | | |
|-------------------------|---------------|
| • unspecified (default) | • TACACS (65) |
| • BOOTP/DHCP (67/68) | • TFTP (69) |
| • NBNS/NBDD (137) | • NTP (123) |
| • NBDD (138) | • Other |
| • DNS (53) | |

Unreachables

See the “[Unreachables](#)” parameter in section [203.1](#).

Unreachables Time (seconds)

See the “[Unreachables Time \(seconds\)](#)” parameter in section [203.1](#).

Use GI Address

(useGiAddress)

The Use GI Address parameter specifies whether a gateway IP address is used. When the value is set to true, the IP address is set based on an available gateway IP address. The address is offered even if authentication fails or there is no local user database configured. When the value is set to false, the IP address must be specified and included in the local database. The options are:

- True
- False (default)

Use Pool From Client

(usePoolFromClient)

The Use Pool From Client parameter specifies whether the DHCP server uses the pool name in vendor-specific DHCP-attributes. The options are:

- enabled
- disabled (default)

Use Virtual MAC Address

(useVirtualMac)

The Use Virtual MAC Address parameter specifies whether to use a virtual MAC address when routing advertisement messages are sent from this router. Both the Use Virtual MAC Address and the [Send Advertisement](#) parameters must be enabled for the router advertisement on the parent interface when creating an L3 access interface for IPv6 VRRP. The options are:

- Enabled
- Disabled (default)

Value

(optionValue)

The Value parameter specifies additional values for the DHCP option. Some DHCP options have additional attributes that can be used to identify a DHCP client. For example Option 53 DHCP Message has 13 types of messages associated with the option. To further identify a DHCP server a value of 2 can be configured, so that only DHCP OFFER messages are identified. All DHCP protocol options and values are defined in RFC 2131.

You can choose 0 when the [Type](#) parameter is set to Hex String. The range is 0 to 127. There is no default.

VRF Name

(vRFName)

The VRF Name parameter requires a VRF name to be created for routing instance configuration on the OS 9700E or OS 9800E. The range is 1 to 20 characters.

187 –Bridge Instance parameters

187.1 Bridge Instance parameters 187-2

187.1 Bridge Instance parameters

This chapter describes the parameters on the bridge instance property form, the L2 network interface form, and child forms launched from the right-click contextual menu options for bridges.

Admin Edge

(portAdminEdge)

The Admin Edge parameter specifies the administrative edge port status of a port or group of ports for the flat mode CIST. The status determines whether a port is an edge or non-edge port when the [Auto Edge](#) parameter is disabled for the port or group of ports. When the [Auto Edge](#) parameter is enabled for the port or group of ports, the Admin Edge parameter status is overridden. The options are:

- Disabled (default)
- Enabled

Administrative State

(lpsAdminStatus)

The Administrative State parameter enables or disables LPS on the switch port. When LPS is enabled, only devices with a source MAC address that complies with LPS restrictions are learned on the port. The options are:

- Enable (default)
- Disable

Auto Edge

(portAutoEdge)

The Auto Edge parameter specifies whether the STP automatically determines the operational edge port status of a port or a group of ports for the flat mode CIST. The [Admin Edge](#) parameter is used to determine if a port is an edge or non-edge port when the Auto Edge parameter is disabled for the port. If the Auto Edge parameter is enabled for the port, then the Admin Edge parameter status is overridden. The options are:

- Disabled
- Enabled (default)

Auto VLAN Containment

(stpBridgeAutoVlanContainment)

The Auto VLAN Containment parameter specifies whether auto VLAN containment is enabled on the bridge. When the parameter is enabled, a port that has no VLANs mapped to an MSTI cannot become the root port for that instance. These ports are automatically assigned an infinite path cost value to make them an inferior choice for root port. The options are:

- Enabled
- Disabled (default)

Bridge Max Hops

(bridgeMaxHops)

The Bridge Max Hops parameter specifies the maximum number of hops that are authorized to receive MST regional information. Use this parameter to designate how many hops a BPDU is allowed to traverse before the BPDU is discarded and related information is discarded. The range is 1 to 40. The default is 20.

CLI Name

The CLI Name parameter specifies the device/shelf/port identifier of the physical port on the 7250 SAS or Telco device. There is no default.

Connection Type

(portAdminConnectionType)

The Connection Type parameter specifies the connection type for a port or a group of ports for the flat mode CIST instance or a one-per-VLAN instance. Table 187-1 describes the parameter options.

Table 187-1 Connection Type parameter

Option	Option Description	Dependencies
No Point-to-Point (default)	Specifies the port connection type as a no point-to-point link; the port connects to multiple switches	—
Point-to-Point	Specifies the port connection type as a point-to-point link; the port connects directly to another switch	—
Auto Point-to-Point	Specifies that the switch software automatically defines the connection type as point-to-point or no point-to-point	—
Edge Port	Specifies that the port is at the edge of a bridged LAN, does not receive BPDUs, and has only one MAC address learned. Edge ports, however, operationally revert to a no point-to-point or point-to-point connection type if a BPDU is received on the port.	—

Default Bridged Disposition

(defaultBridgeDisposition)

The Default Bridged Disposition parameter specifies the default disposition for bridged traffic (Layer 2) that arrives at the switch and does not match any policies. The Bridge (Edit) form displays the configured value in the drop-down menu and the applied value for the parameter. When you select a value from the drop-down menu and apply the change, the configured and applied values should be the same. Table 187-2 describes the parameter options.

Table 187-2 Default Bridged Disposition parameter

Option	Option Description	Dependencies
Accept (default)	The switch accepts the flow.	—
Drop	The switch silently drops the flow.	—
Deny	The switch drops the flow and issues an ICMP message indicating that the flow was dropped for administrative reasons. Currently, this option provides the same result as the drop option.	—

Default IGMP Disposition

(defaultMulticastDisposition)

The Default IGMP Disposition parameter specifies the default disposition for multicast traffic that arrives at the switch and does not match any policies. The Bridge (Edit) form displays the configured value in the drop-down menu and the applied value for the parameter. When you select a value from the drop-down menu and apply the change, the configured and applied values should be the same. Table 187-3 describes the parameter options.

Table 187-3 Default IGMP Disposition parameter

Options	Options Description	Dependencies
Accept (default)	The switch accepts the flow.	—
Drop	The switch silently drops the flow.	—
Deny	The switch drops the flow and issues an ICMP message indicating the flow was dropped for administrative reasons. Currently, this option provides the same result as the drop option.	—

Default Routed Disposition

(defaultRoutedDisposition)

The Default Routed Disposition parameter specifies the default disposition for routed traffic (Layer 3) that arrives at the switch and does not match any policies. The Bridge (Edit) form displays the configured value in the drop-down menu and the applied value for the parameter. When you select a value from the drop-down menu and apply the change, the configured and applied values should be the same. Table 187-4 describes the parameter options.

Table 187-4 Default Routed Disposition parameter

Options	Options Description	Dependencies
Accept (default)	The switch accepts the flow.	—
Drop	The switch silently drops the flow.	—
Deny	The switch drops the flow and issues an ICMP message indicating that the flow was dropped for administrative reasons. Currently, this option provides the same result as the drop option.	—

Default Servicing Mode

(servicingMode)

The Default Servicing Mode parameter specifies the default queuing scheme for destination (egress) ports. Table 187-5 describes the parameter options.

Table 187-5 Default Servicing Mode parameter

Options	Options Description	Dependencies
Strict Priority (default)	Specifies the strict priority queuing scheme as the default servicing mode. All eight available queues on a port are serviced strictly by priority.	—
WRR	Specifies the WRR queuing scheme as the default servicing mode.	—
DRR	Specifies the DRR queuing scheme as the default servicing mode.	—

Description

See the [Description](#) parameter in section 203.1.

Displayed Name

See the [Name](#) parameter in section 203.1.

Ethertype

(ethertypeValue)

The Ethertype parameter specifies the 802.1Q tag for the Ethernet packet representing the VLAN ID. The default is 0x8100, which is the standard tag for 802.1Q traffic. The range is a supported hexadecimal number in the format 0x1234.

Hello Time (seconds)

(bridgeHelloTime)

The Hello Time parameter specifies the hello time of the spanning tree for a flat mode CIST instance or for a one-per-VLAN instance. This value specifies the amount of time between each transmission of a BPDU on any port that is the spanning tree root or is attempting to become the spanning tree root. The range is 1 to 10. The default is 2.

High MAC Range

(IpsHiMacRange)

The High MAC Range parameter specifies the high end of a range of authorized MAC addresses allowed on a LPS enabled port. The default is FF-FF-FF-FF-FF-FF.

IGMP Snooping

(igmpSnoopEnable)

The IGMP Snooping parameter specifies whether the bridge checks for IGMP membership, and controls the access to multicast streams. Table 187-6 describes the parameter options.

Table 187-6 IGMP Snooping parameter

Option	Option description	Dependencies
Enabled	Allow IGMP snooping	You must set the parameter to Enabled to provide BTV services across a VLAN.
Disabled (default)	Do not allow IGMP snooping	—

Instance BPDU Switching

(insBpduSwitching)

The Instance BPDU Switching parameter enables or disables the switching of spanning tree BPDUs on the flat mode CIST instance or for an individual VLAN instance when the switch is running in the 1x1 mode. When this parameter is enabled, the BPDUs received for this instance are switched when spanning tree is disabled. When this parameter is disabled, the BPDUs received on this instance are dropped when the spanning tree is disabled. The options are:

- Enabled
- Disabled (default)

Instance Index

(id)

The Instance Index parameter specifies the spanning tree instance identification number. The range is 0 to 4095. The default is 0.

Instance Name

(mstInstanceName)

The Instance Name parameter specifies an optional name for an MST instance. The parameter can contain up to 32 characters. By default, the parameter is blank.

Jumbo Frame

(jumboFrame)

The Jumbo Frame parameter specifies whether the Telco device allows Ethernet payloads in frames larger than 1500 bytes. You can configure the parameter when the Enabled parameter is enabled from the TLS tab button. Use the parameter to allow the transport of large frames for Gigabit Ethernet interfaces, where a larger MTU frame size is required. The options are:

- Enabled
- Disabled (default)

Devices in the L2 VPN service and the VLAN must be capable of supporting larger frame sizes. All devices in the same ring must have the same parameter setting. For example, all devices can have the parameter enabled, or all of them can have it disabled. You must reboot the node for a change to the parameter to take effect.

Last-Member Interval (seconds)

(igmpSnoopLastMember)

The Last-Member Interval (seconds) parameter specifies, in seconds, one of several parameters that determine the query packet interval values to check for leave messages from host ports. The parameter specifies the expected response time for answering a query. This sequence describes how each parameter is used to determine group membership:

- 1 The device receives an IGMP leave message from an user.
- 2 The device queries the group, using the Query Interval (seconds) parameter and the Robustness (packets) parameter.
- 3 The device waits for a response from the group, using the Last-Member Interval (seconds) parameter.
- 4 When an IGMP join message is received, the device refreshes the group membership values.
- 5 The device sends a general query to the group, and expects a response back using the Response Time (seconds) parameter.

The parameter is configurable when the IGMP Snooping parameter is set to Enabled. The range is 1 to 125. The default is 10.

Learning Time Window (minutes)

(IpsLearningWindowTime)

The Learning Time Window (minutes) parameter specifies the amount of time to allow source learning to occur on all LPS enabled ports. This parameter applies to the entire switch; when the time limit expires, source learning of new MAC addresses is stopped on all LPS enabled ports. Only configured, authorized MAC addresses are allowed on LPS enabled ports after this timer expires. All dynamically learned MAC addresses are converted to static MAC addresses if the [Status](#) parameter is enabled. The range is 0 to 65 536. The default is 0, which means that MAC learning takes place continuously.

Low MAC Range

(IpsLoMacRange)

The Low MAC Range parameter specifies the low end of a range of authorized MAC addresses allowed on a learned port security enabled port. The default is 00-00-00-00-00-00.

MAC Address

See the [MAC Address](#) parameter in section 203.1.

MAC Address

(IpsL2MacAddress)

The MAC Address parameter specifies an authorized static MAC address for a port that belongs to a VLAN. The port must belong to a VLAN and have learned port security enabled on the port. There is no default.

Max Age (seconds)

(bridgeMaxAge)

The Max Age (seconds) parameter specifies the amount of time that spanning tree information learned from the network on any port is retained, for a flat mode CIST instance or a 1x1 mode VLAN instance. When the age of the information exceeds the maximum age, the information is discarded. The range is 6 to 40. The default is 20.

Max. Filtered MACs to Learn

(IpsMaxFilteredMacNum)

The Max. Filtered MACs to Learn parameter specifies the maximum number of filtered source MAC addresses that an LPS enabled port is allowed to learn. The range is 1 to 100. The default is 5.

Max. MAC Addresses to Learn

(IpsMaxMacNum)

The Max. MAC Addresses to Learn parameter specifies the maximum number of source MAC addresses that an LPS enabled port is allowed to learn. The range is 1 to 100. The default is 1.

Max VLAN

(maxVLAN)

The Max VLAN parameter specifies the maximum number of VLANs that can be managed through an MVRP configuration on a bridging instance. The range is 32 to 4094. The default is 256.

Mode

Table 187-7 lists where to find more information about the Mode parameter.

Table 187-7 Mode Parameter

Parameter	See
Mode for a BTV MVR	Mode parameter in this section
Mode for a VLAN instance port	Mode parameter in this section

Mode

(mvrMode)

The Mode parameter specifies the mode of the BTV MVR. When a resynchronization is performed on the Telco device, the options are:

- Dynamic (default)
- Static

You can configure the parameter on a resynchronized Telco device to Dynamic, but you cannot change the parameter to Static.

Mode

(portManualMode)

The Mode parameter specifies the manual (forwarding or blocking) or dynamic mode to manage the state of a port or a group of ports for the specified VLAN instance. Dynamic mode defers the management of the port state to the spanning tree algorithm. The options are:

- Dynamic (default)
- Blocking
- Forwarding

MVR Admin Status

(mvrEnable)

The MVR Admin Status parameter specifies whether the bridge is administratively ready to be involved in BTV VLAN services. The options are:

- Enabled
- Disabled (default)

MVR Source Interface

(mvrSource)

The MVR Source Interface parameter specifies the type of VLAN and service interworking involvement between the network port on the Telco device and the 7450 ESS. MVR source interface determines whether Telco ring device provides an connectivity to BTV VLAN services. The options are:

- Enabled
- Disabled (default)

Path Cost

Table 187-8 lists where to find more information about the Path Cost parameter.

Table 187-8 Path Cost parameter

Parameter	See
Path cost for a bridge STP	Path Cost parameter in this section
Path cost for a spanning tree port	Path Cost parameter in this section

Path Cost

(portPathCost)

The Path Cost parameter specifies the spanning tree path cost of a port or a group of ports for a flat mode CIST instance or a 1x1 mode VLAN instance. This value is the contribution of this port to the path cost toward the spanning tree root bridge that includes this port. The path cost is based on the number of hops from the port to the root bridge. The range is 0 to 200 000 000. The default is 0.

Path Cost

(stpBridgePathCostMode)

The Path Cost parameter specifies whether the bridge path cost is automatically assigned based on the selected spanning tree protocol or a 32-bit value is assigned to all paths. Table 187-9 describes the parameter options.

Table 187-9 Path Cost parameter

Option	Option Description	Dependencies
Auto (default)	The port path cost value is automatically set depending on which STP protocol is active (32-bit for MSTP, 16-bit for STP and RSTP).	—
32-bit	A 32-bit value is used for the port path cost value regardless of which STP protocol is active.	—

Port Action

(maxGroupExceedAction)

The Port Action parameter specifies the action to be performed if the IGMP group addresses dynamically learned on the port exceed the value specified by the [Port Max Group](#) parameter. Table 187-10 describes the parameter options.

Table 187-10 Max Group Action parameter

Option	Description
None (default)	When the Port Max Group parameter is 0, the number of dynamically learned IGMP group addresses is not limited. When the Port Max Group parameter is not 0, dynamically learned IGMP group addresses that exceed the Port Max Group value are dropped.
Drop	IGMP group addresses that are dynamically learned after the Port Max Group value is exceeded are dropped.
Replace	IGMP group addresses that are dynamically learned after the Port Max Group value is exceeded replace the oldest learned group address.

Port Max Group

(maxGroupLimit)

The Port Max Group parameter specifies the maximum number of IGMP group addresses that can be dynamically learned on the port. The range is 0 to 4 294 967 295. The default is 0.

Priority

Table 187-11 lists where to find more information about the Priority parameter.

Table 187-11 Priority Parameter

Parameter	See
Priority level for QoS	Priority parameter in this section
Priority for an STP port	Priority parameter in this section

(1 of 2)

Parameter	See
Priority for a bridge	Priority parameter in this section

(2 of 2)

Priority

(portPriority)

The Priority parameter specifies the spanning tree priority value for a port or a group of ports for a flat mode CIST instance or a 1x1 VLAN instance. The spanning tree algorithm uses the value to determine the most favorable port when a bridge has multiple ports with the same path cost to the root bridge. The range is 0 to 15. The default is 8.

Priority

(priority)

The Priority parameter specifies the priority of a flat mode CIST or MSTI bridge instance. In 1x1 mode, the parameter specifies the bridge priority for an individual VLAN instance. Bridge priority determines which bridge the spanning tree algorithm designates as the root bridge. The lower the bridge priority number, the higher the priority that is associated with the bridge.

If the protocol is STP or RSTP, any value in the range of 0 to 65535 is allowed.

If the protocol is MSTP, the value must be a multiple of 4096. If a specified value is not a multiple of 4096, the value is replaced by the closest multiple of 4096 that is lower than the value specified. The range is 0 to 65 535. The default is 32768.

Priority

(priority)

The Priority parameter specifies the QoS priority level manually for each destination MAC address per interface on the bridge. All traffic destined for a specific MAC address, per VLAN and port, can be assigned a priority level. The lower the number, the higher the priority. The range is 0 to 7. The default is 0.

Protocol

(stpProtocol)

The Protocol parameter specifies the STP used for a flat mode CIST instance or for an individual VLAN instance if the switch is using the 1x1 mode. STP flat mode supports STP, RSTP, and MSTP; 1x1 mode supports STP and RSTP. The parameter must be set to MSTP to configure MSTI in flat mode. The options are:

- STP (default)
- RSTP
- MSTP

Q0**(qosConfigLowPriorityWeight)**

The Q0 parameter specifies the switch global value of the desired weight for the Q0 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

Q1**(qosConfigMediumPriorityWeight)**

The Q0 parameter specifies the switch global value of the desired weight for the Q1 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

Q2**(qosConfigHighPriorityWeight)**

The Q0 parameter specifies the switch global value of the desired weight for the Q2 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

Q3**(qosConfigUrgentPriorityWeight)**

The Q0 parameter specifies the switch global value of the desired weight for the Q3 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

Q4**(qosConfigQ4PriorityWeight)**

The Q0 parameter specifies the switch global value of the desired weight for the Q4 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

Q5**(qosConfigQ5PriorityWeight)**

The Q0 parameter specifies the switch global value of the desired weight for the Q5 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

Q6**(qosConfigQ6PriorityWeight)**

The Q0 parameter specifies the switch global value of the desired weight for the Q6 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

Q7

(qosConfigQ7PriorityWeight)

The Q0 parameter specifies the switch global value of the desired weight for the Q7 queue when WRR or DRR is the active queuing scheme. The range is 0 to 15. The default is 1.

QoS Status

(qosEnabled)

The QoS Status parameter specifies whether global QoS is enabled on the switch. When QoS policies are configured and applied, the switch attempts to classify traffic and apply relevant policy actions. When QoS is disabled globally, traffic that arrives at the switch is not classified. The options are:

- Enabled (default)
- Disabled

Query Interval (seconds)

(igmpSnoopQuery)

The Query Interval (seconds) parameter specifies, in seconds, one of several parameters that determine the query packet interval values for checking leave messages from host ports. The parameter specifies the interval that the device waits, after sending a specific query to a group, to determine if group members still want to receive a specific multicast IP address stream. This sequence describes how each parameter is used to determine group membership:

- 1 The device receives an IGMP leave message from a user.
- 2 The device queries the group, using the Query Interval (seconds) parameter and the Robustness (packets) parameter.
- 3 The device waits for a response from the group, using the Last-Member Interval (seconds) parameter.
- 4 When an IGMP join message is received, the device refreshes the group membership values.
- 5 The device sends a general query to the group, and expects a response back using the Response Time (seconds) parameter.

The parameter is configurable when the IGMP Snooping parameter is set to Enabled. The range is 11 to 32 762 s. The default is 120 s.

Query Source IP Zero

(querySourceIpZero)

The Query Source IP Zero parameter specifies whether to query a source IP address of 0.0.0.0. The options are:

- Enabled
- Disabled (default)

Query Time (seconds)

(mvrQuerytime)

The Querytime (seconds) parameter specifies, in seconds, the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The range is 0 to 25. The default is 10.

Region Name

(regionName)

The Region Name parameter specifies the name for an MST region. This parameter is one of three attributes (region name, region revision, and a VLAN to MST instance association) that define an MST region. Switches that share the same attribute values are considered part of the same MST region. Each switch can only belong to one MST region at a time. The parameter can contain up to 32 characters. By default, the parameter is blank.

Region Revision

(regionRevision)

The Region Revision parameter specifies the revision level of an MST region. This parameter is one of three attributes (region name, region revision, and a VLAN to MST instance association) that define an MST region. Switches that share the same attribute values are considered part of the same MST region. Each switch can only belong to one MST region at a time. The range is 0 to 65 535. The default is 0.

Response Time (seconds)

(igmpSnoopResponse)

The Response Time (seconds) parameter specifies one of several parameters that determine the query packet interval values to check for leave messages from host ports. The parameter specifies the expected response time for answering a general query. This sequence describes how each parameter is used to determine group membership:

- 1 The device receives an IGMP leave message from an user.
- 2 The device queries the group, using the Query Interval (seconds) parameter and the Robustness (packets) parameter.

- 3 The device waits for a response from the group, using the Last-Member Interval (seconds) parameter.
- 4 When an IGMP join message is received, the device refreshes the group membership values.
- 5 The device sends a general query to the group, and expects a response back using the Response Time (seconds) parameter.

The parameter is configurable when the IGMP Snooping parameter is set to Enabled. The range is 1 to 125 s. The default is 10 s.

Restricted Role

(portRestrictedRole)

The Restricted Role parameter specifies whether the restricted role status for a port or a group of ports for the flat mode CIST is enabled. When this parameter is enabled, the port cannot become the root port, even if it is the best candidate. After a root port is selected, the restricted port is selected as an alternate port. The options are:

- Disabled (default)
- Enabled

Restricted TCN

(portRestrictedTcn)

The Restricted TCN parameter specifies the topology change notification status for a port or an aggregate of ports for the flat mode CIST. When this parameter is enabled, the port does not propagate topology changes and notifications to or from other ports. It is used to prevent bridges outside of a core network from causing flushes within the core network. The options are:

- Disabled (default)
- Enabled

Robustness (packets)

(igmpSnoopRobustness)

The Robustness (packets) parameter specifies, in packets, one of several values that determine the query packet interval for checking for leave messages from host ports. The parameter specifies the number of specific query packets sent by the device. This sequence describes how each parameter is used to determine group membership:

- 1 The device receives an IGMP leave message from an user.
- 2 The device queries the group, using the Query Interval (seconds) parameter and the Robustness (packets) parameter.
- 3 The device waits for a response from the group, using the Last-Member Interval (seconds) parameter.

- 4 When an IGMP join message is received, the device refreshes the group membership values.
- 5 The device sends a general query to the group, and expects a response back using the Response Time (seconds) parameter.

The parameter is configurable when the IGMP Snooping parameter is set to Enabled. The range 2 to 524. The default is 2.

Status

(lpsLearningWinTimeWithStaticConversion)

The Status parameter specifies whether the conversion of dynamic MAC addresses to static MAC addresses on an LPS enabled port is enabled. When this parameter is enabled and the [Learning Time Window \(minutes\)](#) parameter timer has expired, all dynamic MAC addresses are converted to static MAC addresses. This stops the MAC addresses from aging out. The options are:

- Enabled
- Disabled (default)

Status

(mvrpStatus)

The Status parameter specifies whether MVRP is enabled on a bridge instance. The options are:

- Enabled
- Disabled (default)

STP Mode

(stpBridgeMode)

The STP Mode parameter specifies the mode of the STP that is activated on the bridge instance. The flat mode applies a single spanning tree instance across all VLAN port connections. Flat mode supports the use of STP (802.1D), RSTP (802.1w), and MSTP. The 1x1 mode provides a separate spanning tree instance for each VLAN that is configured on the switch. The 1x1 mode supports STP and RSTP. The options are:

- Flat
- 1x1(default)

Super VLAN Uplink Interface

(superVlanUplink)

The Super VLAN Uplink Interface parameter specifies the type of VLAN and service interworking involvement between the network port on the Telco device and the 7450 ESS. Super VLAN uplink interface determines whether the Telco ring device provides an uplink to Super VLAN services. The options are:

- Enabled
- Disabled (default)

TLS Admin Status

(tlsEnabled)

The TLS Admin Status parameter specifies whether the bridge is administratively ready to be used in TLS L2 VPN services. The options are:

- Enabled
- Disabled (default)

TLS Mode

(tlsMode)

The TLS Mode parameter enables legacy or Ethernet service mode. If you change the mode to Ethernet Service when legacy SVLANs are configured on the switch, a deployment error occurs. Remove the legacy SVLANs using the CLI before you change the mode. The options are:

- Legacy (default)
- Ethernet Service

TLS Uplink Interface

(tlsUplink)

The TLS Uplink Interface parameter specifies the type of VLAN and service interworking involvement between the network port on the Telco device and the 7450 ESS. TLS uplink interface determines whether the Telco ring device provides an uplink to L2 VPN services. The options are:

- Enabled
- Disabled (default)

Transparent Switching Status

(mvrpTransparentSwitchingStatus)

The Transparent Switching Status parameter specifies whether MVRP transparent switching is enabled on a bridging instance. The options are:

- Enabled
- Disabled (default)

Trap Threshold

(IpsLearnTrapThreshold)

The Trap Threshold parameter specifies the number of bridged MAC addresses to learn before sending a trap. The range is 1 to 100. The default is 5.

Trust Ports

(trustPorts)

The Trust Ports parameter specifies whether the global trust mode for QoS ports is enabled. Trusted ports can accept 802.1p and ToS/DSCP values in incoming packets; untrusted ports set any 802.1p or ToS/DSCP values to zero in incoming packets, unless a default 802.1p or ToS/DSCP value is configured. By default, 802.1Q-tagged ports and mobile ports are trusted; any other port is untrusted. The options are:

- No (default)
- Yes

TX Hold Count

(insBridgeTxHoldCount)

The TX Hold Count parameter specifies the number of PDUs that can be transmitted per port per second for this instance. The range is 1 to 10. The default value is 6.

Upper Ring Adjacency

(adjacentToUpperRing)

The Upper Ring Adjacency parameter specifies the type of VLAN and service interworking involvement between the network port on the Telco device and the 7450 ESS. Upper ring adjacency determines that the interface in the Telco device is directly connected with the 7450 ESS that is the start and end of the ring. The options are:

- Enabled
- Disabled (default)

Violation

(IpsViolationOption)

The Violation parameter specifies the method to handle traffic that does not comply with LPS restrictions. Table [187-12](#) describes the parameter options.

Table 187-12 Violation parameter

Option	Description
Restrict	Filters (blocks) unauthorized traffic, but allows traffic that complies with LPS restrictions to be forwarded on the port
Disabled	Disable the port when the port receives unauthorized traffic; traffic is not allowed on the port

VLAN ID

(switchingInstanceId)

The VLAN ID parameter specifies the VLAN to which the bridge belongs. The VLAN ID is used to identify devices in the ring that receive multicast BTV channels, as identified in the Multicast Groups tab. There can be one MVR VLAN ID for each ring. The same VLAN ID can be used by multiple rings. The range is 1 to 4094. The default is 1. The supported ID range for 7250 SAS is 2 to 4092.

VLAN Registration Protocol Type

(vlanRegistrationProtocol)

The VLAN Registration Protocol Type parameter specifies the VLAN registration mode for a multiple VLAN registration configuration. The default is MVRP.

188 –Interface parameters

188.1 Interface parameters 188-2

188.1 Interface parameters

This chapter describes the parameters on the Interface and interface IP address forms, and the child forms launched from the right-click contextual menu options for Interfaces and interface IP addresses.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Administration Status

(adminStatus)

The Administration Status parameter specifies whether Bi-directional Forwarding Detection is enabled. This parameter must be configured before BFD parameters are accessible on router interfaces. The options are:

- Up
- Down (default)

Allow Directed Broadcasts

See the [Allow Directed Broadcasts](#) parameter in section 203.1.

Broadcast

See the [Broadcast](#) parameter in section 203.1.

Broadcast Address Format

See the [Broadcast Address Format](#) parameter in section 203.1.

Cflowd Type

See the [Cflowd Type](#) parameter in section 203.1.

Class

See the [Class](#) parameter in section 203.1.

Description

See the [Description](#) parameter in section 203.1.

Echo Interval

(bfdEchoInterval)

The Echo Interval parameter specifies the minimum echo receive interval, in milliseconds, for the BFD session. The range is 100 to 100 000. The default is 100.

Egress Filter ID

See the [Egress Filter ID](#) parameter in section 203.1.

Enable Local Proxy

(localProxy)

The Enable Local Proxy parameter specifies whether local proxy neighbor discovery can be used on the interface. Proxy neighbor discovery allows an interface, such as a network interface, to respond to neighbor discovery queries that are intended for another interface. The options are:

- true
- false (default)

Enable Local Proxy ARP

(proxyArpLocal)

The Enable Local Proxy ARP parameter specifies whether local proxy ARP can be used on the device. Proxy ARP allows a device, such as a router, to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without configuring routes to the subnet or a default gateway device. The options are:

- true
- false (default)

IGP Inhibit

See the [IGP Inhibit](#) parameter in section 203.1.

Ingress Filter ID

See the [Ingress Filter ID](#) parameter in section 203.1.

Interface ID

(id)

The Interface ID parameter specifies a unique ID for the routing instance interface. The parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 0 to 5119. The default is 0.

IP Address

See the [IP Address](#) parameter in section 203.1.

Lifetime (seconds)

(preferredLifetime)

The Lifetime (seconds) parameter specifies the length of time in seconds that a router advertisement prefix remains preferred. The range is 0 to 4 294 967 295. The default is 604 800. The 4 294 967 295 value represents infinity. A preferred lifetime must not be longer than a valid lifetime. See the [Lifetime \(seconds\)](#) parameter in this section for more information.

Lifetime (seconds)

(validLifetime)

The Lifetime (seconds) parameter specifies the length of time in seconds that a router advertisement prefix remains valid. The range is 0 to 4 294 967 295. The default is 25 920 000. The 4 294 967 295 value represents infinity. A valid lifetime must be longer than a preferred lifetime. See the [Lifetime \(seconds\)](#) parameter in this section for more information.

MAC Address

See the [MAC Address](#) parameter in section 203.1.

Mask Reply

See the [Mask Reply](#) parameter in section 203.1.

Multiplier

(bfdMultiplier)

The Multiplier parameter specifies the number of consecutive BFD messages that must be missed before the BFD session state is changed to the down state. OSPF, IS-IS and PIM are notified of the fault. The range is 3 to 20. The default is 3.

Name

See the [Name](#) parameter in section 203.1.

Network Policy ID

See the [Network Policy ID](#) parameter in section 203.1.

No Expiry

(preferredLifetimeNoExpiry)

The No Expiry parameter sets the preferred lifetime of a router advertisement prefix to infinity, which is represented by the 4 294 967 295 value. See the [Lifetime \(seconds\)](#) parameter in this section for more information. The options are:

- true
- false (default)

No Expiry

(validLifetimeNoExpiry)

The No Expiry parameter sets the valid lifetime of a router advertisement prefix to infinity, which is represented by the 4 294 967 295 value. See the [Lifetime \(seconds\)](#) parameter in this section for more information. The options are:

- true
- false (default)

Number of Redirects

See the [Number of Redirects](#) parameter in section 203.1.

Number of TTL Expired

See the [Number of TTL Expired](#) parameter in section 203.1.

Number of Unreachables

See the [Number of Unreachables](#) parameter in section 203.1.

Physical Address

See the [Physical Address](#) parameter in section 203.1.

Policy 1

See the [Policy 1](#) parameter in section 203.1.

Policy 2

See the [Policy 1](#) parameter in section 203.1.

Policy 3

See the [Policy 1](#) parameter in section 203.1.

Policy 4

See the [Policy 1](#) parameter in section 203.1.

Policy 5

See the [Policy 1](#) parameter in section 203.1.

Port

(port)

The Port parameter specifies the underlying physical port that is associated with the interface. The physical port name is used to create the association. A physical port name is based on the slot, daughter card slot, and port number, for example, 1/1/11 specifies slot 1, daughter card slot 1, and port 11.

Primary

See the [Primary](#) parameter in section [203.1](#).

Proxy Arp Policy 1

(proxyArpPolicy1)

The Proxy Arp Policy parameter specifies the name of the proxy ARP policy to use for this device.

Enter an appropriate name for the proxy ARP policy. The proxy ARP policies are applied in order, from 1 to 5.

Proxy ARP allows a device, such as a router, to answer ARP requests intended for another device. This allows a device reach a remote subnet without configuring routes to the subnet or a default gateway device.

Proxy Arp Policy 2

(proxyArpPolicy2)

See the [Proxy Arp Policy 1](#) parameter in this section.

Proxy Arp Policy 3

(proxyArpPolicy3)

See the [Proxy Arp Policy 1](#) parameter in this section.

Proxy Arp Policy 4

(proxyArpPolicy4)

See the [Proxy Arp Policy 1](#) parameter in this section.

Proxy Arp Policy 5

(proxyArpPolicy5)

See the [Proxy Arp Policy 1](#) parameter in this section.

Receive Interval

(bfdRxInterval)

The Receive Interval parameter specifies the receive interval in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Redirects

See the [Redirects](#) parameter in section 203.1.

Redirects Time (seconds)

See the [Redirects Time \(seconds\)](#) parameter in section 203.1.

Remote Proxy ARP

(proxyArp)

The Remote Proxy ARP parameter specifies whether proxy ARP can be used on the device. Proxy ARP allows a device, such as a router, to answer ARP requests that are intended for another device. This allows a device to reach a remote subnet without configuring routes to the subnet or a default gateway device. The options are:

- true
- false (default)

When the Remote Proxy ARP parameter is set to true, you can configure a proxy ARP policy to specify the type of ARP management that is allowed on the device.

Router ID

See the [Router ID](#) parameter in section 203.1.

Routing Instance ID

See the [Router ID](#) parameter in section 203.1.

Subnet Mask

See the [Subnet Mask](#) parameter in section 203.1.

Transmit Interval

(bfdTxInterval)

The Transmit Interval parameter specifies the time in milliseconds for the BFD session. The range is 100 to 100 000. The default is 100.

Timeout

See the [Timeout \(seconds\)](#) parameter in section 203.1.

Trusted

(isTrusted)

The Trusted parameter specifies whether the ToS bits of packets that ingress an IP interface can be trusted by the system. Packets received on a trusted interface are only remarked at network egress when the network egress Remark function is enabled, except for VPRN packets, which are not affected. A packet that ingresses a non-trusted IP interface is always remarked at egress network interfaces regardless of the Remark parameter value of the egress network interface. The options are:

- true (default for VPRN and network IP interfaces)
- false (default for IES IP interfaces)

TTL Expired

See the [TTL Expired](#) parameter in section 203.1.

TTL Expired Time (seconds)

See the [TTL Expired Time \(seconds\)](#) parameter in section 203.1.

Unnumbered Reference

(referenceType)

The Unnumbered Reference parameter specifies a text string to describe the reference to the unnumbered interface. The range is 1 to 32 characters.

Unnumbered Type

(unnumberedReferenceType)

The Unnumbered Type parameter specifies the type of unnumbered interface to use when the Class parameter is set to Unnumbered. Table 188-1 describes the parameter options.

Table 188-1 Unnumbered Type parameter

Option	Option description	Dependencies
System (default)	Specifies the use of the system IP address	The Class parameter is set to Unnumbered. Alcatel-Lucent recommends that you use the System option because the system IP address is not associated with an interface and is therefore always reachable.
IP address	Specifies the use of another IP address	
Name	Specifies the use of a name	

Unreachables

See the [Unreachables](#) parameter in section [203.1](#).

Unreachables Time (seconds)

See the [Unreachables Time \(seconds\)](#) parameter in section [203.1](#).

View the newly created Network Interface

The View the newly created Network Interface parameter specifies whether the properties form for the interface is displayed when the current configuration form is closed. The options are:

- Enabled
- Disabled (default)

What type of interface would you like to create?

The What type of interface would you like to create? parameter specifies the type of network interface that you are creating. The options are:

- MPLS (default)
- OSPFv2
- OSPFv3
- RIP
- ISIS
- LDP

189 –BGP parameters

189.1 BGP parameters 189-2

189.1 BGP parameters

This chapter describes the parameters on the BGP forms, and the child forms launched from the right-click contextual menu options for BGP.

Address Family

(advertiseExternal)

The Advertise External Address Family parameter specifies the address families which are enabled on this router instance to advertise the best external route to the destination even when its best overall route is an internal route. The options are:

- IPv4
- IPv6

One or both of these options can be enabled. The default state is to have no address family specified, which means that the Advertise External function is disabled.

Address Family

(rapidUpdate)

The Rapid Update Address Family parameter specifies which address families to enable or disable for BGP rapid update. When BGP is used to transport C-multicast routes between PEs, it is essential to send BGP updates for those routes as fast as possible to improve the join/prune latency. All routes in the mvpn-ipv4 address family are treated as a whole, so that these routes are advertised or withdrawn rapidly with minimum delay. MDT SAFI facilitates discovery of other PEs in the same mVPN. The options are:

- L2 VPN
- Multicast VPN IPv4
- MDT SAFI

One or more of these options can be enabled. The default state is to have no address family specified, which means that the BGP rapid update function is disabled.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Advertise Inactive Routes

(advertiseInactiveRts)

The Advertise Inactive Routes parameter specifies whether the BGP instance advertises inactive BGP routes to the BGP peers. The options are:

- True
- False (default)

Advertise Label

(advertiseLabel)

The Advertise Label parameter specifies the advertisement label address family to support the exchange of appropriate address prefix types.

Enabling the IPv4 option allows the interconnection of IP-VPNS using VPRN Option-C. Distribution of IP-VPN routing information is handled using either direct MP-BGP peering between PEs in different ASNs, or more commonly, using one or more route reflectors in ASN.

The IPv4 option specifies the advertisement label address family to support 6PE (also known as “IPv6 over MPLS”) and configures the IPv4 transport peers to exchange IPv6 prefixes using 6PE as well as RFC3107-labeled IPv4 routes. If the IPv4 option is enabled, all IPv4 routes advertised to the remote BGP peer is sent with a VPRN Option-C formatted label. The options are:

- IPv4
- IPv6

You can enable either, both, or neither of the options. The default is neither option selected.

For VPRN routing instances, the Advertise Label parameter is available with only the IPv4 option, and only at the BGP peer level.

Advertise LDP Prefix

(advertiseLdpPrefix)

The Advertise LDP Prefix parameter specifies whether or not all the activated LDP FEC prefixes will be sent to remote BGP peers to support stitching of an LDP FEC to a BGP labeled route. This ability allows LDP-capable PE devices to offer services to PE routers in areas or domains where BGP labelled routes are not supported. The options are:

- true
- false (default)

In addition to enabling the advertising of LDP prefixes, tunnel table route export policies must also be configured in LDP to fully enable this ability. To assign tunnel table policies to BGP, existing BGP export policies are used and no additional policy configuration is required.

Aggregator ID Zero

(aggregatorIdZero)

The Aggregator ID Zero parameter specifies whether to set the router ID in the BGP aggregator path attribute to 0 when BGP aggregates routes. This prevents different devices within the AS from creating aggregate routes that contain different AS paths. The BGP aggregator path attribute is internal to the BGP protocol and is not configurable. Table [189-1](#) describes the parameter options.

Table 189-1 Aggregator ID Zero parameter

Option	Option description	Dependencies
false (default)	BGP adds the AS number and the router ID to the aggregator path. This prevents different routers within an AS from creating aggregate routes that contain different AS paths. When BGP aggregates routes, it adds the aggregator path attribute to the BGP update messages.	—
true	The aggregator path is set to 0 when BGP aggregates routes, rather than using the AS number and the router ID.	

Apply Export Route Policies

(vpnApplyExport)

The Apply Export Route Policies parameter specifies whether to use export route policies. Export route policies are used to determine which routes are advertised to peers. Table 189-2 describes the parameter options.

Table 189-2 Apply Export Route Policies parameter

Option	Option description	Dependencies
true	Export policies are used based on the order of policies configured for the Policy 1 to Policy 5 parameters. When no export policies are specified, the default export policy is used.	—
false (default)	Export policies are not used.	

Apply Import Route Policies

(vpnApplyImport)

The Apply Import Route Policies parameter specifies whether to use import route policies. Import route policies are used to determine which routes are accepted from peers. Table 189-3 describes the parameter options.

Table 189-3 Apply Import Route Policies parameter

Option	Option description	Dependencies
true	Import policies are used based on the order of policies configured for the Policy 1 to Policy 5 parameters. When no import policies are specified, the default import policy is used.	—
false (default)	Import policies are not used.	

AS Override

(overrideAS)

The AS Override parameter specifies whether the network provider AS number that is configured for a BGP group in a VPRN overrides the customer AS number for the group. When the parameter is set to true for an egress eBGP session, the customer AS number is overwritten with the network provider AS number before the route is advertised to the other VPRN sites. The override behavior is required when BGP is the PE-CE protocol and some of the CE sites are in the same AS; normally, BGP loop detection does not permit two sites in the same AS to reach each other directly. The options are:

- true
- false (default)

AS Path Ignore

(pathIgnore)

The AS Path Ignore parameter specifies whether or not the AS path is used in the BGP route selection process to determine the optimum BGP route. The default value of this parameter is false, which means that all address families will be included in the AS path selection process. If you set this parameter to true, all address families are initially excluded from AS path selection process. However, you can refine this and specify which families to exclude by configuring the [AS Path Ignore Family](#) parameter.

AS Path Ignore Family

(pathIgnoreFamily)

The AS Path Ignore Family parameter specifies which address families to ignore in the AS path selection process to determine the optimum BGP route. This allows BGP routes which do not have equal AS paths to be considered equal and therefore load-balanced across BGP routes.

The AS Path Ignore Family parameter can only be configured if the [AS Path Ignore](#) parameter is set to true. All address families are initially selected. You can deselect any of the address families. The AS paths of incoming routes will not be used in the route selection process for all address families that remain selected. Table [189-4](#) describes the parameter options.



Note — If you are configuring a BGP Site in a VPRN service then only the IPv4 and IPv6 options will be displayed for this parameter.

Table 189-4 AS Path Ignore Family parameter

Option	Description
IPv4	The AS path length will be ignored for all IPv4 routes.

(1 of 2)

Option	Description
VPN IPv4	The AS path length will be ignored for all VPN IPv4 routes.
IPv6	The AS path length will be ignored for all IPv6 routes.
VPN IPv6	The AS path length will be ignored for all VPN IPv6 routes.
Multicast IPv4	The AS path length will be ignored for all Multicast IPv4 routes.
Multicast VPN IPv4	The AS path length will be ignored for all Multicast VPN IPv4 routes.
L2 VPN	The AS path length will be ignored for all L2 VPN NLRIs.

(2 of 2)

Cluster ID

(clusterId)

The Cluster ID parameter specifies the cluster ID for a route reflector server. Route reflector servers are used to reduce the number of IBGP sessions within an AS. Specify an IPv4 address in dotted-decimal format. When the parameter is set to 0.0.0.0, BGP assigns no cluster ID.

Each route reflector server must be assigned a cluster ID and must specify which neighbors are clients and which are not clients to determine which neighbors should receive reflected routes and which should be treated as a standard IBGP peer.

Connect Retry Time (seconds)

(connectRetryTime)

The Connect Retry Time (seconds) parameter specifies the BGP connect retry timer value in seconds. When the timer expires, the BGP tries to reconnect to the configured peer. The range is 1 to 65 535. The default is 120.

Damping

(damping)

The Damping parameter specifies whether to prevent BGP systems from sending excessive route changes to BGP peers for learned routes. Damping can reduce the number of update messages that are sent between BGP peers and the load on peers without adversely affecting the route convergence time for stable routes. Table 189-5 describes the parameter options.

Table 189-5 Damping parameter

Option	Option description	Dependencies
false (default)	Disable route damping.	—

(1 of 2)

Option	Option description	Dependencies
true	Enable route damping.	<p>When the parameter is set to true, and a route policy does not specify a damping profile, the default damping profile is used. You cannot configure the default damping profile, which has the following attributes:</p> <ul style="list-style-type: none"> • half life of 15 min • maximum suppression time of 60 min • suppression threshold of 3000 • reuse threshold of 750

(2 of 2)

Description

See the [Description](#) parameter in section [203.1](#).

Disable 4Byte ASN

(disable4ByteASN)

The Disable 4Byte ASN parameter specifies whether to allow the Autonomous System Number to be specified as four-byte integer, with a maximum value of 4294967295. The AS Number is used in many places to configure or specify the BGP autonomous system ID. If the parameter is set to True, then you can only specify the AS Number as a two-byte integer, with a maximum value of 65535. The options are:

- true
- false (default)

Disable Client Reflect

(disableClientReflect)

The Disable Client Reflect parameter specifies whether to enable the reflection of routes by the route reflector to the clients in a specific group or neighbor. This parameter only disables the reflection of routes from other client peers. Routes learned from non-client peers are still reflected to all clients. Table [189-6](#) describes the parameter options.

Table 189-6 Disable Client Reflect parameter

Option	Option description	Dependencies
false (default)	Enable the reflection of routes to all client peers in the specific group or neighbor.	—
true	Disable the reflection of routes.	

Disable Extended Communities

(disableExtComms)

The Disable Extended Communities parameter specifies whether to send information about the BGP community to BGP neighbors directly, rather than using routing policy statements. Table 189-7 describes the parameter options.

Table 189-7 Disable Extended Communities parameter

Option	Option description	Dependencies
true	Do not send BGP community information to an associated peer. No BGP community information is advertised to local BGP peers.	—
false (default)	Send BGP community information to an associated peer and override the community information associated with this route as specified in a routing policy statement.	

Disable Fast External Failover

(fastExtFailover)

The Disable Fast External Failover parameter specifies whether the device should stop an EBGp session after an interface goes down or whether the EBGp session should remain up until the appropriate hold time values are reached. Table 189-8 describes the parameter options.

Table 189-8 Disable Fast External Failover parameter

Option	Option description	Dependencies
true	The EBGp session stops after an interface goes down.	—
false (default)	The EBGp session remains up until the appropriate hold time values are reached. When the BGP routes become unavailable because the interface is down, BGP withdraws the unavailable route information from peers.	

Disable Standard Communities

(disableComms)

The Disable Standard Communities parameter specifies whether to send information about the BGP community to BGP standard neighbors directly, rather than using routing policy statements. Table 189-9 describes the parameter options.

Table 189-9 Disable Standard Communities parameter

Option	Option description	Dependencies
true	Do not send BGP community information to an associated BGP standard peer. No BGP community information is advertised to BGP standard peers.	—
false (default)	Send BGP community information to an associated BGP standard peer and override the community information associated with this route as specified in a routing policy statement.	

Disallow IGP

See the [Disallow IGP](#) parameter in section 203.1.

Dynamic Peer

(dynamicPeer)

The Dynamic Peer parameter specifies whether dynamically created BGP peers can belong to a group. If the parameter is enabled, non-dynamic BGP peers cannot be configured in the group. The parameter is set to False by default.

This parameter can only be configured during the BGP group creation. It cannot be modified afterwards.

This parameter can only be configured on only applies to VPRN BGP sites. It cannot be configured on a base router.

EIBGP LoadBalance

(eibgpMultipath)

The EIBGP LoadBalance parameter specifies whether the NE uses multiple BGP routes that can resolve to both direct IPv4 next hops, which are typically directly attached customer sites, and MP-BGP learned routes, which are MPLS LSPs, simultaneously. The parameter is configurable on a 7450 ESS in mixed mode, and on a Release 7.0 R4 or later 7710 SR or 7750 SR. The options are:

- enabled
- disabled (default)

Enable Inter AS VPRN

(enableInterAsVprn)

The Enable Inter AS VPRN parameter specifies whether the ASBR advertises VPRN routes to peers in other ASs to redistribute the unicast and multicast routes learned by BGP into MP-BGP routes, and the MP-BGP routes into BGP routes. The options are:

- true
- false (default)

Enable Peer Tracking

(enabledPeerTracking)

The Enable Peer Tracking parameter specifies whether the BGP instance tracks BGP peers. BGP peer tracking allows faster BGP route convergence. The parameter is configurable on a 7450 ESS in mixed mode, and on a 7750 SR. The options are:

- true
- false (default)

Enable Rapid Withdrawal

(enableRapidWithdrawal)

The Enable Rapid Withdrawal parameter specifies whether there is a delay before sending BGP withdrawal messages to BGP peers. When the value is enabled, there is no delay before sending BGP withdrawal messages. Withdrawal messages are sent immediately. When the value is disabled, BGP withdrawal messages may be delayed up to the minimum route advertisement delay. This delay allows for BGP updates to be efficiently packed to reduce BGP processing load. For voice applications, or applications that are sensitive to delays, you should allow Enable Rapid Withdrawal to ensure quality of service levels. The options are:

- enabled
- disabled (default)

Graceful Restart

See the [Graceful Restart](#) parameter in section [203.1](#).

Hold Time (seconds)

(holdTime)

The Hold Time (seconds) parameter specifies, in seconds, the maximum time that the BGP waits between successive keep-alive or update messages from its peer before closing the connection. The range is 0 or 3 to 65 535. The default is 90.

When the Hold Time (seconds) parameter value is less than the Keep Alive (seconds) parameter, the Keep Alive (seconds) parameter should be set to one-third of the Hold Time (seconds) parameter value. When the Hold Time (seconds) parameter is set to 0, the Keep Alive (seconds) parameter must be set to 0. This indicates that the connection with the peer is permanently up and no keep-alive packets are sent to the peer.

Hold Time Strict

(holdTimeIsStrict)

The Hold Time Strict parameter specifies whether or not there is strict adherence to the Hold Time (seconds) parameter. The options are:

- enabled
- disabled (default)

IBGP MultiPath

(ibgpMultipath)

The IBGP MultiPath parameter specifies whether to allow IBGP multipath load balancing when BGP routes are added to the route table and the route that resolves the BGP next hop offers multiple next hops. Table 189-10 describes the parameter options.

Table 189-10 IBGP MultiPath parameter

Option	Option description	Dependencies
false (default)	Do not allow IBGP multipath load sharing.	—
true	Allow IBGP multipath load sharing.	

Inherit Value

See the [Inherit Value](#) parameter in section 203.1.

Keep Alive (seconds)

(keepAlive)

The Keep Alive (seconds) parameter specifies the BGP keep-alive time. A keep-alive message is sent every time this timer expires. The range is 0 to 21 845. The default is 30.

The Keep Alive (seconds) parameter setting should be one-third of the Hold Time parameter interval setting. When the Hold Time (seconds) parameter is less than the Keep Alive (seconds) parameter, the Keep Alive (seconds) parameter should be set to one-third of the Hold Time (seconds) parameter value. When the Hold Time (seconds) parameter is set to 0, the Keep Alive (seconds) parameter must be set to 0. This indicates that the connection with the peer is permanently up and no keep alive packets are sent to the peer.

Key

See the [Key](#) parameter in section 203.1.

Limited

(removePrivateASLmt)

The Limited parameter specifies whether BGP will remove the private AS numbers for this peer. This parameter is configurable for a site if the “[Remove Private AS](#)” parameter is set to true. This parameter is configurable for a group or a peer if the “[Inherit Value](#)” parameter in the Remove Private AS panel is disabled. Table [189-11](#) describes the parameter options.

Table 189-11 Limited parameter

Option	Option description	Dependencies
false (default)	BGP does not remove private AS numbers for the AS Path for this peer.	—
true	BGP removes private AS numbers for the AS Path for this peer.	—

Local Address

(localAddress)

The Local Address parameter specifies the local IP address that is used by the BGP group or neighbor to communicate with BGP peers. Outgoing connections use the parameter as the source of the TCP connection when they initiate connections with a peer. Specify an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format. Specify a DNS address in the form of a string.

When no value for the parameter is specified, the device uses the system IP address to communicate with IBGP peers and the interface address to communicate with directly connected EBGP peers.

Local AS

(localAS)

The Local AS parameter specifies a local, sometimes called a virtual, AS number. The local AS number is added to AS path messages before the AS number of the device to make the local AS the second AS in the AS path. The range is 0 to 4294967295. The default is 0, which means that no AS value is specified.

When you change the Local AS parameter at the BGP global level in an active BGP instance, the BGP instance restarts with the new local AS number. This causes BGP to re-establish the peer relationships with all peers in the group with the same new local AS number. When you change the local AS number at the neighbor level in an active BGP instance, the BGP re-establishes the peer relationship with the new local AS number.

Local Preference

(localPreference)

The Local Preference parameter specifies the BGP local preference for incoming routes, when not otherwise specified. This value is used if the BGP route arrives from a BGP peer without the “Preference” parameter set. The parameter is overridden by any value set using a route policy. The range is 0 to 4 294 967 295. The default is 100.

Loop Detect

(loopDetect)

The Loop Detect parameter specifies how the BGP peer session handles loop detection in the AS path. Table 189-12 describes the parameter options.

Table 189-12 Loop Detect parameter

Option	Option description	Dependencies
drop	Sends a notification to the remote peer to drop the session	—
ignore (default)	Ignores routes with loops in the AS path but maintains peering	
off	Disables loop detection	
Discard Route	Removes the route from the BGP routing table	

MED Compare

(medCompare)

The MED Compare parameter specifies how the MED AS path setting is used in the BGP route selection process. The MED setting is always used in the route selection process regardless of the peer AS that advertised the route. This parameter specifies the MED value that is inserted in the RIB-IN. Table 189-13 describes the parameter options.

Table 189-13 MED Compare parameter

Option	Option description	Dependencies
off (default)	Compare MEDs of routes that have the same peer AS.	When a route has no MED setting, the route is assigned the infinity value, to make the route the least preferable route.
zero	For routes learned without a MED setting, use 0 in the MED comparison. The routes with the lowest metric are the most preferred routes.	
infinity	For routes learned without a MED setting, use a value of infinity ($2^{32}-1$) in the MED comparison. This makes infinity routes the least preferred routes.	

MED Source

(medSource)

The MED Source parameter specifies whether to enable advertising the MED and, if so, specifies the method of the MED advertising used. Table 189-14 describes the parameter options.

Table 189-14 MED Source parameter

Option	Option description	Dependencies
IGP Cost	The MED is set to the IGP cost of the IP prefix.	—
Metric Value	The MED setting is expressed as a decimal integer using the MED Value parameter.	—
None (default)	The MED is not advertised.	—

MED Value

(medValue)

The MED Value parameter specifies the MED path setting or MED value for a peer. The parameter is configurable when the MED Source parameter is set to Metric Value. The range is 0 to 4 294 967 295. The default is 0.

Min AS Origination (seconds)

(minASOrigination)

The Min AS Origination (seconds) parameter specifies, in seconds, the minimum interval in which an AS path setting that is originated by the local device can be advertised to a peer. The range is 2 to 255. The default is 15.

Min. Route Advertisement

(minRouteAdvertisement)

The Min. Route Advertisement parameter specifies the minimum interval, in seconds, at which a path parameter can be advertised to a peer. The range is 1 to 255. The default is 30.

Minimum TTL Value

See the [Minimum TTL Value](#) parameter in section 203.1.

Multi Hop

(multiHop)

The Multi Hop parameter specifies the TTL value entered in the IP header of packets sent to an EBGp peer multiple hops away. The range is 0 to 255. The default is 0.

Multi Path

(multiPath)

The Multi Path parameter specifies the number of equal cost routes to use for multipath routing. This allows BGP load sharing of traffic across multiple links. The range is 1 to 16. The default is 1, which means that BGP load sharing is disabled.

When the number of equal cost routes that are available is greater than the parameter, routes with the lowest next hop IP address value are chosen. When the parameter is set to 1 and multiple equal cost routes are available, the route with the lowest next hop IP address is used.

Name

(siteName)

See the [Name](#) parameter in section 203.1.

Next Hop Self

(nextHopSelf)

The Next Hop Self parameter specifies whether the group or neighbor should always set the next hop AS path setting to its physical interface when advertising to an eBGP peer. Table 189-15 describes the parameter options.

Table 189-15 Next Hop Self parameter

Option	Option description	Dependencies
false (default)	Third-party route advertisements are allowed.	—
true	Third-party route advertisements are not allowed. Use the true option to avoid third-party route advertisements when the device is connected to a multi-access network.	

Passive

(passive)

The Passive parameter specifies whether passive mode is enabled or disabled for BGP. Table 189-16 describes the parameter options.

Table 189-16 Passive parameter

Option	Option description	Dependencies
false (default)	BGP actively tries to connect to all the configured peers.	—

(1 of 2)

Option	Option description	Dependencies
true	BGP is in passive mode. BGP does not attempt to actively connect to the configured BGP peers but responds only when it receives a connect open request from the peer.	—

(2 of 2)

Peer Address

(peerAddress)

The Peer Address parameter specifies the IP address of the far-end peer. Specify an IPv4 address in dotted-decimal format, an IPv6 address in colon-hexadecimal format, or an IPv6 address in colon-hexadecimal format with a zone index. Specify a DNS address in the form of a string. The default is 0.0.0.0, which specifies that the address is not configured.

Peer AS

(peerAS)

The Peer AS parameter specifies a virtual, also known as a local, AS number for the remote peer. The parameter must be configured for each configured peer. The range is 0 to 4294967295. The default is 0, which specifies that the parameter is not set.

For eBGP peers, the value must not be the same as the AS number configured for this device at the global level, because the peer is in a different AS. For IBGP peers, the value must be the same as the AS number of this device at the global level.

Peer Type

(peerType)

The Peer Type parameter specifies the type of BGP peer. Table 189-17 describes the parameter options.

Table 189-17 Peer Type parameter

Option	Option description	Dependencies
None (default)	The type of neighbor is determined from the local AS.	—
Internal	The peer is an IBGP peer.	For connections to devices in internal systems
External	The peer is an EBGP peer.	For connections to devices in external systems

Policy 1

(inheritanceMask)

See the [Policy 1](#) parameter in section [203.1](#).

Policy 2

(inheritanceMask)

See the [Policy 1](#) parameter in section [203.1](#).

Policy 3

(inheritanceMask)

See the [Policy 1](#) parameter in section [203.1](#).

Policy 4

(inheritanceMask)

See the [Policy 1](#) parameter in section [203.1](#).

Policy 5

(inheritanceMask)

See the [Policy 1](#) parameter in section [203.1](#).

Preference

See the [Preference](#) parameter in section [203.1](#).

Prefix Limit

(prefixLimit)

The Prefix Limit parameter specifies the maximum number of routes that the BGP can learn from a peer. When the number of routes reaches 90% of this limit, an SNMP trap is sent from the device to indicate that the threshold limit has almost been reached. If the parameter value is exceeded, BGP peering is dropped and disabled, another SNMP trap is sent to indicate that the threshold limit has been reached. The range is 0 to 4 294 967 295. The default is 0.

Prefix Limit Log Only

(prefixLogOnly)

The Prefix Limit Log Only parameter specifies whether BGP peering will be disabled when tBgpPeerGroupMaxPrefix is exceeded. This parameter is configurable for a peer if the [“Inherit Value”](#) parameter in the Prefix Limit panel is disabled. Table [189-18](#) describes the parameter options.

Table 189-18 Prefix Limit Log Only parameter

Option	Option description	Dependencies
false (default)	BGP peering is disabled.	—
true	BGP peering is enabled.	—

Prefix Limit Threshold

(prefixThreshold)

The Prefix Limit Threshold parameter specifies a percentage of the “[Prefix Limit](#)” parameter. This parameter is configurable for a peer if the “[Inherit Value](#)” parameter in the Prefix Limit panel is disabled. The range is 1 to 100. The default is 90.

Private

(localASPrivate)

The Private parameter specifies whether the Local AS parameter number is displayed in paths that are learned from the peering. Table [189-19](#) describes the parameter options.

Table 189-19 Private parameter

Option	Option description	Dependencies
false (default)	The local AS parameter value is not private.	—
true	The Local AS parameter value is private, and cannot be determined from paths learned from peering.	

Purge Time (minutes)

(purgeTime)

The Purge Time (minutes) parameter specifies, in minutes, the maximum time between. The range is 1 or 3 to 60. The default is 10.

Remove Private AS

(removePrivateAS)

The Remove Private AS parameter specifies whether private AS numbers are removed from the AS path before the path is advertised to BGP peers. Table [189-20](#) describes the parameter options.

Table 189-20 Remove Private AS parameter

Option	Option description	Dependencies
false (default)	The private AS number is advertised to peers.	The following AS numbers are considered private: 64 512 to 65 535.
true	The private AS number is not advertised to peers.	

Router ID

See the [Router ID](#) parameter in section [203.1](#).

Stale Routes Time (seconds)

(**staleRoutesTime**)

The Stale Routes Time parameter specifies the maximum time, in seconds, that stale routes are maintained after a graceful restart is started. You can configure the parameter when the Graceful Restart parameter is set to true. The range is 1 to 3600. The default is 360.

Type

See the [Type](#) parameter in section [203.1](#).

190 –IGMP parameters

190.1 IGMP parameters 190-2

190.1 IGMP parameters

This chapter describes the parameters on the IGMP forms, and the child forms launched from the right-click contextual menu options for IGMP.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Administrative Version

(adminVersion)

The Administrative Version parameter specifies the configured version of IGMP on this IGMP interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP. The options are:

- Version 1
- Version 2
- Version 3 (default)

Configured Source

(configSrcAddr)

The Configured Source parameter specifies a source address for the group range. When a report is received in the range specified by the Start Mcast Address parameter and the End Mcast Address parameter, it is translated to a report with the value of this parameter as the source address. The default is 0.0.0.0, which means that the parameter is not configured.

Configured Source Type

(srcAddrType)

The Configured Source Type parameter specifies the IP protocol type for the multicast address of the group range. The value is set to IPv4 and cannot be changed.

Constraint Admin State

(mCacConstAdminState)

The Constraint Admin State parameter specifies the administrative state of the multicast CAC policy's constraints. The options are:

- Up (default)
- Down

Description

See the [Description](#) parameter in section 203.1.

End Mcast Address

(toGrpAddr)

The End Mcast Address parameter specifies the end of the group range. The value of this parameter must be greater than or equal to the value of the Start Mcast Address parameter. The range is an IP address from 224.0.1.0 to 239.255.255.255. The default is 239.255.255.255.

End Mcast Address Type

(toGrpAddrType)

The End Mcast Address Type parameter specifies the IP protocol type for the multicast address of the end of the group range. The value is set to IPv4 and cannot be changed.

Import Policy

(importPolicy)

The Import Policy parameter specifies the routing policy applied to this IGMP interface. Specify a policy name that is no more than 32 characters long, or click on the Select button to choose a policy.

Last Member Query Interval (seconds)

(genLastMembQueryIntvl)

The Last Member Query Interval (seconds) parameter specifies, in seconds, the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages, and is also the amount of time between Group-Specific Query messages. Tune this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. The range is 1 to 1024. The default is 1.

Last Member Query Interval (tenths of seconds)

(genLastMembQueryIntvl)

The Last Member Query Interval (tenths of seconds) parameter specifies the IGMP last member query interval on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to set the parameter on the system or the specified VLAN.

The IGMP last member query interval refers to the amount of time to reply to an IGMP query message that is sent in response to a leave group message. The range is 1 to 65 535. The default is 10.

Lsp Name

(lspName)

The LSP Name parameter specifies the name of the LSP used by this routing instance. A minimum of one alphanumeric character is required. There is no default.

Mandatory Bandwidth (kbps)

See the [Mandatory Bandwidth \(kbps\)](#) parameter in section 203.1.

Max Group

(igmpMaxGroupLimit)

The Max Group parameter specifies the maximum number of IGMP group addresses that can be dynamically learned by the OmniSwitch. The range is 0 to 4 294 967 295. The default is 0.

Max Group Action

(igmpMaxGroupExceedAction)

The Max Group Action parameter specifies the action performed if the dynamically learned IGMP group addresses exceed the value specified by the [Max Group](#) parameter. Table 190-1 describes the parameter options.

Table 190-1 Max Group Action parameter

Option	Description
None (default)	When the Max Group parameter is 0, the number of dynamically learned IGMP group addresses is not limited. When the Max Group parameter is not 0, any IGMP group addresses that are dynamically learned after the Max Group value is exceeded are dropped.
Drop	Any IGMP group addresses that are dynamically learned after the Max Group value is exceeded are dropped.
Replace	Any IGMP group addresses that are dynamically learned after the Max Group value is exceeded replace the oldest learned group address.

Maximum Number of Groups

(maxGroups)

The Maximum Number of Groups parameter specifies the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on the interface. The range is 0 to 16 000. The default is 0.

Protocol Version

(igmpVersion)

The Protocol Version parameter specifies the default version of the IGMP on the specified VLAN or on the system when a VLAN is not specified. The options are:

- Version 1
- Version 2 (default)
- Version 3

Proxying

(igmpProxying)

The Proxying parameter specifies whether IGMP proxying is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP proxying refers to the processing of membership information on behalf of client systems and the reporting of the membership on their behalf. The options are:

- Disabled (default)
- Enabled

Querier Forwarding

(igmpQuerierForwarding)

The Querier Forwarding parameter specifies whether IGMP querier forwarding is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP querier forwarding refers to the promotion of detected IGMP queriers to receive all IP multicast data traffic. The options are:

- Disable (default)
- Enable

Query Interval (seconds)

(genQueryInterval)

The Query Interval (seconds) parameter specifies the time period between IGMP query messages. Table 190-2 lists the default and range values for the parameter.

Table 190-2 Query Interval (seconds) parameter

Object	Default	Range
OmniSwitch system or VLAN	125	1 to 65 535
Other	125	2 to 1024

Query Response Interval (seconds)

(genQueryResponseIntvl)

The Query Response Interval (seconds) parameter specifies the maximum query response time, which is advertised in IGMPv2 queries. The range is 1 to 1023. The default is 10.

Query Response Interval (tenths of seconds)

(genQueryResponseIntvl)

The Query Response Interval (tenths of seconds) parameter specifies the IGMP query response interval on the specified VLAN or on the system when a VLAN is not specified.

The query response interval refers to the amount of time to reply to an IGMP query message. The range is 1 to 65 535. The default is 100.

Querying

(igmpQuerying)

The Querying parameter specifies whether IGMP querying is enabled on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to set the parameter on the system or specified VLAN.

IGMP querying refers to the requesting of the network's IGMP group membership information by sending IGMP queries. IGMP querying also involves participation in IGMP querier elections. The options are:

- Disable (default)
- Enable

Robust Count

(genRobustCount)

The Robust Count parameter sets the IGMP robustness variable on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to set the parameter on the system or the specified VLAN.

The robustness variable allows you to fine-tune a network that is expected to have high packet loss. The range is 1 to 7. The default is 2.

Robust Count

(robustCount)

The Robust Count parameter allows you to tune for the expected packet loss on a subnet. If a subnet is expected to have high packet loss, you can increase the parameter value. The range is 2 to 10. The default is 2.

Router Timeout (seconds)

(igmpRouterTimeout)

The Router Timeout (seconds) parameter specifies the expiry time of IP multicast routers on the specified VLAN or on the system if no VLAN is specified. IP multicast switching and routing must be enabled to configure the parameter on the system or the specified VLAN. The range is 1 to 65 635. The default is 90.

Source Timeout (seconds)

(igmpSourceTimeout)

The Source Timeout (seconds) parameter specifies the expiry time of IP multicast sources on the specified VLAN or on the system when a VLAN is not specified. IP multicast switching and routing must be enabled to set the parameter on the system or specified VLAN. The range is 1 to 65 635. The default is 30.

Spoofing

(igmpSpoofing)

The Spoofing parameter specifies whether IGMP spoofing is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP spoofing refers to the replacing of a client MAC and IP address with the system MAC and IP address when proxying aggregated IGMP group membership information. The options are:

- Disable (default)
- Enable

Start Mcast Address

(frGrpAddr)

The Start Mcast Address parameter specifies the start of the SSM group range. The range is an IP address from 224.0.1.0 to 239.255.255.255. The default is 224.0.1.0

Start Mcast Address Type

(frGrpAddrType)

The Start Mcast Address Type parameter specifies the IP protocol type for the multicast address of the start of the SSM group range. The value is set to IPv4 and cannot be changed.

Static Multicast Group

(staticGrp)

The Static Multicast Group parameter specifies the IP multicast group address. The range is an IP address from 224.0.1.0 to 239.255.255.255. The default is 224.0.1.0.

Static Source

(staticSrcGrp)

The Static Source parameter specifies the IP address for the source sending multicast traffic to the group. The default is 0.0.0.0.

Subnet Check

(subnetCheck)

The Subnet Check parameter specifies whether to check for subnets on IGMP messages received on the interface. The options are:

- Enabled (default)
- Disabled

When enabled, any IGMP packets that do not have a source address in the local subnet are dropped.

Unconstrained Bandwidth (kbps)

See the [Unconstrained Bandwidth \(kbps\)](#) parameter in section 203.1.

Unsolicited Report Interval (seconds)

(igmpUnsolicitedReportInterval)

The Unsolicited Report Interval (seconds) parameter sets the value of the IGMP unsolicited report interval on the specified VLAN or on the system when a VLAN is not specified. The unsolicited report interval refers to the amount of time to proxy any changed IGMP membership state. The range is 1 to 65 635. The default is 1.

Zapping

(igmpZapping)

The Zapping parameter specifies whether IGMP zapping is enabled on the specified VLAN or on the system when a VLAN is not specified. IGMP zapping refers to the processing of membership and source filter removals immediately without waiting for the protocol specified time period. This mode facilitates IP TV applications that need to change quickly between IP multicast groups. The options are:

- Disabled (default)
- Enabled

191 –L2TP parameters

191.1 L2TP parameters 191-2

191.1 L2TP parameters

This chapter describes the parameters on the L2TP form, and the child forms opened using the contextual menu options for L2TP.

Administrative State

See [Administrative State](#) in section 203.1.

Authentication Protocol

(authenticationProtocol)

The Authentication Protocol parameter specifies the PPP authentication protocol that is used for negotiation. The value Pref CHAP indicates that an attempt is made to negotiate CHAP first, followed by an attempt to negotiate PAP. When you choose the value PAP (Password Authentication Protocol) or CHAP (Challenge Handshake Authentication Protocol) as the parameter value, you must set the “Password (password)” parameter. The options are:

- Inherit (default)
- PAP
- CHAP
- Pref CHAP

The Inherit option is available on the L2TP tunnel profile PPP form. The Inherit value indicates that the L2TP tunnel profile inherits the configuration from the L2TP tunnel group profile template.

Auto Established

(autoEstablished)

The Auto Established parameter specifies whether the L2TP tunnel is to be set up automatically by the 5620 SAM. If Auto Established is not enabled, the L2TP tunnel is set up on the first attempt to establish a session. The options are:

- enabled
- disabled (default)

AVP Hiding

(avpHiding)

The AVP Hiding parameter specifies whether sensitive data, such as user passwords, are sent as clear text in an AVP. The options are:

- Always
- Never

- Sensitive—AVP Hiding is used only for sensitive information such as usernames or passwords
- Inherit—default, no AVP Hiding (applies only to L2TP tunnel profiles)

The Inherit option uses the value from the L2TP tunnel group profile.

Calling Number Format

(callingNumFmt)

The Calling Number Format parameter specifies the string used in the Calling Number AVP for L2TP control messages related to a session in the L2TP protocol instance. The value applies only when the callingNumber bit is set in the object `tmnxL2tpAvpExclude`. The options are:

- S—system name
- r—Agent Remote ID
- s—SAP ID, formatted as a character string

The default is `%S%s`.

Challenge

(challenge)

The Challenge parameter specifies when challenge-response is to be used for the authentication of L2TP tunnel profiles and L2TP tunnel group profiles in an L2TP group. The options are:

- Always
- Never
- Inherit (default)

Description

See [Description](#) in section [203.1](#).

Destruct Timeout (seconds)

(destructTimeOut)

The Destruct Timeout (seconds) parameter specifies the period of time, in seconds, that the data of a closed tunnel persists before it is removed from the NE.

Table 191-1 Destruct Timeout (seconds) parameter

Object	Range	Default
Tunnel profile	The range is -2, or 60 to 86 400. The values from -1 to 59 are not valid.	-2

(1 of 2)

Object	Range	Default
Tunnel group profile ⁽¹⁾	60 to 86 400	60

(2 of 2)

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Excluded AVPs

(excludeAvp)

The Excluded AVPs parameter specifies whether to exclude L2TP AVPs. For more information, see Calling Number Format in this section. The options are:

- enabled
- disabled (default)

Group Name

(groupName)

The Group Name parameter specifies the name of the tunnel group template. The range is 1 to 63 characters. The default is an empty string.

Hello Interval (seconds)

(helloInterval)

The Hello Interval (seconds) parameter specifies the time interval between consecutive tunnel Hello messages. The Hello message is an L2TP control message sent by LAC-LNS control connection peers.

Table 191-2 Hello Interval (seconds) parameter

Object	Range	Default
Tunnel profile	The range is -2, -1, or 60 to 3600.	-2
Tunnel group profile ⁽¹⁾	The range is -1, or 60 to 3600.	-1

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Idle Timeout (seconds)

(idleTimeOut)

The Idle Timeout parameter specifies how long, in seconds, an established tunnel with no active sessions persists before it is closed. The range is 0 to 3600. The default is -1.

Table 191-3 Idle Timeout (seconds) parameter

Object	Range	Default
Tunnel profile	-2 to 3600	-2
Tunnel group profile ⁽¹⁾	-1 to 3600	-1

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

IPCP Subnet Negotiation

(ipcpNegotiation)

The IPCP Subnet Negotiation parameter specifies whether or not IPCP subnet negotiation is enabled for the tunnels in the L2TP Tunnel Group.

Table 191-4 IPCP Subnet Negotiation parameter

Object	Options	Default
Tunnel profile	<ul style="list-style-type: none"> always inherit never 	inherit
Tunnel group profile ⁽¹⁾	<ul style="list-style-type: none"> always never 	never

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Keep-Alive Interval (seconds)

(keepAliveInterval)

The Keep-Alive Interval (seconds) parameter specifies how often the LCP echo requests are transmitted for tunnels using the Tunnel Group Profile.

Table 191-5 Keep-Alive Interval (seconds) parameter

Object	Range	Default
Tunnel profile	The range is 0, or 10 to 300.	0

(1 of 2)

Object	Range	Default
Tunnel group profile ⁽¹⁾	10 to 300	30

(2 of 2)

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Keep-Alive Multiplier

(keepAliveMultiplier)

The Keep-Alive Multiplier parameter specifies, for the tunnels using the Tunnel Group Profile, how many LCP keepalive messages can be missed before the associated session is brought down.

Table 191-6 Keep-Alive Multiplier parameter

Object	Range	Default
Tunnel profile	0 to 5	5
Tunnel group profile ⁽¹⁾	1 to 5	3

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

LNS Group ID

(lnsGroup)

The LNS Group ID parameter specifies the L2TP ISA group for the L2TP tunnel. If the LNS Group ID parameter is not configured on an L2TP tunnel profile, the L2TP tunnel automatically inherits the value specified on the L2TP tunnel group profile. The range is 0 to 4. The default is 0.

Local IP Address

(localAddress)

The Local IP Address parameter specifies the local L2TP endpoint. On an LNS, the local L2TP endpoint is usually a loopback interface IP address. On a LAC, the local L2TP endpoint is the system interface or a local physical interface. You can specify a local physical interface address only if the interface is on an IOM3 XP in a Release 8.0 or later NE. Specify an IPv4 address in dotted-decimal notation. The default is 0.0.0.0, which means that the parameter is not configured.

Local Name

(localName)

The Local Name parameter specifies the host name used by the 5620 SAM for the L2TP tunnel during the authentication phase of tunnel establishment. The range is 1 to 64.

Max Retries Established

(maxRetriesEstablished)

The Max Retries Established parameter specifies the number of retries for an established tunnel before the control connection goes down.

Table 191-7 Max Retries Established parameter

Object	Range	Default
Tunnel profile	The range is -2, or 2 to 7.	-2
Tunnel group profile ⁽¹⁾	2 to 7	5

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Max Retries Not Established

(maxRetriesNotEstablished)

The Max Retries Not Established parameter specifies the number of retries for a non-established tunnel before the control connection goes down.

Table 191-8 Max Retries Not Established parameter

Object	Range	Default
Tunnel profile	The range is -2, or 2 to 7.	-2
Tunnel group profile ⁽¹⁾	2 to 7	5

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

MTU (bytes)

(mtu)

The MTU (bytes) parameter specifies, in bytes, the maximum PPP MTU size.

Table 191-9 MTU (bytes) parameter

Object	Range	Default
Tunnel profile	The range is 0, or 512 to 9212.	0
Tunnel group profile ⁽¹⁾	512 to 9212	1500

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Password

(password)

The Password parameter specifies the password used for challenge/response calculation and AVP hiding. The maximum length can be up to 20 characters if unhashed, 32 characters if hashed, and 54 characters if the hash2 keyword is specified.

Peer Address Change Policy

(peerAddrChangePcly)

The Peer Address Change Policy parameter specifies the reaction to a change of tunnel peer IP address on the NE. For example, if peer A sends a StartControlConnectionRequest from ip-address X to peer B ip-address Y, peer B can send the corresponding StartControlConnectionReply from another ip-address Z to ip-address X. The options are:

- reject—IP address changes are not allowed. Always transmit to destination-address Y, and accept messages only from source-address Y.
- accept—allow address changes on the StartControlConnectionReply. If the message is received from ip-address Z, transmit to destination-address Z only. Accept messages from source-address Z only.
- ignore—accept messages from any source-address, but always transmit to destination-address Y

Peer IP Address

(peerAddress)

The Peer IP Address parameter specifies the remote L2TP endpoint. The remote L2TP endpoint must match the corresponding local IP address on the other end of the L2TP tunnel. The default is 0.0.0.0.

Preference

(preference)

The Preference parameter specifies the relative preference assigned to a tunnel in a weighted session assignment. The range is 0 to 16 777 215. The value 0 corresponds to the highest preference. The default is 50.

Proxy Authentication

(proxyAuthentication)

The Proxy Authentication parameter specifies the AVP authentication received from the LAC. The options are:

- Always
- Never
- Inherit (default)

Proxy LCP

(proxyLcp)

The Proxy LCP parameter specifies whether the 5620 SAM reuses the result of the LCP negotiation done by the proxy. The options are:

- Always
- Never
- Inherit (default)

Receive Window Size

(receiveWindowSize)

The Receive Window Size parameter specifies the receive window size of each tunnel in the L2TP tunnel group.

Table 191-10 Receive Window Size parameter

Object	Range	Default
Tunnel profile	The range is 0, or 4 to 1024.	64
Tunnel group profile ⁽¹⁾	The range is 0, or 4 to 1024.	64

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Remote Name

(remoteName)

The Remote Name parameter specifies the host name used by the L2TP tunnel peer during the authentication phase of tunnel establishment. This parameter is related to the RADIUS attribute Tunnel-Server-Auth-ID. The range is 0 to 64 characters.

Session Assign Method

(sessionAssignMethod)

The Session Assign Method specifies how new sessions are assigned to one of the set of suitable tunnels that are available or could be made available. The options are:

- None—Each new session is placed by preference in an existing tunnel.
- Weighted—The sessions are shared among the available tunnels. If required, new tunnels are set up until the maximum number is reached. The distribution aims at an equal ratio of the actual number of sessions to the maximum number of sessions.

Session Limit

(sessionLimit)

The Session Limit parameter specifies the number of L2TP sessions allowed on an NE. L2TP is connection-oriented. The LNS and LAC maintain the state for each call that is initiated or answered by a LAC. An L2TP session is created between the LAC and LNS when an end-to-end PPP connection is established between a remote system and the LNS. Datagrams associated with the PPP connection are sent over the tunnel between the LAC and LNS. There is a one-to-one relationship between established L2TP sessions and the associated calls.

Table 191-11 Session Limit parameter

Object	Range	Default
Tunnel profile	1 to 65 535	65 535
Tunnel group profile ⁽¹⁾	1 to 131 071	131 071

Note

- ⁽¹⁾ A tunnel group profile defines the L2TP tunnel configuration used by all L2TP tunnels in the group. A tunnel group profile value is overridden by the configuration of the same parameter for the L2TP tunnel profile.

Tunnel Name

(tunnelName)

The Tunnel Name parameter specifies the name of an L2TP tunnel. A tunnel exists between a LAC-LNS pair and consists of a control connection and zero or more L2TP sessions. The tunnel carries encapsulated PPP datagrams and control messages between the LAC and the LNS. The range is 1 to 32.

Type

See [Type](#) in section 203.1.

192 –LDP parameters

192.1 LDP parameters 192-2

192.1 LDP parameters

This chapter describes the parameters on the LDP form, and the child forms launched from the right-click contextual menu options for LDPs.

Address Type

(addressType)

The Address Type parameter specifies the transport address to be used when you set up the LDP TCP sessions. Table 192-1 describes the parameter options.

Table 192-1 Address Type parameter

Option	Option description	Dependencies
interface	Uses the IP interface address to set up the LDP session between neighbors	Cannot be set when there are multiple interfaces between two neighbors because only one LDP session can be set up between two neighbors
system (default)	Uses the system IP address	—

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Administrative State

(aggPrefixMatchAdminState)

The Administrative State parameter specifies whether the aggregate prefix matching capability is administratively enabled. The options are:

- Up (default)
- Down

Administrative State

(autoAdminState)

The Administrative State parameter specifies whether the LDP tree discovery process starts or stops. When the Administrative State is In Service, the LDP tree discovery process starts, and performs checks periodically on previously discovered paths. When the Administrative State is Out Of Service, the LDP tree discovery process and periodic checking on the discovered paths stop. The options are:

- In Service
- Out Of Service (default)

Administrative State

(egrAccountingAdminState)

The Administrative State parameter specifies whether the object is administratively enabled. The options are:

- Up (default)
- Down

Advertised Label

(advertisedLabel)

The Advertised Label parameter specifies the label value that is advertised to the upstream peer device. The range is 32 to 4 294 967 295. The default is 4 294 967 295, which specifies that the ingress label is dynamically assigned.

When the parameter is not configured, the advertised label is drawn from the label pool. When the configured label is not available, then the IP prefix is not advertised.

Aggregate Prefix Match Enabled

(aggPrefixMatchEnabled)

The Aggregate Prefix Match Enabled parameter specifies whether to allow LDP to install a prefix binding in the LDP FIB by performing a longest match against an aggregate prefix in the routing table, as opposed to requiring an exact match of the prefix. The options are:

- Disabled (default)
- Enabled

Description

See the [Description](#) parameter in section 203.1.

Discovery Interval (Minutes)

(autoDiscIntvl)

The Discovery Interval (minutes) parameter specifies the number of minutes before repeating the LDP tree discovery process. The range is 60 to 1440. The default is 60.

Discovery Timeout (Seconds)

(autoTrTimeOut)

The Discovery Timeout (seconds) parameter specifies the number of seconds before a LSP trace request will timeout during the tree discovery. The range is 1 to 60. The default is 30.

DoD Label Distribution

(dodLabel)

The DoD Label Distribution parameter

This feature adds support for Downstream on-Demand (DoD) label allocation, as per RFC 5036. This feature can only be enabled on a link level LDP session and applies to prefix labels only, not service labels.

When this option is enabled, LDP sets the A-bit in the Label Initialization message after the LDP session to the peer is established. When both peers set the A-bit, they both use the DoD label distribution method over the LDP session. The options are:

- Disabled (default)
- Enabled

Enforce Graceful Restart

(gracefulRestart)

The Enforce Graceful Restart parameter specifies whether the device acts as a graceful restart helper for LDP peers. The options are:

- Disabled (default)
- Enabled

FEC Prefix

(prefix)

The FEC Prefix parameter specifies the IP address of the FEC element for which statistics are collected. The default value is 0.0.0.0.

Forward State Holding Time (seconds)

(fwdStateHoldingTime)

The Forward State Holding Time parameter specifies the amount of time, in seconds, that the LDP router retains its MPLS forwarding state after a graceful restart. The range is 15 to 1800. The default is 120.

Forwarding Class

See the [Forwarding Class](#) parameter in section 37.1.

Hello Factor

(helloFactor)

The Hello Factor parameter specifies, for an interface or a targeted peer, the number of LDP hello messages that should be sent on an idle LDP session within the Hello Timeout (seconds) interval. The range is 1 to 255. The default is 3.

LDP hello messages are used to discover neighbors and to detect a loss of neighbor connectivity.

Hello Timeout (seconds)

(helloTimeout)

The Hello Timeout (seconds) parameter specifies for an interface or a targeted peer, in s, the interval to wait before a neighbor is declared down. The range is 2 to 65 535. The default is 15.

The Hello Factor parameter derives the hello interval. The Hello Factor parameter setting is local to the system and sent in the LDP hello messages to the neighbor. The Hello Factor parameter setting cannot be less than three times the Hello Timeout (seconds) parameter interval. The hold time can be configured globally or for each interface.

When an LDP session is set up, the hold time is negotiated to the value that is lower for the two peers. After an operational value is agreed upon, the Hello Timeout (seconds) parameter is used to derive the value of the Hello Factor parameter.

IP Prefix

(ipPrefix)

The IP Prefix parameter specifies the IP address prefix for the configured FEC. The value is an IPv4 address in dotted-decimal format. There is no default.

Keep-Alive Factor

(keepAliveFactor)

The Keep-Alive Factor parameter specifies, for an interface or a targeted peer, the number of keep-alive messages that should be sent on an idle LDP session in the Keep-Alive Timeout (seconds) parameter interval. The range is 1 to 255. The default is 3.

Keep-alive messages are used to prevent the LDP session from timing out when no LDP traffic is being exchanged between devices.

Keep-Alive Timeout (seconds)

(keepAliveTimeout)

The Keep-Alive Timeout (seconds) parameter specifies for an interface, in seconds, the interval that LDP waits before tearing down the session. The Keep-Alive Factor parameter derives the keep-alive interval. The range is 2 to 65 535. The default is 30.

If no LDP messages are exchanged for the configured time interval, the LDP session is torn down. The parameter setting is typically three times the Keep-Alive Factor parameter value. To maintain the session permanently, regardless of inactivity, set the parameter to 0.

When LDP session is set up, the keep-alive timeout value is negotiated to the lower of the two peers. After an operational value is agreed upon, the Keep-Alive Factor parameter value is used to derive the value of the keep-alive interval.

Key

See the [Key](#) parameter in section [203.1](#).

LDP Prefix

(ldpPrefix)

The LDP Prefix parameter specifies the address prefix of the destination node for a testTargetType of router. This parameter is specified when test TargetType is ldpPrefix. The value is an IPv4 address in dotted-decimal format. The default is 0.0.0.0.

LDP Prefix Length

(ldpPrefixLen)

The LDP Prefix Length parameter specifies the Internet address prefix length for the LDP based LSP for the OAM LDP Tree discovery test. The value of this parameter is valid only when the [IP Prefix](#) parameter is configured. The parameter can be set to 32. The default is 32.

Local LSR ID

(localLsrType)

The Local LSR ID parameter specifies whether the local interface address or the system interface address should be used as the source Label Switch Router identifier (LSR ID) to establish a link LDP adjacency with an LDP peer. The options are:

- Interface
- System (default)

Maximum Failures

See the [Maximum Failures](#) parameter in section [116.1](#).

Maximum Paths

(autoMaxPath)

The Maximum Paths parameter specifies the maximum number of paths that can be discovered for a selected FEC IP Address. The range is 1 to 128. The default is 128.

Maximum Recovery Time (seconds)

(maximumRecoveryTime)

The Maximum Recovery Time (seconds) parameter specifies the local maximum recovery time, in seconds, after the detection of a graceful restart. When the neighbor LSR advertises a non-zero Recovery Time to indicate that the MPLS forwarding state is preserved, the local LSR retains the label-to-FEC bindings for the lesser of the parameter value and the advertised recovery time. The parameter is configurable when the [Enforce Graceful Restart](#) parameter is enabled. The range is 15 to 1800. The default is 120.

Maximum Time to Live

See the [Maximum Time to Live](#) parameter in section [116.1](#).

Maximum TTL

(autoTrMaxTtl)

See the [Maximum TTL](#) parameter in section [203.1](#).

Minimum TTL Value

See the [Minimum TTL Value](#) parameter in section [203.1](#).

Multicast Forwarding

(multicastFwdEnabled)

The Multicast Forwarding parameter specifies whether multicast traffic forwarding is enabled on the interface. The options are:

- Enabled (default)
- Disabled

Multi Path Make Before Break Time (seconds)

(mpMBBTime)

The Multi Path Make Before Break Time (seconds) parameter specifies the maximum time an MP transit node must wait before switching over to a new path if the new node does not send a MBB, TLV to indicate the availability of the data plane. The range is 0 to 10. The default is 3.

Name

(localLsrPointer)

The Name parameter specifies the name of a Local LSR ID interface. You configure this by clicking the associated Select button. The parameter provides the ability to configure and initiate multiple T-LDP sessions on the same system using different LDP LSR IDs. In addition, it allows you to use the LDP local interface address instead of the system address as the LSR ID for the LDP sessions. You can use the system interface, but also any other router loopback interface or local interface address on a per T-LDP/LDP session basis. By default, a T-LDP session uses the system interface.

Neighbor Liveness Time (seconds)

(neighborLivenessTime)

The Neighbor Liveness Time (seconds) parameter specifies the time, in seconds, that the LSR compares with the FT reconnect timeout advertised by the neighbor. The lesser of the values determines how long the LSR retains label-to-FEC bindings after the detection of a graceful restart. If the LSR does not establish an LDP session with the neighbor before this time elapses, the bindings are considered stale and are deleted. The parameter is configurable when the [Enforce Graceful Restart](#) parameter is enabled. The range is 5 to 300. The default is 120.

NE Persistent

See the [NE Persistent](#) parameter in section [116.1](#).

Next Hop

(nextHopAddr)

The Next Hop parameter specifies the next hop of the LSP. The parameter is configurable when the Next Hop Type parameter is set to IP Address. The range is an IPv4 address in dotted-decimal format. There is no default.

Next Hop Type

(nextHopType)

The Next Hop Type parameter specifies the type of next hop. Table [192-2](#) describes the parameter options.

Table 192-2 Next Hop Type parameter

Option	Option description	Dependencies
unspecified (default)	Specifies that the next hop has not been configured	You must change the default to one of the two valid options: IP Address or Pop.
IP Address	Specifies that the next hop is an IP address	You must configure the Next Hop Address parameter.
Pop	Specifies that there is no next hop	—

Number of Test Probes

See the [Number of Test Probes](#) parameter in section [116.1](#).

Probe History Size

(rows)

See the [Probe History Size \(rows\)](#) parameter in section [116.1](#).

Probe Interval (seconds)

See the [Probe Interval \(seconds\)](#) parameter in section [116.1](#).

Peer Address**(peerAddress)**

The Peer Address parameter specifies the IP address of the targeted LDP peer. Specify an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format. Specify a DNS address in the form of a string. For an LDP peer, specify an IPv4 address in dotted-decimal format.

Policy 1

See the [Policy 1](#) parameter in section [203.1](#).

Policy 2

See the [Policy 1](#) parameter in section [203.1](#).

Policy 3

See the [Policy 1](#) parameter in section [203.1](#).

Policy 4

See the [Policy 1](#) parameter in section [203.1](#).

Policy 5

See the [Policy 1](#) parameter in section [203.1](#).

Prefer Tunnel-in-Tunnel**(preferTunnelInTunnel)**

The Prefer Tunnel-in-Tunnel parameter specifies whether LDP tunnel-in-tunnel is preferred over link-level LDP tunnel. The parameter is configurable on the 7710 SR, 7450 ESS, and 7750 SR. The options are:

- enabled
- disabled (default)

Prefix Length**(prefixLength)**

The Prefix Length parameter specifies the IP-address bit mask for the configured FEC. The range is 1 to 32. The default is 0, which means that the bit mask is unspecified.

Probe Interval (Minutes)

(autoProbeIntvl)

The Probe Interval parameter specifies the number of minutes to wait before repeating a probe on a discovered path. The range is 1 to 60. The default is 1.

Probe Timeout (seconds)

See the [Probe Timeout \(seconds\)](#) parameter in section 116.1.

Probe Timeout (Minutes)

(autoPrTimeOut)

The Probe Timeout parameter specifies the time-out value, in minutes, for a ping request during probing. Probe Timeout cannot be greater than the value of the [Probe Interval \(Minutes\)](#) parameter. The range is 1 to 3. The default is 1.

Profile

See the [Profile](#) parameter in section 37.1.

Reconnect Time (seconds)

(reconnectTime)

The Reconnect Time parameter is used to specify the amount of time, in seconds, that neighboring LDP routers should wait for the sender of the LDP message to gracefully restart and resume sending LDP messages to the neighbor. The range is 15 to 1800. The default is 120.

Remote Peer

(peerAddress)

The Remote Peer parameter specifies the IP address of the targeted LDP peer to determine the address for MD5 authentication.

Retry Count

(autoPrMaxFailures)

The Retry Count parameter specifies the maximum number of consecutive timeouts allowed before failing a path probe. The range is 1 to 10. The default is 3.

Retry Count

(autoTrMaxFailures)

The Retry Count parameter specifies the maximum number of consecutive timeouts allowed before terminating an LSP trace request to a hop. The range is 1 to 10. The default is 3.

Retry Counter

(retryCount)

The Retry Counter parameter specifies the maximum number of consecutive timeouts allowed before failing a path probe. The range is 1 to 255. The default is 3.

Swap Label

(swapLabel)

The Swap Label parameter specifies the egress label associated with the next hop. The LSR switches the incoming label with the configured swap label. The range is 16 to 1 048 575, or 4 294 967 295, indicating that the parameter is disabled. The default is 4 294 967 295. The default action is for the LSR to pop the incoming label if the Next Hop parameters are unspecified. The parameter is configurable when the Next Hop Type parameter is set to IP Address.

Targeted Sessions Allowed

(targetedSessions)

The Targeted Sessions Allowed parameter specifies whether to configure the router for T-LDP. Table 192-3 describes the parameter options.

Table 192-3 Targeted Sessions Allowed parameter

Option	Option description	Dependencies
true (default)	Enable T-LDP on the router. Targeted LDP sessions are used to distribute labels between non-directly connected peers. The discovery messages are sent to the specific peer, rather than to the multicast address.	—
false	Disable T-LDP.	

Timeout (seconds)

(timeOut)

The Time Out parameter specifies the time-out value, in seconds, for an LSP trace request during tree discovery. The range is 1 to 60. The default is 30.

Trap Generation

See the [Trap Generation](#) parameter in section 116.1.

Tree Trace

(autoRowStatus)

The Tree Trace parameter specifies the configuration state of the LDP ECMP OAM trace tree. The options are:

- Not Configured (default)
- Configured
- Unspecified

Tunnel Down Damp Time (seconds)

(tunnelDownDampTime)

The Tunnel Down Damp Time (seconds) parameter specifies how long, in seconds, an LDP waits before sending a tunnel down event to the route table manager. The range is 0 to 20. The default is 3. A value of 0 specifies that tunnel down event messages are not sent.

Tunneling Enabled

(tunnelingEnabled)

The Tunneling Enabled parameter specifies whether tunneling of LDP over RSVP tunnels is enabled. The options are:

- enabled (default)
- disabled

Type

See the [Type](#) parameter in section [203.1](#).

193 –MLD parameters

193.1 MLD parameters 193-2

193.1 MLD parameters

This chapter describes the parameters on the MLD forms and the child forms launched from the right-click contextual menu options for MLD.

Configured Source

(configSrcAddr)

The Configured Source parameter is used when static SSM translation is created for an MLD routing instance. The parameter specifies a unicast IPv6 address for the group source in the colon-hexadecimal format. There is no default.

End Multicast Address

(toGrpAddr)

The End Multicast Address parameter is used when static SSM translation is created for an MLD routing instance. The parameter specifies an end multicast IPv6 address for the group range in the colon-hexadecimal format. There is no default.

End Multicast Address

(groupAddress2)

The End Multicast Address parameter is used when static SSM translation is created for an MLD interface. The parameter specifies an end multicast IPv6 address for the group range in the colon-hexadecimal format. There is no default.

Group Address

(groupAddress)

The Group Address parameter is used when a static multicast group is created for an MLD interface. The parameter specifies a multicast IPv6 address for the group in the colon-hexadecimal format. There is no default.

Group Source Address

(groupSourceAddress)

The Group Source Address parameter is used when a static multicast group source is created for an MLD interface. The parameter specifies a unicast IPv6 address for the group source in the colon-hexadecimal format. There is no default.

Import Policy

(importPolicy)

The Import Policy parameter specifies the routing policy statement applied to an MLD interface. Specify a policy name between 0 to 32 characters long, or click on the Select button to choose a policy.

Last Member Query Interval (seconds)

(lastMemberQueryInterval)

The Last Member Query Interval (seconds) parameter specifies the amount of time to reply to an MLD query message that is sent in response to a leave group message. Use this value to modify the leave latency for an MLD routing instance. A reduced value results in reduced time to detect the loss of the last member of a group. The range is 0, or 1 to 1023. The default value of 0 indicates that an interval is not configured.

Maximum Number of Groups

(maxGroups)

The Maximum Number of Groups parameter specifies the maximum number of multicast groups for which an MLD interface can have local receiver information based on received MLD reports on the interface. The range is 0, or 1 to 16 000. The default value of 0 indicates that a maximum value is not configured.

Maximum Response Time between Group Messages (seconds)

(lastMembQueryIntvl)

The Maximum Response Time between Group Messages (seconds) parameter specifies a maximum response time for answering leave group messages, at an MLD interface level. The range is 0, or 1 to 1023. The default value of 0 indicates that a maximum value is not configured.

Maximum Response Time For MLDv2 (seconds)

(queryResponseIntvl)

The Maximum Response Time For MLDv2 parameter specifies the maximum response time for answering general MLDv2 queries, at an MLD interface level. The range is 0, or 1 to 1023. The default value of 0 indicates that a maximum value is not configured.

Query Interval (seconds)

(queryInterval)

The Query interval (seconds) parameter specifies the frequency at which the MLD Host-Query packets are transmitted, for an MLD routing instance. The range is 2 to 1024. The default is 125.

Query Interval (seconds)

(queryInterval)

The Query interval (seconds) parameter specifies the time period between MLD query messages, for an MLD interface. The range is 0, or 2 to 1024. The default value of 0 indicates that an interval is not configured.

Query Response Interval (seconds)

(queryResponseInterval)

The Query Response Interval (seconds) parameter specifies the maximum query response time for Mldv2 queries, at an MLD routing instance level. The range is 1 to 1023. The default is 10.

Robust Count

(robustCount)

The Robust Count parameter allows you to modify the expected packet loss for an MLD routing instance subnet. If a subnet is expected to have high packet loss, you can increase the parameter value. The range is 2 to 10. The default is 2.

Start Multicast Address

(groupAddress1)

The Start Multicast Address parameter is used when static SSM translation is created for an MLD interface. The parameter specifies a start multicast IPv6 address for the group range in the colon-hexadecimal format. There is no default.

Start Multicast Address

(frGrpAddr)

The Start Multicast Address parameter is used when static SSM translation is created for an MLD routing instance. The parameter specifies a start multicast IPv6 address for the group range in the colon-hexadecimal format. There is no default.

194 –MPLS parameters

194.1 MPLS parameters 194-2

194.1 MPLS parameters

This chapter describes the parameters on the MPLS forms, and the child forms launched from the right-click contextual menu for MPLS in the network navigation tree.

Adjust Multiplier

(autoBWAdjMul)

The Adjust Multiplier parameter specifies the global default for collection intervals in an adjust interval. The range is 1 to 16 383. The default is 288.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Administrative State

(ingAccountingAdminState)

The Administrative State parameter specifies whether the object is administratively enabled. The options are:

- Up (default)
- Down

Collect Accounting Statistics

(ingAccountingOn)

The Collect Accounting Statistics parameter specifies whether the collection of ingress accounting statistics on the routing instance is enabled. The options are:

- Enabled (default)
- Disabled

CSPF On Loose Hop

(cspfOnLooseHop)

The CSPF On Loose Hop parameter specifies whether the CSPF calculation is enabled or not for next hop. The options are:

- Enabled
- Disabled (default)

Description

See the [Description](#) parameter in section 203.1.

Enable

(holdTimer)

The Enable parameter specifies whether the ingress NE waits before it programs the LSP data plane and signals to the service module that the LSP is operationally up. The parameter works in conjunction with the [Hold Timer \(seconds\)](#) parameter. Disabling the parameter sets the [Hold Timer \(seconds\)](#) parameter to 0. The options are:

- Enabled (default)
- Disabled

Enable

(resignalTimer)

The Enable parameter specifies whether to resignal LSPs at a regular interval. The parameter works in conjunction with the [Resignal Timer \(min\)](#) parameter. The options are:

- Enabled
- Disabled (default)

The following rules apply when the parameter is set to Enabled.

- Only LSPs with CSPF enabled are resigned.
- Only LSPs configured for make-before-break functionality are resigned.
- After the device performs a resignal, the [Resignal Timer \(min\)](#) parameter specifies the interval, in minutes, before the next LSP resignal attempt.

If the resignal timer expires because the new recorded hop list for an LSP has a better metric than the current recorded hop list, MPLS attempts to resignal the LSP using the make-before-break mechanism. If the attempt to resignal an LSP fails, the LSP continues to use the existing path and MPLS attempts to resignal the LSP when the timer expires.

The Next Resignal parameter indicates the time remaining, in minutes, for the resignal timer to expire.

Enable SRLG for FRR

(enableSrlgFrr)

The Enable SRLG for FRR parameter specifies whether a Shared Risk Link Group constraint is used in the computation of an FRR bypass or detour to be associated with any primary LSP path on the system. When the Enable SRLG for FRR parameter is enabled, the SRLG constraint is used. The options are:

- Enabled
- Disabled (default)

Exponential Backoff Retry

(expBackoffRetry)

The Exponential Backoff Retry parameter specifies the state of the exponential backoff retry mechanism. When the parameter is enabled, an exponential backoff timer is employed when an LSP retries as a result of being in the unmapped state or when the path message fails. The options are:

- Enabled
- Disabled (default)

Fast Reroute

(fastRerouteEnabled)

The Fast Reroute parameter specifies whether fast reroute is signaled for LSPs that use facility bypass. The options are:

- true (default)
- false

Groups Included

(adminGroupInclude)

The Groups Included parameter specifies the MPLS administrative group that the MPLS interface belongs to, in a bitmap format. You can create these groups by choosing Policies→MPLS Administration Groups. You can add or exclude groups from the Groups Included parameter by choosing the Administrative Groups tab.

Hold Timer (seconds)

(holdTimer)

The Hold timer (seconds) parameter specifies the time, in seconds, that the ingress NE waits before it programs the LSP data plane and signals to the service module that the LSP is operationally up. The parameter is configurable when the [Enable](#) parameter is enabled. The range is 0 to 10. The default is 1. A value of 0 means that the parameter is not configured.

Include Groups Assigned

(adminGroupInclude)

The Include Groups Assigned parameter specifies the assigned MPLS administrative groups to include on an MPLS interface. You can create MPLS administrative groups by choosing Policies→MPLS Administration Groups.

Include Groups Unassigned

(adminGroupInclude)

The Include Groups Unassigned parameter specifies the unassigned MPLS administrative groups to include on an MPLS interface. You can create MPLS administrative groups by choosing Policies→MPLS Administration Groups.

Inter Area CSPF To First Loose Hop

(cspfToFirstLooseHop)

The Inter Area CSPF To First Loose Hop parameter specifies whether the CSPF calculation until the first loose hop on ingress Label Edge Router (LER) is enabled or disabled for this Labeled Switched Path (LSP). The options are:

- Enabled
- Disabled (default)

Least Minimum Threshold

(leastFillMinThd)

The Least Minimum Threshold parameter is utilized by CSPF in the least-fill path selection process, for LSP paths that have the [Least-Fill Path Selection](#) parameter enabled. It specifies the percentage of least-available link bandwidth in a path, below which paths that are being compared by CSPF are considered to be equal.

This parameter is a percentage and the range is from 1 to 100. The default value is 5.

Least Reoptimization Threshold

(leastFillReoptThd)

The Least Reoptimization Threshold parameter is utilized by CSPF in the least-fill path selection process. During a timer-based re-signaling of an LSP path that has the [Least-Fill Path Selection](#) parameter enabled, CSPF first updates the least-available link bandwidth figure for this current LSP path. It then applies the least-fill path selection method to select a new path for the LSP.

If the new computed path has the same or lower cost as the current path, CSPF compares the least-available link bandwidth figures of the two paths. If the difference exceeds the Least Reoptimization Threshold parameter that you set, MPLS indicates to 5620 SAM that a better least-fill path is available for this LSP. 5620 SAM then triggers a manual re-signaling of the LSP path to adopt the new path.

This parameter is a percentage and the range is from 1 to 100. The default value is 10.

LSP Name

(lspName)

The LSP Name parameter specifies the name of the dynamic LSP used by this MPLS routing instance. A minimum of one alphanumeric character is required. There is no default.

Propagate Admin Group

(propAdminGroup)

The Propagate Admin Group parameter specifies whether the propagation of the session attribute object with resource affinity (C-type 1) in the PATH message is enabled. The options are:

- Enabled
- Disabled (default)

Resignal Timer (min)

(resignalTimer)

The Resignal Timer (min) parameter specifies the interval, in minutes before another LSP resignal is performed. The range is 0, or 30 to 10 080. The default is 0, which means that the parameter is disabled.

You can configure the parameter when the [Enable](#) parameter is set to Enabled.

If the resignal timer expires because the new recorded hop list for an LSP has a better metric than the current recorded hop list, an attempt is made to resignal that LSP using the make-before-break mechanism. If the attempt to resignal an LSP fails, the LSP continues to use the existing path, and a resignal is attempted the next time that the timer expires.

The Next Resignal parameter indicates the time remaining, in minutes, for the resignal timer to expire.

Sample Multiplier

(autoBWSampleMul)

The Sample Multiplier parameter specifies the global default for collection intervals in a sample interval. The range is 1 to 511. The default is 1.

Sender Address

(senderAddress)

The Sender Address parameter specifies the IPv4 address of the NE for which you need to enable the collection of ingress accounting statistics. The default is 0.0.0.0.

Static LSPs Fast Retry Timer (seconds)

(staticLspFRTimer)

The Static LSPs Fast Retry Timer (seconds) parameter specifies the value, in seconds, used as fast retry timer for static LSPs which are not currently up. The range is 1 to 30 seconds. The default value is 1.

Strict

(srlgStrict)

The Strict parameter specifies whether to associate the LSP with a bypass or signal detour if a bypass or detour satisfies all other constraints except the SRLG constraints. When the Strict parameter is enabled but a path that meets SRLG constraints is not found, then the bypass or detour is not set up. The Strict parameter can only be configured when the [Enable SRLG for FRR](#) parameter is enabled. The options for the Strict parameter are:

- enabled
- not enabled (default)

View the newly created MPLS path

The View the newly created MPLS path parameter specifies whether you want to view the configuration information for the newly created MPLS path using the MPLS Path form. The options are:

- Enabled
- Disabled (default)

195 –MSDP parameters

195.1 MSDP parameters 195-2

195.1 MSDP parameters

This chapter describes the parameters on the MSDP forms and the child forms launched from the right-click contextual menu options for MSDP.

Administrative State

See the [Administrative State](#) parameter in section [203.1](#).

Data Encapsulation

(encapsulation)

The Data Encapsulation parameter specifies whether to encapsulate multicast data received from MSDP register messages inside forwarded MSDP source active messages. The options are:

- Enabled (Default)
- Disabled

Default Peer

(defaultPeer)

The Default Peer parameter specifies whether source-active messages from a peer is accepted without the usual peer-reverse-path-forwarding (RPF) check. The options are:

- Enabled
- Disabled (Default)

IP Prefix

(ipAddress)

The IP Prefix parameter specifies the IP address of the source from which the source active messages that is accepted. The default is 0.0.0.0.

Key

See the [Key](#) parameter in section [203.1](#).

Local IP Address

(localIpAddress)

The Local IP Address parameter specifies the IP address that is used by the local end of an MSDP session to communicate with MSDP peers. Outgoing connections use the parameter as the source of the TCP connection when they initiate connections with a peer. The default is 0.0.0.0.

Mask

(mask)

The Mask parameter specifies the mask to be used along with the IP Prefix parameter to obtain the range of addresses from which the router can accept source active messages. The range is 0 to 128. The default is 24.

Mode

(mode)

The Mode parameter specifies whether a group of peers is configured in a full mesh topology. The options are:

- Standard (Default)
- Mesh

When the Mesh option is selected, source-active messages received from a mesh group member are always accepted but are not flooded to other members of the same mesh group. The result is that the source-active messages are only flooded to non-mesh group peers or members of other mesh groups.

Name

See the [Name](#) parameter in section 203.1.

Peer Address

(peerAddress)

The Peer Address parameter specifies an IPv4 address for the MSDP peer in dotted-decimal format.

Receive Message Interval (seconds)

(receivingRateTime)

The Receive Message Interval (seconds) parameter specifies the period of time, in seconds, that messages specified in the Receive Message Rate parameter are processed during a TCP session. The parameter is configurable when the Receive Message Rate parameter is configured. The range is 1 to 600. The default is 0.

Receive Message Rate

(receivingRate)

The Receive Message Rate parameter specifies the number of MSDP messages, including source active messages, that are read from a TCP session in the interval specified by the Receive Message Interval (seconds) parameter. When the number of MSDP packets defined in the Receive Message Threshold parameter have been processed, additional MSDP packets are no longer accepted from the TCP session until the number of seconds specified in the Receive Message Interval parameter have elapsed. The range is 10 to 10 000. The default is 0, which specifies that messages are not read from the TCP session.

Receive Message Threshold

(receivingRateThreshold)

The Receive Message Threshold parameter specifies the number of MSDP messages that can be processed in a TCP session before the Receive Message Rate parameter is configured. This is useful during system startup and initialization. If the limit is exceeded, MSDP messages are not accepted until the interval specified in Receive Message Interval has elapsed. The parameter is configurable when the Receive Message Rate parameter is configured. The range is 1 to 1 000 000. The default is 0, which specifies that messages are not read from the TCP session.

RPF Lookup Sequence

See the [IPv4 RPF Lookup Sequence](#) parameter in section [203.1](#).

SA Cache Lifetime (seconds)

(sACacheLifetime)

The SA Cache Lifetime (seconds) parameter specifies the lifetime, in seconds, assigned to SA Cache entries, from the time they are received to the time they expire if not refreshed. The range is 90 to 600. The default is 90.

SA Limit

(maxActiveSources)

The SA Limit parameter specifies the maximum number of source active messages to be accepted for an MSDP routing instance. By default, no limit is placed on the number of source active messages, which is specified by the default value of -1. A value of 0 specifies that no source active messages are accepted. The range is -1 to 1 000 000.

Type

See the [Type](#) parameter in section [203.1](#).

196 –PIM parameters

196.1 PIM parameters 196-2

196.1 PIM parameters

This chapter describes the parameters on the PIM forms, and the child forms launched from the right-click contextual menu options for PIM.

Administrative State

See the [Administrative State](#) parameter in section [203.1](#).

Administrative State IPv4

(administrativeStateIpV4)

The Administrative State parameter specifies whether the IPv4-related object is administratively enabled. The options are:

- Up (default)
- Down

Apply To

(applyTo)

The Apply To parameter specifies how PIM interfaces are created and removed. Table [196-1](#) describes the parameter options.

Table 196-1 Apply To parameter

Option	Option description
IES	All PIM interfaces are IES interfaces.
Non-IES	PIM removes all IES interfaces.
All	PIM creates IES and non-IES interfaces.
None (default)	PIM removes all interfaces that are not manually created or modified.

Assert Period

(assertPeriod)

The Assert Period parameter specifies the interval, in seconds, at which PIM assert messages are refreshed on an interface. The range is 1 to 300. The default is 60.

Auto-Discovery

(mdtSafiAutoDiscovery)

The Auto-Discovery parameter specifies the auto-discovery mechanism to be used for discovering peers using BGP. When the value of is set to None, BGP auto-discovery is disabled. When the value is set to Default, BGP auto-discovery is enabled using the default IPMSI AD format. When the value is set to MDT SAFI, BGP auto-discovery is enabled using the MDT-SAFI format. The options are:

- None (default)
- Default
- MDT SAFI

Bandwidth (kbps)

(bandwidth)

The Bandwidth (kbps) parameter specifies the bandwidth in kbps for the level. The range is 1 to 2 147 483 647. The default is 1.

BFD Enabled

(bfdEnabled)

See the [BFD Enabled](#) parameter in section [203.1](#).

BSM Check Router Alert

(bsmCheckRouterAlert)

The BSM Check Router Alert parameter specifies whether checking of the router alert option in a received bootstrap message is enabled. The options are:

- true
- false (default)

CBSR Address

(bsrCandidateAddress)

The CBSR Address parameter specifies the IPv4 address of the candidate BSR. To participate in the bootstrap election, the router sends bootstrap messages that contain the router BSR address. The default is 0.0.0.0.

CBSR Address

(bsrCandidateAddressIPv6)

The CBSR Address parameter specifies the IPv6 address of the candidate BSR. To participate in the bootstrap election, the router sends bootstrap messages that contain the router BSR address. The default is 0:0:0:0:0:0:0:0.

CBSR Admin State

(bsrCandidateAdminState)

The CBSR Admin State parameter specifies whether the IPv4 router participates in the BSR election. When the parameter value is Up, the CBSR Address must be configured and the CBSR Priority parameter value must be non-zero, or bootstrap messages are not sent. The options are:

- Down (default)
- Up

CBSR Admin State

(bsrCandidateAdminStateIPv6)

The CBSR Admin State parameter specifies whether the IPv6 router participates in the BSR election. When the parameter value is Up, the CBSR Address must be configured and the CBSR Priority parameter value must be non-zero, or bootstrap messages are not sent. The options are:

- Down (default)
- Up

CBSR Hash Mask Length

(bsrCandidateHashMaskLength)

The CBSR Hash Mask Length parameter specifies the length of a mask that is to be logically ANDed with the IPv4 group address before the hash function is called. All groups with the same hash map to the same RP. The CBSR Hash Mask Length maps one group or multiple groups to an RP. The range is 0 to 32. The default is 30.

CBSR Hash Mask Length

(bsrCandidateHashMaskLengthIPv6)

The CBSR Hash Mask Length parameter specifies the length of a mask that is to be logically ANDed with the IPv6 group address before the hash function is called. All groups with the same hash map to the same RP. The CBSR Hash Mask Length maps one group or multiple groups to an RP. The range is 0 to 128. The default is 126.

CBSR Priority

(bsrCandidatePriority)

The CBSR Priority parameter specifies whether the router is eligible to be an IPv4 bootstrap router. If the value of this object is set to zero, the router does not participate in the bootstrap election. The range is 0 to 255. The default is 0.

CBSR Priority

(bsrCandidatePriorityIPv6)

The CBSR Priority parameter specifies whether the router is eligible to be an IPv6 bootstrap router. If the value of this object is set to zero, the router does not participate in the bootstrap election. The range is 0 to 255. The default is 0.

C-RP Address

(crpAddress)

The C-RP Address parameter specifies the Candidate Rendezvous Point IPv4 address. This address is sent in the C-RP advertisements to the bootstrap router. The default is 0.0.0.0.

C-RP Address

(crpAddressIPv6)

The C-RP Address parameter specifies the Candidate Rendezvous Point (C-RP) IPv6 address. This address is sent in the C-RP advertisements to the bootstrap router. The default is 0:0:0:0:0:0:0:0.

C-RP Hold Time (seconds)

(crpHoldTime)

The C-RP Hold Time (seconds) parameter specifies the amount of hold time, in seconds, of the candidate RP. The value is used by the IPv4 bootstrap router to time out the RP entries if it does not listen to another C-RP advertisement within the hold time specified by the C-RP Hold Time (seconds) parameter. The range is 5 to 255. The default is 150.

C-RP Hold Time (seconds)

(crpHoldTimeIPv6)

The C-RP Hold Time (seconds) parameter specifies the amount of hold time, in seconds, of the candidate RP. The value is used by the IPv6 bootstrap router to time out the RP entries if it does not listen to another C-RP advertisement within the hold time specified by the C-RP Hold Time (seconds) parameter. The range is 5 to 255. The default is 150.

C-RP Priority

(crpPriority)

The C-RP Priority parameter specifies the IPv4 C-RP priority to become an RP. This value is used to elect RP for a group range. A value of 0 has the highest priority. The range is 0 to 255. The default is 192.

C-RP Priority

(crpPriorityIPv6)

The C-RP Priority parameter specifies the IPv6 C-RP priority to become an RP. This value is used to elect RP for a group range. A value of 0 has the highest priority. The range is 0 to 255. The default is 192.

Data MDT Delay Interval

(dataMdtDelayInterval)

The Data Mdt Delay Interval parameter specifies the interval, in seconds, before the PE router that is connected to the source switches traffic from the default MDT to the data MDT group. The range is 3 to 180. The default is 3.

Data MDT Prefix

(dataMdtPrefix)

The Data Mdt Prefix parameter combines with the Data Mdt Prefix Length parameter to specify the range of SSM group addresses on which the router monitors traffic thresholds. Specify an IP address in dotted-decimal format.

Data MDT Prefix Length

(dataMdtPrefixLength)

The Data Mdt Prefix Length parameter combines with the Data Mdt Prefix parameter to specify the range of SSM group addresses on which the router monitors traffic thresholds.

The range is 0 to 32. The default is 0.

Delay Interval (seconds)

(dataMdtDelayInterval)

The Delay Interval (seconds) parameter specifies the interval (in seconds) before a PE router connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel. The range is 3 to 180. The default is 3.

Description

See the [Description](#) parameter in section [203.1](#).

DR Priority

(drPriority)

The DR Priority parameter specifies the designated router priority for the current interface. The configured DR Priority parameter is sent in PIM Hello messages and is used by routers to elect the DR. The DR election priority is a 32-bit unsigned number and the numerically larger priority takes precedence. The range is 1 to 4 294 967 295. The default is 1.

ECMP Balancing Enabled

(ecmpBalance)

The ECMP Balancing Enabled parameter specifies whether the multicast balancing of traffic over ECMP links is enabled or not.

If the parameter is enabled, each and every multicast stream that needs to be forwarded over an ECMP link is re-evaluated for the total multicast utilization. Re-evaluation occurs on the specific ECMP interface.

This parameter is mutually exclusive with the [ECMP Hashing Enabled](#) parameter. It is not possible to enable ECMP Balancing Enabled when [ECMP Hashing Enabled](#) is enabled.

The default is enabled.

ECMP Hashing Enabled

(ecmpHashing)

The ECMP Hashing Enabled parameter specifies whether or not the multicast balancing of traffic over ECMP links is hash based. If this parameter is enabled, then the multicast balancing of traffic over ECMP links is performed based on the Upstream Multicast Hop (UMH) algorithm.

This parameter is mutually exclusive with the [ECMP Balancing Enabled](#) parameter. It is not possible to enable ECMP Hashing Enabled when [ECMP Balancing Enabled](#) is enabled.

The default is disabled.

Embedded-RP Administrative State

(embeddedRpAdminState)

The Embedded-RP Administrative State parameter specifies whether the Embedded-RP functionality is administratively up or down. The options are:

- Down (default)
- UP

Enable Embedded-RP

(embeddedRp)

The Enable Embedded-RP parameter specifies whether multicast messages are checked for embedded RP information. If the parameter is set to true, then embedded RP is enabled and you can configure group ranges where embedded RP information is used. When the parameter is set to false, embedded RP is disabled and administratively shutdown, and user-configured group ranges are deleted. The options are:

- false (default)
- true

Group Address

(mdtGroupIPAddress)

The Group Address parameter specifies the MVPN multicast group IP address. Specify an IPv4 multicast address in dotted-decimal format. The default is 0.0.0.0.

Group IP Address

(groupAddress)

The Group IP Address parameter specifies the multicast group IP address. Specify an IPv4 multicast address in dotted-decimal format, or an IPv6 multicast address in colon-hexadecimal format.

Group Prefix Length

(groupPrefixLength)

The Group Prefix Length parameter specifies the length of the bit mask that is associated with the Group IP Address parameter. For IPv4, the range is 4 to 32. For IPv6, the range is 8 to 128.

Hello Interval (seconds)

(helloInterval)

The Hello Interval (seconds) parameter specifies the interval, in seconds, at which PIM transmits Hello messages on the routing instance. The range is 0 to 255. The default is 30.

Hello Multiplier

(helloMultiplier)

The Hello Multiplier parameter, combined with the Hello Interval (seconds) parameter, specifies the frequency at which hello messages are sent to neighboring routers. A neighboring router is declared down if it does not respond within a period of 3.5 times the set hello interval. This time ratio can be altered by specifying a hello interval that follows the formula of (hello-interval * hello-multiplier)/10. The range is 20 to 100. The default is 35.

Hold Time (minutes)

(ecmpBalanceHoldTime)

The Hold Time (minutes) parameter specifies the hold time in minutes that applies after an interface has been added to the ECMP link. The range is 1 to 600. The default is 1.

Improved assert

(improvedAssert)

The Improved assert parameter specifies whether improved assert processing on this interface is enabled. The PIM assert process establishes a forwarder for a LAN and requires interaction between the control and forwarding planes. The assert process starts when an outgoing interface receives data and prevents the continuous receipt of data on this interface, which could affect performance. If the parameter is enabled, PIM performs the assert process entirely on the control plane without interaction with the forwarding plane. The options are:

- true (default)
- false

Inclusive Tunnel Type

(mvpnIpmsiType)

The Inclusive Tunnel Type parameter specifies the type of MVPN inclusive tunnel. The options are:

- None (default)
- PIM
- RSVP
- MLDP

Infinity For Threshold

(infinityForThreshold)

The Infinity For Threshold parameter specifies whether an SPT switchover threshold is enabled. If the value of this parameter is false, the Threshold parameter is enabled. The Threshold parameter allows you to specify the traffic volume, in kbps, when the device switches from the shared tree to the source-specific tree. The options are:

- true
- false (default)

IPv4 Administrative State

(administrativeStateIPv4)

The Administrative State parameter specifies whether the IPv4-related object is administratively enabled. The options are:

- Up (default)
- Down

IPv6 Administrative State

(administrativeStateIPv6)

The IPv6 Administrative State parameter specifies whether the IPv6-related object is administratively enabled. The options are:

- Up (default)
- Down

IPv4 RPF Lookup Sequence

See the [IPv4 RPF Lookup Sequence](#) parameter in section [203.1](#).

IPv6 RPF Lookup Sequence

(rpfLookupSequenceIPv6)

The IPv6 RPF Lookup Sequence parameter allows you to indicate which IPv6 routing tables PIM and MDSP use for standard unicast traffic and multicast RPF lookups. When the parameter option is set to Both, PIM and MDSP perform RPF lookups in the unicast routing table first. The options are:

- Multicast Route Table
- Unicast Route Table (default)
- Both

Lag Usage Optimization

(lagUsageOptimize)

The Lag Usage Optimization parameter specifies whether the router should optimize use of the LAG so that traffic for a specific multicast stream destined for an IP interface using the LAG is sent only to the forwarding address that owns the LAG link. When this parameter is set to False, traffic is sent to all the forwarding addresses that own at least one link in the LAG. Changing the value of this parameter causes the PIM protocol to be restarted. The options are:

- True
- False (default)

Level ID

(levelId)

The Level ID parameter specifies the priority of the multicast CAC. The range is 0 to 8. Level 1 has the highest priority; level 8 has the lowest priority. The default is 0.

Level

(level)

The Level parameter specifies the level ID to use when the value of the [Number of Ports Down](#) parameter matches the actual number of ports down in a LAG. The range is 1 to 8. The default is 1.

Lsp Name

(lspName)

The LSP Name parameter specifies the name of the LSP that is used by the routing instance. At least one alphanumeric character is required. There is no default.

Mandatory Bandwidth (kbps)

See the [Mandatory Bandwidth \(kbps\)](#) parameter in section [203.1](#).

Mask

(mask)

The Mask parameter specifies the mask that, combined with the Group IP Address parameter, is used to obtain the range of multicast group addresses to which the router advertises to become the Candidate RP. For IPv4, the range is 4 to 32. For IPv6, the range is 8 to 128.

Max Groups

(maxGroups)

The Max Groups parameter specifies the maximum number of multicast groups for the interface. The range is 0 to 1600. The default is 0.

MCast Signaling

(mcastSignaling)

The MCast Signaling parameter specifies which protocol to use for PE-to-PE signaling of CE multicast states. When the parameter is set to PIM and neighbor discovery using BGP is disabled, then PIM peering is enabled on the inclusive tree. The options are:

- PIM (default)
- BGP
- None

MDT Default Group Address

(mdtGroupIPAddress)

The MDT Default Group Address parameter specifies the default group address used for the multicast distribution tree. The parameter is applicable only when its value corresponds to a multicast tunnel interface for a VPRN. For all other interfaces, this object has a value of 0.0.0.0. For the MDT Default Group Address parameter, specify a multicast IP address in dotted-decimal format that is not in the SSM range. The range is an IP address from 224.0.0.0 to 239.255.255.255 with the exclusion of the 232.0.0.0/8 range, which is reserved for SSM. The default is 0.0.0.0, which indicates that the parameter is not configured.

Multicast Senders

(multiCastSenders)

The Multicast Senders parameter specifies subnet matching for the data packets coming on the routing instance from the multicast senders.

The default value is Auto, which specifies that the subnet of a packet entering the interface must match the subnet of the host. If the subnets do not match, the interface drops the packet. If the interface is unnumbered, or the host is on a different subnet from that of the interface, this parameter should be set to Always, meaning that packets do not go through the regular subnet check and are not dropped. If, for broadcast interfaces, there are no multicast senders, the Multicast Senders parameter should be set to Never. The options are:

- Auto (default)
- Always
- Never

Non DR Attract Traffic

(nonDrAttractTraffic)

The Non DR Attract Traffic parameter specifies whether the router should ignore the designated router state and attract traffic even when it is not the designated router. If the value is set to true, the DR state is ignored. If the value is set to false, the DR state is honored. The default is false.

Number of Ports Down

(numberOfPortsDown)

The Number of Ports Down parameter specifies the number of ports that are down. The range is 0 to 8. The default is 0.

P2MP Administrative State

(mvpnIpmsiP2MPAdminState)

The P2MP Administrative State parameter specifies whether P2MP is enabled for an RSVP inclusive tunnel. The options are:

- Up
- Down (default)

P2MP Administrative State

(mvpnMLDPIpmsiP2MPAdminState)

The P2MP Administrative State parameter specifies whether P2MP is enabled for an MLDP inclusive tunnel. The options are:

- Up
- Down (default)

Pack Data Join TLV

(dataMdtJoinTlvPack)

The Pack Data Join TLV parameter specifies whether to enable packing of MDT join TLVs into a single PDU to improve efficiency, if multiple Join TLVs are available at the time of transmission. The options are:

- true (default)
- false

Peer IP Address

(peerIPAddress)

The Peer IP Address parameter configures a peer in the anycast RP. The parameter value specifies the RP candidacy address that is configured on the other node in the anycast RP. Ensure that the address is the same for all peers in the anycast RP for a specific multicast group address range. The default is 0.0.0.0, which means that the parameter is not configured.



Note — Alcatel-Lucent recommends a maximum of 15 multicast addresses for each anycast RP.

PIM SSM Prefix

(dataMdtPrefix)

The PIM SSM Prefix parameter specifies the PIM SSM IP address to use for the selective provider tunnel. The range is 225.0.0.0 to 239.255.255.255.

PIM SSM Prefix Length

(dataMdtPrefixLength)

The PIM SSM Prefix Length parameter specifies the PIM SSM groups to use for the selective provider tunnel. The range is 0 to 32.

Policy 1

(policy1)

See the [Policy 1](#) parameter in section [203.1](#).

Policy 2

(policy2)

See the [Policy 2](#) parameter in section [203.1](#).

Policy 3

(policy3)

See the [Policy 3](#) parameter in section [203.1](#).

Policy 4

(policy4)

See the [Policy 4](#) parameter in section [203.1](#).

Policy 5

(policy5)

See the [Policy 5](#) parameter in section [203.1](#).

Prefix

(prefix)

The Prefix parameter combined with the Mask parameter indicates the range of the multicast group. Specify a multicast address for a Candidate-RP Group.

Provider Tunnel Inclusive PIM Mode

(groupAddressMode)

The Provider Tunnel Inclusive PIM Mode parameter specifies which PIM mode to use for PIM-based inclusive provider tunnels. The options are:

- None (default)
- ASM
- SSM

RP IP Address

(anycastRpIPAddress)

The RP IP Address parameter configures a PIM anycast protocol instance for the RP. Anycast enables fast convergence if a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP. Specify an IPv4 unicast address in dotted-decimal format, or an IPv6 unicast address in colon-hexadecimal format. The default is 0.0.0.0.

RP Override

(rpOverride)

The RP Override parameter allows the overriding of the dynamic group-to-RP mappings that are learned by the router. When the parameter value is true, static group-to-RP mappings take precedence over dynamic mappings.

The options are:

- true
- false (default)

Sender Address

(senderAddress)

The Sender Address parameter specifies the address of the source P2MP LSP. Specify an IPv4 unicast address in dotted-decimal format or an IPv6 unicast address in colon-hexadecimal format. The default is 0.0.0.0.

Sender Address Type

(senderAddressType)

The Sender Address Type parameter specifies whether the address type is IPv4 or IPv6. The options are:

- IPv4 (default)
- IPv6

SSM Group IP Address

(ssmGroupIPAddress)

The SSM Group IP Address parameter specifies the SSM Group IP address, that, combined with the SSM Group Mask parameter value, provides the range of multicast group addresses that are used for Source Specific Multicast. The range is an IP address from 224.0.0.0 to 239.255.255.255. The default is 0.0.0.0, which means that the parameter is not configured.

SSM Group Mask

(ssmGroupMask)

The SSM Group Mask parameter specifies the mask which, combined with the SSM Group IP address, provides the range of multicast group addresses to be used for Source Specific Multicast. The range is 4 to 32. The default is 24.

Static Group IP Address

(staticGroupIPAddress)

The Static Group IP Address parameter value is combined with the Static Group Mask parameter value to obtain the range of multicast group addresses to which the router advertises to be the static RP. The value of the Static Group IP Address parameter is sent as the RP address. Specify an IPv4 multicast address in dotted-decimal format or an IPv6 multicast address in colon-hexadecimal format.

Static Group Mask

(staticGroupMask)

The Static Group Mask parameter specifies the mask that, combined with the Static Group IP Address parameter value, is used to create the range of multicast group addresses to which the router advertises the intention to become the static Candidate RP. For IPv4, the range is 4 to 32. For IPv6, the range is 8 to 128.

Static RP IP Address

(staticRPIPAddress)

The Static RP IP Address parameter specifies the static RP address for the multicast groups. Specify an IPv4 unicast address in dotted-decimal format or an IPv6 unicast address in colon-hexadecimal format.

Sticky DR

(stickyDR)

The Sticky DR parameter specifies whether PIM uses the Operational DR Priority parameter value as the priority value in PIM hello messages that egress the interface. This action helps avoid forwarding delays during DR recovery after a period of DR unavailability. When the parameter is enabled on an interface, the device continues to act as the DR after the previous DR returns to service. The options are:

- false (default)
- true

Sticky DR Priority

(stickyDRPriority)

The Sticky DR Priority parameter specifies the DR priority value that PIM sends in PIM hello messages after the election of this interface as the DR. The parameter is configurable when the Sticky DR parameter is enabled. The range is 0 to 4 294 967 295. The default is 1024.

Three Way Hello

(threeWayHello)

The Three Way Hello parameter specifies the support for three-way hello. Table 196-2 describes the parameter options.

Table 196-2 Three Way Hello parameter

Option	Option description
Disabled	Specifies support for two-way hello.
Enabled	Specifies support for three-way hello

Threshold (kbps)

(threshold)

The Threshold parameter specifies the traffic volume, in kbps, when the router switches from the shared tree to the source-specific tree. The router attempts a switchover only when the traffic rate on the shared tree for the group exceeds the configured threshold. The range is 0 to 4 294 967 294. The default is 0.

Tracking Support

(trackingSupport)

The Tracking Support parameter provides message-tracking support. If the value of this parameter is set to true, the T bit in the LAN Prune Delay option of the Hello Message is set to allow the router to disable Join message suppression.

The options are:

- true
- false (default)

Unconstrained Bandwidth (kbps)

See the [Unconstrained Bandwidth \(kbps\)](#) parameter in section 203.1.

197 –RIP parameters

197.1 RIP parameters 197-2

197.1 RIP parameters

This chapter describes the parameters on the RIP property form, and child forms launched from the right-click contextual menu options for RIP.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Check Zero

(checkZero)

The Check Zero parameter specifies whether to check for a 0 value in fields that must have a value of 0 in the RIP version 1 (RIPv1) or version 2 (RIPv2) packets.

Table 197-1 describes the parameter options.

Table 197-1 Check Zero parameter

Option	Option description	Dependencies
false (default)	Disable mandatory checking for 0 in the mandatory RIP version packets.	Allows RIP packets that do not contain a mandatory 0 value in the mandatory 0 packet fields
true	Enable mandatory checking for 0 in the mandatory RIP version packets.	RIP packets, with non-0 values in mandatory 0 value fields are allowed

Description

See the [Description](#) parameter in section 203.1.

Flush

(timerFlush)

The Flush parameter specifies how long, in seconds, a route is maintained in the RIP database after it is declared invalid. If the value of the parameter is exceeded, the route is removed from the RIP database. The range is 1 to 1200. The default is 120.

The Flush, Timeout, and Update parameters are used as timers to determine the rate of RIP route updates and how long the routes are maintained.

Inherit Value

See the [Inherit Value](#) parameter in section 203.1.

Key

See the [Key](#) parameter in section 203.1.

Message Size

(messageSize)

The Message Size parameter specifies the maximum number of RIP routes that sent in each RIP update message. The range is 25 to 255. The default is 25.

Metric In

(metricIn)

The Metric In parameter specifies, in hops, the metric value that is added to routes that are received from a RIP neighbor. When you apply an export policy to a RIP configuration, the policy overrides the metric values that are set using calculations involving the Metric In and Metric Out parameter values. The range is 1 to 16. The default is 1.

When a RIP route is received from a neighbor, the metric value 1 is added to the hop count. When a router receives a routing update with new or different destination information, the metric value increases by 1.

The maximum number of hops in a path is 15. When a RIP routing update with a metric value of 15 is received, and the route is updated, increasing the value by 1 causes the metric to reach 16, which represents a value of infinity. The destination of the route is then considered unreachable. When you set the parameter to 16, routes learned from a neighbor on a specific interface are advertised in RIP route updates with a metric of 16, which eliminates counting-to-infinity problems.

Metric Out

(metricOut)

The Metric Out parameter specifies, in hops, the metric value that is assigned to routes that are exported into RIP and advertised to RIP neighbors. When you apply an export policy to a RIP configuration, the policy overrides the metric values determined using protocol-driven calculations involving the Metric In and Metric Out parameter values. The range is 1 to 16. The default is 1.

When a RIP route is received from a neighbor, the metric value 1 is added to the hop count. When a router receives a routing update with new or different destination information, the metric value increases by 1.

The maximum number of hops in a path is 15. When a RIP routing update with a metric of 15 is received, and the route is updated, increasing the value by 1 causes the metric to reach 16, which represents a value of infinity. The destination of the route is then considered unreachable. When you set the parameter to 16, routes learned from a neighbor on a specific interface are advertised in RIP route updates with a metric of 16, which eliminates counting-to-infinity problems.

Name

See the [Name](#) parameter in section 203.1.

Policy 1**(inheritanceMask)**

See the [Policy 1](#) parameter in section [203.1](#).

Policy 2**(inheritanceMask)**

See the [Policy 2](#) parameter in section [203.1](#).

Policy 3**(inheritanceMask)**

See the [Policy 3](#) parameter in section [203.1](#).

Policy 4**(inheritanceMask)**

See the [Policy 4](#) parameter in section [203.1](#).

Policy 5**(inheritanceMask)**

See the [Policy 5](#) parameter in section [203.1](#).

Preference

See the [Preference](#) parameter in section [203.1](#).

Propagate RIP Metric**(propagateRipMetric)**

The Propagate RIP Metric parameter specifies that the RIP metric is used to set the MP-BGP MED attribute when RIP is used as the CE-PE routing protocol in a VPRN. This allows the RIP metric to be exchanged between PE routers. This parameter only applies to a VPRN RIP routing instance. The options are:

- True
- False (default)

Receive**(receive)**

The Receive parameter specifies the type of RIP route updates that are accepted and processed. Table [197-2](#) describes the parameter options.

Table 197-2 Receive parameter

Option	Option description	Dependencies
RIPv1	Receive only version 1 RIP packets. The RIP instance listens for and accepts packets sent to the broadcast address.	—
RIPv2	Receive only version 2 RIP packets. The RIP instance listens for and accepts packets sent to the broadcast and multicast (224.0.0.9) addresses.	—
Both (default)	Receive either RIP version1 or version 2 packets. The RIP instance listens for and accepts packets sent to the broadcast and multicast (224.0.0.9) addresses.	—
None	Do not receive RIP packets.	Does not allow for RIP route updates

Select Locale

(domain)

The Select Locale parameter specifies the type of port selected as the RIP interface. The options are:

- Access
- Network (default)

Send

(send)

The Send parameter specifies the type of RIP route update messages that are sent to neighbors. Table 197-3 describes the parameter options.

Table 197-3 Send parameter

Option	Option description	Dependencies
None	Do not send RIP messages	The RIP interface only listens for route updates and does not forward route updates to other RIP neighbors.
RIPv1 Broadcast	Send only RIPv1 messages to the broadcast address.	The router only needs to listen for and send messages to the broadcast address.
RIPv2 Broadcast (default)	Send only RIPv2 messages to the broadcast address.	
RIPv2 Multicast	Send only RIPv2 messages to the multicast address.	

Split Horizon

(splitHorizon)

The Split Horizon parameter specifies whether split horizon with poison-reverse is used to protect RIP from problems such as counting to infinity. Poison-reverse means that routes, which are learned from a neighbor using an interface, are advertised in updates out of the same interface but with the Metric Out parameter set to 16, which is equivalent to infinity. Table 197-4 describes the parameter options.

Table 197-4 Split Horizon parameter

Option	Option description	Dependencies
true (default)	Enables split horizon and poison-reverse	The Metric Out parameter should be set to 16.
false	Disables split horizon, which allows routes to be advertised on the same interface on which they were learned with the metric increased by the Metric In parameter value.	—

Timeout

(timerTimeout)

The Timeout parameter specifies, in seconds, how long the router waits before a route is declared invalid. The invalid route persists in the RIP database. The range is 1 to 1200. The default is 180.

The Flush, Timeout, and Update parameters are used as timers to determine the rate of RIP route updates and how long the routes are maintained.

Type

(inheritanceMask)

See the [Type](#) parameter in section 203.1.

Update

(timerUpdate)

The Update parameter specifies how often RIP updates are sent. The range is 1 to 600 s. The default is 30 s.

The Flush, Timeout, and Update parameters are used as timers to determine the rate of RIP route updates and how long the routes are maintained.

198 –RSVP parameters

198.1 RSVP parameters 198-2

198.1 RSVP parameters

This chapter describes the parameters on the RSVP property form, and the child forms launched from the right-click contextual menu options for the RSVP.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

BFD Enabled

(bfdEnabled)

See the [BFD Enabled](#) parameter in section 203.1.

Description

See the [Description](#) parameter in section 203.1.

Class Type 0 BW Percent

(ct0BwPercent)

The Class Type 0 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 0. The range is 0 to 100. The default is 0.

Class Type 1 BW Percent

(ct1BwPercent)

The Class Type 1 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 1. The range is 0 to 100. The default is 0.

Class Type 2 BW Percent

(ct2BwPercent)

The Class Type 2 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 2. The range is 0 to 100. The default is 0.

Class Type 3 BW Percent

(ct3BwPercent)

The Class Type 3 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 3. The range is 0 to 100. The default is 0.

Class Type 4 BW Percent

(ct4BwPercent)

The Class Type 4 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 4. The range is 0 to 100. The default is 0.

Class Type 5 BW Percent

(ct5BwPercent)

The Class Type 5 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 5. The range is 0 to 100. The default is 0.

Class Type 6 BW Percent

(ct6BwPercent)

The Class Type 6 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 6. The range is 0 to 100. The default is 0.

Class Type 7 BW Percent

(ct7BwPercent)

The Class Type 7 BW Percent parameter specifies the percentage of the bandwidth assigned to CT 7. The range is 0 to 100. The default is 0.

Diff Serv Model

(diffServModel)

The Diff Serv Model parameter enables the support of Diff-Serv TE classes on RSVP and specifies the admission control model to be used for setting LSP reservations to the links. When a Diff Serv Model is enabled, IS-IS and OSPF start advertising available bandwidth for each configured TE class. The options are:

- Disabled (default)
- MaxAllocModel
- RusDollsModel

The Russian Doll Model (RDM) LSP admission control policy allows bandwidth sharing across Class Types. It provides a hierarchical model by which the reserved bandwidth of a Class Type is the sum of the reserved bandwidths of the numerically equal and higher Class Types.

The enabling or disabling of Diff-Serv TE on the system requires the RSVP and MPLS protocols to be shutdown.

Down Threshold (%)

The Down Threshold (%) parameters (1 through 16) specify the Down Threshold level percentages for reserved bandwidth per interface. Any reserved bandwidth change per interface is compared to the configured threshold levels. An IGP TE update is triggered if the configured threshold levels are crossed, as a result of either an LSP setup or teardown. Threshold levels configured for the NE at the RSVP level can also be inherited by all configured RSVP interfaces under the NE.

You can configure from one to sixteen Down Threshold percentage levels. If you configure one or more thresholds to a non-default value, then the configured Down Thresholds will be rearranged in descending order. The range is -1, 0 to 100, where -1 indicates that the threshold level is disabled. The default values for each Down Threshold level are shown in Table 198-1.

Table 198-1 Down Threshold (%) parameters

Down Threshold (%) parameter name	XML string	Default value
Down Threshold 1 (%)	teThresholdLevelDown1	100
Down Threshold 2(%)	teThresholdLevelDown2	99
Down Threshold 3 (%)	teThresholdLevelDown3	98
Down Threshold 4 (%)	teThresholdLevelDown4	97
Down Threshold 5 (%)	teThresholdLevelDown5	96
Down Threshold 6(%)	teThresholdLevelDown6	95
Down Threshold 7 (%)	teThresholdLevelDown7	90
Down Threshold 8 (%)	teThresholdLevelDown8	85
Down Threshold 9 (%)	teThresholdLevelDown9	80
Down Threshold 10(%)	teThresholdLevelDown10	75
Down Threshold 11 (%)	teThresholdLevelDown11	60
Down Threshold 12 (%)	teThresholdLevelDown12	45
Down Threshold 13 (%)	teThresholdLevelDown13	30
Down Threshold 14 (%)	teThresholdLevelDown14	15
Down Threshold 15 (%)	teThresholdLevelDown15	0
Down Threshold 16 (%)	teThresholdLevelDown16	-1

Enable Graceful Shutdown

(enableGracefulShutdown)

The Enable Graceful Shutdown parameter specifies whether graceful shutdown of the RSVP node or interface is enabled. The options are:

- enabled
- disabled (default)

Enable Refresh Reduction

(enableRefreshReduction)

The Refresh Reduction parameter specifies whether the use of the RSVP overhead refresh reduction capabilities on this RSVP interface is enabled. This parameter must be enabled if you want to enable the Reliable Delivery parameter.

The options are: enabled or disabled. The default is disabled.

Enable Reliable Delivery

(enableReliableDelivery)

The Enable Reliable Delivery parameter specifies whether reliable delivery of RSVP messages over the RSVP interface is enabled. The parameter is configurable when the [Enable Refresh Reduction](#) parameter is enabled.

Reliable delivery is used to improve RSVP-TE protocol scalability, reliability and performance. A MESSAGE_ID object is defined to reduce refresh message processing overhead by allowing the receiver to more readily identify an unchanged message. When it is supported by both peers, an RSVP message is sent with a MESSAGE_ID object. The receiver acknowledges receipt by sending an acknowledge message. This technique is used to detect message loss and support reliable RSVP message delivery on a per-hop basis.

The options are:

- Enabled
- Disabled (default)

FC Name

(fcName)

The FC Name parameter specifies the forwarding class for which this mapping is defined. The choices are:

- af
- be
- ef
- h1
- h2
- l1
- l2
- nc

The default is be.

Hello Interval (milliseconds)

(helloInterval)

The Hello Interval (milliseconds) parameter specifies the interval, in milliseconds, between RSVP hello messages. The range is 0 to 60 000, in multiples of 1000. The default is 3000.

RSVP hello message packets are used to detect the loss of RSVP connectivity with a neighboring device. Hello message packets detect the loss of neighbors more quickly than when the RSVP session times out based on the refresh interval. After the loss of $(2 \times \text{Keep Multiplier parameter} + 1)$ consecutive hello message packets, the neighbor is declared to be in a down state.

Include Node in RRO

(nodeInRRO)

The Include Node in RRO parameter specifies whether or not the node-id is included in the Record Route Object (RRO). The options are:

- Exclude (default)
- Include

Inherit SAM Class Type BW

(inheritGlobalCtBw)

The Inherit SAM Class Type BW parameter specifies whether the RSVP Interface should inherit the operational values of the eight CT bandwidth values that have been set for the RSVP Instance. The options are:

- enabled (default)
- disabled

Inherit TE Down Thresholds

(inheritTeDownThresholds)

The Inherit TE Down Thresholds parameter specifies whether to inherit the TE Down Thresholds from the RSVP Instance. The options are:

- enabled (default)
- disabled

Inherit TE Up Thresholds

(inheritTeUpThresholds)

The Inherit TE Up Thresholds parameter specifies whether to inherit the TE Up Thresholds from the RSVP Instance. The options are:

- enabled (default)
- disabled

Keep Multiplier

(keepMultiplier)

The Keep Multiplier parameter specifies a value used by the RSVP to declare that a reservation or the neighbor is down. The range is 1 to 255. The default is 3.

Key

See the [Key](#) parameter in section [203.1](#).

Max Burst

(maxBurst)

The Max Burst parameter specifies the maximum number of messages that are sent during the specified interval. The range is 10 to 1000 in multiples of 10. The default is 650.

Message Pacing

(msgPacing)

The Message Pacing parameter allows the node to send a fixed number of RSVP messages in bursts during preset intervals. Message Pacing can reduce the number of dropped messages in networks. The options are:

- false (default)
- true

Period (milliseconds)

(period)

The Period (milliseconds) parameter specifies the interval, in milliseconds, between message bursts. The range is 10 to 1000. The default is 100.

Priority

(priority)

The Priority parameter specifies the setup priority associated with the TE class. The range is -1 to 7, where a value of -1 indicates that the priority is not configured. There is no default.

Rapid Retransmit Time (hundred-milliseconds)

(rapidRetransmitTime)

The Rapid Retransmit Time (hundred-milliseconds) parameter specifies the value of the rapid retransmission interval, in units of hundred-milliseconds. This is used in the retransmission algorithm, which is based on an exponential backoff timer to handle unacknowledged message objects. The Rapid Retransmit Time must be smaller than the regular refresh interval, which is the [Refresh Time](#) parameter. The range is 1 to 100. The default is 5.

Rapid Retry Limit

(rapidRetryLimit)

The Rapid Retry Limit parameter is used in the retransmission algorithm, which is based on an exponential backoff timer that handles unacknowledged message objects. A node stops retransmission of unacknowledged RSVP messages whenever the updated backoff interval exceeds the value set for the [Refresh Time](#) parameter, or the number of retransmissions reaches the value set for the Rapid Retry Limit, whichever comes first. The range is 1 to 6. The default is 3.

Refresh Time

(refreshTime)

The Refresh Time parameter specifies the interval, in seconds, between the successive Path and Resv refresh messages. The range is 1 to 65 535. The default is 30.

The RSVP declares the session down after it misses consecutive refresh messages based on the following formula:

$$((\text{Keep Multiplier parameter} + 0.5) \times 1.5 \times \text{Refresh Time parameter})$$

Subscription Ratio

(subscriptionRatio)

The Subscription Ratio parameter specifies the percentage of the link bandwidth that the RSVP can use for reservation. The range is 0 to 1000. The default is 100.

The parameter sets a limit for the amount of over-subscription or under-subscription that is allowed on the interface. When the parameter is set to 0, no new sessions are permitted on this interface. If the parameter setting is exceeded, RSVP rejects the reservation.

TE Class Type

(teClassType)

The TE Class Type parameter specifies the Class Type (CT) associated with either the TE Class or Forwarding Class, as listed in Table [198-2](#).

Table 198-2 TE Class Type parameter

Parameter	See
TE Class Type for TE Class Definition	The TE Class Type parameter specifies the Class Type (CT) associated with the TE Class. The range is -1 to 7, where a value of -1 indicates that the TE Class Type is not configured. There is no default.
TE Class Type for Forwarding Class Maps	The TE Class Type parameter specifies the Class Type (CT) to which the FC is mapped. The range is 0 to 7. The default is 0.

TE Threshold Update Enabled

(teThresholdUpdateEnabled)

The TE Threshold Update Enabled parameter enables IGP TE updates based only on bandwidth reservation thresholds per interface. This blocks IGP TE updates based instead on bandwidth changes for each reservation. Threshold levels are defined at the global RSVP level, or per interface level. The options are:

- disabled (default)
- enabled

Up Threshold (%)

The Up Threshold (%) parameters (1 through 16) specify the Up Threshold level percentages for reserved bandwidth per interface. Any reserved bandwidth change per interface is compared to the configured threshold levels. An IGP TE update is triggered if the configured threshold levels are crossed, as a result of either an LSP setup or teardown. Threshold levels configured for the NE at the RSVP level can also be inherited by all configured RSVP interfaces under the NE.

You can configure from one to sixteen Up Threshold percentage levels. If you configure one or more thresholds to a non-default value, then the configured Up Thresholds will be rearranged in ascending order. The range is -1, 0 to 100, where -1 indicates that the threshold level is disabled. The default values for each Up Threshold level are shown in Table 198-3.

Table 198-3 Up Threshold (%) parameters

Up Threshold (%) parameter name	XML string	Default value
Up Threshold 1 (%)	teThresholdLevelUp1	0
Up Threshold 2(%)	teThresholdLevelUp2	15
Up Threshold 3 (%)	teThresholdLevelUp3	30
Up Threshold 4 (%)	teThresholdLevelUp4	45
Up Threshold 5 (%)	teThresholdLevelUp5	60
Up Threshold 6(%)	teThresholdLevelUp6	75

(1 of 2)

Up Threshold (%) parameter name	XML string	Default value
Up Threshold 7 (%)	teThresholdLevelUp7	80
Up Threshold 8 (%)	teThresholdLevelUp8	85
Up Threshold 9 (%)	teThresholdLevelUp9	90
Up Threshold 10(%)	teThresholdLevelUp10	95
Up Threshold 11 (%)	teThresholdLevelUp11	96
Up Threshold 12 (%)	teThresholdLevelUp12	97
Up Threshold 13 (%)	teThresholdLevelUp13	98
Up Threshold 14 (%)	teThresholdLevelUp14	99
Up Threshold 15 (%)	teThresholdLevelUp15	100
Up Threshold 16 (%)	teThresholdLevelUp16	-1

(2 of 2)

Update On CAC Failure Enabled

(teUpdateOnCacFailEnabled)

The Update On CAC Failure Enabled parameter specifies whether to allow an IGP update that is triggered by a CAC failure. When enabled and a CAC failure occurs, an IGP update is performed using the actual available bandwidth. A TE update triggered by a CAC failure overwrites a pending timer-based IGP update. This configuration is defined globally and applies to all RSVP interfaces. This parameter is only available when the [TE Threshold Update Enabled](#) parameter is enabled. The options are:

- disabled (default)
- enabled

Update Timer (seconds)

(teUpdateTimer)

The Update Timer (seconds) parameter controls timer-based IGP TE updates to allow the forced update of bandwidths across the NEs to synchronize the actual available or reserved bandwidth. This configuration is defined globally and applies to all RSVP interfaces. This parameter is only available when the [TE Threshold Update Enabled](#) parameter is enabled. The range is 0 to 300 seconds. The default is 0 seconds, which disables the timer-based IGP updates.

199 –IS-IS parameters

199.1 IS-IS parameters 199-2

199.1 IS-IS parameters

This chapter describes the parameters on the IS-IS forms, and the child forms launched from the right-click contextual menu options for IS-IS.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Advertise Only Passive Interfaces

(passiveOnly)

The Advertise Only Passive Interfaces parameter specifies whether the ISIS protocol advertises only prefixes that belong to passive interfaces. The options are:

- True
- False (default)

Area ID

(areaId)

The Area ID parameter specifies the area ID portion of a network SAP. This helps identify a point of connection to the network, such as a device interface. Addressing in IS-IS is based on network SAPs, and network entity titles, also called NET addresses. The NET address is exchanged in IS-IS and LSP hello PDUs to help determine routing and priorities for routing messages. The parameter format is `XX.[xx]XX.[xx]XX.[xx]XX.[xx]XX.[xx]XX.[xx]XX.[xx]`, where `XX` or `xx` are bytes that indicate one authority and format ID or the area ID.

The other portions of a NET address consist of the system ID of the device that contains the interface and the selector ID that contains zeros in a NET address.

For level 1 IS-IS interfaces, neighbors may have different area IDs, but they must share at least one area ID. For level 2 IS-IS interfaces, neighbors may have different area IDs, but when they do not share at least one area ID in common, only level 2 neighbor and LSP information is exchanged. For level 1 and 2 IS-IS interfaces, neighbors may have different area IDs, but when they share at least one area ID, they become neighbors and exchange level 2 LSPs.

BFD Enabled

(bfdEnabled)

See the [BFD Enabled](#) parameter in section 203.1.

CSNP Authentication

(csnpAuthentication)

The CSNP Authentication parameter specifies whether CSNP authentication is enabled. The options are:

- true (default)
- false

CSNP Interval (seconds)

(csnpInterval)

The CSNP Interval (seconds) parameter specifies, in seconds, how often the complete sequence number PDUs are sent from the IS-IS interface. The range is 1 to 65 535. The default is:

- 10 s for broadcast LAN interfaces
- 5 s for point-to-point links

Description

See the [Description](#) parameter in section [203.1](#).

Enable Authentication

(enableAuthentication)

The Enable Authentication parameter specifies whether to secure IS-IS routing information between devices. The options are:

- true (default)
- false

When authentication is enabled, any packets received on the IS-IS interface that do not match the authentication type or authentication key used on the interface are rejected.

Enable IPv4

(enableIPv4)

The Enable IPv4 parameter specifies whether IS-IS allows or generates IPv4 PDUs. The options are:

- Enabled (default)
- Disabled

Enable IPv6

(enableIPv6)

The Enable IPv6 parameter specifies whether IS-IS allows or generates IPv6 PDUs. The options are:

- Enabled
- Disabled (default)

Enable LDP Synchronization

See the [Enable LDP Synchronization](#) parameter in section 203.1.

Export Limit

(exportLimit)

The Export Limit parameter specifies the maximum number of routes or route prefixes that the route table can export to IS-IS. The range is 0 to 4 294 967 295. The default is 0, which means that no export limit is configured.

Export Limit Log Percent

(exportLimitLogPercent)

The Export Limit Log Percent parameter specifies the percentage of the [Export Limit](#) value at which the NE creates a warning log message and sends an SNMP trap. IS-IS continues to learn routes until the number of routes specified by [Export Limit](#) is reached. The range is 0 to 100. The default is 0, which means that the parameter is disabled and no log message or SNMP trap is sent.

External

(externalPreference)

See the [Preference](#) parameter in section 203.1.

Graceful Restart

See the [Graceful Restart](#) parameter in section 203.1.

Hello Authentication

(helloAuthentication)

The Hello Authentication parameter specifies whether hello authentication is enabled. The options are:

- true (default)
- false

Hello Interval (seconds)

(helloInterval)

The Hello Interval (seconds) parameter specifies the interval, in seconds, between hello PDU messages issued on the interface for this IS-IS level. The range is 1 to 20 000. The default is 9.

Hello Multiplier

(helloMultiplier)

The Hello Multiplier parameter specifies the number of missing hello PDU messages before the adjacency between IS-IS devices is considered down. The range is 2 to 100. The default is 3.

Helper Mode

See the [Helper Mode](#) parameter in section 203.1.

IID TLV

(iidTlv)

The IID TLV parameter specifies whether Instance Identifier TLV is enabled on the IS-IS instance. The parameter is configurable only on a Release 8.0 or later 7450 ESS, 7710 SR, 7750 SR, 7750 SR-c4, or 7750 SR-c12. The options are:

- disabled (default)
- enabled

To configure the parameter on an IS-IS instance other than the default, which is instance 0, you must set the [L1 MAC Address](#) and [L2 MAC Address](#) parameters for the instance to non-default values.

Instance ID

(isisSysInstance)

The Instance ID parameter specifies the identifier of the IS-IS routing instance. The range is 0 to 31. The default is 0.

The parameter is configurable only on a Release 8.0 or later 7450 ESS, 7710 SR, 7750 SR, 7750 SR-c4, or 7750 SR-c12.



Note — The parameter is configurable only during IS-IS instance creation.

Internal

(preference)

See the [Preference](#) parameter in section 203.1.

IPv6 Routing TLV type

(ipv6RoutingTlvType)

The IPv6 Routing TLV type parameter specifies the TLV type for IPv6 routing. The parameter is configurable when the [Enable IPv6](#) parameter is enabled. The options are:

- Unspecified
- Native (default)
- MT

The IPv6 Routing TLV type parameter is not configurable on the 7705 SAR.

IPv6 Unicast Multi-Topology

(multiTopoIPv6Ucast)

The IPv6 Unicast Multi-Topology parameter specifies whether IPv6 unicast multi-topology is enabled. The parameter is configurable for the 7710 SR and 7750 SR, and for the 7450 ESS in mixed mode. The options are:

- true
- false (default)

The IPv6 Unicast Multi-Topology parameter is not configurable on the 7705 SAR.

Isis Default Route Tag

(defaultRouteTag)

The Isis Default Route Tag specifies a 32-bit integer tag for the ISIS default route. The tag is used to apply an administrative policy. A value of 0 indicates that the tag has not been set. The range is 0 to 4 294 967 295. The default is 0.

Key

See the [Key](#) parameter in section [203.1](#).

L1 MAC Address

(l1MacAddress)

The L1 MAC Address parameter specifies the destination MAC address for each Level 1 IS-IS neighbor of this ISIS instance. Specify a MAC address in dashed hexadecimal notation. The default is 01-80-C2-00-00-14.

L2 MAC Address

(l2MacAddress)

The L2 MAC Address parameter specifies the destination MAC address for each Level 2 IS-IS neighbor of this ISIS instance. Specify a MAC address in dashed hexadecimal notation. The default is 01-80-C2-00-00-15.

LDP Over RSVP Include

(ldpOverRsvp)

See the [LDP over RSVP Include](#) parameter in section 203.1.

Level Capability

(levelCapability)

The Level Capability parameter specifies the routing level for an instance of the IS-IS routing process. An IS-IS-enabled device and an IS-IS interface can operate at level 1, level 2, or both levels 1 and 2. Table 199-1 describes the parameter options.

Table 199-1 Level Capability parameter

Option	Option description	Dependencies
Level 1	Device or interface operates at level 1	Only level 1 adjacencies are formed.
Level 2	Device or interface operates at level 2	Only level 2 adjacencies are formed.
Level 1 and 2 (default)	Device or interface can operate at level 1 and 2	The device or interface runs separate SPF calculations for level 1 area routing and level 2 multi-area routing to create the IS-IS routing table.

LSP Initial Wait (seconds)

(lspInitialWait)

The LSP Initial Wait (seconds) parameter specifies, in seconds, the timer value that determines when to generate the first LSP in a series of LSPs. The range is 1 to 100. The default is 0.

The LSP Second Wait (seconds) parameter specifies the timer value that determines the generation of the second LSP. The LSP Max Wait (seconds) parameter specifies the timer value that determines the third, and all subsequent, LSPs. The LSPs are generated at increasing intervals based on the LSP Max Wait (seconds) parameter.

LSP Lifetime (seconds)

(lspLifetime)

The LSP Lifetime (seconds) parameter specifies how long, in seconds, the device wants the LSP it originates to be considered valid by other devices in the domain. All LSPs are maintained in an LSP database until the parameter value is reached. If a routing update from the originating device for the LSP does not arrive within the parameter time, the LSP is removed from the LSP database. The range is 350 to 65 535. The default is 1200.

LSP Max Wait (seconds)

(lspMaxWait)

The LSP Max Wait (seconds) parameter specifies, in seconds, the timer that determines when to generate the first LSP in a series of LSPs. The LSP Second Wait (seconds) parameter specifies the timer that determines the generation of the second LSP. the LSP Max Wait (seconds) parameter specifies the timer that determines the third, and all subsequent, LSPs. The LSPs are generated at increasing intervals based on the LSP Max Wait (seconds) parameter. The range is 1 to 120. The default is 5.

LSP Pacing Interval (seconds)

(lspPacingInterval)

The LSP Pacing Interval (seconds) parameter specifies the interval for all IS-IS levels, in seconds, between LSP PDUs that are sent from the IS-IS interface. The range is 0 to 65 535. The default is 100. When the parameter is set to 0, the IS-IS interface sends no LSPs.

LSP Second Wait (seconds)

(lspSecondWait)

The LSP Initial Wait (seconds) parameter specifies, in seconds, the timer value that determines when to generate the first LSP in a series of LSPs. The LSP Second Wait (seconds) parameter specifies the timer value that determines the generation of the second LSP. the LSP Max Wait (seconds) parameter specifies the timer value that determines the third, and all subsequent, LSPs. The LSPs are generated at increasing intervals based on the LSP Max Wait (seconds) parameter. The range is 1 to 100. The default is 1.

Mask

(mask)

The Mask parameter specifies the subnet mask of the IP address configured using the Network parameter. This allows the aggregation of addresses for a specific IS-IS summary level to create route summaries, which are used to reduce the size of the link state database and the routing table, and to reduce the chance of route flapping. The range is 1 to 32 for an IPv4 address, and 1 to 128 for an IPv6 address. A value of 32 is typically reserved for an IPv4 system address, but is available for general use in IPv6. The IPv4 default is 24; the IPv6 default is 64.

Mesh Group

(meshGroup)

The Mesh Group parameter specifies the numeric value of a mesh group to uniquely identify each mesh group. The Mesh Group parameter is configurable when the Mesh Group Status parameter value is Enabled. The range is 1 to 2 000 000 000. The default is 1.

Mesh Group Status

(meshGroupStatus)

The Mesh Group Status parameter specifies whether the interface is assigned to a mesh group. Mesh groups limit the amount of flooding when a new or changed LSP is advertised across an IS-IS area. Table 199-2 describes the parameter options.

Table 199-2 Mesh Group Status parameter

Option	Option description	Dependencies
Disabled (default)	Removes the interface from the mesh group	—
Blocked	Prevents the interface from flooding LSPs	When an interface is blocked from flooding LSP information, careful planning is necessary to prevent isolated islands that do not receive updated LSPs.
Enabled	Includes the interface in the mesh group	All devices in a mesh group should be fully meshed. All interfaces in the mesh group should be set to Enabled.

Metric

(metric)

The Metric parameter specifies the metric, also known as the cost, used to identify this interface on this IS-IS level. The range is 0 to 16 777 215. The default is 0.

To calculate the lowest cost to reach a destination, each interface on each level has a cost associated with using the interface. The cost is determined using the Metric parameter value. A lower value indicates a lower cost for using the interface.

Multicast Import

See the [Multicast Import](#) parameter in section 203.1.

Multi-Topology

(multiTopology)

The Multi-Topology parameter specifies whether multi-topology is enabled. The parameter is available for the 7710 SR and 7750 SR, and for the 7450 ESS in mixed mode. The options are:

- true
- false (default)

Name

See the [Name](#) parameter in section [203.1](#).

Network

(network)

The Network parameter specifies the aggregate IPv4 or IPv6 addresses for a specific IS-IS summary level. This allows the creation of route summaries, which are used to reduce the size of the link state database and the routing table, and to reduce the chance of route flapping. The host bits for a network address must be 0. Specify an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format.

Overload

(setOverload)

The Overload parameter specifies whether the IS-IS-enabled device operates in an overload state before attempting to reestablish normal operations. The overload period is configured using the Overload Timeout (seconds) parameter.

During normal operation, the device may enter an overload state because of resource issues. In the overload state, the device is only used if the destination is reachable by the device and is not used for other transit traffic. Table [199-3](#) describes the parameter options.

Table 199-3 Overload parameter

Option	Option description	Dependencies
Enabled	Overload is enabled.	The Overload Timeout (seconds) parameter must be set to a value other than 0.
Disabled (default)	Overload is disabled.	When the Overload Timeout (seconds) parameter is set to 0, the overload state is maintained indefinitely.

Overload On Boot

(overloadOnBoot)

The Overload On Boot parameter specifies that, when the device is in an overload state, the device is used only if there is no other route to reach the destination. This parameter configures the IGP on boot in the overload state until the following occurs:

- The Overload On Boot Timeout (seconds) parameter value is reached
- The Overload On Boot parameter is set to Disabled

Table 199-4 describes the parameter options.

Table 199-4 Overload On Boot parameter

Option	Option description	Dependencies
Disabled (default)	Overload on boot is disabled.	—
Enabled	Overload on boot is enabled and the device is used only if there is no other route to reach the destination.	The Overload On Boot Timeout (seconds) parameter must be set to a value other than 0.
Enabled Wait For BGP	—	—

Overload On Boot Timeout (seconds)

(overloadOnBootTimeout)

The Overload On Boot Timeout (seconds) parameter specifies the timeout value, in seconds, when the Overload On Boot parameter is set to Enabled. The options are:

- 0 (default) to represent indefinite
- 60 to 1800

Overload Timeout (seconds)

(overloadTimeout)

The Overload Timeout (seconds) parameter specifies, in seconds, the timeout value when the Overloading parameters are enabled. The options are:

- 0 (default) to represent indefinite
- 60 to 1800

Passive

(passive)

The Passive parameter specifies whether to advertise the interface as an IS-IS interface without using the IS-IS protocol. Table 199-5 describes the parameter options.

Table 199-5 Passive parameter

Option	Option description	Dependencies
false (default)	The interface is advertised as an IS-IS interface.	—
true	The interface ignores ingress IS-IS PDUs and transmits no IS-IS PDUs.	Service interfaces are set to true.

Policy 1**(inheritanceMask)**See the [Policy 1](#) parameter in section [203.1](#).**Policy 2****(inheritanceMask)**See the [Policy 2](#) parameter in section [203.1](#).**Policy 3****(inheritanceMask)**See the [Policy 3](#) parameter in section [203.1](#).**Policy 4****(inheritanceMask)**See the [Policy 4](#) parameter in section [203.1](#).**Policy 5****(inheritanceMask)**See the [Policy 5](#) parameter in section [203.1](#).**Priority****(priority)**

The Priority parameter specifies the priority of an interface when determining the preferred device used in a multi-access network. The range is 0 to 127. The default is 64. A higher number indicates a higher priority.

When hello PDU messages are sent to other devices on the IS-IS level, the Priority parameter value is included. The device with the highest priority is designated as the preferred device. The designated device is responsible for sending LSPs to this network in the multi-access network.

PSNP Authentication

(psnpAuthentication)

The PSNP Authentication parameter specifies whether PSNP authentication is enabled. The options are:

- true (default)
- false

Reference Bandwidth

(referenceBandwidth)

The Reference Bandwidth parameter specifies the reference bandwidth that provides the basis of bandwidth relative costing. The range is 0 to 100 000 000 bps. The default is 0. When the parameter is set to 0, the reference bandwidth is not defined.

To calculate the lowest cost to reach a specific destination, each configured level on each interface must have a cost. When the reference bandwidth is defined, the cost is calculated using the formula:

$$\text{cost} = \text{reference-bandwidth} \div \text{bandwidth}$$

Remove Key button

The Remove Key button deletes the MD5 key.

Retransmit Interval (seconds)

(retransmitInterval)

The Retransmit Interval (seconds) parameter specifies, in seconds, the minimum time between LSP PDU retransmissions on a point-to-point IS-IS link interface. The range is 1 to 65 535. The default is 5.

Route Tag

(routeTag)

The Route Tag parameter specifies a 32-bit integer tag for the IP addresses of an ISIS interface. The tag is used to apply an administrative policy. A value of 0 indicates that the tag has not been set. The range is 0 to 4 294 967 295. The default is 0.

SPF Initial Wait (milliseconds)

(spfInitialWait)

The SPF Initial Wait (milliseconds) parameter specifies, in milliseconds, the maximum interval between two consecutive SPF calculations. The timers determine when to perform the first, second, and all subsequent calculations. The SPF Second Wait (milliseconds) parameter specifies the timer value that determines the generation of the second SPF. The SPF Max Wait (seconds) parameter specifies the timer that determines the third, and all subsequent, SPFs. The SPFs are generated at increasing intervals based on the SPF Max Wait (seconds) parameter. The range is 10 to 100 000. The default is 1000.

SPF Max Wait (seconds)

(spfMaxWait)

The SPF Max Wait (seconds) parameter specifies, in seconds, the maximum interval between two consecutive SPF calculations. The timers determine when to perform the first, second, and all subsequent calculations. The SPF Second Wait (milliseconds) parameter specifies the timer value that determines the generation of the second SPF. The SPF Max Wait (seconds) parameter specifies the timer that determines the third, and all subsequent, SPFs. The SPFs are generated at increasing intervals based on the SPF Max Wait (seconds) parameter. The range is 10 to 120. The default is 10.

For example, if the SPF Second Wait (milliseconds) parameter is set to 1000, the second calculation occurs at 2000 ms. Subsequent calculations start at 4000 ms, and run until the SPF Max Wait (seconds) parameter value is reached.

SPF Second Wait (milliseconds)

(spfSecondWait)

The SPF Second Wait (milliseconds) parameter specifies the interval between the first and second SPF calculations. After the second calculation, a formula is used to determine the time of subsequent calculations. The timers determine when to perform the first, second, and all subsequent calculations. The SPF Second Wait (milliseconds) parameter specifies the timer value that determines the generation of the second SPF. The SPF Max Wait (seconds) parameter specifies the timer value that determines the third, and all subsequent, SPFs. The SPFs are generated at increasing intervals based on the SPF Max Wait (seconds) parameter. The range is 10 to 100 000. The default is 1000.

For example, if the parameter is set to 1000, the second calculation occurs at 2000 ms. Subsequent calculations start at 4000 ms, and run until the SPF Max Wait (seconds) parameter value is reached.

Strict Adjacency Check

(strictAdjacencyCheck)

The Strict Adjacency Check parameter specifies whether IS-IS forms an adjacency between two routers that do not use the same IP version. When the parameter is enabled, the router IP versions must match for an adjacency to form.

- Disabled (default)
- Enabled

Summary Level

(summaryLevel)

The Summary Level parameter specifies IS-IS summary level for which aggregate IPv4 addresses are to be created. Aggregate IPv4 address route summaries are used to reduce the size of the link state database and the IPv4 routing table, and to reduce the chance of route flapping. The options are:

- Level 1
- Level 2
- Level 1 and 2 (default)

Summary Route Tag

(summaryRouteTag)

The Summary Route Tag parameter specifies a 32-bit integer tag for the ISIS summary route. This tag is used to apply an administrative policy. A value of 0 indicates that the tag has not been set. The range is 0 to 4 294 967 295. The default is 0.

Traffic Engineering

(trafficEngineering)

The Traffic Engineering parameter specifies whether traffic engineering is enabled and determines whether IGP shortcuts are required. The options are:

- true
- false (default)

When the parameter is set to false, the device generates no metrics and ignores incoming metrics.

Type

Table 199-6 lists where to find more information about the Type parameter.

Table 199-6 Type parameter

Parameter	See
Type for Authentication	Type parameter in section 203.1
Type for L3 interface	Type parameter in section 203.1

Unicast Import

See the [Unicast Import](#) parameter in section 203.1.

Wide Metrics Only

(wideMetricsOnly)

The Wide Metrics Only parameter specifies whether to only use wide metrics in LSPs to support traffic engineering. By default, the IS-IS protocol can generate two TLVs: one for adjacency and one for the IP prefix, also known as the narrow TLV. Wide metrics allow the inclusion of a second pair of TLVs. Table 199-7 describes the parameter options.

Table 199-7 Wide Metrics Only parameter

Option	Option description	Dependencies
true	The device generates narrow and wide TLVs.	—
false (default)	The device generates only wide TLVs.	

200 –OSPF parameters

200.1 OSPF parameters 200-2

200.1 OSPF parameters

This chapter describes the parameters on the OSPF forms, and the child forms launched from the right-click contextual menu options for OSPF.

Administrative State

See the [Administrative State](#) parameter in section [203.1](#).

Advertise Subnet

(advertiseSubnet)

The Advertise Subnet parameter specifies whether to advertise the interface as a subnet route, including network number and netmask information. The parameter is configurable only for OSPFv2. The options are:

- Enabled (default)
- Disabled

When the parameter is disabled, the interface is advertised as a host route.

Area ID

(areaId)

The Area ID parameter specifies the context to create an OSPF area. An area is a collection of network segments within an AS that are grouped together. Specify an IPv4 address in dotted-decimal format. The value 0.0.0.0 is reserved for the backbone area. There is no default value.

Authentication Type

(authenticationType)

The Authentication Type parameter specifies the type of authentication used on the OSPFv2 interface. Table [200-1](#) describes the parameter options.

Table 200-1 Authentication Type parameter

Option	Option description	Dependencies
No Authentication (default)	No authentication is used.	—
Simple Password	A plain-text password is used for authentication.	
MD5-based Authentication	MD5 authentication is used as outlined in RFC1321.	When you configure the option, you must configure the Key Index, Key, and Re-enter Key parameters.

Autonomous System Border Router

(isAutonomousSystemBorderRouter)

The Autonomous System Border Router parameter specifies that the device is configured as an ASBR. The options are:

- Enabled
- Disabled (default)

ASBRs are used to export routes from the routing table manager into an instance of OSPF. After a device is configured as an ASBR, export policies in the OSPF domain are in effect.



Note — The Autonomous System Border Router parameter is set to Disabled by default and is read-only in an OSPFv2 routing instance of a VPRN.

BFD Enabled

(bfdEnabled)

See the [BFD Enabled](#) parameter in section [203.1](#).

Blackhole Range

(rangeBlackhole)

The Blackhole Range parameter specifies whether to create a low priority blackhole route. The options are:

- Enabled (default)
- Disabled

Routing loops may occur when addresses in an area or areas have no route by which to reach them. Enable the parameter to use low priority blackhole routes, which eliminates routing loops.

Boot Overload Enabled

(bootOverloadAdministrativeState)

The Boot Overload Enabled parameter specifies that, when the device is in an overload state, the device is used only if there is no other route to reach the destination. When the parameter is enabled, the IGP is placed in the overload state at startup and remains in the overload state until one of the following occurs:

- the Boot Overload Interval (seconds) parameter expires
- the Boot Overload Enabled parameter is set to disabled

Table [200-2](#) describes the parameter options.

Table 200-2 Boot Overload Enabled parameter

Option	Option description	Dependencies
Disabled (default)	Overload on startup is disabled.	—
Enabled	Overload on startup is enabled and the device is used only if there is no other route to reach the destination.	The Boot Overload Interval (seconds) parameter must be set to a value greater than 0.

Boot Overload Interval (seconds)

(bootOverloadInterval)

The Boot Overload Interval (seconds) parameter specifies the interval, in seconds, after which the overload state at startup is reset. The parameter is configurable when the Boot Overload Enabled parameter is enabled. The options are:

- 0 (default) to represent an indefinite interval
- 60 to 1800

Change Password button

You can use the Change Password button to change the text password used to validate OSPF messages between neighbors. The button is enabled when the Authentication Type parameter is set to the Simple Password option.

Configured MTU (bytes)

(mtu)

The Configured MTU (bytes) parameter specifies, in bytes, the largest OSPF packet size that is handled by the interface. Table 200-3 describes the parameter options.

Table 200-3 Configured MTU (bytes) parameter

Option	Option description	Dependencies
0 (default)	The value of the MTU is determined from the configured port MTU value.	The MTU value for supported interfaces varies based on the interface port type to which the OSPF interface is bound. See the <i>5620 SAM User Guide</i> for more information about default MTU values.
512 to 9198	The size, in bytes, of the MTU.	The size includes the IP header information size, but does not include the underlying layer heading information size.

Default Cost

(metric)

The Default Cost parameter specifies, in hops, the default route cost. You can configure the parameter when the Type parameter is set to Stub (No Type 5 External) or Totally Stub (No Summaries). The range is 0, or 1 to 65 535. The default is 0, which means that the parameter is not configured.

Description

(areaDescription)

See the [Description](#) parameter in section 203.1.

Domain ID

(domainId)

The Domain ID parameter specifies the domain ID associated with the OSPF instance on the router. The range is -1, or 1 to 31. The default is 1. If no value is set for the tmnxOspfAsbrDomainId parameter, the Domain ID parameter value is set to -1.

Enable LDP Synchronization

See the [Enable LDP Synchronization](#) parameter in section 203.1.

Effect

(effect)

The Effect parameter specifies whether to advertise the summarized range of IP addresses known by area border routers that fall within the IP address range identified by the Network and Mask parameters. Table 200-4 describes the parameter options.

Table 200-4 Effect parameter

Option	Option description	Dependencies
Advertise Matching (default)	The range of IP addresses is advertised to other OSPF areas.	—
Do Not Advertise Matching	The range of IP addresses is not advertised to other OSPF areas.	

Exit Overflow Interval

(exitOverflowInterval)

The Exit Overflow Interval parameter specifies one of the timers related to establishing limits on the number of non-default, AS-external LSAs entries that can be stored in the link state database. You can limit the number of non-default, AS-external LSA entries to protect the device from receiving an excessive number of external routes that use memory and CPU resources on the device. The range is 0 to 2 147 483 674. The default is 0.

When the value is reached, the link state database is considered to be in an overflow state and the device withdraws any existing AS-external LSAs and does not originate any new ones.

The Exit Overflow Interval and the External LSA Limit parameters must be set identically on all devices in the same OSPF area, unless the devices are in stub or not-so-stubby areas.

External LSA Limit

(externalLsdbLimit)

The External LSA Limit parameter specifies, in seconds, the amount of time that the device waits after reaching a link state database overflow state before non-default, AS-external LSAs are created and processed. The overflow state is determined using the Exit Overflow Interval parameter.

The range is -1 to 2 147 483 674. The default is -1.

The Exit Overflow Interval and the External LSA Limit parameters must be set identically on all devices in the same OSPF area, unless the devices are in stub or not-so-stubby areas.

External

(externalPreference)

See the [Preference](#) parameter in section [203.1](#).

Graceful Restart

See the [Graceful Restart](#) parameter in section [203.1](#).

Hello Interval (seconds)

(helloInterval)

The Hello Interval (seconds) parameter specifies the interval, in seconds, between OSPF hello messages that are issued on the OSPF interface or over the virtual link. The range is 1 to 65 535. The default is 10.

Use the parameter and the Router Dead Interval (seconds) parameter to establish and maintain the health of adjacency between devices. You can increase the rate at which hello messages are sent to allow for faster detection of device failures. However, more processing is required to perform additional checks.

Helper Mode

See the [Helper Mode](#) parameter in section 203.1.

ID

See the [Area ID](#) parameter in this section.

Ignore DN Bit

(ignoreDNBit)

The Ignore DN Bit parameter specifies whether to ignore the DN bit for OSPF LSA packets for this instance of OSPF on the router. When the parameter value is enabled, the DN bit for the OSPF LSA packets is ignored. When the parameter value is disabled the DN bit is not ignored. The options are:

- Enabled (default)
- Disabled

Initial Wait (milliseconds)

(lsaGenerateInitialWait)

The Initial Wait (milliseconds) parameter specifies, in milliseconds, when to generate the second LSA. The range is 10 to 600 000. The default is 5000.

Use the Initial Wait (milliseconds), LSA Generate Max Wait (milliseconds), and Second Wait (milliseconds) parameters to specify the timers between generating the first, second, and subsequent LSAs.

For example, if the Initial Wait (milliseconds) parameter is set to 5000, the first LSA occurs after 5000 ms. If the Second Wait (milliseconds) parameter is set to 5000, then the second LSA occurs after another 5000 ms. The next run is an exponential increase to 10 000 ms, then 20 000 ms, then 40 000 ms, and so on, until the LSA Generate Max Wait (milliseconds) parameter is reached.

Alcatel-Lucent recommends configuring the LSA Generate Max Wait (milliseconds) parameter be a value equal to or greater than the LSA Arrival Wait (milliseconds) parameter value.

Initial Wait (milliseconds)

(spfInitialWait)

The Initial Wait (milliseconds) parameter specifies, in milliseconds, the initial interval before starting SPF calculations. Use the parameter and the SPF Max Wait (milliseconds) and Second Wait (milliseconds) parameters to control the first, second, and subsequent SPF calculations after a topology change. The range is 10 to 100 000. The default is 1000. Values must be entered in hundreds of ms. Any other increment is rejected.

When subsequent SPF runs are required, the runs occur based on the an exponentially increasing interval, based on the Second Wait (milliseconds) parameter following the initial run based on the Initial Wait (milliseconds) parameter.

For example, if the Initial Wait (milliseconds) parameter is set to 1000, the first SPF run occurs after 1000 ms. If the Second Wait (milliseconds) parameter is set to 1000, then the second SPF run occurs after another 1000 ms. The next run is an exponential increase to 2000 ms, then 4000 ms, then 8000 ms, and so on, until the Max Wait Time (milliseconds) parameter is reached. After a full interval with no SPF runs, the timer interval returns to the Initial Wait (milliseconds) value.

Interface Base Reference Cost (kbps)

(ifBaseRefCost)

The Interface Base Reference Cost parameter specifies, in kbps, the bandwidth that is used as a reference when the default cost of interfaces based on link speed is determined. The default is 100 000 000, which is equivalent to 100 Gb/s.

The range depends on the interface link speed. The following lists some of the default costs for interfaces based on various link speeds:

- 10 000 for 10 Mb/s
- 1000 for 100 Mb/s
- 100 for 1 Gb/s
- 10 for 10 Gb/s

Internal

(internalPreference)

See the [Preference](#) parameter in section [203.1](#).

Instance ID

(instanceIndex)

The Instance ID parameter specifies an OSPF route instance. The parameter can be used to identify routes installed by that instance and advertised to neighboring nodes. If you do not specify an instance ID, only routes installed by the base routing instance are advertised to neighboring nodes. The range is 0 to 31. The default is 0.

The parameter is configurable on the 7750 SR, 7450 ESS, and 7710 SR. Only one OSPF instance is supported on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], and 7210 SAS-X24F2XFP.

Interface Name

(interfaceCtpPointer)

The Interface Name parameter specifies the local IP interface to be used by the sham link. You must select an IP interface that is already configured for the OSPF area.

IPsec In Static Security Association

(ospfIfInboundSASNamePointer)

Click on the Select button to list and choose an inbound or bidirectional IPsec static security association to authenticate the OSPFv3 traffic.

IPsec Out Static Security Association

(ospfIfOutboundSASNamePointer)

Click on the Select button to list and choose an outbound or bidirectional IPsec static security association to authenticate the OSPFv3 traffic.

IPsec Security Association Name

(ipsestaticSASName)

The IPsec Security Association Name parameter specifies the direction used in OSPFv3. The options are:

- None (default)
- Bidirectional
- Uni-directional

Key

(key)

The Key parameter specifies a unique MD5 key. The parameter is configurable when the Authentication Type parameter is set to MD5-based Authentication. The range is a string from 1 to 16 characters. There is no default.

Key Index

(keyIndex)

The Key Index parameter specifies a unique identifier for an MD5 key. The parameter is configurable when the Authentication Type parameter is set to MD5-based Authentication. The range is 1 to 255. The default is 0.

LDP over RSVP Include

(ldpOverRsvp)

See the [LDP over RSVP Include](#) parameter in section [203.1](#).

Link State DB Type

(lsdbType)

The Link State DB Type parameter specifies how LSAs are distributed by area border routers that fall within the IP address range identified by the Network and Mask parameters. Table 200-5 describes the parameter options.

Table 200-5 Link State DB Type parameter

Option	Option description	Dependencies
Summary (default)	The range of IP addresses applies to summary LSAs. This applies even when the area is configured as an NSSA.	—
NSSA	The range of IP addresses applies to external routes (using type 7 LSAs) learned within NSSAs when routes are advertised to other areas as type 5 LSAs.	

LSA Arrival Wait (milliseconds)

(lsaArrivalWait)

The LSA Arrival Wait (milliseconds) parameter specifies, in milliseconds, the minimum delay between receipt of the same LSAs that are arriving from neighbors. The range is 0 to 600 000. The default is 1000.

Alcatel-Lucent recommends configuring the LSA Generate Max Wait (milliseconds) parameter be a value equal to or greater than the LSA Arrival Wait (milliseconds) parameter value.

LSA Generate Max Wait (milliseconds)

(lsaGenerateMaxWait)

The LSA Generate Max Wait (milliseconds) parameter specifies, in milliseconds, when to generate the first LSA. The range is 10 to 600 000. The default is 5000.

Use the LSA Generate Max Wait (milliseconds), Initial Wait (milliseconds) and Second Wait (milliseconds) parameters to specify the timers between generating the first, second, and subsequent LSAs.

For example, if the Initial Wait (milliseconds) parameter is set to 5000, the first LSA occurs after 5000 ms. If the Second Wait (milliseconds) parameter is set to 5000, then the second LSA occurs after another 5000 ms. The next run is an exponential increase to 10 000 ms, then 20 000 ms, then 40 000 ms, and so on, until the LSA Generate Max Wait (milliseconds) parameter is reached.

Alcatel-Lucent recommends configuring the LSA Generate Max Wait (milliseconds) parameter be a value equal to or greater than the LSA Arrival Wait (milliseconds) parameter value.

Metric

(metric)

The Metric parameter specifies the cost metric for the OSPF interface. This metric overrides the cost metric based on the speed of the underlying link. A higher number indicates a higher cost for using the interface. Table 200-6 describes the parameter options.

Table 200-6 Metric parameter

Option	Option description	Dependencies
0 (default)	—	You cannot use the 0 option.
1 to 65 535	The cost of the interface	A higher number indicates a higher cost for using the interface.

Multicast Import

See the [Multicast Import](#) parameter in section 203.1.

Name

See the [Name](#) parameter in section 203.1.

Network

(network)

The Network parameter specifies the range of IP addresses that is required on an area border router to summarize or suppress route information to all other devices in the OSPF area.

For OSPFv2, specify an IP address in dotted-decimal format.

For OSPFv3, specify an IPv6 address in colon-hexadecimal format.

Area border routers send summary LSAs to describe routes to other areas. To minimize the number of LSAs, use the parameter and the [Prefix Length](#) parameter to send reachability information to other devices in the OSPF area about the devices within the specified range.

Originate Default Route

(originateDefault)

The Originate Default Route parameter specifies the type of link state advertisement that is generated by a device in an NSSA OSPF. the parameter is configurable when the Type parameter is set to NSSA (No Type 5 External) or NSSA (No Summaries). Table 200-7 describes the parameter options.

Table 200-7 Originate Default Route parameter

Option	Option description	Dependencies
No Originate (default)	The NSSA area border router or ASBR does not originate a default route.	—
Originate Type3	The NSSA area border router or ASBR router originates a type 3 LSA.	When you set the Type parameter to NSSA (No Summaries), you should set the Originate Default Route parameter to Originate Type3. However, some older OSPF implementations may expect a type 7 LSA.
Originate Type7	The NSSA area border router or ASBR originates a type 7 LSA.	

OSPF Router ID

(ospfRouterId)

The OSPF Router ID parameter specifies the routing instance as the IP address of the managed router. The router ID uniquely identifies the device within an autonomous system and is used by OSPF in the routing table manager instance. Specify an IPv4 address in dotted-decimal format.

The 5620 SAM uses the system IP address when you specify the default router ID (0.0.0.0). You can only assign the default router ID to an OSPF instance that is the base instance.

The OSPF Router ID parameter is configurable on the 7210 SAS-M24F, 7210 SAS-M24F2XFP, 7210 SAS-M24F2XFP [ETR], 7210 SAS-X24F2XFP, 7710 SR, 7450 ESS, and 7750 SR.

Overload Enabled

(overloadAdministrativeState)

The Overload Enabled parameter specifies the overload state of the local device. When the parameter is enabled, the device appears to be overloaded; it can participate in OSPF routing but is not used for transit traffic. Traffic destined for directly attached interfaces continues to reach the device. The options are:

- enabled
- disabled (default)

When the parameter is enabled, the Overload Interval parameter is configurable.

Overload Interval (seconds)

(overloadInterval)

The Overload Interval (seconds) parameter specifies the interval, in seconds, after which the overload state of the local device is reset. The parameter is configurable when the Overload Enabled parameter is set to enabled. The options are:

- 0 (default) to represent an indefinite interval
- 60 to 1800

Overload Stubs

(overloadStubs)

The Overload Stubs parameter specifies whether OSPF stub networks are advertised with the maximum metric value when the system goes into overload state. The options are:

- enabled
- disabled (default)

When the parameter is set to enabled, the system uses the maximum metric value. When the parameter is set to enabled and the router is in overload, all stub interfaces, including loopback and system interfaces, are advertised at the maximum metric.

Passive

(isPassive)

The Passive parameter specifies whether the OSPF interface runs the OSPF protocol. The options are:

- Enabled
- Disabled (default)

Disabled indicates that the OSPF interface is active. A passive OSPF interface is still considered an OSPF interface. When the parameter is enabled, the interface ignores ingress OSPF packets and does not transmit OSPF packets. Service interfaces are always considered passive.

Password

(authenticationKey)

The Password parameter specifies the plain-text password authentication string for the OSPFv2 interface. The parameter is configurable when the Authentication Type parameter is set to Simple Password. The range is a string of one to eight characters. There is not default.

Policy 1

(inheritanceMask)

See the [Policy 1](#) parameter in section [203.1](#).

Policy 2**(inheritanceMask)**

See the [Policy 2](#) parameter in section [203.1](#).

Policy 3**(inheritanceMask)**

See the [Policy 3](#) parameter in section [203.1](#).

Policy 4**(inheritanceMask)**

See the [Policy 4](#) parameter in section [203.1](#).

Policy 5**(inheritanceMask)**

See the [Policy 5](#) parameter in section [203.1](#).

Poll Interval (seconds)**(pollInterval)**

The Poll Interval (seconds) parameter specifies, in seconds, the polling interval. The range is 0 to 2 147 483 647. The default is 120.

Prefix Length**(prefixLength)**

The Prefix Length parameter specifies a mask for the range of IP addresses that is used by an OSPF area border router to summarize or suppress route information. The range is 0 to 128. The default is 24.

OSPF area border routers send summary LSAs to describe routes to other areas. To minimize the number of LSAs, the area border routers use the parameter and the [Network](#) parameter to send reachability information about the devices within the specified range to other devices in the OSPF area.

Priority**(priority)**

The Priority parameter specifies the priority of the OSPF interface to determine the designated device. The parameter is configurable when the Type parameter is set to broadcast. Table [200-8](#) describes the parameter options.

Table 200-8 Priority parameter

Option	Option description	Dependencies
0	The device cannot be the designated device.	—
1 (default) to 255	The priority of the device	A higher number indicates a higher priority.

Redistribute External Routes

(nssaRedistribute)

The Redistribute External Routes parameter specifies whether to redistribute external routes into the NSSA or the ABR that exports routes into OSPF non-NSSAs. The parameter is configurable when the Type parameter is set to NSSA (No Type 5 External) or NSSA (No Summaries). The options are:

- enabled (default)
- disabled

Re-enter Key

(key)

The Re-enter Key parameter specifies an unique MD5 key. The range is a string from 1 to 16 characters. The parameter is configurable when the Authentication Type parameter is set to MD5-based Authentication. The parameter value must match the Key parameter. There is no default.

Re-enter Password

(authenticationKey)

The Re-enter Password parameter specifies the plain text password authentication string for the OSPF interface. The parameter is configurable when the Authentication Type parameter is set to Simple Password. The value must match the Password parameter. There is not default.

Remote Neighbor IP Address

(shamNeighborIpAddress)

The Remote Neighbor IP Address parameter specifies the IP address of the sham link neighbor. Specify an IPv4 address in dotted-decimal format. The default value is 0.0.0.0.

Retransmission Interval (seconds)

(retransmissionInterval)

The Retransmission Interval (seconds) parameter specifies how long OSPF waits before retransmitting an unacknowledged LSA to an OSPF neighbor through an interface or across a virtual link or sham link. The parameter value should be greater than the value of the Transit Delay (seconds) parameter. The range is 1 to 1800. The default is 5.

RFC1583 Compatible

(isRFC1583Compatible)

The RFC1583 Compatible parameter specifies whether OSPFv2 and external route calculations are done in compliance with RFC 1583 and earlier RFC documents. The options are:

- true (default)
- false

RFC 1583 and earlier RFCs use different methods to calculate summary and external route costs. To avoid routing problems in an OSPFv2 domain, all devices should use the same calculation methods.

The parameter is not configurable for OSPFv3.

Router Dead Interval (seconds)

(routerDeadInterval)

The Router Dead Interval (seconds) parameter specifies, in seconds, how long OSPF waits before a neighboring device is declared down. When no hello packets are received in the interval, the device is considered down. The parameter should be set to at least twice the value of the Hello Interval (seconds) parameter. The parameter value of both endpoints of the link must match. The range is 0 to 2147483647 for an interface or virtual link, or 1 to 65535 for a sham link. The default is 40 for an interface or sham link, or 60 for a virtual link.

Use the parameter and the Hello Interval (seconds) parameter to establish and maintain the health of adjacency between devices. You can increase the rate at which hello messages are sent to allow faster detection of device failures. However, more processing is required to perform additional checks.

Second Wait (milliseconds)

(lsaGenerateSecondWait)

The Second Wait (milliseconds) parameter specifies, in milliseconds, when to generate the third and subsequent LSAs. The range is 10 to 600 000. The default is 5000.

Use the Initial Wait (milliseconds), LSA Generate Max Wait (milliseconds) and Second Wait (milliseconds) parameters to specify the timers between generating the first, second, and subsequent LSAs. For example, if the Initial Wait (milliseconds) parameter is set to 5000, the first LSA occurs in 5000 ms. If the Second Wait (milliseconds) parameter is set to 5000, then the second LSA occurs in 5000 ms. The next run is an exponential increase to 10 000 ms, then 20 000 ms, then 40 000 ms until the LSA Generate Max Wait (milliseconds) parameter is reached.

Alcatel-Lucent recommends configuring the LSA Generate Max Wait (milliseconds) parameter to a value equal to or greater than the LSA Arrival Wait (milliseconds) parameter.

Second Wait (milliseconds)

(spfSecondWait)

The Second Wait (milliseconds) parameter specifies, in milliseconds, the second and subsequent intervals to perform SPF calculations. Use the parameter and the SPF Max Wait (milliseconds) and Initial Wait (milliseconds) parameters to control the first, second, and subsequent SPF calculations after a topology change. The range is 10 to 100 000. The default is 1000. Values must be entered in 100s of ms. Any other increment is rejected.

When subsequent SPF runs are required, the runs occur based on the an exponentially increasing interval, based on the Second Wait (milliseconds) parameter following the initial run based on the Initial Wait (milliseconds) parameter. For example, if the Initial Wait (milliseconds) parameter is set to 1000, the first SPF run occurs in 1000 ms. If the Second Wait (milliseconds) parameter is set to 1000, then the second SPF run occurs in 1000 ms. The next run is an exponential increase to 2000 ms, then 4000 ms, then 8000 ms until the Max Wait Time (milliseconds) parameter is reached. After a full interval with no SPF runs, the timer interval returns to the Initial Wait (milliseconds) value.

SPF Max Wait (milliseconds)

(spfMaxWait)

The SPF Max Wait (milliseconds) parameter specifies, in milliseconds, the maximum interval between two SPF calculations. Use the parameter and the Initial Wait (milliseconds) and Second Wait (milliseconds) parameters to control the first, second, and subsequent SPF calculations after a topology change. The range is 10 to 120 000. The default is 10 000. Values must be entered in 100s of ms. Any other increment is rejected.

When subsequent SPF runs are required, the runs occur based on the an exponentially increasing interval, based on the Second Wait (milliseconds) parameter following the initial run based on the Initial Wait (milliseconds) parameter. For example, if the Initial Wait (milliseconds) parameter is set to 1000, the first SPF run occurs in 1000 ms. If the Second Wait (milliseconds) parameter is set to 1000, then the second SPF run occurs in 1000 ms. The next run is an exponential increase to 2000 ms, then 4000 ms, then 8000 ms until the Max Wait Time (milliseconds) parameter is reached. After a full interval with no SPF runs, the timer interval returns to the Initial Wait (milliseconds) value.

Super-Backbone

(superBackBone)

The Super-Backbone parameter specifies whether CE-PE functionality is required. The OSPF super-backbone indicates the type of LSA generated as a result of routes redistributed into OSPF. The options are:

- false (default)
- true

When OSPF super-backbone is enabled, the redistributed routes are injected as summary, internal, or type 3 LSAs (internal). When the OSPF super backbone is disabled, the redistributed routes are injected as either external or type 5 LSAs (external).



Note — The Super-Backbone parameter applies only to VPRN instances of OSPF.

Suppress DN Bit

(suppressDNBit)

The Suppress DN Bit parameter specifies whether to suppress the ability to set the DN bit for OSPF LSA packets. When the parameter value is set to enable, the DN bit for the OSPF LSA packets are not set. When the parameter value is set to disable, the OSPF router follows the normal procedures to determine whether to set the DN bit. The options are:

- Enabled (default)
- Disabled

Traffic Engineering Support

(trafficEngineeringSupport)

The Traffic Engineering Support parameter specifies whether traffic engineering route calculations, based on device and link values, are enabled. The parameter is not configurable for OSPFv2 in VPRN or for OSPFv3 in general. The options are:

- false
- true (default)

Transit Area

(transitAreaId)

The Transit Area parameter specifies the IP address of the far-end device that connects the backbone area with the area that has no physical connection to the backbone. See the [Virtual Neighbor Router \(Site\) ID](#) parameter for more information.

Transit Delay (seconds)

(transitDelay)

The Transit Delay (seconds) parameter specifies the estimated time, in seconds, to transmit an LSA on the OSPF interface or virtual link. The parameter value should be less than the value of the Retransmission Interval (seconds) parameter. The range is 1 to 1800. The default is 1.

Transmit Interval

(transmitInterval)

The Transmit Interval parameter specifies, in milliseconds, the interval between LSA advertisements, to prevent the flooding of downstream routers with too many LSA packets. The range is 0 to 4 294 967. The default is 30.

Type

(areaType)

The Type parameter specifies the type of OSPF area. Table 200-9 describes the parameter options.

Table 200-9 Type parameter

Option	Option description	Dependencies
Backbone	The OSPF backbone area must be contiguous and all other areas must be connected to the backbone area. The backbone distributes routing information between areas. If it is not practical to connect an area to the backbone, the area border routers must be connected using a virtual link.	The backbone area is 0.0.0.0
Standard (All LSAs) (default)	A standard area is not an NSSA or a stub area.	—
Stub (No Type 5 External)	A stub area is a designated area that does not allow external route advertisements. Routers in a stub area do not maintain external routes. A single default route to an ABR replaces all external routes.	An area can be stub or NSSA, but not both at the same time.
Totally Stub (No Summaries)		
NSSA (No Type 5 External)	An OSPF NSSA is similar to stub areas, however, an NSSA can flood externally learned routes to the entire OSPF domain using an ABR.	
NSSA (No Summaries)	External routes learned by OSPF routers in the NSSA are advertised as type 7 LSAs within the NSSA and are translated by ABRs into type 5 external route advertisements for distribution into other areas of the OSPF domain.	

The hierarchical design of OSPF areas allows a collection of networks to be grouped into a logical OSPF area. The topology of one area is concealed from the rest of the areas, which significantly reduces OSPF protocol traffic.

Routing in the AS occurs on two levels, depending on whether the source and destination of a packet reside in the same area (intra-area routing) or different areas (inter-area routing). In intra-area routing, the packet is routed solely based on information that is obtained within the area; no routing information obtained from outside the area is used.

Unicast Import

See the [Unicast Import](#) parameter in section [203.1](#).

Version

(version)

The Version parameter specifies whether the OSPF area uses OSPFv2 or OSPFv3. The options are:

- 2 (default)
- 3

Virtual Neighbor Router (Site) ID

(virtualNeighborRouterId)

The Virtual Neighbor Router (Site) ID parameter specifies the creation of virtual links using the IP address of the far-end device to connect a non-backbone OSPF area to the backbone OSPF area. Specify an IPv4 address in dotted-decimal format. The device must be configured as an area border router. The device must be connected by a physical link to the device that is an area border router to the area that is physically connected to the backbone area.

The backbone area in an OSPF AS must be contiguous and all other areas must be connected to the backbone area. This is not always possible because of topology issues.

You can use virtual links to connect to the backbone through a non-backbone area. To configure virtual links, the router must be an ABR. Virtual links are identified by the router ID of the other endpoint, which must be another ABR. The two endpoint routers must be attached to a common area, which is called the transit area. The area through which you configure the virtual link must have full routing information.

Transit areas pass traffic from an area adjacent to the backbone or to another area. The traffic does not originate in, nor is it destined for, the transit area. The transit area cannot be a stub area or an NSSA. Virtual links are part of the backbone, and behave as if they were unnumbered point-to-point networks between the two devices. A virtual link uses the intra-area routing of its transit area to forward packets. Virtual links are created when the shortest-path routes across the transit area are built.

VPN Domain ID (hex)

(vpnDomainId)

The VPN Domain ID parameter specifies the OSPF VPN domain that is exchanged using BGP in the extended community attribute that is associated with a prefix. The parameter is only configurable when the [VPN Domain Type](#) parameter is set to a value other than none. Specify a domain ID using three groups of four hexadecimal digits. The range is 14. The default is 0000.0000.0000.



Note — The VPN Domain ID parameter applies only to VPRN instances of OSPF.

VPN Domain Type

(**vpnDomainType**)

The VPN Domain Type parameter specifies the type of extended community attribute that is exchanged using BGP to carry the OSPF VPN domain ID. The options are:

- none (default)
- type0005
- type0105
- type0205
- type8005



Note — The VPN Domain Type parameter applies only to VPRN instances of OSPF.

VPN Tag

(**vpnTag**)

The VPN Tag parameter specifies the route tag for an OSPF VPN on a PE router. This parameter is configured to prevent routing loops.



Note — The VPN Tag parameter applies only to VPRN instances of OSPF.

201 –Network Domain parameters

201.1 Network Domain parameters 201-2

201.1 Network Domain parameters

This chapter describes the parameters on the Network Domains form, and the child forms launched from the right-click contextual menu options for network domains.

Description

See the [Description](#) parameter in section [203.1](#).

Domain Name

The Domain Name displays the name of the domain that was configured.

Interface Association Count

The Interface Association Count parameter specifies the number of interfaces associated with the domain.

Routing Instance ID

The Routing Instance ID displays the ID of the routing instance in the site.

Routing Instance Name

The Routing Instance Name displays the name of the routing instance in the site.

SDP Association Count

The SDP Association Count lists the number of SDP and tunnels associated with the domain.

Site Name

The Site Name is the name in which the network domain was configured.

Site ID

The Site ID is the ID in which the network domain was configured.

Network Interfaces tab

The Network Interfaces tab lists the details of all the interfaces associated with the network domain. You can enter details in each of the options or select an option from the dropdown menu to filter your criteria.

Service Tunnels tab

The Service Tunnels tab lists the details of all service tunnels and SDP associated with the network domain. You can enter details in each of the options or select an option from the dropdown menu to filter your criteria.

202 –Static Routes parameters

202.1 Static Routes parameters 202-2

202.1 Static Routes parameters

This chapter describes the parameters on the Static Routes property form, and the child forms launched from the right-click contextual menu options for static routes.

Administrative State

See the [Administrative State](#) parameter in section 203.1.

Auto-Assign ID

See the [Auto-Assign ID](#) parameter in section 203.1.

BFD Enabled

(bfdEnabled)

See the [BFD Enabled](#) parameter in section 203.1.

Destination

(destination)

The Destination parameter, in combination with the [Prefix Length](#) parameter, specifies the IP address of the far-end device in the static route. Specify an IPv4 address in dotted-decimal format or an IPv6 address in colon-hexadecimal format.

Disallow IGP

See the [Disallow IGP](#) parameter in section 203.1.

Drop Count

(cpeDropCount)

The Drop Count parameter specifies how many consecutive ping replies must be missed to declare the CPE down and to deactivate the associated static route. The range is 1-255 and the default is 3.

Enable CPE Check

The Enable CPE parameter allows configuration of the CPE check parameters when it is enabled. The CPE check parameters are hidden when it is disabled. The default is disabled.

Interval (seconds)

(cpeInterval)

The Interval (seconds) parameter specifies the interval, in seconds, between ICMP pings to the target CPE IP address. The default is 1.

IP Address

(targetIpAddress)

The IP Address parameter specifies the IP address of the device at the end of the static route. Specify an IPv4 address in dotted-decimal format, or, if IPv6 is enabled, an IPv6 address in colon-hexadecimal format. There is no default.

The IP Address parameter, in the context of a static route, specifies that:

- for indirect static routes, the parameter is an IP address not directly connected to a network configured on this device. The destination can be reachable using multiple paths. The static route remains valid as long as the IP address configured as the indirect address remains a valid entry in the routing table.
- for next hop static routes, the parameter is an IP address on the network side or the access side on this device. This IP address must be associated with a network that is directly connected to a network configured on this device.

Log

(cpeEnableLog)

The Log parameter specifies whether to enable the logging of transitions between active and in-active, based on the CPE connectivity check. The default is Disabled.

Mask

(mask)

The Mask parameter specifies the subnet mask of the far-end device of the static route. Use the parameter and the Destination parameter to specify the address of the far-end device.

Metric

(metric)

The Metric parameter specifies the cost for the static route. The range is 0 to 65 535. The default is 1.

On the OmniSwitch, the Metric parameter can only be modified when creating a static route.

The parameter is used when you import the static route into other protocols, such as OSPF. When the metric is configured as 0, the metric configured in the protocol, for example, OSPF, applies. When there are multiple static routes with the same Preference parameter setting, but different Metric parameter settings, the lower-cost route based on the Metric parameter is used.

Multicast Capable Peers

(multicastCapablePeers)

The Multicast Capable Peers parameter specifies whether multicast capable BGP peers are displayed. The options are:

- Enabled
- Disabled (default)

Preference

See the [Preference](#) parameter in section [203.1](#).

Prefix Length

See the [Prefix Length](#) parameter in section [203.1](#).

Static Route ID

(id)

The Static Route ID parameter specifies the unique ID number for the static route. The parameter is configurable when the Auto-Assign ID parameter is set to Disabled. The parameter must be unique. The range is 1 to 2 147 483 647. The default is the next available 5620 SAM-generated ID.

Target IP Address

(cpeAddress)

The Target IP Address parameter specifies the IP address of the target CPE device. When this object is configured, ICMP pings are sent to this target IP address to determine CPE connectivity and whether this static route should be active. There is no default.

Type

(type)

The Type parameter specifies the type of static route. Table [202-1](#) describes the parameter options.

Table 202-1 Type parameter

Option	Option description	Dependencies
Next Hop (default)	Specifies that the directly connected next hop IP address is used to reach the destination address set using the Destination parameter This is the only option available when configuring OmniSwitch static routes.	When the next hop is across an unnumbered interface, you can configure the Unnumbered Interface parameter

(1 of 2)

Option	Option description	Dependencies
Indirect	Specifies that the route is indirect and that the next hop IP address is used to reach the destination. The configured IP Address parameter for static routes is not directly connected to a network configured on this device. The destination can be reachable using multiple paths. The static route remains valid as long as the IP Address parameter configured as the indirect address remains a valid entry in the routing table.	Indirect static routes cannot use an IP address prefix or subnet mask to another indirect static route
Black Hole	Specifies that the route is a black hole route. If the destination address on a packet matches this static route, the packet is discarded into the black hole route.	—

(2 of 2)

Unnumbered Interface

(interfaceName)

The Unnumbered Interface parameter specifies an IP interface that has been configured as an unnumbered interface. To conserve IP addresses, unnumbered interfaces can be configured. The address used when generating packets on this interface is the IP address.

203 –Common network navigation tree parameters

203.1 Common network navigation tree parameters 203-2

203.1 Common network navigation tree parameters

This chapter describes the parameters that are common to the network navigation tree forms and child forms.

Action

(action)

The Action parameter specifies whether the IP address range configured in the [Start Address](#) and [End Address](#) parameters is included in the subnetwork's free IP address pool. The options are:

- Included (default)
- Excluded

Administrative State

(administrativeState)

The Administrative State parameter specifies whether an object is administratively enabled. The options are:

- Up (default)
- Down

Advertise Tunnel Links Enabled

(advertiseTunnelLink)

The Advertise Tunnel Links Enabled parameter specifies whether or not the advertisement of LSP shortcuts into IGP has been enabled for OSPFv2 and IS-IS. When this parameter is enabled, LSP shortcut advertisement into IGP is allowed. The options are:

- enabled
- disabled (default)

Allow Directed Broadcasts

(directedBroadcast)

The Allow Directed Broadcasts parameter specifies whether the forwarding of directed broadcasts from the IP interface is enabled. A directed broadcast is a packet that is received on a local device interface destined for the subnet broadcast address of another IP interface. The parameter enables or disables the transmission of packets destined to the subnet broadcast address of the egress IP interface. The options are:

- Enabled
- Disabled (default)

When enabled, a frame destined to the local subnet on this IP interface is sent as a subnet broadcast from this interface. When disabled (default) frames are not broadcast from this interface.



Caution — Enabling the parameter allows direct broadcasts. Allowing direct broadcasts is a well-known mechanism used for denial-of-service attacks.

Auto-Assign ID

(id)

The Auto-Assign ID parameter specifies whether the 5620 SAM automatically assigns a unique ID to the created object. The options are:

- Enabled (default)
- Disabled

BFD Enabled

(bfdEnabled)

The BFD Enabled parameter specifies whether bi-directional forwarding detection is enabled for the interface. When the value is configured to true, the interface can establish BFD sessions and use a BFD for signaling. When the value is configured to false, the interface cannot use BFD. The options are:

- True
- False (default)

Broadcast

(broadcast)

The Broadcast parameter specifies whether to allow SNTP broadcasts to be received on the IP interface. The options are:

- Enabled
- Disabled (default)

Broadcast Address Format

(bcastAddrFormat)

The Broadcast Address Format parameter specifies how to override the default broadcast address used by the IP interface when IP broadcasts are sourced on the IP interface. Table [203-1](#) describes the parameter options.

Table 203-1 Broadcast Address Format parameter

Option	Option description	Dependencies
Host Ones (default)	Host Ones specifies that the local broadcast address used by the IP interface for this IP address is the subnet broadcast address. This is an IP address that corresponds to the local subnet specified by the IP address and Subnet Mask parameters with all the host bits set to binary 1. For example, for the subnet 10.10.16.0/20, the address is 10.10.31.255.	—
All Ones	All Ones specifies that the broadcast address used by the IP interface for this IP address is 255.255.255.255, which is also known as the local broadcast.	

Cflowd Type

(cflowdType)

The Cflowd Type parameter specifies whether to collect traffic flow samples through a device for analysis. This is also known as network performance statistics. The statistics are used for network planning and traffic engineering, capacity planning, security, and user profiling, performance monitoring, and SLA measurement. Table 203-2 describes the parameter options.

Table 203-2 Cflowd Type parameter

Option	Option description	Dependencies
None (default)	Do not collect statistics on the network interface.	—
ACL	Collect statistics associated with an ACL filter.	
Interface	Collect statistics associated with an IP interface.	

Class

(rtrInterfaceClass)

The Class parameter specifies an IP interface as an unnumbered interface or an IP address as the numbered interface and then the IP address to be used for the numbered interface. To conserve IP addresses, unnumbered interfaces can be configured. The address used to generate packets on an unnumbered interface is the configured IP Address parameter. Table 203-3 describes the parameter options.

Table 203-3 Class parameter

Option	Option description	Dependencies
Unnumbered	The interface to associate with the unnumbered IP address in dotted-decimal format. The configured IP address must exist on the device.	—

(1 of 2)

Option	Option description	Dependencies
Numbered (default)	The IP address to associate with the numbered IP interface in dotted-decimal format. The configured IP address must exist on the device.	—

(2 of 2)

Constraint Admin State

(mCacConstAdminState)

The Constraint Admin State parameter specifies whether the constraints of the multicast CAC policy are administratively up. The options are:

- Up (default)
- Down

Description

(description)

The Description parameter specifies a unique description for the routing instance interface or other routing object. The range is generally 0 to 80 characters. The range may vary depending on the configuration form. The default is generally an empty string.

Disable Router Alert Check

(disRtrAlertChk)

The Disable Router Alert Check parameter specifies whether router alert checking for IGMP messages is enabled or disabled for an interface. If the parameter is set to True, checking is disabled. The options are:

- true
- false (default)

Disallow IGP

(disallowIGP)

The Disallow IGP parameter specifies whether to allow or disallow the IGP next hop from being used. If Disallow IGP is set and no LSP qualifies as a next hop, the static route becomes inactive. If Disallow IGP is not set and the LSP's far end is reachable using the IGP, the static route remains up, regardless of the LSP status. The options are:

- true
- false (default)

The Disallow IGP parameter is only displayed when you enable one of the [IGP Shortcut](#) options.

When the parameter is set to true, and no tunnel qualifies as the next hop, the next hop to the indirect next hop address is not used. When the parameter is set to false, the indirect next hop address is used as the next hop of last resort.

DoD Label Distribution

(dodLabel)

The DoD Label Distribution parameter provides support for Downstream-on-Demand (DoD) label allocation as per RFC 5036. This ability can only be enabled on a link level LDP session, and applies to prefix labels only, not service labels.

The options are:

- true
- false (default)

Egress Filter ID

(egressFilterId)

The Egress Filter ID parameter specifies the ID of the egress ACL. The ACL is used to prevent traffic from specified addresses from being forwarded from the interface.

Enable DHCP Relay

(administrativeState)

The Enable DHCP Relay parameter specifies the administrative state for DHCP relay. DHCP discover messages are broadcast packets that typically do not leave the IP subnet. DHCP relay agents are used to intercept the requests and forward them as unicast messages to a DHCP server. The options are:

- Up
- Down (default)

Enable Implicit Null Label

(implicitNullLabel)

The Enable Implicit Null Label parameter allows a 7x50 egress LER to receive MPLS packets from the previous hop without the outer LSP label, as specified in RFC 3032 "MPLS Label Stack Encoding". This option is signalled by the egress LER to the previous hop during the LSP signalling with LDP or RSVP control protocols. In addition, the egress LER can be configured to receive MPLS packets with the Implicit Null label on a Static LSP. Accordingly, the Enable Implicit Null Label parameter can be configured in several locations in 5620 SAM, affecting LDP, RSVP, RSVP interfaces, Static LSPs, and MPLS interfaces.

Configuration points to consider:

- An RSVP interface will, by default, inherit the value for Implicit Null Labeling from the parent RSVP site. You can change this behavior by deselecting the associated Inherit From RSVP checkbox.
- The behavior of this parameter for Static LSPs and Static Label Maps is somewhat different. The configured state of the Enable Implicit Null Labeling parameter is not deployed directly to a device, as is the case for LDP and RSVP. Instead, the state of the parameter's checkbox is used to determine the deployed value for the existing [Egress Label](#) parameter. The Egress Label parameter is disabled when the Enable Implicit Null Label checkbox is selected, and it is enabled otherwise.
- Static LSPs must be shutdown before you can modify the [Egress Label](#) (and therefore also the Enable Implicit Null Label) parameter.
- The Static Label Map in an MPLS interface must be shutdown before you can modify the [Egress Label](#) (and therefore also the Enable Implicit Null Label) parameter. The Enable Implicit Null Label parameter here is only configurable when the [Label Action](#) parameter is set to Swap.

For all occurrences of the Enable Implicit Null Label parameter, the options are:

- disabled (default)
- enabled

Enable Ingress Flowspec

(**ingressFlowspec**)

The Enable Ingress Flowspec parameter specifies whether ingress flow specifications are enabled on an interface. The options are:

- enabled
- disabled (default)

Enable LDP Synchronization

(**enableLdpSync**)

The Enable LDP Synchronization parameter specifies whether IGP-LDP synchronization is enabled on all interfaces in the IS-IS or OSPF routing protocol. When the value is set to enable (default), during a failure, IGP temporarily sets the link cost to infinity to allow IGP and LDP to converge. After the timer expires, the actual cost is restored. When the value is set to disabled, IGP and the LDP converge independently.

The options are:

- enabled (default)
- disabled

Family

(family)

The Family parameter specifies the types of routing information that are distributed by a BGP instance. Table 203-4 describes the parameter options.

Table 203-4 Family parameter

Option	Option description	Dependencies
L2 VPN	Enable L2 VPN.	Required to enable BGP Auto-discovery in LDP VPLS. Applies to global-, peer-, and peer-group-level BGP.
IPv4 (default)	Enable IPv4.	Applies to global-, peer-, and peer-group-level BGP
IPv6	Enable IPv6.	Available for global-, peer-, and peer-group-level BGP on the 7710 SR and 7750 SR (chassis modes C and D, and chassis modes A and B with mixed mode enabled), and the 7450 ESS in mixed mode.
Multicast IPv4	Enable MP-BGP for the exchange of IPv4 multicast data.	Applies to global-, peer-, and peer-group-level BGP, and to routing policy entries
Unicast IPv4 (default)	Enable the exchange of IPv4 unicast data.	Applies to routing policy entries
Unicast IPv6	Enable the exchange of IPv6 unicast data.	Applies to routing policy entries on the 7710 SR and 7750 SR, and the 7450 ESS in mixed mode
VPN IPv4	Enable MP-BGP for the exchange of IPv4 routes in VPRN services. The distributed information includes an RD and the IP address prefix. When both IPv4 and IPv6 VPRN services are enabled, the PE router uses the same 8-byte RD for both address families.	Applies to global-, peer-, and peer-group-level BGP, and to routing policy entries NEs that support IPv4 VPRN services require this option. The RD must be unique within the scope of the VPRN to allow overlap of the IP address prefixes in different VRFs.
Multicast VPN IPv4	Enable BGP MCAST-VPN IPv4 address family. The distributed information includes an RD and the IP address prefix. When both IPv4 and IPv6 VPRN services are enabled, the PE router uses the same 8-byte RD for both address families.	Applies to BGP, BGP peer and BGP Group configurations, and to routing policy entries. NEs that support IPv4 VPRN services require this option. The RD must be unique within the scope of the VPRN to allow overlap of the IP address prefixes in different VRFs.
VPN IPv6	Enable MP-BGP for the exchange of IPv6 routes in VPRN services. The distributed information includes an RD and the IP address prefix. When both IPv4 and IPv6 VPRN services are enabled, the PE router uses the same 8-byte RD for both address families.	Applies to global-, peer-, and peer-group-level BGP, and to routing policy entries on the 7710 SR and 7750 SR (chassis modes C and D, and chassis modes A and B with mixed mode enabled), and the 7450 ESS in mixed mode. NEs that support IPv6 VPRN services require this option. The RD must be unique within the scope of the VPRN to allow overlap of the IP address prefixes in different VRFs.
MDT SAFI	Enable MDT SAFI address family. This command enables peer capability to exchange MDT-SAFI address family advertisement.	Applies to BGP, BGP Peer Group and BGP Peer.

Force Q Tag Forwarding

(forceQTagForwarding)

The Force Q Tag Forwarding parameter specifies whether or not to enable the addition of an IEEE 802.1q tag after the Customer MAC address when the PBB header is built as it egresses a related B-VPLS service. This ability allows you to preserve the dot1p priority information of the incoming data and control traffic for PBB Epipe and I-VPLS services.

Configuration points to consider:

- Once 'Force Q Tag Forwarding' is enabled in one I-VPLS / mI-VPLS / PBB Epipe instance, it should be enabled in all of the related instances.
- In 5620 SAM, if one site in an I-VPLS / mI-VPLS / Epipe service has Force Q Tag Forwarding enabled, all other sites in the service should also have this property enabled.
- An operational flag named “Force Q Tag Forwarding Inconsistent” appears in the State Cause block of the I-VPLS, mI-VPLS and EPIPE service configuration form. This flag is checked whenever there is an inconsistent configuration.

The options for this parameter are:

- true
- false (default)

Graceful Restart

(gracefulRestart)

The Graceful Restart parameter specifies whether to allow graceful restart for this routing instance. A graceful restart allows a router to restart or reload device software as it continues to forward data. The options are:

- true
- false (default)

Group IP Address

Table 203-5 lists where to find more information about the Group IP Address parameter.

Table 203-5 Group IP Address parameter

Parameter	See
Group IP Address for the Candidate RP	Group IP Address parameter in this section
Group IP Address for SPT Switchover Threshold	Group IP Address parameter in this section

Group IP Address

(groupAddress)

The Group IP Address parameter is the multicast group IP address that is associated with the spanning tree switchover threshold. The range is an IP address from 224.0.0.0 to 239.255.255.255. The default is 0.0.0.0.

Group IP Address

(groupIPAddress)

The Group IP Address parameter combines with the [Mask](#) parameter to obtain the range of multicast group addresses to which the router advertises to be the candidate RP. The value of the Group IP Address parameter is sent as the RP address. The range is an IP address from 224.0.0.0 to 239.255.255.255. The default is 0.0.0.0.

Helper Mode

(grHelperMode)

The Helper Mode parameter specifies whether the instance to assist in the graceful restart of another router instance. The parameter is configurable when the Graceful Restart parameter is set to true. The options are:

- true (default for IS-IS)
- false (default for OSPF)

IGP Inhibit

(igpInhibit)

The IGP Inhibit parameter specifies whether the secondary IP address should not be recognized as a local interface by the running IGP. The options are:

- Enabled
- Disabled (default)

The parameter is configurable when the Primary parameter is not enabled.

When the parameter is enabled, OSPF and IS-IS are not used as passive interfaces, and are not advertised as internal IP interfaces into the IGP link state database. When the parameter is enabled, RIP does not use the secondary IP addresses as source for RIP updates.

IGP Shortcut

(igpShortcut)

The IGP Shortcut parameter specifies whether or to use Layer 2 tunnels as next hops for prefixes associated with the far-end termination point of the tunnel. The options are:

- LDP
- RSVP-TE
- MPLS

When an option for the IGP Shortcut parameter is enabled, IGP shortcuts associated with the tunnel are used to resolve the next hops.

The RSVP-TE option for BGP next hop route resolution allows forwarding of IPv4 packets to routes resolved to a BGP next hop using an RSVP-TE LSP. The RSVP LSP must have a destination address matching the /32 address of the BGP next hop. When the RSVP-TE shortcut is enabled in BGP, a route resolved to a BGP next hop will use the RSVP LSP towards the BGP next hop, if it is available in the tunnel table. If it is not available, the regular IGP next hop is used.

The MPLS option instructs BGP to first attempt to resolve the BGP next hop to an RSVP LSP. If no RSVP LSP exists or the existing ones are down, BGP automatically searches for the LDP LSP with a FEC prefix corresponding to the same /32 prefix in the tunnel table and resolves the BGP next hop to it.

When you enable one of the IGP Shortcut options, the [Disallow IGP](#) parameter is displayed.

Ingress Filter ID

(**ingressFilterId**)

The Ingress Filter ID parameter specifies the ID of the ingress ACL. The ACL is used to prevent traffic from specified addresses from being sent to the interface.

Inherit Value

The Inherit Value parameter specifies whether to re-use an existing configuration setting for a parameter. The Inherit Value check boxes are located beside the parameters that can inherit a value from the parent object. For example, when you create a BGP peer group, you can inherit values set at the parent BGP global level. The options are:

- Enabled (default)
- Disabled

When you choose the Disabled option, you can specify a new value for the parameter.

Interface Name

(**routerName**)

The Interface Name parameter specifies the routing policy filter of label bindings based on matching bindings received from a neighbor or neighbors adjacent over the interface specified by the parameter. The parameter is configurable on the 7750 SR. The range is an interface name of 0 to 32 characters. The default is an empty string.

IP Address

(**primaryIpAddress**)

The IP Address parameter specifies the IP address for the object. An IP address must be assigned to each IP interface. An IP address and a subnet mask create an IP prefix. The defined IP prefix must be unique within the context of the routing instance. The prefix must not overlap with other IP prefixes that are defined as local subnets on other IP interfaces in the same routing context within the device. Specify an IPv4 address in dotted-decimal format, or, if IPv6 is enabled, an IPv6 address in colon-hexadecimal format. There is no default.

IPv4 RPF Lookup Sequence

(rpfLookupSequence)

The RPF Lookup Sequence parameter allows you to indicate which routing tables PIM and MDSP use for standard unicast traffic and multicast RPF lookups. When the parameter option is set to Both, PIM and MDSP perform RPF lookups in the unicast routing table first. The options are:

- Multicast Route Table
- Unicast Route Table (default)
- Both

IPv6 Allowed

(ipv6Allowed)

The IPv6 Allowed parameter specifies whether an IPv6 addressing scheme is valid for the interface. The options are:

- enabled
- disabled (default)

IPv6 BFD Enabled

(ipv6BfdEnabled)

The IPv6 BFD Enabled parameter specifies whether bi-directional forwarding detection is enabled for the interface. When the value is configured to true, the interface can establish IPv6 BFD sessions and use a BFD for signaling. When the value is configured to false, the interface cannot use BFD. The options are:

- True
- False (default)

Key

(key)

The Key parameter specifies the authentication key that is used by routers to authenticate each other during a protocol session. The key value must consist of 7-bit ASCII characters. The parameter is configurable when the encryption type is MD5. There is no default. Table [203-9](#) lists the ranges for different protocols.

Table 203-6 Key parameter

Protocol	Range (characters)
BGP	0 to 255
IS-IS	0 to 254
LDP	1 to 16
MSDP	0 to 255
OSPF	1 to 16
RIP	0 to 16
RSVP	0 to 16

Lease Populate

(leasePopulate)

The Lease Populate parameter specifies the number of DHCP lease state entries that are allowed for the IES or VPRN SAP. Enabling the parameter also enables DHCP snooping. The range is 0 to 8000. There is no default. Setting the parameter to 0 specifies that dynamic host lease state management for the interface is disabled.

DHCP snooping on the SAP obtains the lease state information for a host from a DHCP ACK message that is sent by a DHCP server to the host. Entries in the DHCP lease state table remain valid for the duration of the IP address lease.

LDP

(ldp)

The LDP parameter specifies whether the IGP short cut uses LDP tunnels as next hops for prefixes associated with the far-end termination point of the tunnel. This parameter is configurable when the static route Type parameter is set to indirect. The options are:

- Enabled
- Disabled (default)

LDP over RSVP Include

(ldpOverRsvp)

The LDP over RSVP Include parameter specifies whether the LSP is available for LDP-over-RSVP usage. The options are:

- enabled
- disabled (default)

LDP Synchronization Timer

(ldpSyncTimer)

The LDP Synchronization Timer parameter specifies a time interval (seconds) used for IGP-LDP synchronization after a failure. The timer starts when the LDP session is up and running over the interface and the FEC bindings are exchanged. When the timer expires, the link cost is restored and re-advertised. IPG announces a new best hop that the LDP can use if the label binding for the neighbor's FEC is available. This parameter can be set when the [Enable LDP Synchronization](#) parameter is set to enabled. The range is 0 to 1800 seconds. The default is 0.

LSR IP Load Balancing

(ifLsrIpLoadBalancing)

The LSR IP Load Balancing parameter specifies at the network interface level whether the IP header is used in the LAG and ECMP LSR hashing algorithm. Table [203-7](#) describes the parameter options.

Table 203-7 LSR IP Load Balancing parameter

Option	Description
System	The hashing algorithm is inherited from the Network Element object.
Label Only	The label is used exclusively in the hashing algorithm.
Label IP	The IP header is included in the hashing algorithm.
IP Only	The IP header is used exclusively in the hashing algorithm.

MAC Address

(physicalAddress)

The MAC Address parameter specifies a 48-bit MAC address for the object in unicast MAC address format. Only one MAC address can be assigned to an IP interface. The default is 00-00-00-00-00-00.

Mandatory Bandwidth (kbps)

(preRsvdMandatoryBandwidth)

The Mandatory Bandwidth (kbps) parameter specifies the bandwidth pre-reserved for mandatory type BTV channels on a specific interface. The Mandatory Bandwidth (kbps) parameter combines with the [Unconstrained Bandwidth \(kbps\)](#) parameter to establish the bandwidth assigned to traffic on an interface using a multicast CAC policy. Table [203-8](#) describes the parameter options.

Table 203-8 Mandatory Bandwidth (kbps) parameter

Mandatory Bandwidth	Unconstrained Bandwidth	Result
0	0	No channels are allowed.
-1	-1	All mandatory and optional channels are allowed.
Equal to the value in the Unconstrained Bandwidth (kbps) parameter	—	All mandatory channels configured for the multicast CAC policy associated with the interface are allowed. Optional channels are not allowed.
Less than the value in the Unconstrained Bandwidth (kbps) parameter	—	All mandatory channels configured for the multicast CAC policy associated with the interface are allowed. Optional channels are allowed depending on bandwidth availability.

The range is –1 to 22 147 483 647. The default is –1. When the Unconstrained Bandwidth parameter is set to either –1 or 0, the Mandatory Bandwidth parameter defaults to the same value. The Mandatory Bandwidth value must be less than or equal to the Unconstrained Bandwidth value.

Mask Reply

(maskReply)

The Mask Reply parameter specifies whether to allow responses to ICMP mask requests on the interface. When a local device sends an ICMP mask request to the interface and the parameter is enabled, the router interface replies to the request. The options are:

- Enabled (default)
- Disabled

Minimum TTL Value

(minTTLValue)

The Minimum TTL Value parameter specifies the expected TTL value of a packet received from a valid neighbor to prevent BGP or LDP packet spoofing. The range is 1 to 255. The default is 0, which disables TTL.

Maximum TTL

(autoTrMaxTtl)

The Maximum TTL Value parameter specifies maximum label time-to-live value for an LSP trace request during the tree discovery. The range is 1 to 255. The default is 30.

Multicast Import

(multicastImport)

The Multicast Import parameter specifies whether IGP routes are submitted to the multicast routing table. The options are:

- True
- False (default)

The parameter is not configurable for OSPFv3, or in a VPRN.

Name

(displayName)

The Name parameter specifies the name of the created object. The range is 1 to 32 characters. The default is generally an empty string.

Network Policy ID

(networkPolicyId)

The Network Policy ID parameter specifies the ID of the network policy that is used to determine the priority and handling of traffic on the network port.

Number of Packet Too Big

(numberOfPacketTooBig)

The Number of Packet Too Big parameter specifies the number of ICMP Packet Too Big messages that the interface issues in the interval specified by the [Packet Too Big Time \(seconds\)](#) parameter. The parameter is configurable when the [Packet Too Big](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Param Problem

(numberOfParamProblem)

The Number of Param Problem parameter specifies the number of ICMP Param Problem messages that the interface issues in the interval specified by the [Param Problem Time \(seconds\)](#) parameter. The parameter is configurable when the [Param Problem](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Redirects

(numberOfRedirects)

The Number of Redirects parameter specifies the maximum number of ICMP Redirect messages that the interface issues in the time specified by the [Redirects Time \(seconds\)](#) parameter. The parameter is configurable when the [Redirects](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Time Exceeded

(numberOfTimeExceeded)

The Number of Time Exceeded parameter specifies the number of ICMP Time Exceeded messages that the interface issues in the interval specified by the [Time Exceeded Time \(seconds\)](#) parameter. The parameter is configurable when the [Time Exceeded](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of TTL Expired

(numberOfTtlExpired)

The Number of TTL Expired parameter specifies the maximum number of ICMP TTL Expired messages that the interface can issue in the time specified by the [TTL Expired Time \(seconds\)](#) parameter. The parameter is configurable when the [TTL Expired](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Number of Unreachables

(numberOfUnreachable)

The Number of Unreachables parameter specifies the maximum number of ICMP Unreachable messages that the interface can issue in the time specified by the [Unreachables Time \(seconds\)](#) parameter. The parameter is configurable when the [Unreachables](#) parameter is enabled. The range is 10 to 1000. The default is 100.

Packet Too Big

(packetTooBig)

The Packet Too Big parameter specifies whether the rate at which the interface issues ICMP Packet Too Big messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Packet Too Big](#) and [Packet Too Big Time \(seconds\)](#) parameters.

Packet Too Big Time (seconds)

(packetTooBigTime)

The Packet Too Big Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Packet Too Big messages specified by the [Number of Packet Too Big](#) parameter. The parameter is configurable when the [Packet Too Big](#) parameter is enabled. The range is 1 to 60. The default is 10.

Param Problem

(paramProblem)

The Param Problem parameter specifies whether the rate at which the interface issues ICMP Packet Too Big messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Param Problem](#) and [Param Problem Time \(seconds\)](#) parameters.

Param Problem Time (seconds)

(paramProblemTime)

The Param Problem Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Packet Too Big messages specified by the [Number of Param Problem](#) parameter. The parameter is configurable when the [Param Problem](#) parameter is enabled. The range is 1 to 60. The default is 10.

Path MTU Discovery Enabled

(pathMtuDiscovery)

The Path MTU Discovery Enabled parameter specifies whether path MTU discovery is enabled for this BGP site, BGP peer group, BGP peer, or LDP peer. The options are:

- enabled
- disabled (default)

Physical Address

(physicalAddress)

The Physical Address parameter specifies a 48-bit MAC address for the static ARP network interface in the unicast MAC address format. Only one physical address can be assigned to an IP interface.

PIM RP Delayed Up Period

(pimRPDelayedUpPeriod)

The PIM RP Delayed Up Period parameter specifies delay before a PIM is in service. The range is 0 to 300. The default is 0.

Policy 1

(policy1)

The Policy 1 and Policy 2 to Policy 5 parameters specify the names of import and export route policies used to determine which routes are sent to peers and which routes are advertised to peers. When multiple Policy 1 to Policy 5 parameters are specified, the policies are evaluated in the order in which they are specified. The first policy that matches is applied.

Use the Select button beside the Policy 1 and Policy 2 to Policy 5 parameters to choose a policy from the list of policies. You must set the Apply Import Route Policy parameter to true to specify import route policies. You must set the Apply Export Route policy parameter to true to specify export route policies.

For example, for RIP routing, import route policies determine which routes are accepted by RIP neighbors. Export route policies determine which routes are exported from the route table to RIP.

For LDP routing, the import route policy filters are based on the received LDP label bindings. When the imported label bindings are received, filtering is based on additional parameters specified for the import route policy, including neighbors, interfaces, or the specified prefix list. For export route policy filters, label binding advertisements to other devices can be filtered based on a prefix list.

For PIM routing, policies determine how the PIM join-prune messages, PIM register messages, and PIM bootstrap messages are filtered.

For the scaling of LDP adjacencies, the FEC prefix import and export policies provide a means of controlling the FEC prefixes that are re-distributed between other LDP / T-LDP peers and the LDP peer you are configuring.

For proxy neighbor discovery, policies determine the interfaces that respond to neighbor discovery queries intended for other interfaces.

Policy 2

(policy2)

See the [Policy 1](#) parameter in this section.

Policy 3

(policy3)

See the [Policy 1](#) parameter in this section.

Policy 4

(policy4)

See the [Policy 1](#) parameter in this section.

Policy 5

(policy5)

See the [Policy 1](#) parameter in this section.

Populate Host Routes

(subscrHostRoutePopulate)

The Populate Host Routes parameter specifies that a subscriber interface uses a specific addresses to route to a subscriber instead of using a network-assigned address. The default is False.

Preference

(preference)

The Preference parameter specifies the preference of this route compared to:

- routes that are advertised by other routing protocols
- routes to external sites, such as IS-IS external preferences

The lower the value, the higher the chance that the route is the active route. The default value for the parameter depends on the type of route that is being configured. The range is 0 or 1 to 255. Table [203-9](#) lists the default values for different route types.

Table 203-9 Preference parameter

Option description	Default	Dependencies
Directly attached	0	Cannot be configured
Static route	5	Configurable
All BGP routes	170	
IS-IS level 1 internal routes	15	
IS-IS level 2 internal routes	18	
IS-IS level 1 external routes	160	
IS-IS level 2 external routes	165	
OSPF internal routes	10	
OSPF external routes	150	
RIP routes	100	

When you modify the preference of an existing static route, the preference metric value is not changed unless specified. Different protocols should not be configured with the same preference. If this occurs, the tie breaker is based on the default preference for each protocol, as listed in Table [203-9](#). If multiple routes are learned with an identical preference using the same protocol, the lowest-cost route is used.

Prefix Length

Table 203-10 describes where to find information about the Prefix Length parameter.

Table 203-10 Prefix Length parameter

Parameter	See
Prefix Length for exported address prefixes	Prefix Length in this section
Prefix Length for monitored address prefixes	Prefix Length in this section
Prefix Length for NAT destination address	Prefix Length in this section
Prefix Length for NAT L2-aware IP address	Prefix Length in this section
Prefix Length for other objects	Prefix Length in this section
Prefix Length for steering route address prefixes	Prefix Length

Prefix Length

(**exportAddrPrefixLen**)

The Prefix Length parameter specifies the prefix length of the [Exported Address Prefix](#) parameter. The range is 0 to 32.

Prefix Length

(**monitoredPrefixLen**)

The Prefix Length parameter specifies the prefix length of the [Monitored Address Prefix](#) parameter. The range is 0 to 32.

Prefix Length

(**prefix**)

The Prefix Length parameter specifies the prefix of the NAT destination address. The range is 16 to 32. The default is 0, which means that the parameter is not configured.

Prefix Length

(**prefixLength**)

When combined with an IP address value, the Prefix Length parameter specifies a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. The prefix must not overlap with other existing IP prefixes that are defined as local subnets on other IP interfaces in the same routing context within the device or service. The range is 1 to 32 for an IPv4 address and 1 to 128 for an IPv6 address. A value of 32 is typically reserved for an IPv4 system address, but is available for general use in IPv6. The IPv4 default is 24; the IPv6 default is 64.

Prefix Length

(prefixLength)

The Prefix Length parameter specifies the prefix of the NAT L2-aware IP address. The range is 16 to 32. The default is 0, which means that the parameter is not configured.

Prefix Length

(steerRtrAddrPrefixLen)

The Prefix Length parameter specifies the prefix length of the [Steering Route Address Prefix](#) parameter. The range is 0 to 32.

Primary

(isPrimary)

The Primary parameter specifies whether the IP address that is associated with the IP interface is an IP address from a set of actual interface addresses. For example, when VRRP sends advertisements to the network and the parameter is enabled, the primary IP address is used. The options are:

- Enabled (default)
- Disabled

Redirects

(redirects)

The Redirects parameter specifies whether the rate at which the interface issues ICMP Redirect messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Redirects](#) and [Redirects Time \(seconds\)](#) parameters.

Redirects Time (seconds)

(redirectsTime)

The Redirects Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Redirect messages specified by the [Number of Redirects](#) parameter. The parameter is configurable when the [Redirects](#) parameter is enabled. The range is 1 to 60. The default is 10.

Router ID

(routingInstanceId)

The Router ID parameter is an IP address that uniquely identifies the router within an AS. In protocols such as OSPF, routing information is exchanged between areas, which are groups of networks that share routing information. The parameter can be set to the same value as the loopback address. The value is used by both OSPF and BGP in the routing table manager instance. Specify an IPv4 address in dotted-decimal format.

RSVP Shortcut Enabled

(**rsvpShortcut**)

The RSVP Shortcut Enabled parameter specifies whether or not to enable RSVP-TE shortcuts for resolving IGP routes for OSPFv2 and IS-IS. Enabling this parameter instructs OSPFv2 or IS-IS to include RSVP LSPs originating on this node and terminating on the router-id of a remote node as direct links, with a metric equal to the operational metric provided by MPLS. The options are:

- enabled
- disabled (default)

Server 1

(**server1**)

The Server 1 parameter specifies a DHCP server for the interface. The DHCP server stores network addresses and delivers configuration parameters to DHCP clients. Specify a unicast IP address in dotted-decimal format for the Server 1 parameter.

Server 2

(**server2**)

See the [Server 1](#) in this section.

Server 3

(**server3**)

See the [Server 1](#) in this section.

Server 4

(**server4**)

See the [Server 1](#) in this section.

Server 5

(**server5**)

See the [Server 1](#) in this section.

Server 6

(server6)

See the [Server 1](#) in this section.

Server 7

(server7)

See the [Server 1](#) in this section.

Server 8

(server8)

See the [Server 1](#) in this section.

Service ID

(serviceID)

The Service ID parameter specifies a unique ID for the service. This parameter is configurable when the Auto-Assign ID parameter is disabled. The range is 1 to 2 147 483 647. The default is 0, which indicates that the parameter is not set.

Subnet Mask

(netMask)

The Subnet Mask parameter specifies the subnet mask for an IP address. An IP address and a subnet mask create a local IP prefix. The defined IP prefix must be unique within the context of the routing instance. It cannot overlap with other existing IP prefixes defined as local subnets on other IP interfaces in the same routing context within the device.

The range is 1 to 24, 31 and 32. The default is 32. Subnet mask 32 is reserved for system IP addresses. You can configure subnet mask 31 for interfaces that are used by routing protocols.

Tag

(staticRouteTag)

The Tag parameter specifies an identifier for the static route. The range is 0 to 4 294 967 295. The default is 0.

TE Metric

(teMetric)

The TE Metric parameter specifies the specific traffic engineering metric for this interface. If the TE Metric parameter is enabled, then it may be used in CSPF computations of the LSP paths. If the TE Metric parameter is not enabled, then the native IGP parameter is used in CSPF computations of the LSP paths. The range is 0 to 16777216. The default is 0.

TE Metric Enabled

(teMetricEnabled)

The TE Metric Enable parameter specifies whether the TE Metric is used for the purpose of the LSP path computation by CSPF. When this parameter is disabled, the IGP metric is used to compute the path of the LSP by CSPF. The options are:

- Enabled
- Disabled (default)

Time Exceeded

(timeExceeded)

The Time Exceeded parameter specifies whether the rate at which the interface issues ICMP Time Exceeded messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Time Exceeded](#) and [Time Exceeded Time \(seconds\)](#) parameters.

Time Exceeded Time (seconds)

(timeExceededTime)

The Time Exceeded Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Time Exceeded messages specified by the [Number of Time Exceeded](#) parameter. The parameter is configurable when the [Time Exceeded](#) parameter is enabled. The range is 1 to 60. The default is 10.

Timeout (seconds)

(timeOut)

The Timeout (seconds) parameter specifies the minimum time, in seconds, an ARP entry learned on the IP interface is stored in the ARP table. ARP entries are automatically refreshed when an ARP request or gratuitous ARP is detected from an IP host. Otherwise, the ARP entry is aged from the ARP table. The range is 0 to 65 535. The default is 14 400. When the parameter is set to 0, ARP aging is disabled.

TTL Expired

(ttlExpired)

The TTL Expired parameter specifies whether the rate at which the interface issues TTL Expired messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of TTL Expired](#) and [TTL Expired Time \(seconds\)](#) parameters.

TTL Expired Time (seconds)

(ttlExpiredTime)

The TTL Expired Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP TTL Expired messages specified by the [Number of TTL Expired](#) parameter. The parameter is configurable when the [TTL Expired](#) parameter is enabled. The range is 1 to 60. The default is 10.

Type

Table [203-11](#) lists where to find more information about the Type parameter.

Table 203-11 IP Address parameter

Parameter	See
Type for Authentication	Type parameter in this section
Type for L3 interface	Type parameter in the section

Type

(authenticationType)

The Type parameter specifies the type of authentication that is used for neighboring routers before a protocol session is set up. Table [203-12](#) describes the parameter options.

Table 203-12 Type parameter

Option	Option description	Dependencies
none (default)	There is no authentication used before a protocol session is started.	—

(1 of 2)

Option	Option description	Dependencies
md5	MD5 authentication is used between the devices involved in a protocol session.	This option is available only for RIP, IS-IS, and VRRP and requires an authentication string to pass between the devices in a protocol session. The authentication string is generally configured using the Password parameter or the Key parameter.
password	A password is used to authenticate devices involved in a protocol session.	

(2 of 2)

Type

(interfaceType)

The Type parameter specifies the type of OSPF or IS-IS interface. Table 203-13 describes the parameter options.

Table 203-13 Type parameter

Option	Option description	Dependencies
Broadcast	Maintains the interface as a broadcast network.	The default value depends on the type of interface. SONET channels default to Point to Point. Ethernet interfaces default to broadcast. Adjacency and network convergence are improved when interfaces are configured as broadcast. Point to point should be configured for two connected devices, even when the network is a broadcast medium, such as Ethernet.
Point to Point	Maintains the interface as a point-to-point link.	
Secondary	Maintains the interface as a point-to-point link which can be applied to multiple OSPFv2 areas.	—

Unconstrained Bandwidth (kbps)

(unconstrainedBandwidth)

The Unconstrained Bandwidth parameter specifies the bandwidth assigned to BTV traffic on an interface using a multicast CAC policy. If the default value of –1 is set, then the value is set to the physical bandwidth available for the interface. If a value of 0 is set, and if a multicast CAC policy is assigned to the interface, BTV traffic from that policy is not allowed on the interface. The range is 0 to 2 147 483 647. The default is –1.

Unicast Import

(unicastImport)

The Unicast Import parameter specifies whether IGP routes are submitted to the unicast routing table. The options are:

- True (default)
- False

The parameter is not configurable for OSPFv3, or in a VPRN.

Unreachables

(unreachables)

The Unreachables parameter specifies whether the rate at which the interface issues ICMP Unreachable messages is configurable. The options are:

- enabled (default)
- disabled

When the parameter is enabled, the rate at which the messages are issued is controlled by the [Number of Unreachables](#) and [Unreachables Time \(seconds\)](#) parameters.

Unreachables Time (seconds)

(unreachablesTime)

The Unreachables Time (seconds) parameter specifies the time, in seconds, during which the interface can issue the number of ICMP Unreachable messages specified by the [Number of Unreachables](#) parameter. The parameter is configurable when the [Unreachables](#) parameter is enabled. The range is 1 to 60. The default is 10.

Ring Group navigation tree parameters

204 — Network parameters

204 –Network parameters

204.1 Network parameters 204-2

204.1 Network parameters

This chapter describes the parameters on the Ring Group form opened using the Network contextual menu in the Ring Group navigation tree.

Description

(groupDescription)

The Description parameter specifies a description for the ring group. The range is 0 to 255 characters.

Enabled

(enabled)

The Enabled parameter specifies whether TLS is enabled for the ring group. When the Enabled parameter is enabled from the TLS tab button, all 7250 SAS or Telco devices added to the ring group inherit the configured TLS parameter settings.

Ethertype

(ethertypeValue)

The Ethertype parameter specifies the 802.1Q tag for the Ethernet packet representing the VLAN ID. You can configure the parameter when the Enabled parameter on the TLS tab is enabled. The default is 0x8100, which is the standard tag for 802.1Q traffic. The range is a supported three- to six-character hexadecimal number in the format 0x1234.

Group Name

(groupName)

The Group Name parameter specifies a name for the ring group. The range is 1 to 10 characters.

Jumbo Frame

(jumboFrame)

The Jumbo Frame parameter specifies whether the 7250 SAS or Telco device allows Ethernet payloads in frames larger than 1500 bytes. You can configure the parameter when the Enabled parameter on the TLS tab is enabled. Use the parameter to allow the transport of large frames for Gigabit Ethernet interfaces, in which a larger MTU frame size is required. The options are:

- Enabled
- Disabled (default)

Devices in the L2 VPN service and the VLAN must be capable of supporting larger frame sizes. All devices in the same ring must have the same parameter setting. For example, all devices can have the parameter enabled, or all of them can have it disabled. You must reboot the node for a change to the parameter to take effect.

Mode

See the [Mode](#) parameter in section 187.1.

Query Response Time (seconds)

(mvrQueryTime)

The Query Response Time (seconds) parameter specifies the maximum time to wait for IGMP report memberships on a receiver port before removing the port from multicast group membership. The range is 0 to 25 s. The default is 10 s.

Ring Group Type

(groupMode)

The Ring Group Type parameter specifies whether the ring group is to be used for VLAN or VPLS services. The options are:

- VLAN (default)
- VPLS

Customer documentation and product support



Customer documentation

<http://www.alcatel-lucent.com/myaccess>

Product manuals and documentation updates are available at [alcatel-lucent.com](http://www.alcatel-lucent.com). If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.



Technical Support

<http://support.alcatel-lucent.com>



Documentation feedback

documentation.feedback@alcatel-lucent.com



© 2011 Alcatel-Lucent. All rights reserved.

3HE 06496 AAAC TQZZA Edition 01