Alcatel-Lucent

Service Access Switch| Release 7.0 Rev.04

7210-SAS D, E, K OS
Services Guide

3HE09512AAABTQZZA

Alcatel·Lucent

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.

Table of Contents

List of Tables

List of Figures

Preface

About This Guide

This guide describes subscriber services, and mirroring support provided by the 7210 SAS-D, E, K presents examples to configure and implement various protocols and services.

On 7210 SAS devices, not all the CLI commands are supported on all the platforms and in all the modes. In many cases, the CLI commands are mentioned explicitly in this document. In other cases, it is implied and easy to know the CLIs that are not supported on a particular platform.

NOTE: 7210 SAS-E, 7210 SAS-D, and 7210 SAS-K operate in access-uplink mode by default. No explicit user configuration is needed for this.

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

Audience

This manual is intended for network administrators who are responsible for configuring the 7210 SAS-D, E, K. It is assumed that the network administrators have an understanding of networking principles and configurations. Protocols, standards, and services described in this manual include the following:

- CLI concepts
- Subscriber services
- Service mirroring
- Operation, Administration and Maintenance (OAM) operations

List of Technical Publications

The 7210 SAS-D, E, K OS documentation set is composed of the following books:

- 7210 SAS-D, E, K OS OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.

- 7210 SAS-D, E, K OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.

- 7210 SAS-D, E, K OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), link aggregation group (LAG), and port provisioning.

- 7210 SAS-D, E, K OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, as well as IP and MAC-based filtering.

- 7210 SAS-D, E, K OS OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for route policies.

- 7210 SAS-D, E, K OS Services Guide

  This guide describes how to configure service parameters such as customer information and user services.

- 7210 SAS-D, E, K OS OS OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.

- 7210 SAS-D, E, K OSQuality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.

Technical Support

If you purchased a service agreement for your 7210 SAS-series router and related products from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance. If you purchased an Alcatel-Lucent service agreement, contact your welcome center:

Web: http://www.alcatel-lucent.com/wps/portal/support

Getting Started

In This Chapter

This book provides process flow information to configure provision services.

Alcatel-Lucent 7210 SAS Services Configuration Process

Table 1 lists the tasks necessary to configure subscriber services and configure mirroring. This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 1: Configuration Process

Area	Task	Chapter
Subscribers	Subscriber services	
	Global entities	Configuring Global Service Entities with CLI on page 57
	VLL services	Ethernet Pipe (Epipe) Services on page 98
	VPLS service	Virtual Private LAN Service on page 161
	IES service	Internet Enhanced Service on page 233
Reference	List of IEEE, IETF, and other proprietary entities.	Standards and Protocol Support on page 485

Services Command Reference

In This Chapter

This chapter provides the command reference trees for the 7210 SAS services.

Topics include:

- Global Services Commands
- Service Configuration Commands
  - → VPLS Service Configuration Commands on page 238
  - → IES Service Configuration Commands on page 323

SERVICES OVERVIEW

In This Section

This section provides an overview of the 7210 SAS D, E-Series subscriber services, service model and service entities. Additional details on the individual subscriber services can be found in subsequent chapters.

Topics in this section include:

Introduction

A service is a globally unique entity that refers to a type of connectivity service for either Internet or VPN connectivity. Each service is uniquely identified by a service ID and an optional service name within a service area. The 7210 SAS-Series service model uses logical service entities to construct a service. In the service model, logical service entities provide a uniform, service-centric configuration, management, and billing model for service provisioning.

In the 7210 SAS-Series, services can provide Layer 2/bridged service between a service access point (SAP) and another service access point (a SAP is where traffic enters and exits the service) on the same (local) router

Service Types

The 7210 SAS-D, E, K offers the following types of subscriber services which are described in more detail in the referenced chapters:

- Virtual Leased Line (VLL) services:
  - → Ethernet pipe (Epipe) — A Layer 2 point-to-point VLL service for Ethernet frames. See Ethernet Pipe (Epipe) Services on page 98.
- Virtual Private LAN Service (VPLS) — A Layer 2 multipoint-to-multipoint VPNbridging service or VPN (using QinQ uplinks).See Virtual Private LAN Service on page 161.

Service Policies

Common to all 7210 SAS-Series connectivity services are policies that are assigned to the service. Policies are defined at a global level and then applied to a service on the router. Policies are used to define 7210 SAS-Series service enhancements. The types of policies that are common to all 7210 SAS-Series connectivity services are:

- SAP Quality of Service (QoS) policies which allow for different classes of traffic within a service at SAP ingress.
- SAP Quality of Service (QoS) policies allow different classes of traffic within a service at SAP ingress. Access egress QoS policies allow differential treatment of various traffic classes within a service (SAPs) which exists in an egress port.

  QoS ingress and egress policies determine the QoS characteristics for a SAP. A QoS ingress policy applied to a SAP specifies the number of meters, meter characteristics (such as forwarding class, committed, and peak information rates, etc.) and the mapping of traffic to a forwarding class. A QoS egress policy defines the queue characteristics (such as CBS, CIR, PIR). A QoS policy must be created before it can be applied to a SAP. A single ingressQoS policy can be associated with a SAP. A single access egress QoS policy can be associated with a port.
- Filter policies allow selective blocking of traffic matching criteria from ingressing or egressing a SAP.

  Filter policies, also referred to as access control lists (ACLs), control the traffic allowed in or out of a SAP based on MAC or IP match criteria. Associating a filter policy on a SAP is optional. Filter policies are identified by a unique filter policy ID. A filter policy must be created before it can be applied to a SAP. A single ingress and single egress filter policy can be associated with a SAP.
- Scheduler policies define the operating parameters (such as scheduling algorithm, weights per priority). Depending on the platform, these are either associated with SAPs or physical ports.
- Accounting policies define how to count the traffic usage for a service for billing purposes.

  The routers provide a comprehensive set of service-related counters. Accounting data can be collected on a per-service, per-forwarding class basis, which enables network operators to accurately measure network usage and bill each customer for each individual service using any of a number of different billing models.

Alcatel-Lucent Service Model

In the Alcatel-Lucent service model, the service edge routers are deployed at the provider edge. Services are provisioned on the service routers and transported across an IP and/or IP/MPLS provider core network in encapsulation tunnels created using generic router encapsulation MPLS label switched paths (LSPs). 7210 SAS-D, E, K support only QinQ and Dot1q Layer 2 uplinks, which are used to transport the services to the provider edge in a hierarchal configuration. The 7210 SAS-D, E, K do not support transport tunnels that use MPLS LSPs or GRE SDPs.

The service model uses logical service entities to construct a service. The logical service entities are designed to provide a uniform, service-centric configuration, management, and billing model for service provisioning. Some benefits of this service-centric design include:

- Many services can be bound to a single customer.
- QoS policies, filter policies, and accounting policies are applied to each service instead of correlating parameters and statistics from ports to customers to services.

Service provisioning uses logical entities to provision a service where additional properties can be configured for bandwidth provisioning, QoS, security filtering, accounting/billing to the appropriate entity.

Service Entities

The basic logical entities in the service model used to construct a service are:

- Customers (see page 27)
- Service Access Points (SAPs) (see page 27)

Customers

The terms customers and subscribers are used synonymously. The most basic required entity is the customer ID value which is assigned when the customer account is created. To provision a service, a customer ID must be associated with the service at the time of service creation.

Service Access Points (SAPs)

Each subscriber service type is configured with at least one service access point (SAP). A SAP identifies the customer interface point for a service on an Alcatel-Lucent router (Figure 2). The SAP configuration requires that slot, MDA, and port information be specified. The slot, MDA, and port parameters must be configured prior to provisioning a service (see the Cards, MDAs, and Ports sections of the 7210 SAS OS Interface Configuration Guide).

A SAP is a local entity to the router and is uniquely identified by:

- The physical Ethernet port
- The encapsulation type
- The encapsulation identifier (ID)

Depending on the encapsulation, a physical port can have more than one SAP associated with it. SAPs can only be created on ports designated as “access” or “access uplink” in the physical port configuration. SAPs can be created on ports designated as core facing “access uplink” ports. These ports have a different set of features enabled in software.

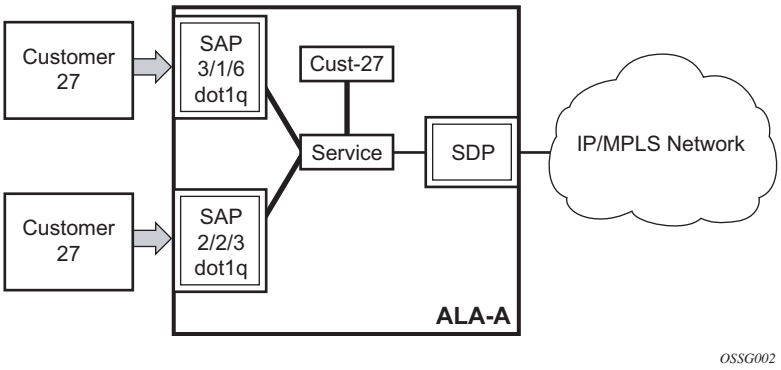


Figure 1: Service Access Point (SAP) for 7210 SAS configured in Network Mode

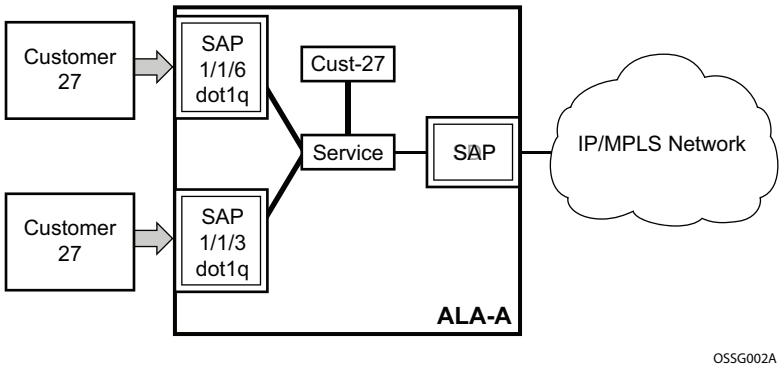


Figure 2: Multiple SAPs in a service using QinQ uplinks in 7210 SAS configured in access-uplink mode

SAP Encapsulation Types and Identifiers

The encapsulation type is an access property of a service Ethernet port. The appropriate encapsulation type for the port depends on the requirements to support multiple services on a single port on the associated SAP and the capabilities of the downstream equipment connected to the port. For example, a port can be tagged with IEEE 802.1Q (referred to as dot1q) encapsulation in which each individual tag can be identified with a service. A SAP is created on a given port by identifying the service with a specific encapsulation ID.

Ethernet Encapsulations

The following lists encapsulation service options on Ethernet ports:

- Null — Supports a single service on the port. For example, where a single customer with a single service customer edge (CE) device is attached to the port. The encapsulation ID is always 0 (zero).
- Dot1q — Supports multiple services for one customer or services for multiple customers (Figure 3). For example, the port is connected to a customer who wants multiple services. The encapsulation ID used to distinguish an individual service is the VLAN ID in the IEEE 802.1Q header.
- QinQ — The QinQ encapsulation type adds a IEEE 802.1Q tag to the 802.1Q tagged packets entering the network to expand the VLAN space by tagging tagged packets, producing a double tagged frame. On the 7210 SAS-E, QinQ encapsulation is supported only on access uplink ports.

The following lists encapsulation service options on Ethernet access uplink ports:

- QinQ — The QinQ encapsulation type adds a IEEE 802.1Q tag to the 802.1Q tagged packets entering the network to expand the VLAN space by tagging tagged packets, producing a double tagged frame. On the 7210 SAS-E, QinQ encapsulation is supported only on access uplink ports.

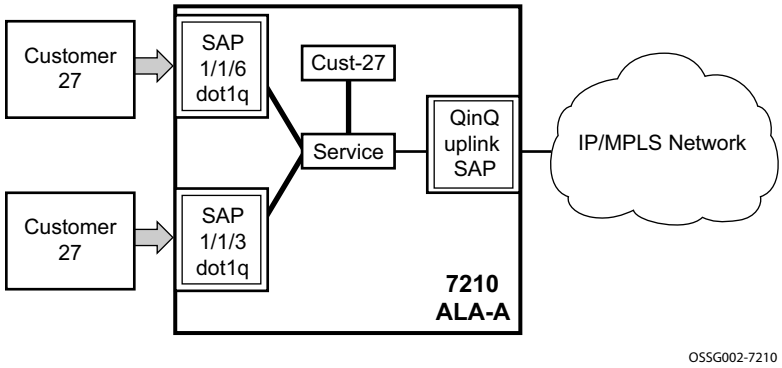


Figure 3: Multiple SAPs on a Single Port

Services and SAP Encapsulations

Table 3 lists the service and SAP Encapsulation information for Ethernet ports:

Table 2: Service and Encapsulation

Port Type	Encapsulation	7210 SAS Platforms Support
Ethernet	Null	7210 SAS-E,D,K
Ethernet	Dot1q	7210 SAS-E,D,K
Ethernet	QinQ	7210 SAS-D,K

Table 3 lists the service and SAP Encapsulation information for Ethernet access uplink ports.

Table 3: Port Type and Encapsulation

Port Type	Encapsulation
Ethernet access uplink	QinQ

Default SAP on a Dot1q Port

This feature introduces default SAP functionality on Dot1q-encapsulated ports. On a dot1q-encapsulated port where a default SAP is configured, all packets with q-tags not matching any explicitly defined SAPs will be assigned to this SAP. SAPs with default Dot1q encapsulation are supported in VPLS and Epipe services. Dot1q Default SAP are not supported in VPRNs. In this context, the character “*” indicates default which means allow through. The default SAP also accepts untagged or priority tagged packets. A default SAP must be configured explicitly. When a default SAP is not configured explicitly, packets not matching any explicitly defined SAPs will be dropped.

One of the applications where this feature can be applicable is an access connection of a customer who uses the whole port to access Layer 2 services. The internal VLAN tags are transparent to the service provider. This can be provided by a null encapsulated port.

In this type of environment, logically two SAPs exist, a management SAP and a service SAP. The management SAP can be created by specifying a VLAN tag which is reserved to manage the CPE. The service SAP covers all other VLANs and behaves as a SAP on a null-encapsulated port.

There a few constraints related for the use of default SAP on a Dot1q-encapsulated port:

- This type of SAP is supported only on VPLS and Epipe services and cannot be created in IES services as it cannot preserve VLAN tag markings.
- For VPLS SAPs with STP enabled, STP listens to untagged and null-tagged BPDUs only. All other tagged BPDUs are forwarded like other customer packets. This is the same behavior as null-encapsulated ports.
- IGMP snooping is not supported on a default SAP. This would require remembering VLAN tags per hosts. By not allowing IGMP snooping of this SAP, all IGMP packets will be transparently forwarded.

Default SAPs on a QinQ Port

Default QinQ SAPs (notation - *.*) are used in ring ports to avoid the need to configure services on all the intermediate nodes in the ring which are transiting the service. Default QinQ SAPs matches all VLAN tagged traffic which is not classified into any other SAP configured on the same port. Only one EPIPE service with default QinQ SAPs is needed for transit service traffic on access-uplink ports. Default QinQ SAPs are allowed only on access-uplink ports and access ports. It can co-exist with 0.* SAP on an access-uplink or access port. A default QinQ SAP accepts only tagged packets. Untagged packets or priority tagged packets are not accepted on Default QinQ SAPs.

When an EPIPE service With default QinQ SAPs on the ring ports is used for transit traffic in a ring deployment, no protection mechanism (example: STP or G.8032) is supported for Default

QinQ SAPs. The upstream or head-end node on which the service originates must ensure the correct path on the ring is selected using either G.8032 or STP. When a VPLS service with default QinQ SAPs on the ring ports is used for transit traffic in a ring deployment, users can use either G8032 or M-VPLS with xSTP for ring protection. When using G8032, the state of the default QinQ SAPs in the VPLS service can be managed using a separate G8032 control instance.
NOTE: G8032 control instance cannot use Default QinQ SAPs.

Default QinQ SAP is available for use only in an EPIPE and a VPLS service created with svc-sap-type parameter set to "null-star". Default QinQ SAP can be configured along with other SAPs allowed in the same service (that is, service with svc-sap-type parameter set to "null-star").

Following features are available for use with Default QinQ SAPs configured in EPIPE and VPLS service (unless explicitly specified, below listed features are applicable for both EPIPE and VPLS service):

For Default QinQ SAPs on either access ports or access-uplink ports:

- MAC learning and aging is available for use in a VPLS service
- Per SAP MAC limit is available for use in a VPLS service
- Mac-move detection and Mac-pinning is available for use in a VPLS service
- Discard-unknown and discard-unknown-source is available for use in a VPLS service
- ETH-CFM and Y.1731 is not available for use
- STP (and all its different flavors) cannot be enabled in the service with Default QinQ SAPs
- MVPLS with xSTP can be used for loop prevention. The Default QinQ SAPs inherit the state from the associated MVPLS instance.
- G.8032 control instance cannot be configured in a service with Default QinQ SAP
- G8032 can be used for loop prevention in ring deployments, where the Default QinQ SAPs are configured on the ring ports in a VPLS service. A separate G8032 control instances needs to be configured for use on the ring ports and the service with Default QinQ ports needs to be associated with this G8032 control instance
- IGMP snooping is not available for use
- L2PT and BPDU translation is not available for use
- IP interface in a VPLS service is not supported in a service using this SAP

For Default QinQ SAPs created on Access-uplink Port:

- Ingress qos policy applied on an access uplink port is available for classification and policing on ingress.
- Egress qos policy applied on an access uplink port is available for egress queue shaping, scheduling and marking.

- SAP Ingress ACLs are available for use
- SAP Egress ACLs are not available for use
- SAP Ingress received count and SAP Egress forwarded count are available for use (appropriate accounting records can be used)

For Default QinQ SAPs created on access ports:

- SAP ingress qos policy is available for use
- Egress qos policy applied on an access port is available for egress shaping, scheduling and marking.
- SAP Ingress ACLs are available for use
- SAP egress ACLs are not available for use
- SAP Ingress Meter counters, SAP Ingress received count and SAP Egress forwarded counter are available for use (appropriate accounting records can be used)

Configuration Notes for use of Default QinQ SAPs for transit service in a ring deployment

- If an Epipe service is used with Default QinQ SAPs on the ring ports for transit service in a ring deployment, no protection mechanism is available for the transit service (that is, Epipe service with the Default QinQ SAPs on ring ports). Both Epipe and VPLS services which are originating on different nodes in the ring can use the transit service. Protection/ Loop-detection mechanisms can be implemented for VPLS service configured in the ring nodes, by using MVPLS with xSTP on the nodes where the VPLS service is configured. No protection mechanisms are available for use with Epipe services on the node that originates the service.
- If a VPLS service is used with Default QinQ SAPs on the ring ports for transit service in a ring deployment, either MVPLS/xSTP or G8032 can be used to protect the transit service (that is, VPLS service with the Default QinQ SAPs on ring ports). In this case, VPLS service which are originating on different nodes in the ring and use the transit VPLS service are also protected. Epipe services which are originating on different nodes in the ring cannot use the transit VPLS service.
- When using VPLS service with Default QinQ SAPs for transit service with either G8032 or MVPLS with xSTP configured for protection, load-balancing of the traffic based on the VLAN IDs is not possible. If load-balancing is desired then it is better to use Epipe service with Default QinQ SAPs as the transit service.

SAP Configuration Considerations (applicable for access-uplink mode)

When configuring a SAP, consider the following:

- A SAP is a local entity and only locally unique to a given device. The same SAP ID value can be used on another 7210 SAS-Series.
- On 7210 SAS-D and 7210 SAS-E, a physical port can have only one SAP to be part of one service. Multiple SAPS can be defined over a physical port but each of these SAPs should belong to a different service.
- On 7210 SAS-K, multiple SAPs configured on the same port can be part of the same service.
- 7210 SAS-K supports use of Q1.0 SAP. This SAP matches packets received on a port with the outermost tag being Q1 and the inner tag being absent (that is, no tag) or the inner tag is a priority tag. It does not accept packets with any other VLAN tag value as the inner tag.
- There are no default SAPs configured on the node. All SAPs in subscriber services must be created.
- The default administrative state for a SAP at creation time is administratively enabled.
- When a SAP is deleted, all configuration parameters for the SAP will also be deleted.

- A SAP is owned by and associated with the service in which it is created in each router.
- A port with a dot1q encapsulation type means the traffic for the SAP is identified based on a specific IEEE 802.1Q VLAN ID value. The VLAN ID is stripped off at SAP ingress and the appropriate VLAN ID placed on at SAP egress. As a result, VLAN IDs only have local significance, so the VLAN IDs for the SAPs for a service need not be the same at each SAP.
- If a port is administratively shutdown, all SAPs on that port will be operationally out of service.
- A SAP cannot be deleted until it has been administratively disabled (shutdown).
- On 7210 SAS-D and 7210 SAS-E, L2PT cannot be configured for use on all the configured SAPs simultaneously. The number of SAPs which can use this simultaneously is lesser than maximum amount of SAPs supported by the node.
- Each SAP can have one each of the following policies assigned:
  - → Ingress filter policy
  - → Egress filter policy
  - → Ingress QoS policy
  - → Accounting policy
  - → Egress QoS policy on 7210 SAS-K only
- An ingress QoS policy and accounting policy is assigned per access uplink port and cannot be assigned per access uplink SAP.
- The `svc-sap-type' parameter value determines the type of SAPs that are allowed to be provisioned in a service. The Table 4, “SAP and Service Combinations for 7210 SAS-E,” on page 36 provides details of SAP and service combinations allowed in access-uplink mode for 7210 SAS-E devices. The Table 5, “SAP and Service Combinations for 7210 SAS-D,” on page 37 provides details of SAP and service combinations allowed in 7210 SAS-D devices. The Table 6, “SAP and Service Combinations for 7210 SAS-K,” on page 40 provides details of SAP and service combinations allowed in 7210 SAS-K devices
- If a service’s sap-type is specified as dot1q-preserve, all the SAPs configured in the service must have the same VLAN ID. The outermost VLAN tag of the packets received on access port is not stripped, when svc-sap-type is set to dot1q-preserve.

Configuration Guidelines for 7210 SAS-E

1. For 7210 SAS-E devices, the traffic usage on a SAP can be monitored by enabling a counter. The counter collects the total number of packets or octets forwarded across the SAP. The user can configure the mode of the counter to collect data in either packets or octets. The mode of the counter can be specified for ingress SAP counters only. The egress SAP counters collect only the number of packets. The accounting records collect the count of packets or octets on a SAP using the accounting logs. The default mode of the ingress SAP counter is set to packets. The egress SAP counter is disabled by default.
2. The mode of the counter cannot be changed if an accounting policy is already associated with a SAP.
3. Ensure that egress SAP counters are enabled before associating accounting records that count egress forwarded packets.
4. Before modifying the counter, disable the account log generation, run the command:
   no collect-stats
5. Egress SAP statistics are not available on any of the SAPs of a port, on which a dot1q SAP and dot1q default SAP configuration are present at the same time. This is a hardware limitation. This limitation also applies for egress ACLs.
6. Egress SAP statistics cannot be configured to use simultaneously on all the configured SAPs. The number of SAPs which can use this feature simultaneously, is less than the maximum amount of SAPs supported by the node.
7. There is no limit to the number of access ports allowed to be configured. In other words all ports can be configured as access ports. The number of access-uplink ports that can be configured is limited. In other words, only a subset of ports can be configured as access-uplink ports at a given time.

Table 4: SAP and Service Combinations for 7210 SAS-E

svc-sap-type	Access SAPs	Access Uplink SAPs
null-star	Null SAP,dot1q Default SAP	Q.* SAP, 0.* SAP
dot1q-preserve	dot1q SAP (dot1q VLAN tag not stripped on ingress)	Q1.Q2
dot1q	dot1q SAP, dot1q explicit null SAP	Q.* SAP, 0.* SAP

Configuration Guidelines for 7210 SAS-D

1. Ensure that egress SAP counters are enabled before associating accounting records that count egress forwarded packets.

2. Before modifying the counter, disable the account log generation, run the command: **no collect-stats**
3. Egress SAP statistics are not available on any of the SAPs of a port, on which a dot1q SAP and dot1q default SAP configuration are present at the same time. This is a hardware limitation. This limitation also applies for egress ACLs.
4. Egress SAP statistics cannot be configured to use simultaneously on all the configured SAPs. The number of SAPs which can use this feature simultaneously is less than the maximum amount of SAPs supported by the node.

Table 5: SAP and Service Combinations for 7210 SAS-D

svc-sap-type	Access SAPs	Access Uplink SAPs
null-star	Null SAP, dot1q Default SAP Q.* SAP, 0.* SAP Default QinQ SAP (*.* SAP)	Q.* SAP, 0.* SAP Default QinQ SAP (*.* SAP)
dot1q-preserve	dot1q SAP (dot1q VLAN tag not stripped on ingress), Q1.Q2 SAP (Q2 tag VLAN must match the dot1q SAP VLAN ID)	Q1.Q2 SAP (Q2 tag VLAN ID must match the dot1q SAP VLAN ID)
any	null SAP, dot1q SAP, dot1q explicit null SAP Q1.Q2 SAP, Q.* SAP, 0.* SAP	Q1.Q2 SAP, Q.* SAP, 0.* SAP
dot1q-range	Dot1q SAP (dot1q VLAN tag not stripped on ingress), Q1.* SAP	Q1.* SAP

NOTES:

- Dot1q Default SAP cannot be configured when svc-sap-type is set to ‘any’.
- When svc-sap-type is set to ‘any’ for a NULL SAP, the system processes and forwards only packets with no VLAN tag (that is, untagged). All other packets with one or more VLAN tags (even those with priority tag only) are not processed and dropped. Users can use the service with svc-sap-type set to ‘null-star’, to process and forward packets with one or more tags (including priority tag) on a NULL SAP.
- The Default QinQ SAP processes only tagged packets received on a QinQ port. All tagged packets that do not match the specific SAP tags configured on the same port are processed

by this SAP. The Default QinQ SAP cannot process un-tagged packets, even if 0.* SAP is not configured for use on that port.

- The Default QinQ SAPs is available for use with 0.* SAPs configured on the same port or in the same service. It is available for use with another default QinQ SAP configured in the same service (on a different port).
- In a VPLS service, the Default QinQ SAP is available for use with any other SAP type configured in a service configured with svc-sap-type parameter set to "null-star".
- SAPs using connection-profile (to specify dot1q VLAN ranges) can be configured in a service only when svc-sap-type is set to 'dot1q-range'.
- When a service is configured to use svc-sap-type 'dot1q-range', the outermost V-LAN tag of the packets are not stripped when the packet is received on access port ingress. For more information on processing behavior for this type of service, see “Ethernet Pipe (Epipe) Services on page 98 ” section.
- The following counters are available on 7210 SAS-D devices:
  - → Ingress and egress counters per SAP
  - → Ingress policer counters per SAP
  - → Egress queue counters per access port
  - → Ingress and egress counters per access-uplink port
  - → The number of counters available to count total received packets or octets on an access-uplink SAP (in a VPLS, VLL or IES service) ingress is limited and hence count of received packets or octets cannot be obtained for all the SAPs simultaneously. By default these counts is not available.
  - → The CLI command **config>service>epipe>sap>statistics>ingress** (this command is supported on vpls and ies services also) is available to associate a counter with the SAP and obtain the counts.
  - → The number of counters available to count total forwarded packets or octets on an access SAP egress and access-uplink SAP egress is limited and hence count of received packets or octets cannot be obtained for all the SAPs simultaneously. By default these counts is not available.
  - → The CLI command *config>service>epipe>sap>statistics>ingress>forwarded-count* (this command is supported on VPLS and IES services also) is available to associate a counter with the SAP and obtain the counts.

Configuration Guidelines for 7210 SAS-K

- The 7210 SAS-K supports the following types of SAPs:
  - → **Access SAPs** – Null, Dot1q (Dot1q, Dot1q Default, Dot1q range, Dot1q explicit NULL), QinQ SAPs (Q1.Q2, Q1. *, Q1.0 QinQ Default SAP (that is, *.* SAP), 0.*) is supported.
  - → **Access Uplink SAPs** – QinQ SAPs (various SAP types such as Q1.Q2, QinQ Default SAP (*.* SAP), 0.*, Q1.*, Q1.0) is supported
- Unlike other 7210 L2 mode platforms (that is, D/E), the 7210 SAS-K supports Q1.0 SAP. This SAP accepts a packet with the outermost tag as Q1 or a packet with outermost tag as Q1 and the following inner tag is a priority tag. Unlike 7x50, it does not accept packets with 2 tags with the outermost tag being Q1 and the inner tag being any tag other than priority tag.
- Allows any port to be configured in either access uplink mode or access mode. Additionally the ports can be in access uplink mode or access mode or they can be mix of the ports using either modes. There is no limit to the number of access ports allowed to be configured. In other words all ports can be configured as access ports. The number of access-uplink ports depends on the number of QoS resources allocated per port. In other words, not all the ports can be configured as access-uplink ports at a given time.
- 7210 SAS-K supports service MTU.
  - → A received frame/packet length is checked against the configured service MTU after subtracting the length of the SAP encapsulation (including the L2 header) from the received frame length. The packet is further processed in the context of the service, if the computed length is less than equal to the configured service MTU or the packet is dropped.
  - → The user must configure the correct service MTU across all the nodes through which the service is transported.
  - → Service MTU is not supported on other 7210 L2 mode platforms.
- Supports L2 VPNs/services
  - → VLL/Epipe with access and/or access uplink SAPs of any encapsulation.
  - → VPLS with access and/or access uplink SAPs of any encapsulation.
  - → Unlike other 7210 L2 mode platforms, 7210 SAS-K supports only the following svc-sap-type parameters:
    - – **'any'** – A service configured with this value for svc-sap-type allows for configuration of all combination of access SAPs and access-uplink SAPs in the same service, except for dot1q range SAPs. A packet that is

received with tags more than the number of SAP tags to which it is mapped to, is forwarded transparently in the service (the processing behavior is similar to any other packet mapped to the SAP).

– **'dot1q-range'** – A service configured with this value for svc-sap-type allows for configuration of dot1q range SAPs and Q1.* access-uplink SAP in the same service.

Table 6: SAP and Service Combinations for 7210 SAS-K

svc-sap-type	Access SAPs	Access Uplink SAPs
any	null SAP, dot1q SAP, dot1q explicit null SAP Q1.Q2 SAP, Q.* SAP, Q1.0 SAP, 0.* SAP QinQ default SAP (*.* SAP)	Q1.Q2 SAP, Q.* SAP, Q1.0 SAP, 0.* SAP, QinQ default SAP (*.* SAP)
dot1q-range	Dot1q SAP (dot1q VLAN tag not stripped on ingress), Q1.* SAP	Q1.* SAP

G.8032 Ethernet Ring Protection Switching

NOTE: G.8032 Ethernet Ring Protection Switching is not supported on 7210 SAS-K.

Ethernet ring protection switching offers ITU-T G.8032 specification compliance to achieve resiliency for Ethernet Layer 2 networks.G.8032 (Eth-ring) is built on Ethernet OAM and often referred to as Ring Automatic Protection Switching (R-APS).

Eth-rings are supported on VPLS SAPs. VPLS services supporting Rings SAPs can connect to other rings and Ethernet service using VPLS, SAPs. Eth-rings enables rings for core network or access network resiliency. A single point of interconnection to other services is supported. The Eth-ring service is a VLAN service providing protection for ring topologies and the ability to interact with other protection mechanisms for overall service protection. This ensures failures detected by Eth-ring only result in R-APS switchover when the lower layer cannot recover and that higher layers are isolated from the failure.

Rings are preferred in data networks where the native connectivity is laid out in a ring or there is a requirement for simple resilient LAN services. Due to the symmetry and the simple topology, rings are viewed a good solution for access and core networks where resilient LANS are required. The Alcatel-lucent implementation can be used for interconnecting access rings and to provide traffic engineered backbone rings.

Eth-rings use one VID per control per ring instance and use one (typically) or multiple VIDs for data instances per control instance. A dedicated control VLAN (ERP VLAN) is used to run the protocol on the control VID. G.8032 controls the active state for the data VLANs (ring data instances) associated with a control instance. Multiple control instances allow logically separate rings on the same topology. The Alcatel-lucent implementation supports dot1q, and qinq encapsulation for data ring instances. The control channel supports dot1q and qinq encapsulation.

Note: In 7210 SAS-D devices, CCMs used for G.8032 Ethernet ring protection service is implemented in hardware. In 7210 SAS-E, CCMs used for G8032 Ethernet ring protection service is implemented in software.

Overview of G.8032 Operation

R-APS messages that carry the G.8032 protocol are sent on dedicated protocol VLAN called ERP VLAN (or Ring Control Instance). In a revertive case, G.8032 Protocol ensures that one Ring Protection Link (RPL) owner blocks the RPL link. R-APS messages are periodically sent around in both directions to inform other nodes in the Ring about the blocked port in the RPL owner node. In non-revertive mode any link may be the RPL link.Y.1731 Ethernet OAM CC is the basis of the RAPs messages. Y.1731 CC messages are typically used by nodes in the ring to monitor the health of each link in the ring in both directions. However CC messages are not mandatory. Other link layer mechanisms could be considered – for example LOS (Loss of Signal) when the nodes are directly connected.

Initially each Ring Node blocks one of its links and notifies other nodes in the ring about the blocked link. Once a ring node in the ring learns that another link is blocked, the node unblocks its blocked link possibly causing FDB flush in all links of the ring for the affected service VLANs, controlled by the ring control instance. This procedure results in unblocking all links but the one link and the ring normal (or idle) state is reached. In revertive mode the RPL link will be the link that is blocked when all links are operable after the revert time. In non-revertive mode the RPL link is no different that other ring links. Revertive mode offers predictability particularly when there are multiple ring instances and the operator can control which links are block on the different instances. Each time there is a topology change that affects Reachability, the nodes may flush the FDB and MAC learning takes place for the affected service VLANs, allowing forwarding of packets to continue. Figure 4 depicts this operational state:

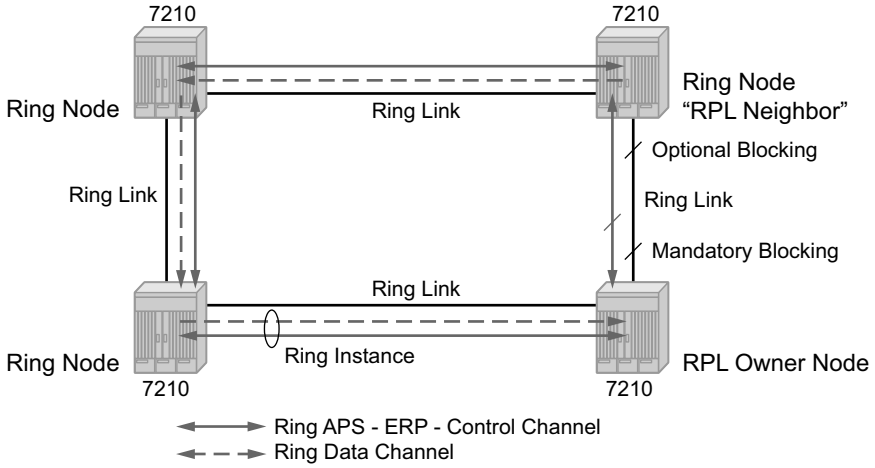


Figure 4: G.8032 Ring in the Initial State

When a ring failure occurs, a node or nodes detecting the failure (enabled by Y.1731 OAM CC monitoring) send R-APS message in both directions. This allows the nodes at both ends of the failed link to block forwarding to the failed link preventing it from becoming active. In revertive mode, the RPL Owner then unblocks the previously blocked RPL and triggers FDB flush for all

nodes for the affected service instances. The ring is now in protecting state and full ring connectivity is restored. MAC learning takes place to allow Layer 2 packet forwarding on a ring. The following picture depicts the failed link scenario.

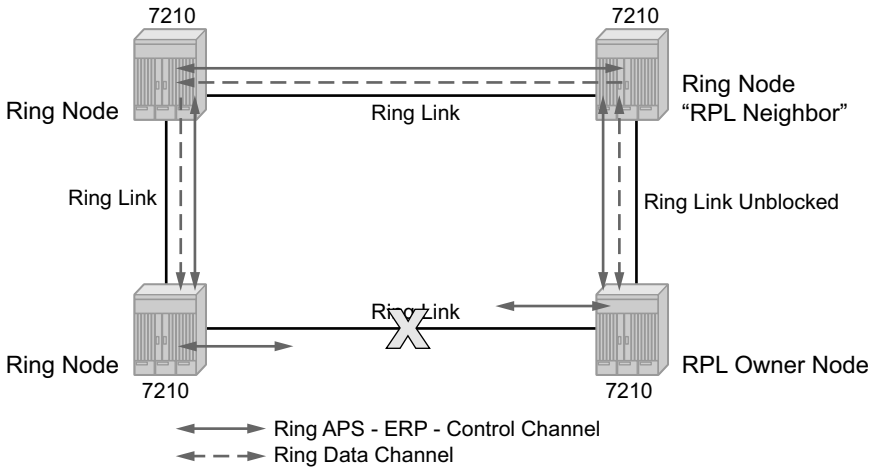


Figure 5: 0-1 G.8032 Ring in the Protecting State

Once the failed link recovers, the nodes that blocked the link again send the R-APS messages indicating no failure this time. This in turn triggers RPL Owner to block the RPL link and indicate the Blocked RPL link the ring in R-APS message, which when received by the nodes at the recovered link cause them to unblock that link and restore connectivity (again all nodes in the ring perform FDB Flush and MAC learning takes place). The ring is back in the normal (or idle) state.

Within each path, Y.1731 Maintenance Entity Group (MEG) Endpoints (MEPs) are used to exchange R-APS specific information (specifically to co-ordinate switchovers) as well as optionally fast Continuity Check Messages (CCM) providing an inherent fault detection mechanism as part of the protocol. Failure detection of a ring path by one of the mechanisms triggers to activate the protection links. Upon failure, re-convergence times are a dependent on the failure detection mechanisms. In the case of Y.1731, the CCM transmit interval determines the response time. The 7210 SAS device supports 100ms (millisecond) message timers that allows for quicker restoration times. Alternatively, 802.3ah (Ethernet in the First Mile) or simple Loss of Signal can act as a trigger for a protection switch where appropriate. In case of direct connectivity between the nodes, there is no need to use Ethernet CC messaging for liveliness detection.

Revertive and non-revertive behaviors are supported. The Ring protection link (RPL) is configured and Eth-rings can be configured to revert to the RPL upon recovery.

G.8032 supports multiple data channels (VIDs) or instances per ring control instance (R-APS tag). G.8032 also supports multiple control instances such that each instance can support RPLs on different links providing for a load balancing capability however once services have been assigned to one instance the rest of the services that need to be interconnected to those services must be on

the same instance. In other words each data instance is a separate data VLAN on the same physical topology. When there is any one link failure or any one node failure in the ring, G.8032 protocols are capable of restoring traffic between all remaining nodes in these data instances.

Ethernet R-APS can be configured on any port configured for access mode using dot1q, q-in-q encapsulation enabling support for Ethernet R-APS protected services on the service edge towards the customer site, or within the Ethernet backbone. ELINE and ELAN services can be afforded Ethernet R-APS protection and, although the Ethernet Ring providing the protection uses a ring for protection the services are configured independent of the Ring properties. The intention of this is to cause minimum disruption to the service during Ethernet R-APS failure detection and recovery.

In the 7210 SAS implementation, the Ethernet Ring is built from a VPLS service on each node with VPLS SAPs that provides Ring path with SAPs. As a result, most of the VPLS SAP features are available on Ethernet rings if desired. This results in a fairly feature rich ring service.

The control tag defined under each eth-ring is used for encapsulating and forwarding the CCMs and the G.8032 messages used for the protection function. If a failure of a link or node affects an active Ethernet ring segment, the services will fail to receive the CC messages exchanged on that segment or will receive a fault indication from the Link Layer OAM module.

For fault detection using CCMs three CC messages plus a configurable hold-off timer must be missed for a fault to be declared on the associated path. The latter mechanism is required to accommodate the existence of additional, 50 ms resiliency mechanism in the optical layer. After it receives the fault indication, the protection module will declare the associated ring link down and the G.8032 state machine will send the appropriate messages to open the RPL and flush the learned addresses.

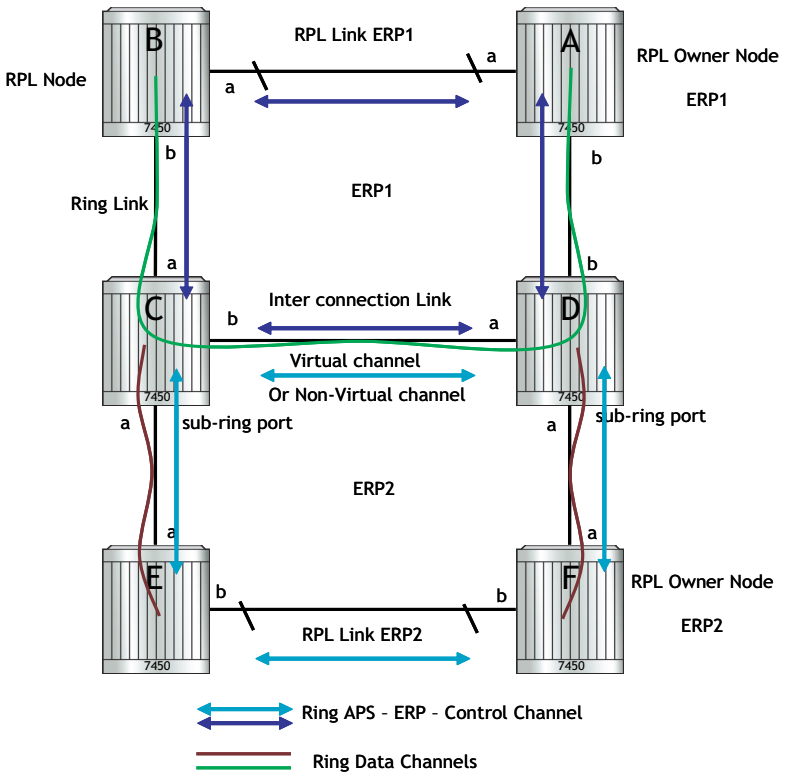
Flushing is triggered by the G.8032 state machine and the 7210 SAS implementation allows flooding of traffic during the flushing interval to expedite traffic recovery.

```
Configure eth-ring 1
    description  "Ring 1"
    revert-time 100
    guard-time 5
    ccm-hold-time down 100 up 200
    rpl-role owner
    path a  1/1/1 raps-tag 100 // CC Tag 100
    description "East CC Link Ring 1"
         rpl-end
         eth-cfm
              mep 1 domain 1 association 1 direction down // Control
              MEP
                  no shutdown
         exit
         exit
[no] shutdown
```

Ethernet Ring Sub-Rings

Ethernet Sub-Rings offer a dual redundant way to interconnect rings. The 7210 SAS supports Sub-Rings connected to major rings and a sub-ring connected to a VPLS (LDP based) for access rings support in VPLS networks. Figure 6 illustrates a Major ring and Sub Ring scenario. In this scenario, any link can fail in either ring (ERP1 or ERP2) and each ring is protected. Furthermore, the sub ring (ERP2) relies on the major Ring (ERP1) as part of its protection for the traffic from C and D. The nodes C and D are configured as inter connection nodes.

NOTE: 7210 SAS-D and 7210 SAS-E cannot be used as the interconnection nodes. They can be used only as the ring nodes in the sub-ring.



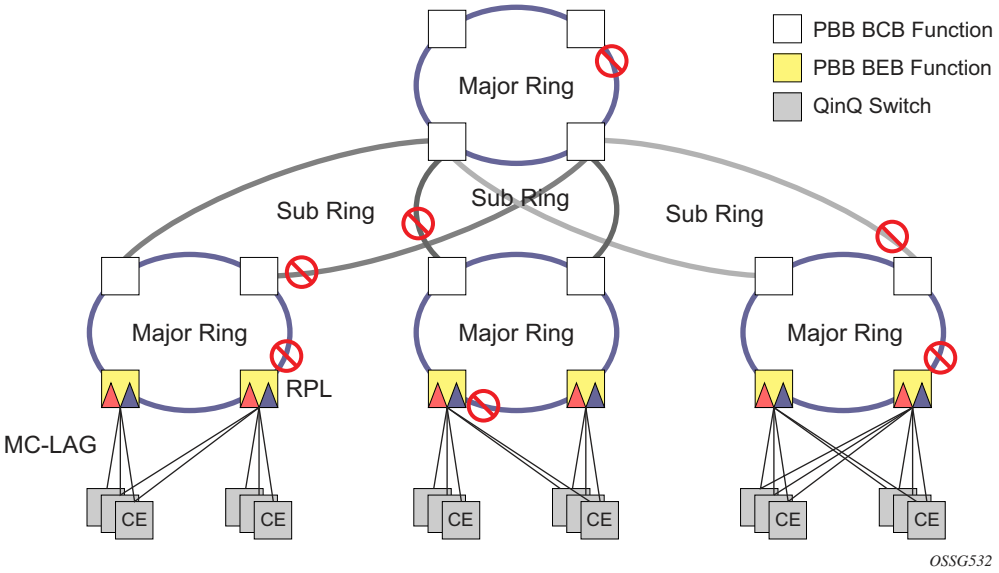


Figure 6: 0-4 G.8032 Sub-Ring

Sub-Rings and Major Rings run similar state machines for the ring logic, however there are some differences. When Sub-Rings protect a link, the flush messages are propagated to the major ring. (A special configuration allows control of this option on the 7210 SAS.) When major rings change topology, the flush is propagated around the major ring and does not continue to any sub-rings. The reason for this is that Major Rings are completely connected but Sub-Rings are dependent on another ring or network for full connectivity. The topology changes need to be propagated to the other ring or network usually. Sub-Rings offer the same capabilities as major rings in terms of control and data so that all link resource may be utilized.

Virtual and Non-Virtual Channel

The following illustrates a sample Sub-Ring using virtual-link configuration on Node C, interconnecting node:

```
eth-ring 2
        description "Ethernet Sub Ring on Ring 1"
            interconnect ring-id 1 // Link to Major Ring 1
                propagate-topology-change
            exit
        exit
        path a 1/1/3 raps-tag 100 // Ring control uses VID 100
            eth-cfm
                mep 9 domain 1 association 4
                    ccm-enable
                    control-mep
                    no shutdown
                exit
            exit
            no shutdown
        exit
        no shutdown

    exit

sub-ring non-virtual-link // Not using a virtual link

# Control Channel for the Major Ring ERP1 illustrates that Major ring
# control is still separate from Sub-ring control
  vpls 10 customer 1 create
      description "Control VID 10 for Ring 1 Major Ring"
      stp shutdown
      sap 1/1/1:10 eth-ring 1 create
          stp shutdown
          exit
      sap 1/1/4:10 eth-ring 1 create
          stp shutdown
          exit
      no shutdown
  exit

# Data configuration for the Sub-Ring

  vpls 11 customer 1 create
      description "Data on VID 11 for Ring 1"
      stp shutdown
      sap 1/1/1:11 eth-ring 1 create // VID 11 used for ring
          stp shutdown
      exit
      sap 1/1/4:11 eth-ring 1 create
          stp shutdown
      exit
      sap 1/1/3:11 eth-ring 2 create // Sub-ring data
          stp shutdown
      exit
      sap 3/2/1:1 create
```

```
        description "Local Data SAP"
            stp shutdown
        no shutdown
    exit

  # Control Channel for the Sub-Ring using a virtual link. This is
  # a data channel as far as Ring 1 configuration. Other Ring 1
  # nodes also need this VID to be configured.

    vpls 100 customer 1 create
        description "Control VID 100 for Ring 2 Interconnection"
        split-horizon-group "s1" create //Ring Split horizon Group
        exit
        stp shutdown
        sap 1/1/1:100 split-horizon-group "s1" eth-ring 1 create
            stp shutdown
        exit
        sap 1/1/4:100 split-horizon-group "s1" eth-ring 1 create
            stp shutdown
        exit
        sap 1/1/3:100 eth-ring 2 create
            stp shutdown
        exit
        no shutdown
    exit
```

Ethernet Ring Sub Ring using non-virtual-link

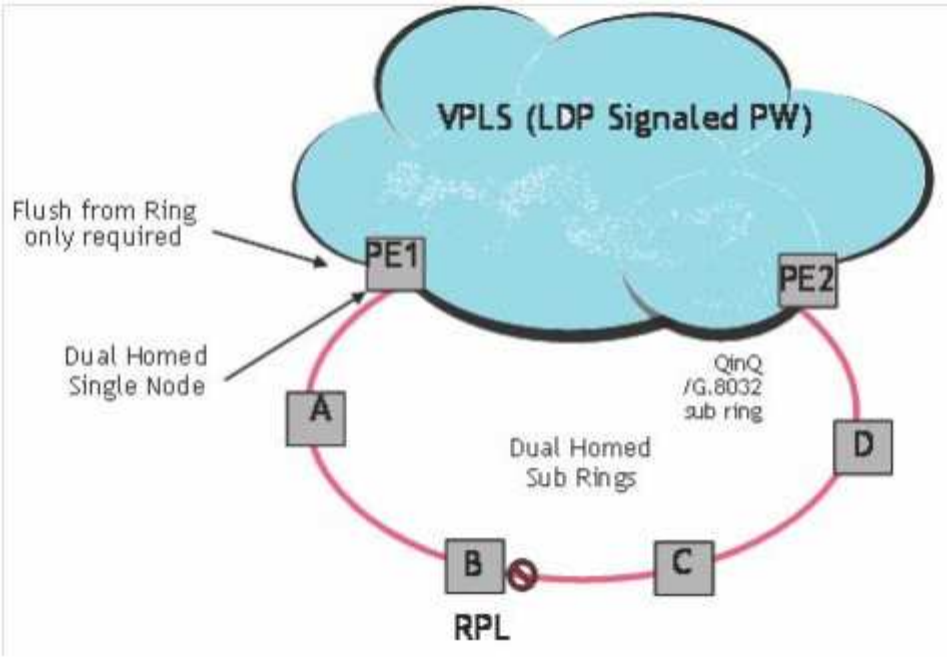


Figure 7: 0-6 Sub-Ring Homed to VPLS

NOTE: In this solution the 7210 SAS nodes can only be the ring nodes. It cannot be used as the interconnection PE nodes.

The following illustrates a sample Sub-Ring using non-virtual-link configuration on PE1, interconnecting node:

```
eth-ring 1
      description "Ethernet Ring 1"
      guard-time 20
      no revert-time
      rpl-node nbr
      sub-ring non-virtual-link
          interconnect vpls // VPLS is interconnection type
              propagate-topology-change
          exit
      exit
      path a 1/1/3 raps-tag 1.1
```

```
          description "Ethernet Ring : 1 Path on LAG"
          eth-cfm
          mep 8 domain 1 association 8
               ccm-enable
               control-mep
               no shutdown
            exit
        exit
        no shutdown
    exit
    no shutdown
exit
```

All the Sub Ring nodes part of Sub Ring with non-virtual-link should be configured with “sub-ring non-virtual-link” option.

```
eth-ring 1
        sub-ring non-virtual-link
        exit
        path a 1/1/1 raps-tag 1.1
            eth-cfm
                mep 5 domain 1 association 4
                    ccm-enable
                    control-mep
                    no shutdown
                exit
            exit
            no shutdown
        exit
        path b 1/1/2 raps-tag 1.1
            eth-cfm
                mep 6 domain 1 association 3
                    ccm-enable
                    control-mep
                    no shutdown
                exit
            exit
            no shutdown
        exit
        no shutdown
    exit
# Control Channel for Sub-Ring using non-virtual-link on interconnecting node:
vpls 1 customer 1 create
      description "Ring 1 Control termination"
      stp shutdown
      sap 1/1/3:1.1 eth-ring 1 create //path a control
          stp shutdown
      exit
      no shutdown
  exit
# Configuration for the ring data into the VPLS Service

  vpls 5 customer 1 create
      description "VPLS Service at PE1"
      stp
          no shutdown
      exit
      sap 1/1/3:2.2 eth-ring 1 create
```

```
            stp shutdown
        exit
        sap 1/1/5:1 create
        exit
        mesh-sdp 5001:5 create //sample LDP MPLS LSPs
        exit
        mesh-sdp 5005:5 create
        exit
        mesh-sdp 5006:5 create
        exit

        no shutdown
    exit
# Control Channel for Sub-Ring using non-virtual-link on sub-Ring nodes:
vpls 1 customer 1 create
            stp
                shutdown
            exit
            sap 1/1/1:1.1 eth-ring 1 create
                stp
                    shutdown
                exit
            exit
            sap 1/1/2:1.1 eth-ring 1 create
                stp
                    shutdown
                exit
            exit
            no shutdown
        exit
```

OAM Considerations

Ethernet CFM can be enabled on each individual path under an Ethernet ring. Only down MEPs can be configured on each of them and CCM sessions can be enabled to monitor the liveliness of the path using interval of 100 msec. Different CCM intervals can be supported on the path a and path b in an Ethernet ring. CFM is optional if hardware supports Loss of Signal for example.

In 7210 SAS-D, UP MEPs on service SAPs which multicast into the service and monitor the active path may be used to monitor services.

NOTE: 7210 SAS-E does not support UP MEPs.

QoS Considerations

Ethernet ring CC messages transmitted over the SAP queues using the default egress QoS policy will use NC (network class) as a forwarding class. If user traffic is assigned to the NC forwarding class, it will compete for the same bandwidth resources with the Ethernet CCMs. As CCM loss

could lead to unnecessary switching of the Ethernet ring, congestion of the queues associated with the NC traffic should be avoided. The operator must configure different QoS Policies to avoid congestion for the CCM forwarding class by controlling the amount of traffic assigned into the corresponding queue.

Note: The operator must configure appropriate ingress QoS policies to ensure that R-APS messages get appropriate QoS treatment and is processed and/or transmitted without delays to enable better failover time.

Support Service and Solution Combinations

The Ethernet rings are supported Layer 2 service. The following considerations apply:

- Only ports in access mode can be configured as eth-ring paths.
- Dot1q and QinQ ports are supported as eth-ring path members.

Configuration guidelines for G.8032

The following are the configuration guidelines for G.8032:

- Service level MEPs are not available on all SAPs tied to an eth-ring instance on a port.
- G8032 instances cannot be configured over a LAG.
- For 7210 SAS-D devices, to improve the service fail-over time due to failures in the ring path, fast flood is enabled by default.On a failure detection in one of the paths of the ethring, along with MAC flush the system starts to flood the traffic onto the available path.No explicit user configuration is needed for this and it does not affect scaling for filters.For 7210 SAS-D devices, down MEPs used with services and G.8032 share common hardware resources.

Service Creation Process Overview

Figure 8 displays the overall process to provision core and subscriber services.

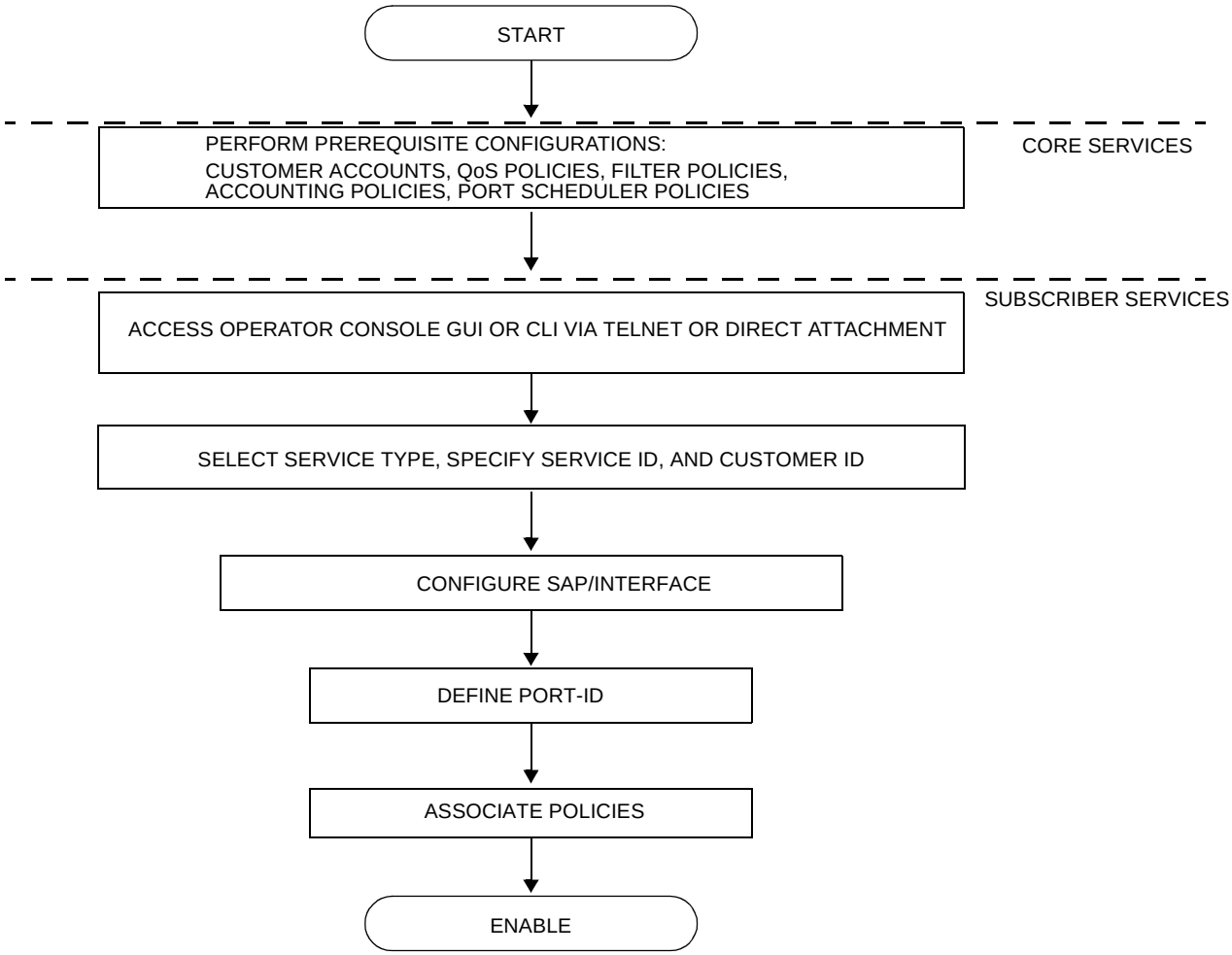


Figure 8: Service Creation and Implementation Flow

Deploying and Provisioning Services

The service model provides a logical and uniform way of constructing connectivity services. The basic steps for deploying and provisioning services can be broken down into three phases.

Phase 1: Core Network Construction

Before the services are provisioned, the following tasks should be completed:

- Build the IP or IP/MPLS core network.
- Configure routing protocols.

Phase 2: Service Administration

Perform preliminary policy configurations to control traffic flow, operator access, and to manage fault conditions and alarm messages, the following tasks should be completed:

- Configure group and user access privileges.
- Build templates for QoS, filter and/or accounting policies needed to support the core services.

Phase 3: Service Provisioning

- Provision customer account information.
- If necessary, build any customer-specific QoS, filter or accounting policies.
- Provision the customer services on the service edge routers by defining SAPs, binding policies to the SAPs.

Configuration Notes

This section describes service configuration caveats.

General

Service provisioning tasks can be logically separated into two main functional areas, core tasks and subscriber tasks and are typically performed prior to provisioning a subscriber service.

Core tasks include the following:

- Create customer accounts
- Create template QoS, filter, scheduler, and accounting policies

Subscriber services tasks include the following:

- Configure interfaces (where required) and SAPs
- Create exclusive QoS and filter policies

Configuring Global Service Entities with CLI

This section provides information to create subscriber (customer) accounts using the command line interface.

Topics include:

- Service Model Entities on page 57
- Configuring Customers on page 59
- ETH-CFM Features on page 84
- Service Management Tasks on page 74

Service Model Entities

The Alcatel-Lucent service model uses logical entities to construct a service. The service model contains four main entities to configure a service.

- Subscribers on page 59
- Services:
  - → Ethernet Pipe (Epipe) Services on page 98
  - → VPLS on page 205
- Service Access Points (SAPs)
  - → Ethernet Pipe (Epipe) Services on page 98
  - → VPLS SAP on page 217

Basic Configuration

The most basic service configuration must have the following:

- A customer ID
- A service type
- A service ID
- A SAP identifying a port and encapsulation value

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure a customer account

---

Configuring Customers

The most basic customer account *must* have a customer ID. Optional parameters include:

- Description
- Contact name
- Telephone number

Customer Information

Use the following CLI syntax to create and input customer information:

CLI Syntax:

```
config>service# customer customer-id create
  contact contact-information
  description description-string
  phone phone-number
```

The following displays a basic customer account configuration.

```
A:ALA-12>config>service# info
----------------------------------------
...
       customer 5 create
           description "Alcatel Customer"
           contact "Technical Support"
           phone "650 555-5100"
       exit
...
----------------------------------------
A:A:ALA-12>config>service#
```

Ethernet Connectivity Fault Management (ETH-CFM)

Ethernet Connectivity Fault Management (ETH-CFM) is defined in two similar standards: IEEE 802.1ag and ITU-T Y.1731. They both specify protocols, procedures, and managed objects to support transport fault management, including discovery and verification of the path, detection and isolation of a connectivity fault for each Ethernet service instance. CFM functionalities are supported on 7210 SAS platforms.

The configuration is split into multiple areas. There is the base ETH-CFM configuration which defines the different Management constructs and administrative elements. This is performed in the ETH-CFM context. The individual management points are configure within the specific service contexts in which they are applied.

The 7210 SAS Services Guide provides the basic service applicable material to build the service specific management points, MEPs and MIPs.

The different service types support a subset of the features from the complete ETH-CFM suite.

ETH-CC used for continuity is available to all MEPs configured within a service. 7210 support Down MEPs and UP MEPs, though the support is not available on all platforms. For more information, see the table below.

NOTE: UP MEPs cannot be created by default on system bootup. The user needs to explicitly allocate hardware resources for use with UP MEP feature, using the commands that appear under *configure> system> resource-profile* CLI context. Only after resources have been allocated by the user, UP MEPs are allowed to be created. Until resources are not allocated to UP MEP, the software fails all attempts to create an UP MEP.The troubleshooting tools ETH-LBM/LBR, LTM/LTR ETH-TST defined by the IEEE 802.1ag specification and the ITU-T Y.1731 recommendation are applicable to all MEPs (MIPs where appropriate).

The advanced notification function AIS defined by the ITU-T Y.1731 is supported on Epipe services.

The advanced performance functions, 1DM, DMM/DMR and SLM/SLR are supported on all service MEPs.

For a description of the individual features and functions that are supported, see the OAM and Diagnostics Guide.

Acronym	Callout
1DM	One way Delay Measurement (Y.1731)
AIS	Alarm Indication Signal
CCM	Continuity check message
CFM	Connectivity fault management
DMM	Delay Measurement Message (Y.1731)
DMR	Delay Measurement Reply (Y.1731)
LBM	Loopback message
LBR	Loopback reply
LTM	Linktrace message
LTR	Linktrace reply
ME	Maintenance entity
MA	Maintenance association
MA-ID	Maintenance association identifier
MD	Maintenance domain
MEP	Maintenance association end point
MEP-ID	Maintenance association end point identifier
MHF	MIP half function
MIP	Maintenance domain intermediate point
OpCode	Operational Code
RDI	Remote Defect Indication
TST	Ethernet Test (Y.1731)
SLM	Synthetic Loss Message (Y.1731)
SLR	Synthetic Loss Reply (Y.1731)

ETH-CFM capabilities may be deployed in many different Ethernet service architectures. The Ethernet based SAPs and SDP bindings provide the endpoint on which the management points may be created. The basic functions can be used in different services, VPLS and Epipe . The ETH-CFM functionality is also applicable to broadband access networks. Two models of broadband access are shown below to illustrate how ETH-CFM could be deployed in these cases. (Figure 9 and Figure 10).

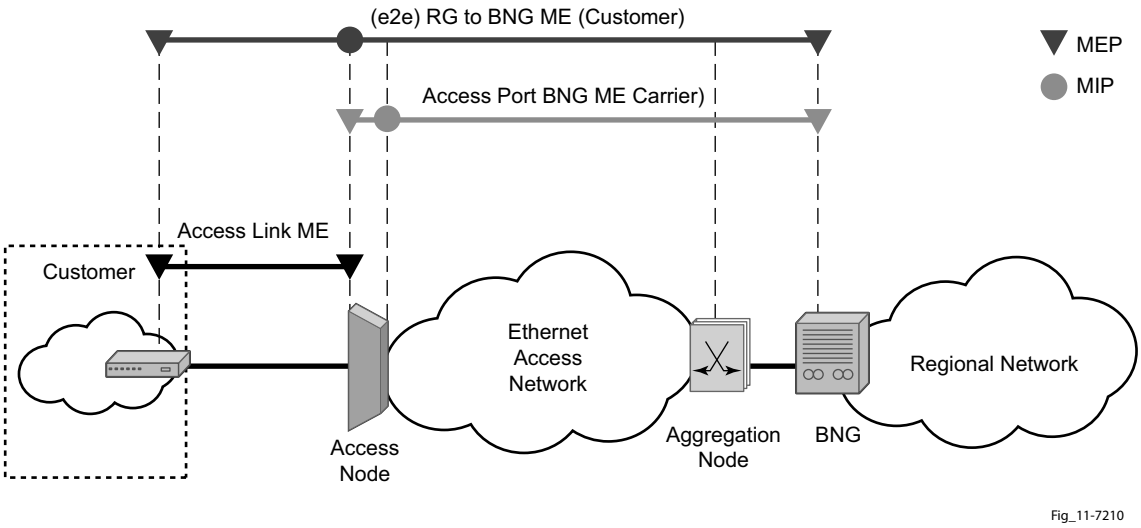


Figure 9: Ethernet OAM Model for Broadband Access - Residential

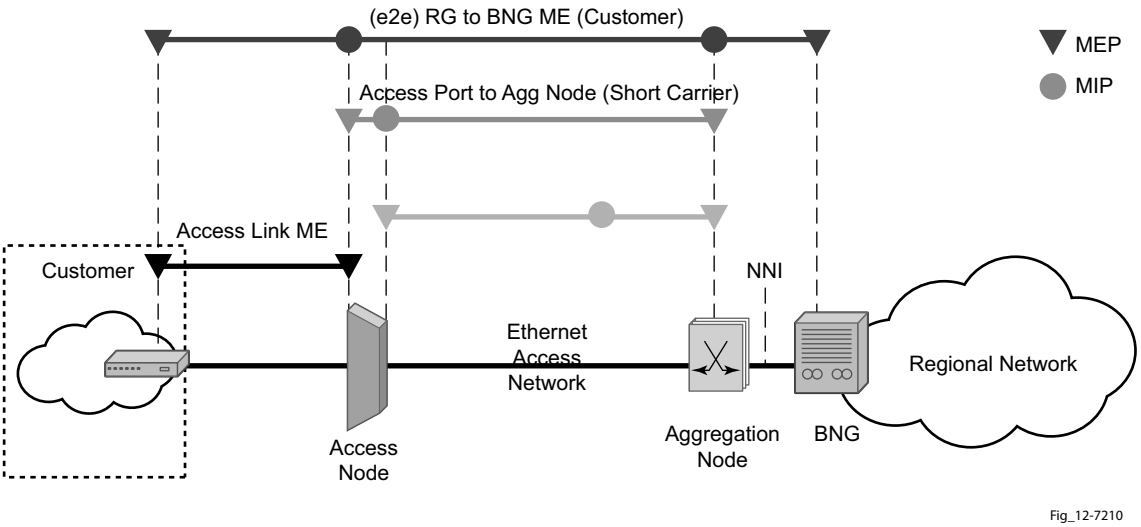


Figure 10: Ethernet OAM Model for Broadband Access - Wholesale

As shown in Figure 13 and Figure 14, the following functions are supported:

- CFM can be enabled or disabled on a SAP basis.
- The eight ETH-CFM levels are suggested to be broken up numerically between customer 7-5, service provider 4-3 and Operator 2-1. Level 0 is meant to monitor direct connections without any MIPs and should be reserved for port-based facility MEPs. These can be configured, deleted or modified.
- Down MEP and UP MEP with an MEP-ID on a SAP/SDP binding for each MD level can be configured, modified, or deleted. Each MEP is uniquely identified by the MA-ID, MEP-ID tuple.
  - → MEP creation on a SAP is allowed only for Ethernet ports (with null, q-tags, qinq encapsulations).
- MIP creation on a SAP for each MD level can be enabled and disabled. MIP creation is automatic or manual when it is enabled. When MIP creation is disabled for an MD level, the existing MIP is removed. For more information on MEP and MIP support, see MEP and MIP Support on page 66

Common Actionable Failures

It is important to note that AIS operates independently from the **low-priority-defect** setting. The **low-priority-defect** setting configuration parameter affects only the ETH-CFM fault propagation and alarming outside the scope of AIS. Any fault in the MEP state machine generates AIS when it is configured. Table 4 illustrates the ETH-CC defect condition groups, configured low-priority-defect setting, priority and defect as it applies to fault propagation.

Table 7: ETH-CC defect condition groups

Defect	Low Priority Defect	Description	Causes	Priority
DefNone	n/a	No faults in the association	Normal operations	n/a
DefRDICCM	allDef	Remote Defect Indication	Feedback mechanism to inform unidirectional faults exist. It provides the feedback loop to the node with the unidirectional failure conditions	1
DefMACStatus (default)	macRemErrXcon	MAC Layer	Remote MEP is indicating a remote port or interface not operational.	2
DefRemoteCCM	remErrXon	No communication from remote peer.	MEP is not receiving CCM from a configured peer. The timeout of CCM occurs at 3.5x the local CC interval. As per the specification, this value is not configurable.	3
DefErrorCCM	errXcon	Remote and local configures do not match required parameters.	Caused by different interval timer, domain level issues (lower value arriving at a MEP configured with a higher value), MEP receiving CCM with its MEPID	4
DefXconn	Xcon	Cross Connected Service	The service is receiving CCM packets from a different association. This could indicate that two services have merged or there is a configuration error on one of the SAP or bindings of the service, incorrect association identification.	5

MEP and MIP Support

The following is a general table that indicates the ETH-CFM support for the different services and endpoints. It is not meant to indicate the services that are supported or the requirements for those services on the individual platforms.

Table 8: ETH-CFM Support Matrix for 7210 SAS-D

Service	Ethernet Connection Type	Down MEP	UP MEP	MIP	Primary VLAN
Epipe	SAP (Access and Access-uplink SAP)	Yes	Yes	Ingress and Egress	Not Supported
VPLS	SAP (Access and Access-uplink SAP)	Yes	Yes	Ingress MIP only	Not Supported
RVPLS	SAP	Not Supported	Not Supported	Not Supported	Not Supported
IES	IES IPv4 interface	Not Supported	Not Supported	Not Supported	Not Supported
	SAP	Not Supported	Not Supported	Not Supported	Not Supported

Table 9: ETH-CFM Support Matrix for 7210 SAS-E

Service	Ethernet Connection Type	Down MEP	UP MEP	MIP	Primary VLAN
Epipe	SAP (Access and Access-uplink SAP)	Yes	Not Supported	Not Supported	Not Supported
VPLS	SAP (Access and Access-uplink SAP)	Yes	Not Supported	Ingress MIP only	Not Supported

Service	Ethernet Connection Type	Down MEP	UP MEP	MIP	Primary VLAN
RVPLS	SAP	Not Supported	Not Supported	Not Supported	Not Supported
IES	IES IPv4 interface	Not Supported	Not Supported	Not Supported	Not Supported
	SAP	Not Supported	Not Supported	Not Supported	Not Supported

Table 10: ETH-CFM Support Matrix for 7210 SAS-K

Service	Ethernet Connection Type	Down MEP	UP MEP	MIP	Primary VLAN
Epipe	SAP (Access and Access-uplink SAP)	Yes	Yes	Ingress and Egress	Not Supported
VPLS	SAP (Access and Access-uplink SAP)	Yes	Yes	Ingress and Egress	Not Supported
RVPLS	SAP	Not Supported	Not Supported	Not Supported	Not Supported
IES	IES IPv4 interface	Not Supported	Not Supported	Not Supported	Not Supported
	SAP	Not Supported	Not Supported	Not Supported	Not Supported

NOTES:

- To achieve better scaling on the 7210 SAS-E, it is recommended that the MEPs are configured at particular levels. The recommended levels are 0, 1, 3 and 7.
- Ethernet-Rings are not configurable under all service types. Any service restrictions for MEP direction or MIP support will override the generic capability of the Ethernet-Ring MPs. For more information on Ethernet-Rings, refer to the 7210 SAS Interfaces Guide.

- 100ms timer value is supported only for service Down MEPs and G8032 Down MEPs on 7210 SAS-D. The minimum timer for service UP MEPs on 7210 SAS-D is 1 second.
- On 7210 SAS-E, the minimum timer value supported for Down MEPs (including G8032 Down MEPs) is 1 second.
- On 7210 SAS-K, the minimum timer value supported for both Down MEPs and UP MEPs is 1 second.

Configuring ETH-CFM Parameters

Configuring ETH-CFM requires commands at two different hierarchy levels of the CLI.

A sample of the global ETH-CFM configuration which defines the domains, associations, linkage o the service id or function, and the globally applicable CCM parameters including the interval and building of the remote MEPs database is shown below.

The following example displays a sample configuration.

```
*A:ALU-7_A>config>eth-cfm# info
----------------------------------------------
        domain 1 name "1" level 1
            association 2 name "1345"
                bridge-identifier 100
                exit
                ccm-interval 60
                remote-mepid 2
                remote-mepid 3
            exit
        exit
----------------------------------------------
*A:ALU-7_A>config>eth-cfm#
```

Defining the MEP and configuring service specific ETH-CFM parameters is performed within the service on the specific SAP or SDP binding. The example using the service VPLS 100 shows this configuration on the SAP.

```
#*A:ALU-7_A>config>service# info
----------------------------------------------
     vpls 100 customer 1 create
          description "VPLS service 100 - Used for MEP configuration example"
               sap 2/2/1:20 create
                    description "2/2/1:20"
                    eth-cfm
                         mep 1 domain 1 association 1 direction down
                              no shutdown
                         exit
                    exit
               exit
          exit
          no shutdown
          exit
          customer 1 create
               description "Default customer"
          exit
          exit
----------------------------------------------
*A:ALU-7_A>config>service#
```

All of the examples shown above were based on IEEE 802.1ag. They are not capable of running Y.1731 functions. To build a Y.1731 context the domain format must be none.

The examples below show the global ETH-CFM configuration and the advanced Y.1731 functions that can be configured. The configuration will reject the configuration of Y.1731 functions within an IEEE 802.1ag context.

```
*A:7210-2# config>eth-cfm# info
----------------------------------------------
        domain 1 format none level 1
            association 1 format icc-based name "1234567890123"
                bridge-identifier 100
                exit
                ccm-interval 1
            exit
        exit


*A:7210-2# config>service# info
----------------------------------------------
        vpls 100 customer 1 create
            stp
                shutdown
            exit
            sap 2/2/1:40 create
                eth-cfm
                    mep 1 domain 1 association 1 direction up
                        ais-enable
                            priority 2
                            interval 60
                        exit
                        eth-test-enable
                            test-pattern all-ones crc-enable
                        exit
                        no shutdown
                    exit
                exit
            exit
            no shutdown
        exit
----------------------------------------------
```

Notes:

- To be able to transmit and also receive AIS PDUs, a Y.1731 MEP must have **ais-enable** set.
- To be able to transmit and also receive ETH-Test PDUs, a Y.1731 MEP must have **eth-test-enable** set.

Applying ETH-CFM Parameters

Apply ETH-CFM parameters to the following entities.

CLI Syntax:
```
config>service>epipe>sap
 eth-cfm
    mep mep-id domain md-index association ma-index [direction
    {up | down}]
          ais-enable
             client-meg-level [[level [level ...]]
             interval {1 | 60}
             priority priority-value
          ccm-enable
          ccm-ltm-priority priority
          eth-test-enable
             test-pattern {all-zeros | all-ones} [crc-enable]
          low-priority-defect {allDef | macRemErrXcon | remEr-
          rXcon | errXcon | xcon | noXcon}
          [no] shutdown
```

CLI Syntax:
```
config>service>epipe>spoke-sdp
 eth-cfm
    mep mep-id domain md-index association ma-index [direction
    {up | down}]
       ccm-enable
       ccm-ltm-priority priority
       eth-test-enable
          test-pattern {all-zeros | all-ones} [crc-enable]
       low-priority-defect {allDef|macRemErrXcon|remErrXcon|
          errXcon|xcon|noXcon}
       [no] shutdown
```

CLI Syntax:
```
config>service>vpls>sap
 eth-cfm
    mip
    mep mep-id domain md-index association ma-index [direction
    {up | down}]
    no mep mep-id domain md-index association ma-index
       ccm-enable
       ccm-ltm-priority priority
       eth-test-enable
          test-pattern {all-zeros | all-ones} [crc-enable]
       low-priority-defect {allDef|macRemErrXcon|remErrX-
          con|errXcon|xcon|noXcon}
       mac-address mac-address
       [no] shutdown
```

CLI Syntax: `config>service>vpls>mesh-sdp` *sdp-id*[*:vc-id*] [vc-type {ether|vlan}]

```
            eth-cfm
               mep mep-id domain md-index association ma-index [direction
               {up | down}]
                  ccm-enable
                  ccm-ltm-priority priority
                  eth-test-enable
                     test-pattern {all-zeros | all-ones} [crc-enable]
                  low-priority-defect {allDef|macRemErrXcon|remErrXcon|
                  errXcon|xcon|noXcon}
                  mac-address mac-address
                  no] shutdown
```

CLI Syntax: `config>service>vpls`

```
            spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}] [split-hori-
            zon-group group-name] [no-endpoint]
            spoke-sdp sdp-id:vc-id [vc-type {ether | vlan}] [split-hori-
            zon-group group-name] endpoint endpoint
               eth-cfm
               map mep-id domain md-index association ma-index [direction
               {up | down}]
                  ccm-enable
                  ccm-ltm-priority priority
                  eth-test-enable
                     test-pattern {all-zeros | all-ones} [crc-enable]
                  low-priority-defect {allDef | macRemErrXcon|remErrX-
                     con|errXcon|xcon|noXcon}
                  mac-address mac-address
                  no] shutdown
```

CLI Syntax: `oam`

```
            eth-cfm linktrace mac-address mep mep-id domain md-index as-
            sociation ma-index [ttl ttl-value]

            eth-cfm loopback mac-address mep mep-id domain md-index as-
            sociation ma-index [send-count send-count] [size data-size]
            [priority priority]

            eth-cfm eth-test mac-address mep mep-id domain md-index as-
            sociation ma-index [priority priority] [data-length data-
            length]

            eth-cfm one-way-delay-test mac-address mep mep-id domain md-
            index association ma-index [priority priority]

            eth-cfm two-way-delay-test mac-address mep mep-id domain md-
            index association ma-index [priority priority]
```

eth-cfm two-way-slm-test *mac-address* mep *mep-id* domain *md-index* association *ma-index* [priority *priority*]

Service Management Tasks

This section discusses the following service management tasks:

- Modifying Customer Accounts on page 74
- Deleting Customers on page 75

Modifying Customer Accounts

To access a specific customer account, you must specify the customer ID.
To display a list of customer IDs, use the show service customer command.
Enter the parameter (description, contact, phone) and then enter the new information.

CLI Syntax:

```
config>service# customer customer-id create
    [no] contact contact-information
    [no] description description-string
    [no] phone phone-number
```

Example:

```
config>service#  customer 27 create
config>service>customer$ description “Western Division”
config>service>customer# contact “John Dough”
config>service>customer# no phone “(650) 237-5102”
```

Deleting Customers

The no form of the customer command removes a customer ID and all associated information. All service references to the customer must be shut down and deleted before a customer account can be deleted.

CLI Syntax: `config>service# no customer customer-id`

Example:

```
config>service# epipe 5 customer 27 shutdown
config>service# epipe 9 customer 27 shutdown
config>service# no epipe 5
config>service# no epipe 9
config>service# no customer 27
```

Layer 2 Control Processing (L2CP)

Operators providing Epipe service need to be able to transparently forward Layer-2 control frames received from the customers. This allows their customers to run these control protocols between the different locations which are part of the L2 VPN service. The 7210 SAS platforms provide user with the following capability:

- An option to tunnel, discard or peer for EFM OAM, LLDP, Dot1x, and LACP.
- BPDU translation and Layer 2 Protocol Tunnelling support for xSTP and CISCO control protocols. This is supported only in a VPLS service. For more information, see the "L2PT and BPDU Translation on page 183".

NOTE: The CDP, VTP, DTP, PAgP, and UDLD management protocols, are forwarded transparently in an Epipe service.

By default, LACP, LLDP, EFM OAM, and Dot1x Layer-2 control protocol untagged packets are discarded if the protocol is not enabled on the port where these frames are received. User has an option to enable peering by enabling the protocol on the port and configuring the appropriate parameters for the protocol. User also has an option to tunnel these packets using an Epipe or VPLS service.

In a VPLS service, the layer-2 control frames are sent out of all the SAPs configured in the VPLS service. It is recommended to use this feature carefully and only when an VPLS is used to emulate an end-to-end Epipe service (that is, an Epipe configured using a 3-point VPLS Service, with one access SAP and 2 access-uplink SAP/SDPs for redundant connectivity). In other words, if the VPLS service is used for multipoint connectivity, it is not recommended to use this feature. When a layer-2 control frame is forwarded out of dot1q SAP or a QinQ SAP, the SAP tags of the egress SAP are added to the packet.

The following SAPs can be configured for tunneling the untagged L2CP frames (corresponding protocol tunneling needs to be enabled on the port):

- If the port encapsulation is null, user has an option to tunnel these packets by configuring a NULL SAP on a port
- If the port encapsulation is dot1q, user an option to use dot1q explicit null SAP (e.g. 1/1/10:0) or a dot1q default SAP (For example: 1/1/11:*) to tunnel these packets.
- If the port encapsulation is QinQ, user has an option to use 0.* SAP (For example 1/1/10:0.*) to tunnel these packets.

In addition to the protocols listed above, protocols that are not supported on 7210, For example: GARP, GVRP, ELMI, and others are transparently forwarded in case of a VPLS service. These protocols are transparently forwarded if a NULL SAP, dot1q default SAP , dot1q explicit null SAP or 0.* SAP is configured on the port and received packet is untagged. If the received packet is tagged and matches the tag of any of the SAPs configured on the port, it is forwarded in the

context of the SAP and the service. Else if the received packet is untagged and none of the NULL or dot1q default or dot1q explicit null or 0.* SAP is configured, it is discarded.

If a 7210 receives a tagged L2CP packet on any SAP (includes NULL, dot1q, dot1q range, QinQ, QinQ default), it is forwarded transparently in the service similar to normal service traffic (xSTP processing behavior is different in VPLS service and is listed below).

The xSTP processing behavior in a VPLS service is as follows:

- If xSTP is enabled in the service , and if the tag in the STP BPDU matches the tag of the configured SAP, the received xSTP BPDU is processed by the local xSTP instance on the node for that service when xSTP is enabled on the SAP and discarded when xSTP is disabled on the SAP.
- If the tags do not match, xSTP BPDU packets are transparently forwarded in the service similar to normal service traffic.
- If xSTP is disabled in the service, STP BPDU packets are transparently forwarded in the service similar to normal service traffic.

Table 12: L2CP for 7210 SAS-D, E, and K platforms

Packet Type	7210 SAS-E	7210 SAS-D	7210 SAS-K
LACP	Option to Discard or Peer or Tunnel	Option to Tunnel or Discard or Peer	Option to Tunnel or Discard or Peer
Dot1x	Option to Discard or Peer	Option to Tunnel or Discard or Peer	Option to Discard
LLDP	Option to Discard or Peer	Option to Tunnel or Discard or Peer (see **Note1**)	Option to Tunnel or Discard or Peer (see **Note1**)
EFM	Option to Tunnel or Discard or Peer	Option to Tunnel or Discard or Peer	Option to Tunnel or Discard or Peer
L2PT	Supported (see **Note2**)	Supported (see **Note2**)	Not Supported
BPDU Tunneling	Supported	Supported	Not Supported
xSTP	Option to Peer or Tunnel	Option to Peer or Tunnel	Forwarded transparently. No option to Peer or Discard.

Note1: For more information read the 7210 SAS Interfaces guide to know more about options available for LLDP tunnelling.

Note2: L2TP support on 7210 SAS platforms varies among the platforms. Not all platforms support tunneling of all CISCO protocols. For more information, see "L2PT and BPDU Translation on page 183".

Global Services Command Reference

Command Hierarchies

- Customer Commands on page 79
- ETH-CFM Configuration Commands on page 82
- SAP Commands for 7210 SAS-E on page 80
- SAP Commands for 7210 SAS-D on page 80
- Show Commands on page 83

Customer Commands

config
— **service**
— [**no**] **customer** *customer-id* **[create]**
— **contact** *contact-information*
— **no contact**
— **description** *description-string*
— **no description**
— [**no**] **phone** *phone-number*

SAP Commands for 7210 SAS-E

config
— **service**
— **epipe** *service-id* [customer *customer-id*] [create] [svc-sap-type **{null-star**| **dot1q**| **dot1q-preserve}] [customer-vid** *vlan-id***]**
— **no epipe** *service-id*
— **sap** *sap-id* [**create**]
— **no sap** *sap-id*
— **ies** *service-id* **[customer** *customer-id***] [create]**
— **no ies** *service-id*
— **sap** *sap-id* [**create**]
— **no sap** *sap-id*
— **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star**|**dot1q**|**dot1q-preserve**}] [**customer-vid** *vlan-id*]
— **no vpls** *service-id*
— **sap** *sap-id* [**create**] [**eth-ring** *ring-index*]
— **no sap** *sap-id*

SAP Commands for 7210 SAS-D

config
— **service**
— **epipe** *service-id* [customer *customer-id*] [create] [svc-sap-type **{null-star**|**dot1q-preserve**|**any**|**dot1q-range}] [customer-vid** *vlan-id***]**
— **no epipe** *service-id*
— **sap** *sap-id* [**create**]
— **no sap** *sap-id*
— **ies** *service-id* **[customer** <*customer-id*>**] [create]**
— **no ies** *service-id*
— **sap** *sap-id* [**create**]
— **no sap** *sap-id*
— **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star | any | dot1q-preserve**}] [**customer-vid** *vlan-id*]
— **no vpls** *service-id*
— **sap** *sap-id* [**create**] [**eth-ring** *ring-index*]
— **no sap** *sap-id*

SAP Commands for 7210 SAS-K

config
— **service**
— **epipe** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any**| **dot1q-range}]**
— **no epipe** *service-id*

- — **sap** *sap-id* [**create**]
- — **no sap** *sap-id*

— **ies** *service-id* **[customer** *customer-id***] [create] [vpn** *vpn-id***]**
— **no ies** *service-id*
— **vpls** *service-id* [**customer** *customer-id*] [**create**] **[m-vpls] [svc-sap-type {any|dot1q-range}] [r-vpls]**
— **no vpls** *service-id*

- — **sap** *sap-id* [**create**] [**split-horizon-group** *group-name*]
- — **no sap** *sap-id*

ETH-CFM Configuration Commands

config
- **eth-cfm**
  - **domain** *md-index* [**format** *md-name-format*] [**name** *md-name*] **level** *level*
  - **domain** *md-index*
  - **no domain** *md-index*
    - **association** *ma-index* [**format** *ma-name-format*] **name** *ma-name*
    - **association** *ma-index*
    - **no association** *ma-index*
      - [**no**] **bridge-identifier** *bridge-id*
        - **mhf-creation** {**none** | **explicit**}
        - **no mhf-creation**
        - **vlan** *vlan-id*
        - **no vlan**
      - **no ccm-interval** {100ms|1|10|60|600}
      - [**no**] **remote-mepid** *mep-id*
  - **slm**
    - **[no] inactivity-timer** *timer*

Show Commands

show
- — **service**
  - — **customer** [*customer-id*] [**site** *customer-site-name*]
  - — **id** *service-id*
  - —
  - — **service-using** [**epipe**] [**ies**] [**vpls**][**mirror**][**customer** *customer-id*]
- — **eth-ring** [**status**]
- — **eth-ring** *ring-index* **hierarchy**
- — **eth-ring** *ring-index* [**path** *{a|b}*]
- — **eth-cfm**
  - — **association** [*ma-index*] [**detail**]
  - — **cfm-stack-table** [**port** [*port-id* [**vlan** *vlan-id*]][**level** 0..7] [**direction down**]
  - — **domain** [*md-index*] [**association** *ma-index* | **all-associations**] [**detail**]
  - — **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**loopback**] [**linktrace**]
  - — **mep** *mep-id* **domain** *md-index* **association** *ma-index* **remote-mepid** *mep-id* | **all-remote-mepids**
  - — **mep** *mep-id* **domain** *md-index* **association** *ma-index* **eth-test-results** [**remote-peer** *mac-address*]
  - — **mep** *mep-id* **domain** *md-index* **association** *ma-index* **one-way-delay-test** [**remote-peer** *mac-address*]
  - — **mep** *mep-id* **domain** *md-index* **association** *ma-index* **two-way-delay-test** [**remote-peer** *mac-address*]
  - — **pw-template**

Global Service Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context config>eth-cfm>mep

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

Special Cases **Service Admin State —** While the service is shutdown, all customer packets are dropped and counted as discards for billing and debugging purposes.

description

Syntax **description** *description-string*
no description

Context config>service>customer

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Customer Management Commands

customer

Syntax **customer** *customer-id* [**create**]
no customer *customer-id*

Context config>service

Description This command creates a customer ID and customer context used to associate information with a particular customer. Services can later be associated with this customer at the service level.

Each *customer-id* must be unique. The *create* keyword must follow each new **customer** *customer-id* entry.

Enter an existing **customer** *customer-id* (without the *create* keyword) to edit the customer's parameters.

Default **customer 1** always exists on the system and cannot be deleted.

The **no** form of this command removes a *customer-id* and all associated information. Before removing a *customer-id*, all references to that customer in all services must be deleted or changed to a different customer ID.

Parameters *customer-id* — Specifies the ID number to be associated with the customer, expressed as an integer.

Values 1 — 2147483647

contact

Syntax **contact** *contact-information*
no contact *contact-information*

Context config>service>customer

Description This command allows you to configure contact information for a customer.

Include any customer-related contact information such as a technician's name or account contract name.

Default No contact information is associated with the *customer-id*.

The **no** form of this command removes the contact information from the customer ID.

Parameters *contact-information* — The customer contact information entered as an ASCII character string up to 80 characters in length. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Any printable, seven bit ASCII characters may be used within the string.

phone

Syntax [**no**] **phone** *string*

Context config>service>customer *customer-id*

Description This command adds telephone number information for a customer ID.

Default none

The **no** form of this command removes the phone number value from the customer ID.

Parameters *string* — The customer phone number entered as an ASCII string string up to 80 characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Any printable, seven bit ASCII characters may be used within the string.

ETH-CFM Configuration Commands

eth-cfm

Syntax **eth-cfm**

Context config

Description This command enables the context to configure ETH CFM parameters.

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* **vlan** *vlan-id]*
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context config>port>ethernet>
config>lag>
config>router>if>

Description This command provisions the maintenance endpoint (MEP).

The **no** form of the command reverts to the default values.

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 — 81921

md-index — Specifies the maintenance domain (MD) index value.

Values 1 — 4294967295

ma-index — Specifies the MA index value.

Values 1 — 4294967295

vlan-id — Specific to tunnel facility MEPs which means this option is only applicable to the `lag>eth-cfm>` context. Used to specify the outer vlan id of the tunnel.

Values 1 — 4094

ais-enable

Syntax [**no**] **ais-enable**

Context config>port>ethernet>eth-cfm>mep
config>lag>eth-cfm>mep

Description This command enables the reception of AIS messages.

The **no** form of the command reverts to the default values.

client-meg-level

Syntax **client-meg-level** [[*level* [*level* ...]]
no client-meg-level

Context config>port>ethernet>eth-cfm>mep>ais-enable
config>lag>eth-cfm> mep>ais-enable

Description This command configures the client maintenance entity group (MEG) level(s) to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level. Only the lowest client MEG level will be used for facility MEPs.

The **no** form of the command reverts to the default values.

Parameters *level* — Specifies the client MEG level.

Values 1 — 7

Default 1

interval

Syntax **interval** {**1** | **10** | **60** | **600**}
no interval

Context config>port>ethernet>eth-cfm>mep>ais-enable
config>lag>eth-cfm> mep>ais-enable

Description This command specifies the transmission interval of AIS messages in seconds.

The **no** form of the command reverts to the default values.

Parameters **1** | **10** | **60** | **600** — The transmission interval of AIS messages in seconds.

Default 1

priority

Syntax **priority** *priority-value*
no priority

Context config>port>ethernet>eth-cfm>mep>ais-enable
config>lag>eth-cfm> mep>ais-enable

Description This command specifies the priority of the AIS messages generated by the node.

The **no** form of the command reverts to the default values.

Parameters *priority-value* — Specify the priority value of the AIS messages originated by the node.

Values 0 — 7

Default 7

ccm-enable

Syntax [**no**] **ccm-enable**

Context config>port>ethernet>eth-cfm>mep
config>lag>eth-cfm>mep

Description This command enables the generation of CCM messages.

The **no** form of the command disables the generation of CCM messages.

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context config>port>ethernet>eth-cfm>mep>
config>lag>eth-cfm>mep>
config>router>if>eth-cfm>mep

Description This command specifies the priority of the CCM and LTM messages transmitted by the MEP. Since CCM does not apply to the Router Facility MEP only the LTM priority is of value under that context.

The **no** form of the command reverts to the default values.

Default *priority* — Specifies the priority value

Values 0 — 7

Default 7

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context config>port>ethernet>eth-cfm>mep>
config>lag>eth-cfm>mep>
config>router>if>eth-cfm>mep

Description For this test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

oam eth-cfm eth-test *mac-address* mep *mep-id* domain *md-index* association *ma-index* [priority *priority*] [data-length *data-length*]

The **no** form of the command disables eth-test capabilities.

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context config>port>ethernet>eth-cfm>mep>eth-test>
config>lag>eth-cfm>mep>eth-test>
config>router>if>eth-cfm>mep>eth-test

Description This command specifies the test pattern of the ETH-TEST frames. This does not have to be configured the same on the sender and the receiver.

The **no** form of the command reverts to the default values.

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Default all-zeros

low-priority-defect

Syntax **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}

Context config>port>ethernet>eth-cfm>mep>eth-test>
config>lag>eth-cfm>mep>eth-test>

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm. This setting is also used to determine the fault state of the MEP which, well enabled to do so, causes a network reaction.

Default macRemErrXcon

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or
noXcon	No defects DefXcon or lower are to be reported

mac-address

Syntax **mac-address** *mac-address*
no mac-address

Context config>port>ethernet>eth-cfm>mep>
config>lag>eth-cfm>mep>
config>router>if>eth-cfm>mep

Description This command specifies the MAC address of the MEP.

The **no** form of the command reverts to the MAC address of the MEP back to the default, that of the port, since this is SAP based.

Parameters *mac-address* — Specifies the MAC address of the MEP.

Values 6-byte unicast mac-address (xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx) of the MEP. Using the all zeros address is equivalent to the no form of this command.

Default no mac-address

domain

Syntax **domain** *md-index* [**format** *md-name-format*] [**name** *md-name*] **level** *level*
domain *md-index*
no domain *md-index*

Context config>eth-cfm

Description This command configures Connectivity Fault Management domain parameters.

The **no** form of the command removes the MD index parameters from the configuration.

Parameters *md-index* — Specifies the Maintenance Domain (MD) index value.

Values 1 — 4294967295

format {**dns** | **mac** | **none** | **string**} **—** Specifies a value that represents the type (format).

Values

dns:	Specifies the DNS name format.
mac:	X:X:X:X:X:X-u X: [0..FF]h u: [0..65535]d
none:	Specifies a Y.1731 domain format and the only format allowed to execute Y.1731 specific functions.
string	Specifies an ASCII string.

Default string

name *md-name* **—** Specifies a generic Maintenance Domain (MD) name.

Values 1 — 43 characters

level *level* **—** Specifies the integer identifying the maintenance domain level (MD Level). Higher numbers correspond to higher maintenance domains, those with the greatest physical reach, with the highest values for customers' CFM packets. Lower numbers correspond to lower maintenance domains, those with more limited physical reach, with the lowest values for single bridges or physical links.

Values 0 — 7

association

Syntax **association** *ma-index* [**format** *ma-name-format*] **name** *ma-name*
association *ma-index*
no association *ma-index*

Context config>eth-cfm>domain

Description This command configures the Maintenance Association (MA) for the domain.

Parameters *ma-index* — Specifies the MA index value.

Values 1 — 4294967295

format {**icc-based** | **integer** | **string** | **vid** | **vpn-id**} **—** Specifies a value that represents the type (format).

Values		
	icc-based:	Only applicable to a Y.1731 context where the domain format is configured as none. Allows for exactly a 13 character name.
	integer:	0 — 65535 (integer value 0 means the MA is not attached to a VID.)
	string:	raw ascii
	vid:	0 — 4095
	vpn-id:	RFC-2685, *Virtual Private Networks Identifier* xxx:xxxx, where x is a value between 00 and FF. for example 00164D:AABBCCDD

Default integer

name *ma-name* — Specifies the part of the maintenance association identifier which is unique within the maintenance domain name.

Values 1 — 45 characters

bridge-identifier

Syntax [**no**] **bridge-identifier** *bridge-id*

Context config>eth-cfm>domain>association

Description This command configures the service ID for the domain association. The value must be configured to match the *service-id* of the service where MEPs for this association will be created. Note that there is no verification that the service with a matching *service-id* exists. This is not used for facility MEPs as they are not tied to services.

Parameters *bridge-id* — Specifies the bridge ID for the domain association.

Values 1 — 2147483647

mhf-creation

Syntax **mhf-creation** {**none** | **explicit**}
no mhf-creation

Context config>eth-cfm>domain>association>bridge-identifier

Description This command determines whether to allow automatic MIP creation for the MA.

NOTE: Please refer to ETH-CFM Support Matrix for 7210 SAS-D on page 66 ETH-CFM Support Matrix for 7210 SAS-K on page 67 ETH-CFM Support Matrix for 7210 SAS-E on page 66 for MEP and MIP support available for different services on different platforms

Default none

Parameters *default* — Specifies that MHFs can be created for this VID only on bridge ports through which this VID can pass without the requirement for a MEP at some lower MA level.

none — Specifies that no MHFs can be created for this VID.

explicit — Specifies that MHFs can be created for this VID only on bridge ports through which this VID can pass, and only if a MEP is created at some lower MA level. There must be at least one lower level MEP provisioned on the same SAP.

vlan

Syntax **vlan** *vlan-id*
no vlan

Context config>eth-cfm>domain>association>bridge-identifier

Description This command configures the bridge-identifier primary VLAN ID. Note that it is informational only, and no verification is done to ensure MEPs on this association are on the configured VLAN.

Parameters *vlan-id* — Specifies a VLAN ID monitored by MA.

Values 0 — 4094

ccm-interval

Syntax **ccm-interval** {**100ms** | **1** | **10** | **60** | **600**}
no ccm-interval

Context config>eth-cfm>domain>association

Description This command configures the CCM transmission interval for all MEPs in the association.

NOTES:

- 100ms timer value is supported only for Down MEPs on 7210 SAS-D. The minimum timer for UP MEPs on 7210 SAS-D is 1 second.
- On 7210 SAS-E, the minimum timer value supported for Down MEPs (including G8032 Down MEPs) is 1 second.
- On 7210 SAS-K, the minimum timer value supported for both Down MEPs and UP MEPs is 1 second.

The **no** form of the command reverts the value to the default.

Default 10 seconds

Parameters **interval —** Specifies the interval between CCM transmissions to be used by all MEPs in the MA.

remote-mepid

Syntax [**no**] **remote-mepid** *mep-id*

Context config>eth-cfm>domain>association

Description This command configures the remote maintenance association end point (MEP) identifier.

Parameters *mep-id* — Maintenance association end point identifier of a remote MEP whose information from the MEP database is to be returned.

Values 1 — 8191

slm

Syntax **slm**

Context config>eth-cfm

Description This is the container that provides the global configuration parameters for ITU-T Synthetic Loss Measurement (ETH-SL).

inactivity-timer

Syntax **inactivity-timer** *timer*
[no] inactivity-timer

Context config>eth-cfm>slm

Description The time the responder keeps a test active. The time between packets exceed this values within a test the responder marks the previous test as complete. The timer treats any new packets from a peer with the same test-id, source-mac and MEP-ID as a new test responding with the sequence number one.

Default 100 seconds

Parameters *timer* — Specifies the amount of time in seconds.

Values 10 100

VLL Services

In This Chapter

This section provides information about Virtual Leased Line (VLL) services and implementation notes.

Topics in this section include:

Ethernet Pipe (Epipe) Services

This section provides information about the Epipe service and implementation notes.

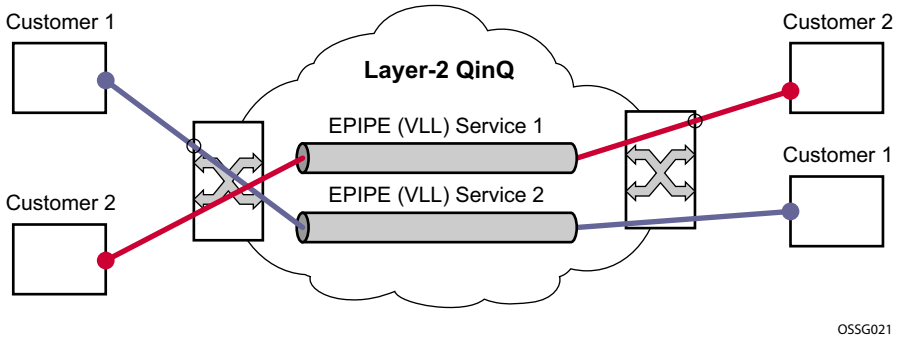
Topics in this section include:

Epipe Service Overview

An Epipe service is a Layer 2 point-to-point service where the customer data is encapsulated and transported across a service provider's network.The 7210 SAS D, E, K provide QinQ SAPs or Dot1q SAPs to provide a point-point Layer 2 service. An Epipe service is completely transparent to the subscriber's data and protocols. The 7210 SAS Epipe service does not perform any MAC learning. A local Epipe service consists of two SAPs on the same node, whereas a distributed Epipe service consists of two SAPs on different nodes. The 7210 SAS D, E, K only support local Epipe services.

Each SAP configuration includes a specific port on which service traffic enters the 7210 SAS router from the customer side (also called the access side). Each port is configured with an encapsulation type. If a port is configured with an IEEE 802.1Q (referred to as Dot1q) encapsulation, then a unique encapsulation value (ID) must be specified.

Figure 11: Epipe/VLL Service



devices configured

Epipe Oper State decoupling

Note: This feature is supported only on 7210 SAS-D and 7210 SAS-K devices.

An epipe service transitions to an operation state, ‘Down’ when only a single entity SAP or Binding is active and the operation state of the mate is down or displays an equivalent state. The default behavior does not allow operators to validate the connectivity and measure performance metrics. With this feature an option is provided to allow operators to validate the connectivity and measure performance metrics of an epipe service prior to the customer handoff. The operator can also maintain performance and continuity measurement across their network regardless of the connectivity between the terminating node and the customer. If the SAP between the operator and the customer enters a Oper Down state, the epipe remains Operationally UP, so the results can continue to be collected uninterrupted. The operator receives applicable port or SAP alerts/alarms. This option is available only for the customer facing SAP failures. If a network facing SAP or Spoke-SDP fails the operational state of the epipe service is set to 'Down'. In other words, there is no option to hold the service in an UP state, if a network component fails.

The following functionality is supported:

- Configuration under SAP is required to change the default behavior of the epipe service in response to the SAP failure.
- The user can create a SAP on a LAG where the LAG has no port members. In this case, the operator configures the “*ignore-oper-state*” on the SAP and the service remains operational. However, as there are no ports existing in the LAG member group, there is no extraction function that can be created. This feature protects against an established working configuration with full forwarding capabilities from failing to collect PM data. The user should shutdown their equipment and place the epipe SAP in an operationally down state.
- The SAP connecting the provider equipment to the customer is configured to hold the epipe service status UP when the customer facing SAP enters any failed state. Only one SAP per epipe is allowed to be configured.
- Any failure of the network entity (network SAP or SDP-Binding) still cause the epipe service to transition to OPER=DOWN.
- As the service remains operationally up, all bindings should remain operationally up and should be able to receive and transmit data. The PW status represents the failed SAP in the LDP status message, but this does not prevent the data from using the PW as a transport, in or out. This is the same as LDP status messaging.
- The SAP failure continues to trigger normal reactions, except the operational state of the service

- ETH-CFM PM measurement tools (DMM/SLM) can be used with the UP MEP on the failed SAP to collect performance metric. Additionally, CFM troubleshooting tools & connectivity (LBM, LTM, AIS, CCM) can be used and will function normally.
- ETH-CFM CCM processing and fault propagation does not change. Even when a SAP fails with the hold service UP configuration, CCM sets the Interface Status TLV to "*Down*".
- VPLS services remain operationally UP until the final entity in the service enters a failed operational state. There are no changes to VPLS services and the change is specific to epipe.

.

VLAN Range for SAPs in an Epipe Service

7210 SAS VLAN ranges provide a mechanism to group a range of VLAN IDs as a single service entity. This allows the operator to provide the service treatment (forwarding, ACL, QoS, Accounting, and others) to the group of VLAN IDs as a whole.

NOTE: Grouping a range of VLAN IDs to a SAP is supported only for Virtual Leased Lines (VLL) Ethernet services.

Processing behavior for SAPs using VLAN ranges in access-uplink mode

NOTE: Dot1q range SAPs are supported only on 7210 SAS-K and 7210 SAS-D. It is not supported on 7210 SAS-E.

The access SAPs that specifies VLAN range values using connection-profile (also known as, dot1q range SAPs) is allowed in Epipe service and in VPLS service. For more information on functionality supported, see VLAN Range SAPs feature Support and Restrictions on page 104. The system allows only one range SAP in an Epipe service. It fails any attempt to configure more than one range SAP in an Epipe service. Range SAP can be configured only on access ports. The other endpoint in the Epipe service has to be a “Q.* SAP” in access-uplink mode. The processing and forwarding behavior for packets received on range SAPs are listed below:

- No VLAN tags are removed/stripped on ingress of access dot1q SAP configured to use VLAN ranges. A single tag (Q1) is added to the frame when it is forwarded out of the Q1.* access-uplink SAP.
- When a packet is received on the access-uplink Q1.* SAP, the outermost tag is removed and the packet is forwarded out of the access dot1q range SAP. The system does not check if the inner VLAN tag matches the VLANs IDs (both range and individual values specified in the “connection-profile”) of the dot1q access SAPs configured in the service.
- The dot1q range sap can be supported in a service with svc-sap-type set to ‘dot1q-range’.

VLAN Range SAPs feature Support and Restrictions

- The access SAPs that specifies VLAN range values (using connection-profile) is allowed only in E-Pipe service. The system allows only one range SAP in an Epipe service. It will

fail any attempt to configure more than one range SAP in an Epipe service. Range SAP can be configured only on access ports.

- In access-uplink mode, the dot1q range sap is allowed to be configured only in a service with svc-sap-type set to ‘dot1q-range’.
- The access SAPs using VLAN range values are allowed only for Dot1q encapsulation port or LAG. A connection profile is used to specify either range of VLAN IDs or individual VLANs to be grouped together in a single SAP.
- A “connection profile” is used to specify either range of VLAN IDs or individual VLANs to be grouped together in a single SAP.
- No Dot1q default sap is allowed on the same access port as the one on which a SAP with a range is configured.
- Multiple “connection-profile” can be used per port or Lag as long as the VLAN value specified by each of them does not overlap. The number of VLAN ranges available per port/LAG is limited. The available number must be shared among all the SAPs on the port/LAG.
- “Connection-profile”, associated with a SAP cannot be modified. To modify a connection profile, it must be removed from all SAPs that are using it.
- ACL support - Filter policies are supported on SAP ingress. In 7210 SAS-D access-uplink mode, IP criteria and MAC criteria based filter policy is available for use with access SAPs. **Note**: For more information on ACL on range SAPs, see The 7210 SAS Router Configuration Guide.**Note**: For more information on ACL on range SAPs, see The 7210 SAS Router Configuration Guide.
- Access SAP egress filter are not supported.
- Access-uplink SAP egress filter are not supported.
- SDP egress and ingress filter are not supported.
- QoS – Ingress classification, metering with hierarchical metering, marking, queuing and shaping for SAP ingress and SAP egress. On egress per port queues and shaping is available on 7210 SAS-D.
  - → SAP ingress classification criteria is available for use with VLAN range SAPs is similar to that available for other SAPs supported in an Epipe service. Dot1p based ingress classification uses the Dot1p bits in the outermost VLAN tag for matching. On access egress, dot1p received from the SDP (on a network port) from another access port is preserved.
- The amount of hardware resources (such as CAM entries used for matching in QoS classification and ACL match, meters used in SAP ingress policy, and others.) consumed by a single range SAP is equivalent to the amount of resources consumed by a single SAP that specifies a single VLAN ID for service identification. In other words, the hardware has the ability to match a range of VLAN values and hence uses ‘X’ resources for a SAP using a VLAN range instead of X * n, where ‘n’ is the number of VLANs specified in the range and X is the amount of QoS or ACL resources needed.

- Ingress accounting support is similar to the support available for other SAPs in an Epipe service. Count of packets or octets received from individual VLANs configured in the connection profile is not available. No support for Egress SAP statistics and accounting is available.
- Mirroring is supported. In network mode, the use of service resiliency mechanisms such as MC-LAG and Epipe PW redundancy is supported.

VLL Service Considerations

This section describes various of the general service features and any special capabilities or considerations as they relate to VLL services.

SDPs

The most basic SDPs must have the following:

- A locally unique SDP identification (ID) number.
- The system IP address of the originating and far-end routers.
- An SDP encapsulation type, MPLS.

SAP Encapsulations

The Epipe service is designed to carry Ethernet frame payloads, so it can provide connectivity between any two SAPs that pass Ethernet frames. The following SAP encapsulations are supported on the Epipe service:

- Ethernet null
- Ethernet dot1q
- QinQ

Note that while different encapsulation types can be used, encapsulation mismatch can occur if the encapsulation behavior is not understood by connecting devices and are unable to send and receive the expected traffic. For example if the encapsulation type on one side of the Epipe is dot1q and the other is null, tagged traffic received on the null SAP will potentially be double tagged when it is transmitted out of the Dot1q SAP.

QoS Policies

Traffic Management - Traffic management of Ethernet VLLs is achieved through the application of ingress QoS policies to SAPs and access egress QoS policies applied to the port. All traffic management is forwarding-class aware and the SAP ingress QoS policy identifies the forwarding

class based on the rules configured to isolate and match the traffic ingressing on the SAP. Forwarding classes are determined based on the Layer 2 (Dot1p, MAC) or Layer 3 (IP, DSCP) fields of contained packets and this association of forwarding class at the ingress will determine both the queuing and the Dot1P bit setting of packets on the Ethernet VLL on the egress.

SAP ingress classification and Policing - The traffic at the SAP ingress is classified and metered according to the SLA parameters. All the traffic ingressing on the SAP is classified to a particular forwarding class. All the forwarding class is metered through and marked in-profile or put-profile based on the Meter parameters.

When applied to Epipe services, service ingress QoS policies only create the unicast meters defined in the policy. The multipoint meters are not created on the service.

Egress Network DOT1P Marking - Marking of IEEE DOT1P bits in VLAN tag is as per the FC-to-Dot1p map. For details see the default network QoS policy in the QoS user guide. This marking is applied at the port level on access ports and access uplink ports.

Ingress Network Classification - Ingress network classification is based on the Dot1p bits in the outer VLAN tag received on the access uplink port. Dot1p-to-FC mapping is based on the network ingress QoS policy.

For details refer to the 7210 SAS QoS user guide. Note that both Layer 2 or Layer 3 criteria can be used in the QoS policies for traffic classification in a service.

Filter Policies

7210 SAS Epipe services can have a single filter policy associated on both ingress and egress. Both MAC and IP filter policies can be used on Epipe services.

MAC Resources

Epipe services are point-to-point layer 2 VPNs capable of carrying any Ethernet payloads. Although an Epipe is a Layer 2 service, the Epipe implementation does not perform any MAC learning on the service, so Epipe services do not consume any MAC hardware resources.

Configuring a VLL Service with CLI

This section provides information to configure Virtual Leased Line (VLL) services using the command line interface.

Topics in this section include:

Basic Configurations

- Creating an Epipe Service for 7210 SAS-E on page 112

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure the VLL services and provides the CLI commands.

- Associate the service with a customer ID.
- Define SAP parameters
  - → Optional - select ingress QoS policies (configured in the **config>qos** context).
  - → Optional - select accounting policy (configured in the **config>log** context).
- Enable the service.

Creating an Epipe Service for 7210 SAS-E

Use the following CLI syntax to create an Epipe service.

CLI Syntax: `config>service# epipe service-id [customer customer-id] [create] [svc-sap-type {null-star | dot1q | dot1q-preserve}] [customer-vid vlan-id]`
`description description-string`
`no shutdown`

The following displays an Epipe configuration example:

```
A:ALA-1>config>service# info
---------------------------------------------
...
        epipe 500 customer 1 svc-sap-type null-star create
            description "Local Epipe Service with NULL  SVC_SAP_TYPE"
            no shutdown
        exit
----------------------------------------------
A:ALA-1>config>service#
```

Creating an Epipe Service for 7210 SAS-D

Use the following CLI syntax to create an Epipe service.

CLI Syntax: `config>service# epipe service-id [customer customer-id] [create] [svc-sap-type {null-star | any | dot1q-preserve}] [customer-vid vlan-id]`

The following displays an Epipe configuration example:

```
A:ALA-1>config>service# info
---------------------------------------------
...
        epipe 15 customer 40 svc-sap-type any create
            description "Local Epipe Service with ANY SVC_SAP_TYPE"
            no shutdown
        exit
----------------------------------------------
A:ALA-1>config>service#
```

Creating an Epipe Service with range SAPs

The following displays an example of connection-profile used to configure a range of SAPs and an Epipe configuration using the connection profile:

```
*A:7210SAS>config>connprof# info
----------------------------------------------
        ethernet
            ranges 0 2804-2805 2810-2811 2813 2832-2839
        exit
----------------------------------------------

*A:7210SAS>config>service>epipe# info
----------------------------------------------
            description "Default epipe description for service id 292"
            sap 1/1/4:292.* create
                description "Default sap description for service id 292"
                exit
            exit
            sap 1/1/9:cp-292 create
                description "Default sap description for service id 292"
                exit
            exit
            no shutdown
----------------------------------------------
```

Creating an Epipe Service for 7210 SAS-K

Use the following CLI syntax to create an Epipe service.

CLI Syntax:

The following displays an Epipe configuration example:

```
*A:SAH01-051>config>service>epipe$ info detail
----------------------------------------------
            shutdown
            no description
            service-mtu 1514
            eth-cfm
            exit
            pbb
            exit
----------------------------------------------
*A:SAH01-051>config>service>epipe$

----------------------------------------------
```

Creating an Epipe Service for 7210 SAS-K with range SAPs

The following displays an example of connection-profile used to configure a range of SAPs and an Epipe configuration using the connection profile:

```
*A:SAH01-051>config>connprof$ info detail
----------------------------------------------
        no description
        ethernet
            no ranges
        exit
----------------------------------------------
```

```
*A:SAH01-051>config>connprof$


*A:SAH01-051>config>service>epipe$ info detail
----------------------------------------------
            shutdown
            no description
            service-mtu 1514
            eth-cfm
            exit
            pbb
            exit
----------------------------------------------
*A:SAH01-051>config>service>epipe$

----------------------------------------------
```

Configuring Epipe SAP Parameters

A default QoS policy is applied to each ingress SAP. and a default access egress QoS policy is applied on the port where SAP is egressing. The access egress QoS policy is common to all SAPs on that port. Additional QoS policies can be configured in the **config>qos** context. Filter policies are configured in the `config>filter` context and explicitly applied to a SAP. There are no default filter policies.

Use the following CLI syntax to create:

- Local Epipe SAPs on page 116

CLI Syntax:

```
config>service# epipe service-id [customer customer-id]
         sap sap-id
               accounting-policy policy-id
               collect-stats
               description description-string
               no shutdown
               egress
                  filter {ip ip-filter-name | mac mac-filter-name}
               ingress
                  filter {ip ip-filter-name | mac mac-filter-name}
                  qos policy-id
```

Local Epipe SAPs

To configure a basic local Epipe service, enter the **sap** *sap-id* command twice with different port IDs in the same service configuration.

By default, QoS policy ID 1 is applied to ingress service SAPS. Existing filter policies or other existing QoS policies can be associated with service SAPs on ingress and egress ports.

Ingress and Egress SAP parameters can be applied to local and distributed Epipe service SAPs.

This example displays the SAP configurations for local Epipe service 500 on SAP 1/1/2 and SAP 1/1/3 on ALA-1.

```
A:ALA-1>config>service# epipe 500 customer 5 create
config>service>epipe$ description "Local epipe service
config>service>epipe# sap 1/1/2 create
config>service>epipe>sap? ingress
config>service>epipe>sap>ingress# qos 20
config>service>epipe>sap>ingress# filter ip 1
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# egress
config>service>epipe# sap 1/1/3 create
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# qos 555
config>service>epipe>sap>ingress# filter ip 1
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# no shutdown
config>service>epipe>sap# exit

A:ALA-1>config>service# info
----------------------------------------------
...
        epipe 500 customer 5 create
            description "Local epipe service"
            sap 1/1/2 create
                ingress
                    qos 20
                    filter ip 1
                exit
            exit
            sap 1/1/3 create
                ingress
                    qos 555
                    filter ip 1
                exit
            exit
            no shutdown
        exit
----------------------------------------------
A:ALA-1>config>service#
```

The following example displays the SAP configurations for ALA-1 and ALA-2:

```
A:ALA-1>config>service# info
----------------------------------------------
...
```

```
        epipe 5500 customer 5 vpn 5500 create
            description "Distributed epipe service to east coast"
            sap 221/1/3:21 create
                ingress
                    qos 555
                    filter ip 1
                exit

            exit
        exit
        epipe 5500 customer 5 vpn 5500 create
            description "Distributed epipe service to west coast"
            sap 441/1/4:550 create
                ingress
                    qos 654
                    filter ip 1020
                exit

            exit
        exit
...
```

Configuring Ingress and Egress SAP Parameters

By default, QoS policy ID 1 is applied to ingress service SAPs. Existing filter policies or other existing QoS policies can be associated with service SAPs on ingress and egress ports.

Ingress and egress SAP parameters can be applied to local and distributed Epipe service SAPs.

This example displays SAP ingress and egress parameters.

```
ALA-1>config>service# epipe 5500
     config>service>epipe# sap 1/1/3:21
     config>service>epipe>sap# ingress
     config>service>epipe>sap>ingress# qos 555
     config>service>epipe>sap>ingress# filter ip 1
     config>service>epipe>sap>ingress# exit
     config>service>epipe>sap#
```

The following example displays the Epipe SAP ingress and egress configuration:

```
A:ALA-1>config>service#
-----------------------------------------------
...
        epipe 5500 customer 5 vpn 5500 create
            description "Distributed epipe service to east coast"
            sap 1/1/3:21 create
                ingress
                    qos 555
                    filter ip 1
                exit
            exit
            no shutdown
        exit
-----------------------------------------------
A:ALA-1>config>service#
```

Configuring Default QinQ SAPs for Epipe Transit Traffic in a Ring Scenario

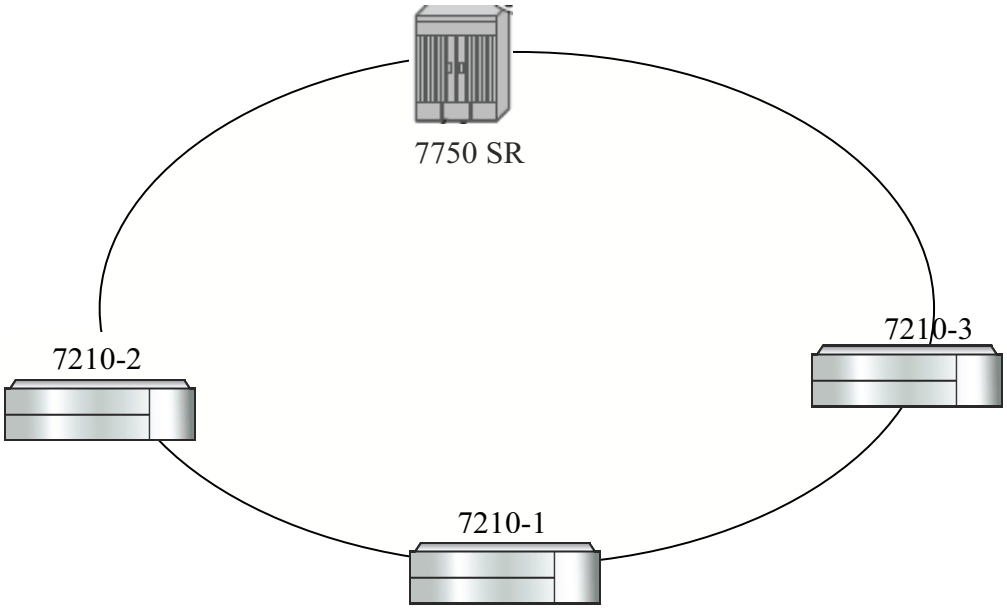


Figure 12: Default QinQ SAP for Transit Traffic in a Ring Scenario

In the Figure 12, 7210-1 is used to deliver some services to customers connected to the device and additionally it needs to pass through transit from other nodes on the ring (example – traffic from 7210-2 to 7210-3 OR from 7210-2 to 7750 –SR onto the core network).

Without Default QinQ SAPs, user would need to configure a service on 7210-1, with access-uplink SAPs for each service originating on some other node in the ring. With support for Default QinQ SAPs, all traffic which does not need to be delivered to any customer service configured on 7210-1 can be switched using the EPIPE service. The example shown below provides the sample configuration commands in this scenario:

```
ALA-1>config>service# epipe 8 customer 1 svc-sap-type null-star create
            sap 1/1/5:*.* create
                statistics
                    ingress
                    exit
                exit
            exit
            sap 1/1/6:*.* create
                statistics
                    ingress
                    exit
                exit
            exit
            no shutdown
        exit
```

Service Management Tasks

This section discusses the following Epipe service management tasks:

- Modifying Epipe Service Parameters on page 121
- Disabling an Epipe Service on page 121
- Re-Enabling an Epipe Service on page 122
- Deleting an Epipe Service on page 122

Modifying Epipe Service Parameters

The following displays an example of adding an accounting policy to an existing SAP:

```
Example:config>service# epipe 2
        config>service>epipe# sap 1/1/3:21
        config>service>epipe>sap# accounting-policy 14
        config>service>epipe>sap# exit
```

The following output displays the SAP configuration:

```
ALA-1>config>service# info
----------------------------------------------
     epipe 2 customer 6 vpn 2 create
            description "Distributed Epipe service to east coast"
            sap 1/1/3:21 create
              accounting-policy 14
            exit
            no shutdown
        exit
----------------------------------------------
ALA-1>config>service#
```

Disabling an Epipe Service

You can shut down an Epipe service without deleting the service parameters.

CLI Syntax: `config>service> epipe` *service-id*
shutdown

Example:
```
config>service# epipe 2
        config>service>epipe# shutdown
        config>service>epipe# exit
```

Re-Enabling an Epipe Service

To re-enable an Epipe service that was shut down.

CLI Syntax:
```
config>service# epipe service-id
            no shutdown
```

```
Example:config>service# epipe 2
       config>service>epipe# no shutdown
       config>service>epipe# exit
```

Deleting an Epipe Service

Perform the following steps prior to deleting an Epipe service:

1. Shut down the SAP.
2. Delete the SAP.
3. Shut down the service.

Use the following CLI syntax to delete an Epipe service:

CLI Syntax:
```
config>service
            [no] epipe service-id
               shutdown
               [no] sap sap-id
                  shutdown
```

Example:
```
config>service# epipe 2
       config>service>epipe# sap 1/1/3:21
       config>service>epipe>sap# shutdown
       config>service>epipe>sap# exit
       config>service>epipe# no sap 1/1/3:21
       config>service>epipe# epipe 2
       config>service>epipe# shutdown
       config>service>epipe# exit
       config>service# no epipe 2
```

VLL Services Command Reference

Epipe Service Configuration Commands

Epipe Global Commands

config
- **service**
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type {null-star**|**dot1q-preserve**|**any**|**dot1q-range}]** [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **epipe** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any**| **dot1q-range}] (for 7210 SAS-K)**
  - **no epipe** *service-id*
    - **description** *description-string*
    - **no description**
    - **sap** *sap-id* [**create**]
    - **no sap** *sap-id*
    - **service-mtu** *octets* (for 7210 SAS-K only)
    - **no service-mtu**
    - [**no**] **shutdown**

Epipe SAP Configuration Commands

config
- **service**
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type {null-star|dot1q-preserve|any|dot1q-range}**] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **epipe** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any| dot1q-range}] (for 7210 SAS-K)**
  - **no epipe** *service-id*
    - **no sap** *sap-id*
      - **accounting-policy** *acct-policy-id*
      - **no accounting-policy** *acct-policy-id*
      - [**no**] **collect-stats**
      - **description** *description-string*
      - **no description**
      - **eth-cfm**
        - [**no**] **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {up | down}]
          - [**no**] **ais-enable**
            - [**no**] **client-meg-level** [[**level** [level ...]]
            - [**no**] **interval** {**1** | **60**}
            - [**no**] **priority** *priority-value*
            - **no send-ais-on-port-down**
            - **send-ais-on-port-down**
          - [**no**] **ccm-enable**
          - [**no**] **ccm-ltm-priority** *priority*
          - [**no**] **description**
          - [**no**] **eth-test-enable**
            - [**no**] **bit-error-threshold** *bit-errors*
            - [**no**] **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
          - [**no**] **mac-address** *mac-address*
          - [**no**] **one-way-delay-threshold** *seconds*
          - [**no**] **shutdown**
        - **ethernet**
          - [**no**] **llf**
      - [**no**] **ignore-oper-down**
      - [**no**] **shutdown**

Epipe SAP Meter Override Commands for 7210 SAS-E and 7210 SAS-D

config
- **service**
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type {null-star|dot1q-preserve|any|dot1q-range}**] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **no epipe** *service-id*
    - **no sap** *sap-id*
      - **ingress**

— **meter** *meter-id* **[create]**
— **no meter** *meter-id*
— **adaptation-rule [pir** ***adaptation-rule*****] [cir** ***adaptation-rule*****]**
— **cbs** ***size-in-kbytes***
— **no cbs**
— **mbs** ***size-in-kbits***
— **no mbs**
— **mbs** ***mode***
— **no mode**
— **no mode**
— **rate cir** ***cir-rate*** **[pir** ***pir-rate*****]**

Epipe SAP Statistics commands for 7210 SAS-E and 7210 SAS-D

config
— **service**
— **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
— **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type {null-star|dot1q-preserve|any|dot1q-range}]** [**customer-vid** *vlan-id*] (for 7210 SAS-D)
— **no epipe** *service-id*
— **no sap** *sap-id*
— **statistics**
— **egress**
— [no] **forwarded-count** (supported only on 7210 SAS-D)
— [**no**] **packets-forwarded-count (**supported only on 7210 SAS-E)
— **ingress**
— **counter-mode {packet | octet} {in-out-profile-count|forward-drop-count}(**supported only on 7210 SAS-E)
— [**no**] **shutdown**
— **counter-mode {in-out-profile-count|forward-drop-count}(**supported only on 7210 SAS-D)
— **[no] received-count** (supported only on 7210 SAS-D)

Epipe SAP Configuration- QoS and Filter command for 7210 SAS-D and SAS-E

config
- **service**
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type {null-star|dot1q-pre-serve|any|dot1q-range}]** [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **epipe** *service-id* [**customer** *customer-id*] [**create**] [**svc-sap-type {null-star|dot1q-pre-serve|dot1q}]** [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **epipe** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any| dot1q-range}] (for 7210 SAS-K)**
  - **no epipe** *service-id*
    - **no sap** *sap-id* **[create]**
      - **egress**
        - **filter** [**ip** *ip-filter-id*]
        - **filter [ipv6** *ipv6 -filter-id***]**
        - **filter** [**mac** *mac-filter-id*] (app
        - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6 -filter-id***]** [**mac** *mac-filter-id*]
      - **ingress**
        - **aggregate-meter-rate** *rate-in-kbps* [**burst** *burst-in-kbits*] - **SAS-D**
        - **no aggregate-meter-rate**
        - **filter** [**ip** *ip-filter-id*]
        - **filter [ipv6** *ipv6-filter-id***]**
        - **filter** [**mac** *mac-filter-id*]
        - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6-filter-id***]** [**mac** *mac-filter-id*]
        - **qos** *policy-id*
        - **no qos**

Epipe SAP Configuration- QoS and Filter command for 7210 SAS-K

config
- **service**
  - **epipe** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any**| **dot1q-range}]**
  - **no epipe** *service-id*
    - **no sap** *sap-id* **[create]**
      - **egress**
        - **agg-shaper-rate cir** *cir-rate* **[pir** *pir-rate***]**
        - **no agg-shaper-rate**
        - **dot1p-inner** *dot1p-inner*
        - **no dot1p-inner**
        - **no dot1p-outer**
        - **dot1p-outer** *dot1p-outer*
        - **filter** [**ip** *ip-filter-id*]
        - **filter [ipv6** *ipv6 -filter-id***]**
        - **filter** [**mac** *mac-filter-id*] (app
        - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6 -filter-id***]** [**mac** *mac-filter-id*]
        - **qos** *policy-id*
        - **no qos**
      - **ingress**
        - **agg-shaper-rate cir** *cir-rate* **[pir** *pir-rate***]**
        - **no agg-shaper-rate**
        - **filter** [**ip** *ip-filter-id*]
        - **filter [ipv6** *ipv6-filter-id***]**
        - **filter** [**mac** *mac-filter-id*]
        - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6-filter-id***]** [**mac** *mac-filter-id*]
        - **qos** *policy-id*
        - **no qos**

Connection Profile Commands

config
- **connection-profile** *conn-prof-id [create]*
- **no connection-profile** *conn-prof-id*
  - **description** *description-string*
  - **no description**
  - **ethernet**
    - **no ranges**
  - **ranges** *vlan ranges [vlan ranges...(upto 32 max)]*

Show Commands

show
- **service**
  - **id** *service-id*
    - **all**
    - **base**
    - **sap**
    - **stp** *[sap-id]* **[detail]]**
  - **sap-using** *[sap sap-id]*
  - **sap-using [ingress | egress] filter** *filter-id*
  - **sap-using [ingress] qos-policy** *qos-policy-id*
  - **service-using [epipe] [vpls] [mirror] [cpipe] [i-vpls] [m-vpls] [sdp** *sdp-id***] [customer** *customer-id***]**

show
- **connection-profile [conn-prof-id] [associations]**

Clear Commands

clear
- **service**
  - **id** *service-id*
  - **statistics**
    - **id** *service-id*
    - **counters**
    - **sap** *sap-id* **{all | counters | stp| l2pt}**

VLL Service Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**
config>service>epipe
config>service>epipe>sap
config>service>epipe>sap>eth-cfm>mep

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

description

Syntax **description** *description-string*
no description

Context config>service>epipe
config>service>epipe>sap

config>connection-profile

Description This command creates a text description stored in the configuration file for a configuration context. The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

eth-cfm

Syntax **eth-cfm**

Context config>service>vll>sap

Description This command enables the context to configure ETH-CFM parameters.

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {up | down}]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context config>service>epipe>sap>eth-cfm

Description This command provisions the maintenance endpoint (MEP).

The no form of the command reverts to the default values.

Note: For more information on ETH-CFM support for different services, see Table 12, "ETH-CFM Support Matrix for 7210 SAS-D Devices," on page 100.

Parameters *mep-id* — Specifies the maintenance association end point identifier.

Values 1 — 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 — 4294967295

ma-index — Specifies the MA index value.

Values 1 — 4294967295

direction up| down — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction is not supported when a MEP is created directly under the vpls>eth-cfm construct (vMEP).

down — Sends ETH-CFM messages away from the MAC relay entity.

up — Sends ETH-CFM messages towards the MAC relay entity.

VLL Global Commands

epipe

Syntax **epipe** *service-id* [**customer** *customer-id*] [create] [***vpn*** vpn-id] [**svc-sap-type** {null-star | dot1q | dot1q-preserve|any| qinqinner-tag-preserve}] [customer-vid vlan-id] (for 7210 SAS devices in Access uplink mode) (for 7210 SAS-E)
epipe *service-id* [**customer** *customer-id*] [create] [**svc-sap-type** {null-star|dot1q-preserve|any|dot1q-range}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
epipe *service-id* [**customer** *customer-id*] [create] [**svc-sap-type** {**any|dot1q-range**}] (for 7210 SAS-K)
no **epipe** *service-id*

Context config>service

Description This command configures an Epipe service instance. This command is used to configure a point-to-point epipe service. An Epipe connects two endpoints defined as Service Access Points (SAPs). Both SAPs may be defined in one 7210 SAS.

No MAC learning or filtering is provided on an Epipe.

When a service is created, the **customer** keyword and *customer-id* must be specified and associates the service with a customer. The *customer-id* must already exist having been created using the **customer** command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified will result in an error.

By default, no epipe services exist until they are explicitly created with this command.

The **no** form of this command deletes the epipe service instance with the specified *service-id*. The service cannot be deleted until the service has been shutdown.

Parameters *service-id* — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7210 SAS on which this service is defined.

Values *service-id*: 1 — 2147483648
svc-name: 64 characters maximum

customer *customer-id* **—** Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 — 2147483647

svc-sap-type **—** Specifies the type of service and allowed SAPs in the service.

null-star **—** Specifies that the allowed SAP in the service, which can be null SAPs, Dot1q default, Q.* SAP,0.* SAP or Default QinQ SAP (also known as *.* SAP).

dot1q — Specifies that the allowed SAP in the service are Dot1q SAPs and dot1q explicit null SAPs. This is supported only on 7210 SAS-E.

dot1q-preserve — Specifies that the allowed SAP in the service are Dot1q. The Dot1q ID is not stripped after packets matches the SAP.

dot1q-range — Specifies that the access SAP in the service can use VLAN ranges as the SAP tags. The VLAN ranges are configured using the configure> connection-profile CLI command. On ingress of the access dot1q SAP using VLAN ranges, the outermost tag is not removed before forwarding. This is supported only for 7210 SAS-D.

any — Allows any SAP type. This is supported only on 7210 SAS-D.

customer-vid *vlan-id* — Defines the dot1q VLAN ID to be specified while creating the local Dot1q SAP for **svc-sap-type dot1q-preserve**.

Values 1 — 4094

create — Keyword used to create the service instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

service-mtu

Syntax **service-mtu** *octets*
no service-mtu

Context config>service>epipe

Description **Platforms Supported:** 7210 SAS-K.

This command configures the service payload (Maximum Transmission Unit – MTU), in bytes, for a service. The specified MTU value overrides the service-type default MTU. The service-mtu defines the payload capabilities of the service. It is used by the system to validate the operational states of SAP in a service.

On 7210 SAS-K, when a packet is received on a SAP, the service MTU check does not include the length of the packet excluding the SAP delineation encsapsulation overhead (that is, 4 bytes for a dot1q SAP or 8 bytes for a QinQ SAP).

If the required payload is larger than the port MTU, the SAP transitions to an inoperative state.

If the required MTU is equal to or less than the port MTU, the SAP transitions to an operative state.

If a service MTU, is dynamically or administratively modified, the operational states of all associated SAP are automatically re-evaluated.

The **no** form of the command restores the default service-mtu of the indicated service type to default value.

epipe: 1514 **Default**

The following table displays MTU values for specific VC types.

SAP VC-Type	Example Service MTU	Advertised MTU

Ethernet	1514	1500
Ethernet (with preserved dot1q)	1518	1504
VPLS	1514	1500
VPLS (with preserved dot1q)	1518	1504
VLAN (dot1p transparent to MTU value)	1514	1500
VLAN (Q-in-Q with preserved bottom Qtag)	1518	1504

octets — The size of the MTU in octets, expressed as a decimal integer, between 1 — 9194.

VLL SAP Commands

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context config>service>epipe

Description This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the 7210 device. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

On 7210 SAS-E and 7210 SAS-D, in This restriction does not apply to 7210 SAS-K.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port. Additionally, in access-uplink mode, SAPs can be defined also on access-uplink port. Access-uplink SAPs are network facing SAPs representing Dot1q or QinQ tunnels used to transport traffic towards the service nodes.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded.

The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The following encapsulations are supported:

- Ethernet access SAPs support null, dot1q, and qinq (QinQ SAP on access ports is not supported on 7210 SAS-E).
- Ethernet access-uplink SAPs support only QinQ encapsulation.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed.

Default No SAPs are defined.

Special Cases A default SAP has the following format: port-id:*. This type of SAP is supported only on Ethernet MDAs and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS).

sap-id — Specifies the physical port identifier portion of the SAP. See Common CLI Command Descriptions on page 483 for command syntax.

create — Keyword used to create a SAP instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

tod-suite

Syntax **tod-suite** *tod-suite-name*
no tod-suite

Context config>service>epipe>sap

Description This command applies a time-based policy (filter or QoS policy) to the service SAP. The suite name must already exist in the **config**>**cron** context.

Default no tod-suite

Parameters *tod-suite-name* — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy [<acct-policy-id>]

Context config>service>epipe>sap

Description This command creates the accounting policy context that can be applied to a SAP.

An accounting policy must be defined before it can be associated with a SAP. If the *policy-id* does not exist, an error message is generated.

A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config**>**log** context.

The **no** form of this command removes the accounting policy association from the SAP, and the acccounting policy reverts to the default.

Default Default accounting policy.

Parameters *acct-policy-id* — Enter the accounting *policy-id* as configured in the **config**>**log**>**accounting-policy** context.

Values 1-99

collect-stats

Syntax [**no**] **collect-stats**

Context config>service>epipe>sap

Description This command enables accounting and statistical data collection for either the SAP, network port, or IP interface. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default no collect-stats

ethernet

Syntax **ethernet**

Context config>service>epipe>sap

Description Use this command to configure Ethernet properties in this SAP.

llf

Syntax [**no**] **llf**

Context config>service>epipe>sap>ethernet

Description This command enables Link Loss Forwarding (LLF) on an Ethernet port or an ATM port. This feature provides an end-to-end OAM fault notification for Ethernet VLL service. It brings down the Ethernet port (Ethernet LLF) towards the attached CE when there is a local fault on the Pseudowire or service, or a remote fault on the SAP or pseudowire, signaled with label withdrawal or T-LDP status bits. It ceases when the fault disappears.

The Ethernet port must be configured for null encapsulation.

ignore-oper-down

Syntax **[no] ignore-oper-down**

Context config>service>epipe>sap

Description This command enables the user to configure the optional command for a specific SAP to ignore the transition of the operational state to down when a SAP fails. Only a single SAP in an ePipe may use this option.

Default no ignore-oper-down

send-ais-on-port-down

Syntax **[no] send-ais-on-port-down**

Context config>service>epipe>sap>eth-cfm>mep>ais-enable
config>service>vpls>sap>eth-cfm>mep>ais-enable

Description By default, the system generates an ETH-AIS message, if enabled, when CCM messages are not received within the configured time period. This command allows the user to specify that ETH-AIS should be generated for client MEPs immediately when port down event is detected on the port where the server MEP (and the associated SAP) resides. On a subsequent port up event, the AIS messages continue to be sent until valid CCMs are received. If there are no remote-meps configured for the MEP then on a subsequent port up event, the AIS messages are not sent.

The no form of the command reverts to default behavior.

Default no send-ais-on-port-down

bit-error-threshold

Syntax **bit-error-threshold** *errors*
no bit-error-threshold

Context config>service>epipe>sap>eth-cfm>mep>eth-test-enable

Description This command is used to specify the threshold value of bit errors.

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context config>service>vpls>sap>eth-cfm>mep

Description This command enables/disables eth-test functionality on MEP.

Parameters *seconds* — Specifies the one way delay threshold in seconds.

Values 0-600

Default 3

mip

Syntax **mip [mac mac-address]**
mip default-mac
no mip

Context config>service>epipe>sap>eth-cfm
config>service>epipe>spoke-sdp>eth-cfm

Description This command allows Maintenance Intermediate Points (MIPs) to be created if mhf-creation for the MA is configured using the default option.

Note: This command is supported on 7210 SAS-D. This command is not supported in 7210 SAS-E devices.

Parameters *mac-address* — Specifies the MAC address of the MIP.

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MIP. The MAC must be unicast. Using the all zeros address is equivalent to the no form of this command.

default-mac — Using the no command deletes the MIP. If the operator wants to change the mac back to the default mac without having to delete the MIP and reconfiguring this command is useful.

Default no mip

Connection Profile Commands

connection-profile

Syntax **connection-profile** *conn-prof-id [create]*
no connection-profile *conn-prof-id*

Context config

Description This command creates a profile for the user to configure the list VLAN values to be assigned to an Dot1q SAP in an Epipe service.

A connection profile can only be applied to a Dot1q SAP which is part of an Epipe Service.

The no form of this command deletes the profile from the configuration.

Default none

Parameters *conn-prof-id* — Specifies the profile number.

Values 1 — 8000

ethernet

Syntax ethernet

Context config>connprof

Description Provides the context to configure the VLAN ranges values.

Default none

ranges

Syntax no ranges
ranges vlan-ranges *[vlan-ranges...(upto 32 max)]*

Context config>connprof>ethernet

Description Specifies the list of VLAN ranges or individual VLAN ID to be used for mapping the given VLANs to the Epipe SAP.

The system validates that the values specified are valid VLAN ID in the range 0-4094 (VLAN ID 4095 is reserved). Ranges are specified in the format ‘a-b ’, the expression (a < b) should be true. Up to about 32 individual VLAN values or VLAN ranges can be specified. A maximum of up to 8 VLAN ranges are allowed per connection profile.

Default none

Parameters *vlan-ranges* — Specifies the list of VLAN ranges or individual VLAN ID to be used for mapping the given VLANs to the Epipe SAP.

A list of space separated values specified as either a-b or individual VLAN IDs. Both the VLAN IDs and the value used for 'a' and 'b' must be in the range of 0-4094. Additionally, value 'a' must be less than value 'b'.
For example:

ranges	100-200 5 6 4000-4020
ranges	4 5 6 10 11 12
ranges	250-350 500-600 1000-1023

Service Filter and QoS Policy Commands

egress

Syntax **egress**

Context config>service>epipe>sap

Description This command enables the context to configure egress SAP parameters.

ingress

Syntax **ingress**

Context config>service>epipe>sap

Description This command enables the context to configure ingress SAP Quality of Service (QoS) policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing.

agg-shaper-rate

Syntax **agg-shaper-rate cir** *cir-rate* **[pir** *pir-rate]*
no agg-shaper-rate

Context config> service> vpls> sap> ingress
config> service> vprn> sap> ingress
config> service> ies> sap> ingress

Description This command allows user to specify the aggregate rate for the SAP shaper. The aggregate SAP shaper is available to limit only the unicast traffic across all the FCs of the SAP that are configured to use ingress queues. User can specify the CIR rate and the PIR rate. User must not oversubscribe the total bandwidth available for use by ingress queues.
The no form of the command is equivalent to setting CIR to 0 and PIR to max.

Default no agg-shaper-rate

Parameters *cir <cir-rate>* — Specifies the rate in kilobits per second.

Values 0 — 20000000 | max

Default 0

pir <pir-rate> — Specifies the rate in kilobits per second.

Values 0 — 20000000 | max

Default max

aggregate-meter-rate

Syntax **aggregate-meter-rate** *rate-in-kbps* [**burst** *burst-in-kbits*]
no aggregate-meter-rate

Context config>service>epipe>sap>ingress
config>service>ies>sap>ingress
config>service>vprn>sap>ingress

Description This command allows the user to configure the SAP aggregate policer. The rate of the SAP aggregate policer must be specified by the user. The user can optionally specify the burst size for the SAP aggregate policer. The aggregate policer monitors the traffic on different FCs and determines the destination of the packet. The packet is either forwarded to an identified profile or dropped.

Note: The sum of CIR of the individual FCs configured under the SAP cannot exceed the PIR rate configured for the SAP. Though the 7210 SAS software does not block this configuration, it is not recommended for use.

The table below provides information about the final disposition of the packet based on the operating rate of the per FC policer and the per SAP aggregate policer:

Per FC meter Operating Rate	Per FC Assigned Color	SAP aggre-gate meter Operating Rate	SAP aggre-gate meter color	Final Packet Color
Within CIR	Green	Within PIR	Green	Green or In-profile
Within CIR*	Green	Above PIR	Red	Green or In-profile
Above CIR, Within PIR	Yellow	Within PIR	Green	Yellow or Out-of-Profile
Above CIR, Within PIR	Yellow	Above PIR	Red	Red or Dropped
Above PIR	Red	Within PIR	Green	Red or Dropped
Above PIR	Red	Above PIR	Red	Red or Dropped

Table 13: Final Disposition of the packet based on per FC and per SAP policer or meter.

Note*: The row number 2 in the above table is not recommended for use. For more information on this, see the Note in the "**aggregate-meter-rate**" description.

When the SAP aggregate policer is configured, per FC policer can be only configured in "trtcm2" mode (RFC 4115).

Note: The meter modes "srtcm" and "trtcm1" are used in the absence of an aggregate meter.

The SAP ingress meter counters increment the packet or octet counts based on the final disposition of the packet.

If ingress Frame-based accounting is used, the SAP aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter.

The **no** form of the command removes the aggregate policer from use.

Default no aggregate-meter-rate

Parameters *rate-in-kbps* — Specifies the rate in kilobits per second.

Values 01 — 20000000 | max

Default max

burst <*burst-in-kilobits*> — Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 —2146959

Default 512

filter

Syntax
filter [**ip** *ip-filter-id*]
filter [**ipv6** *ipv6-filter-id*]
filter [**mac** *mac-filter-id*]
no filter [**ip** *ip-filter-id*]
no filter [**ipv6** *ipv6-filter-id*]
no filter [**mac** *mac-filter-id*]

Context
config>service>epipe>sap>egress
config>service>epipe>sap>ingress

Description This command associates an IP filter policy with an ingress or egress Service Access Point (SAP) or IP interface.

Filter policies control the forwarding and dropping of packets based on IP matching criteria. Only one filter can be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified *filter-id* with an ingress or egress SAP. The *filter-id* must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

IP filters apply only to RFC 2427-routed IP packets. Frames that do not contain IP packets will not be subject to the filter and will always be passed, even if the filter's default action is to drop.

NOTE: For filter support available on different 7210 platforms, see the 7210 SAS Router Configuration User Guide.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system.

Special Cases **Epipe —** Both MAC and IP filters are supported on an Epipe service SAP.

Parameters **ip** *ip-filter-id* **—** Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 — 65535

ipv6 *ipv6-filter-id* — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 — 65535

mac *mac-filter-id* **—** Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 — 65535

dot1p-inner

Syntax **no dot1p-inner**
dot1p-inner

Context config>service>epipe>sap>egress
config>service>vpls>sap>egress

Description **Platforms supported:** 7210 SAS-K.

This command allows the user to define the Dot1p marking values to be used per SAP on egress for the inner tag when the SAP encapsulation is QinQ (that is, Q1.Q2 SAP)r. The command takes effect only if remarking is enabled in the remark policy associated with this SAP (under the egress context). It overrides the marking values defined in the remark policy associated with this SAP, if any.

Table 14: Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured:

Ingress SAP Type	Dot1p value extracted from received packet when Use-rcvd-inner-dot1p	Dot1p values extracted from received packet when Use-rcvd-outer-dot1p
Null SAP	None	None
Dot1q SAP	Dot1p from the outermost VLAN tag	Dot1p from the outermost VLAN tag
Dot1q Default SAP (that is, * SAP)	None	None
Dot1q Explicit NULL SAP (that is,:0 SAP)	Dot1p from the outermost VLAN tag (if priority tagged packet), else none.	Dot1p from the outermost VLAN tag (if priority tagged packet), else none.
Dot1q range SAP	Dot1p from the outermost VLAN tag	Dot1p from the outermost VLAN tag

Q1.Q2 SAP	Dot1p of the inner tag	Dot1p from the outermost VLAN tag
Q1.* SAP	Dot1p from the outermost VLAN tag	Dot1p from the outermost VLAN tag
0.* SAP	Dot1p from the outermost VLAN tag	Dot1p from the outermost VLAN tag
Q1.0 SAP	Dot1p of the inner priority tag, if available, else from outermost VLAN tag	Dot1p from the outermost VLAN tag
QinQ Default SAP (that is,. *.* SAP)	None	None

Table 15: Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured

Egress SAP Type	Dot1p-inner - Dot1p value marked in the packet sent out of this SAP when Use-rcvd-inner-dot1p	Dot1p-inner Dot1p value marked in the packet sent out of this SAP when Use-rcvd-outer-dot1p	Dot1p-outer Dot1p value marked in the packet sent out of this SAP when Use-rcvd-inner-dot1p	Dot1p-outer Dot1p value marked in the packet sent out of this SAP when Use-rcvd-outer-dot1p
Null SAP	NA	NA	NA	NA
Dot1q SAP	NA	NA	Dot1p bits in the outermost tag	Dot1p bits in the outermost tag
Dot1q Default SAP (that is, * SAP)	NA	NA	NA	NA
Dot1q Explicit NULL SAP (that is, :0 SAP)	NA	NA	NA	NA
Dot1q range SAP	NA	NA	NA	NA
Q1.Q2 SAP	Dot1p bits from the inner tag	Dot1p bits from the outermost tag	Dot1p bits from the inner tag	Dot1p bits from the outermost tag
Q1.* SAP	NA	NA	Dot1p bits from the inner tag	Dot1p bits from the outermost tag
0.* SAP	NA	NA	NA	NA
Q1.0 SAP	NA	NA	Dot1p bits from the inner tag	Dot1p bits from the outermost tag
QinQ Default SAP (that is, *.* SAP)	NA	NA	NA	NA

NOTE: **NA** – egress encapsulation is not done, neither remark policy nor ‘use-rcvd’ command will be applicable at that level.

If the no form of the command is executed, software will use the values defined in the remark policy associated with this SAP, if any. If no remark policy is associated with SAP egress, then the default values are used.

Default no dot1p-inner

Parameters *use-rcvd-inner-dot1p* — For more informatio, see Table 14, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured:,” on page 147 and Table 15, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured,” on page 149

use-rcvd-outer-dot1p — For more informatio, see Table 14, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured:,” on page 147 and Table 15, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured,” on page 149

dot1p-outer

Syntax **no dot1p-outer**
dot1p-outer

Context config>service>epipe>sap>egress
config>service>vpls>sap>egress
config>service>ies>interface>sap>egress

Description **Platforms supported:** 7210 SAS-K.

This command allows the user to define the Dot1p marking values to be used per SAP on egress for the outer tag when the SAP encapsulation is QinQ or Dot1q. The command takes effect only if remarking is enabled in the remark policy associated with this SAP (under the egress context). It overrides the marking values defined in the remark policy associated with this SAP, if any.

For more informatio, see Table 14, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured:,” on page 147 and Table 15, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured,” on page 149

If the no form of the command is executed, software will use the values defined in the remark policy associated with this SAP, if any. If no remark policy is associated with SAP egress, then the default values are used.

Default no dot1p-outer

Parameters *use-rcvd-inner-dot1p* — For more informatio, see Table 14, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured:,” on page 147 and Table 15, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured,” on page 149

user-rcvd-outer-dot1p — For more informatio, see Table 14, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured:,” on page 147 and Table 15, “Table for Dot1p values extracted from the packet on SAP (ingress) when Dot1p-inner and Dot1p-outer CLI command are configured,” on page 149

meter-override

Syntax **[no] meter-override**

Context config>service>epipe>sap>ingress
config>service>vpls>sap>ingress
config>service>ies>interface>sap>ingress
config>service>vprn>interface>sap>ingress

Description **Platforms supported:** 7210 SAS-D and 7210 SAS-E.

This command, within the SAP ingress contexts, is used to create a CLI node for specific overrides to one or more meters created on the SAP through the sap-ingress QoS policies.

The no form of the command is used to remove any existing meter overrides.

Default no meter-overrides

meter

Syntax **meter meter-id [create]**
no meter meter-id

Context config>service>epipe>sap>ingress>meter-override
config>service>vpls>sap>ingress>meter-override
config>service>ies>interface>sap>ingress>meter-override
config>service>vprn>interface>sap>ingress>meter-override

Description This command, within the SAP ingress contexts, is used to create a CLI node for specific overrides to a specific meter created on the SAP through a sap-ingress QoS policies.

The no form of the command is used to remove any existing overrides for the specified meter-id.

Parameters *meter-id* — The meter-id parameter is required when executing the meter command within the meter-overrides context. The specified meter-id must exist within the sap-ingress QoS policy applied to the SAP. If the meter is not currently used by any forwarding class or forwarding type mappings, the meter will not actually exist on the SAP. This does not preclude creating an override context for the meter-id.

create — The create keyword is required when a meter *meter-id* override node is being created and the system is configured to expect explicit confirmation that a new object is being created. When the system is not configured to expect explicit confirmation, the create keyword is not required.

adaptation-rule

Syntax **adaptation-rule** [**pir** *adaptation-rule*] [**cir** *adaptation-rule*]
no adaptation-rule

Context config>service>epipe>sap>ingress>meter-override>meter
config>service>vpls>sap>ingress>meter-override>meter
config>service>ies>interface>sap>ingress>meter-override>meter
config>service>vprn>interface>sap>ingress>meter-override>meter

Description This command can be used to override specific attributes of the specified meter adaptation rule parameters. The adaptation rule controls the method used by the system to derive the operational CIR and PIR settings when the meter is provisioned in hardware. For the CIR and PIR parameters individually, the system attempts to find the best operational rate depending on the defined constraint.

The **no** form of the command removes any explicitly defined constraints used to derive the operational CIR and PIR created by the application of the policy. When a specific **adaptation-rule** is removed, the default constraints for **rate** and **cir** apply.

Default no adaptation-rule

Parameters *pir* — The **pir** parameter defines the constraints enforced when adapting the PIR rate defined within the meter-override meter *meter-id* command. The **pir** parameter requires a qualifier that defines the constraint used when deriving the operational PIR for the queue. When the **meter-override** command is not specified, the default applies.

NOTE: When the meter mode in use is 'trtcm2', this parameter is interpreted as EIR value. For more information, see the description and relevant notes for meter modes in the 7210 SAS QoS user guide.

cir — The **cir** parameter defines the constraints enforced when adapting the CIR rate defined within the meter-override meter *meter-id* command. The **cir** parameter requires a qualifier that defines the constraint used when deriving the operational CIR for the queue. When the **cir** parameter is not specified, the default constraint applies.

adaptation-rule — Specifies the criteria to use to compute the operational CIR and PIR values for this meter, while maintaining a minimum offset.

Values **max** — The **max** (maximum) keyword is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR for the meter will be equal to or less than the administrative rate specified using the **meter-override** command.

min — The **min** (minimum) keyword is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR for the queue will be equal to or greater than the administrative rate specified using the **meter-override** command.

closest — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR for the meter will be the rate closest to the rate specified using the **meter-override** command.

cbs

Syntax **cbs** *size-in-kbytes*
no cbs

Context config>service>epipe>sap>ingress>meter-override>meter
config>service>vpls>sap>ingress>meter-override>meter
config>service>ies>interface>sap>ingress>meter-override>meter
config>service>vprn>interface>sap>ingress>meter-override>meter

Description This command, within the SAP ingress meter-overrides contexts, is used to override the sap-ingress QoS policy configured cbs parameter for the specified meter-id.

The no form of the command is used to restore the meter cbs setting to the meter defined value.

Default no mbs

Parameters *size-in-kbytes* — The size parameter is an integer expression of the number of kilobytes reserved for the meter. If a value of 10KBytes is desired, enter the value 10. A value of 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can still be applied for scheduling purposes).

Values [4..2146959 | default]

mbs

Syntax **mbs** *size-in-kbits*
no mbs

Context config>service>epipe>sap>ingress>meter-override>meter
config>service>vpls>sap>ingress>meter-override>meter
config>service>ies>interface>sap>ingress>meter-override>meter
config>service>vprn>interface>sap>ingress>meter-override>meter

Description This command, within the SAP ingress meter-overrides contexts, is used to override the sap-ingress QoS policy configured mbs parameter for the specified meter-id.

The no form of the command is used to restore the meter mbs setting to the meter defined value.

Default no mbs

Parameters *size-in-kbits* — The size parameter is required when specifying mbs override and is expressed as an integer representing the required size in either bytes or kilobytes. The default is kilobytes. The optional byte and kilobyte keywords are mutually exclusive and are used to explicitly define whether size represents bytes or kilobytes. When byte is defined, the value given for size is interpreted as the meter MBS value given in bytes. When kilobytes is defined, the value is interpreted as the meter MBS value given in kilobytes.

Values [4..2146959 | default]

mode

Syntax **mode** *mode*
no mode

Context config>service>epipe>sap>ingress>meter-override>meter
config>service>vpls>sap>ingress>meter-override>meter
config>service>ies>interface>sap>ingress>meter-override>meter
config>service>vprn>interface>sap>ingress>meter-override>meter

Description This command within the SAP ingress meter-overrides contexts is used to override the sap-ingress QoS policy configured mode parameters for the specified meter-id.

The no mode command is used to restore the policy defined metering and profiling mode to a meter.

Parameters *mode* — Specifies the rate mode of the meter-override.

Values trtcm1|trtcm2|srtcm

rate

Syntax **rate cir** *cir-rate* **[pir** *pir-rate***]**
no rate

Context config>service>epipe>sap>ingress>meter-override>meter
config>service>vpls>sap>ingress>meter-override>meter
config>service>ies>interface>sap>ingress>meter-override>meter
config>service>vprn>interface>sap>ingress>meter-override>meter

Description This command within the SAP ingress meter-overrides contexts is used to override the sap-ingress QoS policy configured rate parameters for the specified meter-id.

The no rate command is used to restore the policy defined metering and profiling rate to a meter.

Default **max —** The **max** default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The **max** value is mutually exclusive to the **pir-rate** value.

Parameters *pir-rate* — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a valid PIR setting must be explicitly defined. When the **rate** command has not been executed, the default PIR of **max** is assumed.
Fractional values are not allowed and must be given as a positive integer.

NOTE: When the meter mode is set to 'trtcm2' the PIR value is interpreted as the EIR value. For more information, see the 7210 SAS QoS user guide.

The actual PIR rate is dependent on the queue's **adaptation-rule** parameters and the actual hardware where the queue is provisioned.

Values [0..20000000 | max]

Default max

cir-rate — The **cir** parameter overrides the default administrative CIR used by the queue. When the **rate** command is executed, a CIR setting is optional. When the **rate** command has not been executed or the **cir** parameter is not explicitly specified, the default CIR (0) is assumed.
Fractional values are not allowed and must be given as a positive integer.

Values **[0..20000000 | max]**

Default 0

qos

Syntax **qos** *policy-id*
no qos

Context config>service>epipe>sap>ingress

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP).

QoS ingress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP or IP interface. If the *policy-id* does not exist, an error will be returned.

The **qos** command is used to associate ingress policies. The **qos** command only allows ingress policies to be associated on SAP ingress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress QoS policy can be associated with a SAP or IP interface at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, if no specific QoS policy is associated with the SAP for ingress, so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

policy-id — The ingress policy ID to associate with SAP on ingress. The policy ID must already exist.

Values 1 — 65535

statistics

Syntax **statistics**

Context config>service>epipe>sap

Description This command enables the context to configure the counters associated with SAP ingress and egress.

egress

Syntax **egress**

Context config>service>epipe>sap>statistics

Description This command enables the context to configure the egress SAP statistics counter and set the mode of the counter.

This counter counts the number of packets forwarded through the SAP.

ingress

Syntax **ingress**

Context config>service>epipe>sap>statistics

Description This command enables the context to configure the ingress SAP statistics counter.

For 7210 E, by default, SAP ingress counters are associated with a SAP and cannot be disabled.

In 7210 SAS-D devices, for access-uplink SAPs the ingress counters are not enabled by default. For access SAPs if the ingress counter is enabled by default, it can be disabled.

The two types of ingress SAP counters are:

- A counter that counts the total packets or octets received on the SAP
- A counter associated with meters defined in the QoS policy of the SAP. This counter counts the in-profile and out-of-profile packets or octets received on the SAP.

forwarded-count

Syntax [**no**] **forwarded-count**

Context config>service>epipe>sap>statistics>egress
config>service>vpls>sap>statistics>egress
config>service>ies>sap>statistics>egress

Platform supported: 7210 SAS-D

Description This command associates a counter with the SAP. The counter counts the number of packets forwarded through the SAP.

A limited amount of such counters are available for use with access SAPs and access-uplink SAPs.

Use this command before enabling applicable accounting record collection on the SAP to associate a counter with the SAP.

The **no** form of this command disables the packet count

packets-forwarded-count

Syntax [**no**] **packets-forwarded-count**

Context config>service>epipe>sap>statistics>egress

Platform supported: 7210 SAS-E

Description This command associates a counter with the SAP. The counter counts the number of packets forwarded through the SAP.

A limited amount of such counters are available for use with access SAPs and access-uplink SAPs.

Use this command before enabling applicable accounting record collection on the SAP to associate a counter with the SAP.

The **no** form of this command disables the packet count.

received-count

Syntax [**no**] **recieved-count**

Context config>service>epipe>sap>statistics>ingress
config>service>vpls>sap>statistics>ingress
config>service>ies>sap>statistics>ingress

Platform supported: 7210 SAS-D

Description This command associates a counter with the SAP. It counts the number of packets and octets received on the SAP (ingress).

A limited amount of such counters are available for use with access-uplink SAPs.

Use this command before enabling applicable accounting record collection on the SAP.

The **no** form of this command disables counter.

counter-mode

Syntax **counter-mode** {in-out-profile-count| forward-drop-count} {**packet** | **octet**}

Context config>service>epipe>sap>statistics>ingress
config>service>vpls>sap>statistics>ingress

Platform supported: 7210 SAS-E

Description This command sets the mode of ingress counters associated with the SAP The mode of the counter can be set to any of the following:

- in-out-profile-count
- forward-drop-count
- packet
- octet

Note: On 7210 SAS-E devices the counter can only count packets or octets at a given time.

The mode of the counter cannot be changed if an accounting policy is already associated with a SAP. Changing the mode of the counter results in loss of previously collected counts and resets the counter. The **no** form of this command is not supported.

Default when either in-out-profile-count or forward-drop-count is in use packet

Parameters **forward-drop-count** — If the counter mode is specified as "forward-drop-count", one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets/octets received on SAP ingress. The dropped count is count of packets/octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

in-out-profile-count — If the counter mode is specified as "in-out-profile-count", one counter counts the total in-profile packets and octets received on ingress of a SAP and another counts the total out-of-profile packets and octets received on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

octet — Sets the mode of ingress counters associated with the SAP to octets.

packet — Sets the mode of ingress counters associated with the SAP to packets.

counter-mode

Syntax **counter-mode** {in-out-profile-count| forward-drop-count}

Context config>service>epipe>sap>statistics>ingress
config>service>vpls>sap>statistics>ingress

Platform supported: 7210 SAS-D

Description This command allows the user to set the counter mode for the counters associated with sap ingress meters (a.ka. policers). A pair of counters is available with each meter. These counters count different events based on the counter mode value.

Note: The counter mode can be changed if an accounting policy is associated with a SAP. If the counter mode is changed the counters associated with the meter are reset and the counts are cleared. If an accounting policy is in use when the counter-mode is changed a new record will be written into the current accounting file.

Execute the following sequence of commands to ensure a new accounting file is generated when the counter-mode is changed:

1. Execute the command **config>service>epipe/vpls>sap> no collect-stats**, to disable writing of accounting records.
2. Change the counter-mode to the desired value, execute the command **config>service>epipe/vpls>sap>counter-mode {in-out-profile-count| forward-drop-count}**.
3. Execute the command **config>service>epipe/vpls>sap> collect-stats**, to enable writing of accounting records.

The **no** form of the command restores the counter mode to the default value.

Default in-out-profile-count

Parameters **forward-drop-count —** If the counter mode is specified as "forward-drop-count", one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets/octets received on SAP ingress. The dropped count is count of packets/octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

in-out-profile-count — If the counter mode is specified as "in-out-profile-count", one counter counts the total in-profile packets and octets received on ingress of a SAP and another counts the total

out-of-profile packets and octets received on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

Virtual Private LAN Service

In This Chapter

This chapter provides information about Virtual Private LAN Service (VPLS), process overview, and implementation notes.

Topics in this chapter include:

VPLS Service Overview

Virtual Private LAN Service (VPLS) is a class of virtual private network service that allows the connection of multiple sites in a single bridged domain over a provider-managed IP/MPLS network. The customer sites in a VPLS instance appear to be on the same LAN, regardless of their location. VPLS uses an Ethernet interface on the customer-facing (access) side which simplifies the LAN/WAN boundary and allows for rapid and flexible service provisioning. The 7210 SAS supports provisioning of access or uplink SAPs to connect to the provider edge IP/MPLS routers.

VPLS offers a balance between point-to-point Frame Relay service and outsourced routed services . VPLS enables each customer to maintain control of their own routing strategies. All customer routers in the VPLS service are part of the same subnet (LAN) which simplifies the IP addressing plan, especially when compared to a mesh constructed from many separate point-to-point connections. The VPLS service management is simplified since the service is not aware of nor participates in the IP addressing and routing.

A VPLS service provides connectivity between two or more SAPs on one (which is considered a local service) or more (which is considered a distributed service) service routers. The connection appears to be a bridged domain to the customer sites so protocols, including routing protocols, can traverse the VPLS service. The 7210 SAS supports only local VPLS service.

Other VPLS advantages include:

- VPLS is a transparent, protocol-independent service.
- There is no Layer 2 protocol conversion between LAN and WAN technologies.
- There is no need to design, manage, configure, and maintain separate WAN access equipment, thus, eliminating the need to train personnel on WAN technologies such as Frame Relay.

VPLS Packet Walkthrough

This section provides an example of VPLS processing of a customer packet sent across the network from site-A, which is connected to PE-Router-A through a 7210 SAS to site-C, which is connected through 7210 SAS to PE-Router-C (Figure 13). This section does not discuss the processing on the PE routers, but only on 7210 SAS routers.

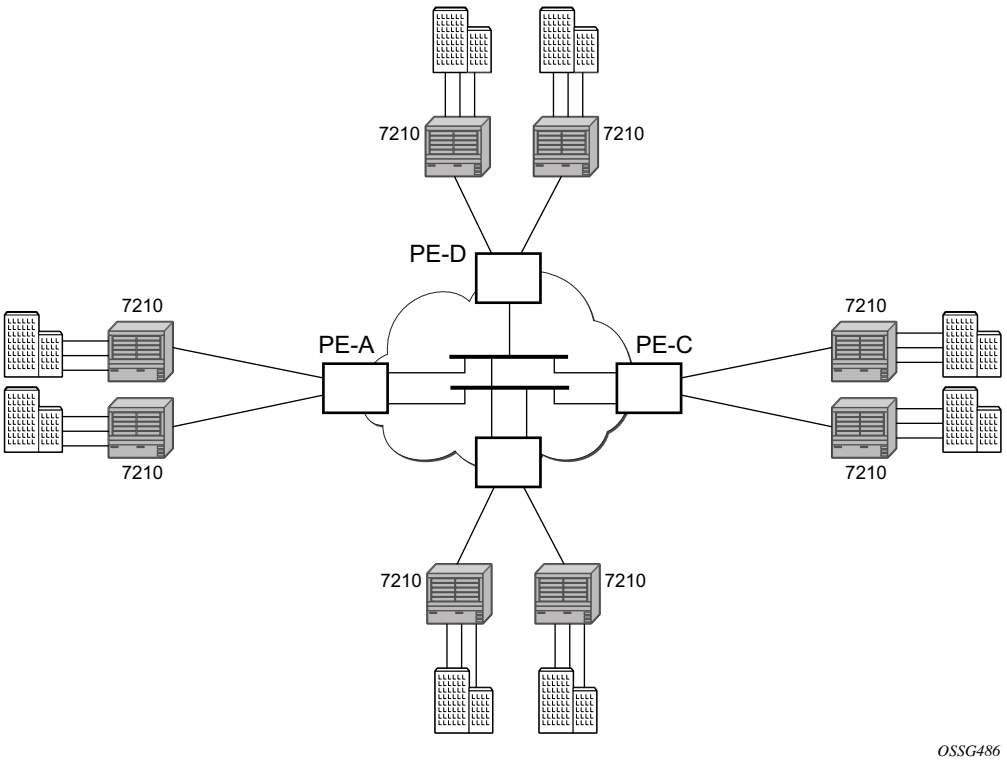


Figure 13: VPLS Service Architecture

1. 7210-A (Figure 14)
   a. Service packets arriving at 7210-A are associated with a VPLS service instance based on the combination of the physical port and the IEEE 802.1Q tag (VLAN-ID) in the packet

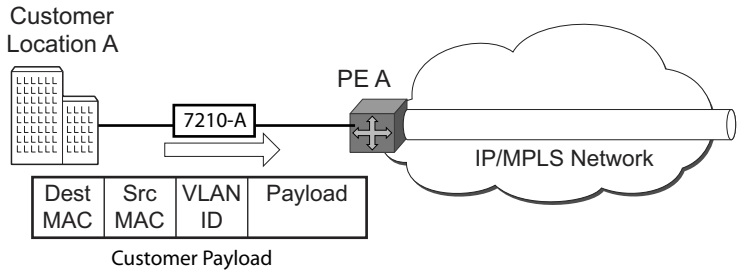


Figure 14: Access Port Ingress Packet Format and Lookup

b. 7210-A learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the service access point (SAP) on which it was received.

c. The destination MAC address in the packet is looked up in the FIB table for the VPLS instance. There are two possibilities: either the destination MAC address has already been learned (known MAC address) or the destination MAC address is not yet learned (unknown MAC address).

For a Known MAC Address (Figure 15):

d. If the destination MAC address has already been learned by 7210 an existing entry in the FIB table identifies destination uplink QinQ SAP to be used for sending the packet towards the PE-Router-A.

e. The customer packet is sent on this uplink SAP once the IEEE 802.1Q tag is stripped and the uplink SAP tag is added to the packet.

For an Unknown MAC Address (Figure 15):

f. If the destination MAC address has not been learned, 7210 will flood the packet to all the uplink SAPs that are participating in the service.

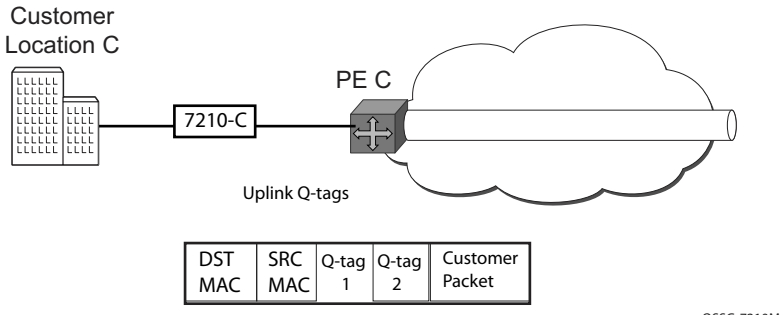


Figure 15: Network Port Egress Packet Format and Flooding

2. Core Router Switching

   a. The PE router will encapsulate this packet in the appropriate MPLS header and transport it across the core network to the remote 7210-C.

3. 7210-C (Figure 14)

   a. 7210-C associates the packet with the VPLS instance based on the VLAN tags in the received packet.

   b. 7210-C learns the source MAC address in the packet and creates an entry in the FIB table that associates the MAC address to the access uplink port on which the packet was received.

   c. The destination MAC address in the packet is looked up in the FIB table for the VPLS instance. Again, there are two possibilities: either the destination MAC address has already been learned (known MAC address) or the destination MAC address has not been learned on the access side of 7210-C (unknown MAC address).

   d. If the destination MAC address has been learned by 7210-C, an existing entry in the FIB table identifies the local access port and the IEEE 802.1Q tag (if any) to be added before sending the packet to customer Location-C. The egress Q tag may be different than the ingress Q tag.

   e. If the destination MAC address has not been learned, 7210 will flood the packet to all the access SAPs that are participating in the service.

VPLS Features

This section features:

VPLS Enhancements

Alcatel-Lucent's VPLS implementation includes several enhancements beyond basic VPN connectivity. The following VPLS features can be configured individually for each VPLS service instance:

- Extensive MAC and IP filter support (up to Layer 4). Filters can be applied on a per SAP basis.
- Forwarding Information Base (FIB) management features including:
  - → Configurable FIB size limit
  - → FIB size alarms
  - → MAC learning disable
  - → Discard unknown
  - → Aging timers for learned MAC addresses.
- Implementation of Spanning Tree Protocol (STP) parameters on a per VPLS and per SAP basis. (Not supported on 7210 SAS-K).
- IGMP snooping on a per-SAP basis (Not supported on 7210 SAS-K).

VPLS over QinQ SAPs

7210 SAS-D, E devices support QinQ SAPs or Dot1q SAPs, which allows them to connect to upstream PE nodes which provides IP/MPLS transport.

VPLS is provided over QinQ/Dot1q SAPs by:

- Connecting bridging-capable 7210 SAS devices.
- Replicating unknown and broadcast traffic in a service domain.
- Enabling MAC learning over QinQ/Dot1q SAPs and access ports (see VPLS MAC Learning and Packet Forwarding).
- Using a separate forwarding information base (FIB) per VPLS service.

VPLS MAC Learning and Packet Forwarding

The 7210 SAS edge devices perform the packet replication required for broadcast and multicast traffic across the bridged domain. MAC address learning is performed by the 7210 SAS device to reduce the amount of unknown destination MAC address flooding.

7210 SAS routers learn the source MAC addresses of the traffic arriving on their access ports.

Access uplink SAPS connects customers to the uplink network. Each 7210 SAS maintains a Forwarding Information Base (FIB) for each VPLS service instance and learned MAC addresses are populated in the FIB table of the service. All traffic is switched based on MAC addresses using QinQ SAPs created on access uplink ports Unknown destination packets (for example, the destination MAC address has not been learned) are forwarded on all SAPs for that service until the target station responds and the MAC address is learned by the 7210 SAS associated with that service.

IGMP Snooping

NOTE: 7210 SAS-K does not support IGMP snooping.

In Layer 2 switches, multicast traffic is treated like an unknown MAC address or broadcast frame, which causes the incoming frame to be flooded out (broadcast) on every port within a VLAN. Although this is acceptable behavior for unknowns and broadcast frames, this flooded multicast traffic may result in wasted bandwidth on network segments and end stations, as IP multicast hosts can join and be interested in only specific multicast groups.

IGMP snooping entails using information in Layer 3 protocol headers of multicast control messages to determine the processing at Layer 2. By doing so, an IGMP snooping switch provides the benefit of conserving bandwidth on those segments of the network in which no node has expressed interest in receiving packets addressed to the group address.

IGMP snooping can be enabled in the context of VPLS services. The IGMP snooping feature allows for optimization of the multicast data flow to only those SAPs that are members of the group. The system builds a database of group members per service by listening to IGMP queries and reports from each SAP:

- When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry.
- When it receives an IGMP leave message from a host, it removes the host port from the table entry, if no other group members are present. It also deletes entries if it does not receive periodic IGMP membership reports from the multicast clients.

The following are IGMP snooping features:

- IGMP v1, v2, and v3 are supported (RFC 1112, *Host Extensions for IP Multicasting*, and RFC 2236, *Internet Group Management Protocol, Version 2*).
- IGMP snooping can be enabled and disabled on individual VPLS service instances.
- IGMP snooping can be configured on individual SAPs that are part of a VPLS service. When IGMP snooping is enabled on a VPLS service, all its contained SAPs automatically have snooping enabled.
- Fast leave terminates the multicast session immediately, rather than using the standard group-specific query to check if other group members are present on the network.
- SAPs can be statically configured as multicast router ports. This allows the operator to control the set of ports to which IGMP membership reports are forwarded.
- Static multicast group membership on a per SAP basis can be configured.
- The maximum number of multicast groups (static and dynamic) that a SAPcan join can be configured. An event is generated when the limit is reached.

- The maximum number of multicast groups (static and dynamic) that a VPLS instance simultaneously supports can be configured.
- Proxy summarization of IGMP messages reduces the number of IGMP messages processed by upstream devices in the network.
- IGMP filtering allows a subscriber to a service or the provider to block, receive, or transmit permission (or both) to individual hosts or a range of hosts.
  The following types of filters can be defined:
  - → Filter group membership that report from a particular host or range of hosts. This filtering is performed by importing an appropriately-defined routing policy into the SAP.
  - → Filters that prevent a host from transmitting multicast streams into the network. The operator can define a data-plane filter (ACL) that drops all multicast traffic, and apply this filter to a SAP.
-

Multicast VLAN Registration (MVR) support

NOTE: 7210 SAS-K does not support MVR.

Multicast VPLS Registration (MVR) is a bandwidth optimization method for multicast in a broadband services network. MVR allows a subscriber on a port to subscribe and unsubscribe to a multicast stream on one or more network-wide multicast VPLS instances.

MVR assumes that subscribers join and leave multicast streams by sending IGMP join and leave messages. The IGMP leave and join message are sent inside the VPLS to which the subscriber port is assigned. The multicast VPLS is shared in the network while the subscribers remain in separate VPLS services. Using MVR, users on different VPLS cannot exchange any information between them, but still multicast services are provided.

On the MVR VPLS, IGMP snooping must be enabled. On the user VPLS, IGMP snooping and MVR work independently. If IGMP snooping and MVR are both enabled, MVR reacts only to join and leave messages from multicast groups configured under MVR. Join and leave messages from all other multicast groups are managed by IGMP snooping in the local VPLS. This way, potentially several MVR VPLS instances could be configured, each with its own set of multicast channels.

MVR by proxy — In some situations, the multicast traffic should not be copied from the MVR VPLS to the SAP on which the IGMP message was received (standard MVR behavior) but to another SAP. This is called MVR by proxy.

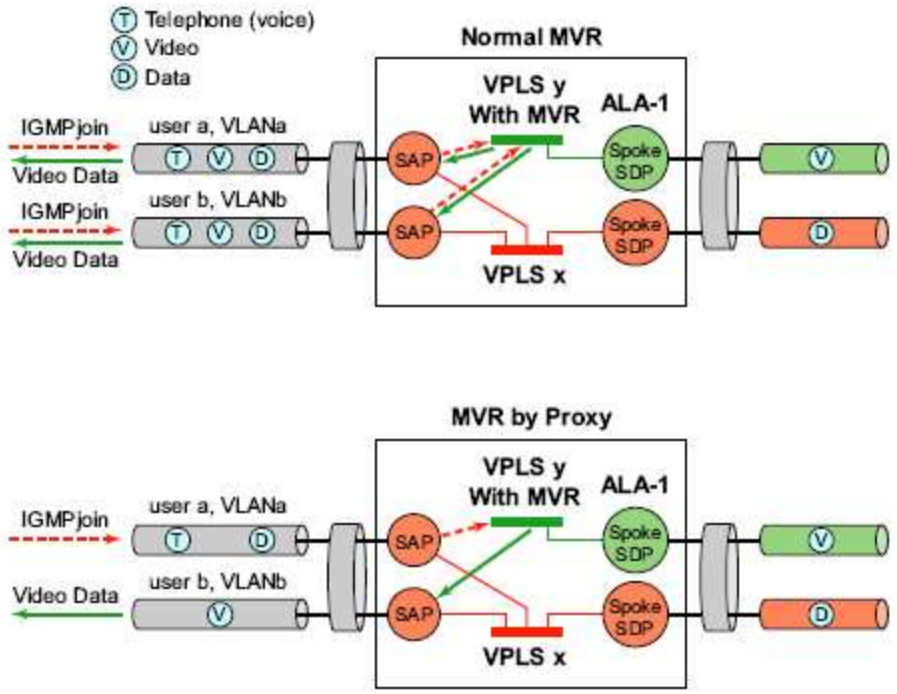


Figure 16: MVR and MVR by Proxy

Configuration Guidelines for MVR

In a MVR configuration, the svc-sap-type of the VPLS service that is the source, which is also known as 'mvr vpls service' and the svc-sap-type of the VPLS service that is the sink, which is also known as 'user vpls service' should match.

L2 Forwarding Table Management

The following sections describe VPLS features related to management of the Forwarding Information Base (FIB).

FIB Size

The following MAC table management features are required for each instance of a SAPwithin a particular VPLS service instance:

- MAC FIB size limits — Allows users to specify the maximum number of MAC FIB entries that are learned locally for a SAP. If the configured limit is reached, then no new addresses will be learned from the SAPuntil at least one FIB entry is aged out or cleared.
  - → When the limit is reached on a SAP, packets with unknown source MAC addresses are still forwarded (this default behavior can be changed by configuration). By default, if the destination MAC address is known, it is forwarded based on the FIB, and if the destination MAC address is unknown, it will be flooded. Alternatively, if discard unknown is enabled at the VPLS service level, unknown destination MAC addresses are discarded.
  - → The log event SAP MAC limit reached is generated when the limit is reached. When the condition is cleared, the log event SAP MAC Limit Reached Condition Cleared is generated.
  - → Disable learning at the VPLS service level allows users to disable the dynamic learning function on the service. Disable learning is not supported at the SAP level.
  - → Disable aging allows users to turn off aging for learned MAC addresses on a SAP of a VPLS service instance.

FIB Size Alarms

The size of the VPLS FIB can be configured with a low watermark and a high watermark, expressed as a percentage of the total FIB size limit. If the actual FIB size grows above the configured high watermark percentage, an alarm is generated. If the FIB size falls below the configured low watermark percentage, the alarm is cleared by the system.

Local Aging Timers

Like a Layer 2 switch, learned MACs within a VPLS instance can be aged out if no packets are sourced from the MAC address for a specified period of time (the aging time). The age timer for the VPLS instance specifies the aging time for locally learned MAC addresses.

The aging mechanism is considered a low priority process. In most situations, the aging out of MAC addresses can happen in within tens of seconds beyond the age time. To minimize overhead, local MAC addresses on a LAG port, in some circumstances, can take up to two times their respective age timer to be aged out.

Disable MAC Aging

The MAC aging timers can be disabled which will prevent any learned MAC entries from being aged out of the FIB. When aging is disabled, it is still possible to manually delete or flush learned MAC entries. Aging can be disabled for learned MAC addresses on a SAP of a VPLS service instance.

Disable MAC Learning

When MAC learning is disabled for a service, new source MAC addresses are not entered in the VPLS FIB. MAC learning can be disabled for services.

Unknown MAC Discard

Unknown MAC discard is a feature which discards all packets ingressing the service where the destination MAC address is not in the FIB. The normal behavior is to flood these packets to all end points in the service.

Unknown MAC discard can be used with the disable MAC learning and disable MAC aging options to create a fixed set of MAC addresses allowed to ingress and traverse the service.

VPLS and Rate Limiting

Traffic that is normally flooded throughout the VPLS can be rate limited on SAP ingress through the use of service ingress QoS policies. In a service ingress QoS policy, individual meters can be defined per forwarding class to provide rate-limiting/policing of broadcast traffic, MAC multicast traffic and unknown destination MAC traffic.

MAC Move

The MAC move feature is useful to protect against undetected loops in a VPLS topology, as well as the presence of duplicate MACs in a VPLS service.

If two clients in the VPLS have the same MAC address, the VPLS will experience a high relearn rate for the MAC. When MAC move is enabled, the 7210 SAS D, E shuts down the SAP and create an alarm event when the threshold is exceeded.

Split Horizon SAP Groups on 7210 SAS-K

Note: Split Horizon group per service is supported only on 7210 SAS-K devices.

In many applications, the split-horizon group concept involving a group of SAPs is useful to prevent direct customer-to-customer traffic exchange (without the traffic being sent to the head-end service nodes). This extension is referred to as a split horizon SAP group. Traffic arriving on a SAP or a spoke SDP within a split horizon group will not be forwarded to other SAPs configured in the same split horizon group, but will be forwarded to other SAPs, which are not part of the split horizon group.

VPLS and Spanning Tree Protocol

NOTE: STP and its flavors (RSTP, MSTP, mVPLS/xSTP) are not supported on 7210 SAS-K.

Alcatel-Lucent's VPLS service provides a bridged or switched Ethernet Layer 2 network. Equipment connected to SAPs forward Ethernet packets into the VPLS service. The 7210 SAS participating in the service learns where the customer MAC addresses reside, on ingress SAPs.

Unknown destinations, broadcasts, and multicasts are flooded to all other SAPs in the service. If SAPs are connected together, either through misconfiguration or for redundancy purposes, loops can form and flooded packets can keep flowing through the network. Alcatel-Lucent's implementation of the Spanning Tree Protocol (STP) is designed to remove these loops from the VPLS topology. This is done by putting one or several SAPs in the discarding state.

Alcatel-Lucent's implementation of the Spanning Tree Protocol (STP) incorporates some modifications to make the operational characteristics of VPLS more effective.

The STP instance parameters allow the balancing between resiliency and speed of convergence extremes. Modifying particular parameters can affect the behavior. For information on command usage, descriptions, and CLI syntax, refer to Configuring a VPLS Service with CLI on page 205.

Spanning Tree Operating Modes

Per VPLS instance, a preferred STP variant can be configured. The STP variants supported are:

- `rstp` — Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1D-2004 - default mode
- `dot1w` — Compliant with IEEE 802.1w
- `comp-dot1w` — Operation as in RSTP but backwards compatible with IEEE 802.1w (this mode allows interoperability with some MTU types)
- `mstp` — Compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q-REV/D5.0-09/2005. This mode of operation is only supported in an mVPLS.

While the 7210 SAS initially uses the mode configured for the VPLS, it will dynamically fall back (on a per-SAP basis) to STP (IEEE 802.1D-1998) based on the detection of a BPDU of a different format. A trap or log entry is generated for every change in spanning tree variant.

Some older 802.1W compliant RSTP implementations may have problems with some of the features added in the 802.1D-2004 standard. Interworking with these older systems is improved with the comp-dot1w mode. The differences between the RSTP mode and the comp-dot1w mode are:

- The RSTP mode implements the improved convergence over shared media feature, for example, RSTP will transition from discarding to forwarding in 4 seconds when operating over shared media. The comp-dot1w mode does not implement this 802.1D-2004 improvement and transitions conform to 802.1w in 30 seconds (both modes implement fast convergence over point-to-point links).
- In the RSTP mode, the transmitted BPDUs contain the port's designated priority vector (DPV) (conforms to 802.1D-2004). Older implementations may be confused by the DPV in a BPDU and may fail to recognize an agreement BPDU correctly. This would result in a slow transition to a forwarding state (30 seconds). For this reason, in the comp-dot1w mode, these BPDUs contain the port's port priority vector (conforms to 802.1w).

The 7210 SAS supports one BDPU encapsulation formats, and can dynamically switch between the following supported formats (on a per-SAP basis):

- IEEE 802.1D STP
- Cisco PVST

Multiple Spanning Tree

The Multiple Spanning Tree Protocol (MSTP) extends the concept of the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) by allowing grouping and associating VLANs to Multiple Spanning Tree Instances (MSTI). Each MSTI can have its own topology, which provides architecture enabling load balancing by providing multiple forwarding paths. At the same time, the number of STP instances running in the network is significantly reduced as compared to Per VLAN STP (PVST) mode of operation. Network fault tolerance is also improved because a failure in one instance (forwarding path) does not affect other instances.

The 7210 SAS implementation of Management VPLS (mVPLS) is used to group different VPLS instances under single RSTP instance. Introducing MSTP into the mVPLS allows the following:

- Interoperation with traditional Layer 2 switches in access network.
- Provides an effective solution for dual homing of many business Layer 2 VPNs into a provider network.

Redundancy Access to VPLS

The GigE MAN portion of the network is implemented with traditional switches. Using MSTP running on individual switches facilitates redundancy in this part of the network. In order to provide dual homing of all VPLS services accessing from this part of the network, the VPLS PEs must participate in MSTP.

This can be achieved by the following:

- Configuring mVPLS on VPLS-PEs (only PEs directly connected to GigE MAN network).
- Assign different managed-vlan ranges to different MSTP instances.

Typically, the mVPLS would have SAPs with null encapsulations (to receive, send, and transmit MSTP BPDUs) and a mesh SDP to interconnect a pair of VPLS PEs.

Different access scenarios are displayed in Figure 17 as example network diagrams dually connected to the PBB PEs:

- **Access Type A** — Source devices connected by null or Dot1q SAPs
- **Access Type B** — One QinQ switch connected by QinQ/801ad SAPs
- **Access Type C** — Two or more ES devices connected by QinQ/802.1ad SAPs

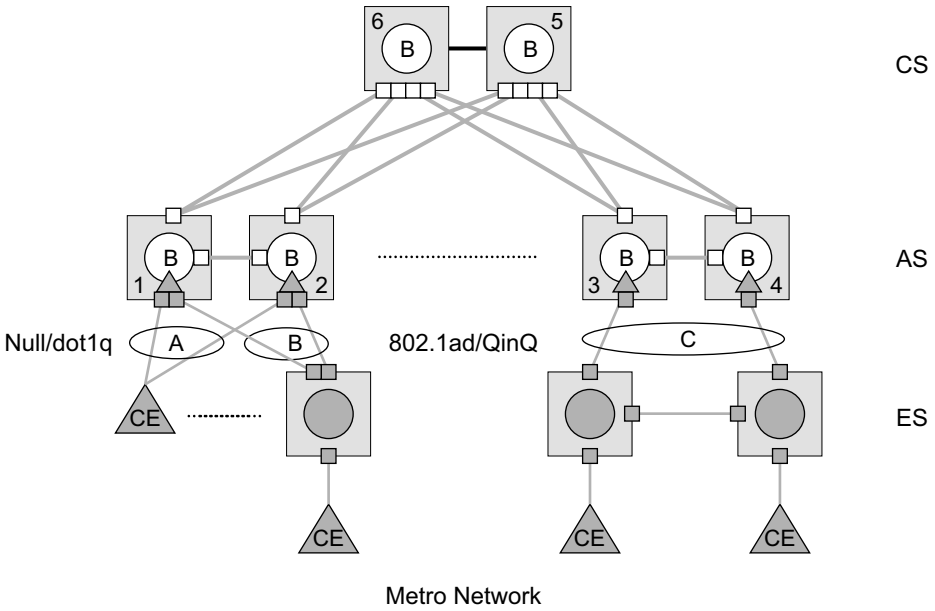


Figure 17: Access Resiliency

The following mechanisms are supported for the I-VPLS:

- **STP/RSTP** can be used for all access types
- **M-VPLS with MSTP** can be used as is just for access Type A. MSTP is required for access type B and C.
- **LAG and MC-LAG** can be used for access Type A and B.
- **Split-horizon-group** does not require residential.

MSTP for QinQ SAPs

MSTP runs in a MVPLS context and can control SAPs from source VPLS instances. QinQ SAPs are supported. The outer tag is considered by MSTP as part of VLAN range control

MSTP General Principles

MSTP represents modification of RSTP which allows the grouping of different VLANs into multiple MSTIs. To enable different devices to participate in MSTIs, they must be consistently configured. A collection of interconnected devices that have the same MST configuration (region-name, revision and VLAN-to-instance assignment) comprises an MST region.

There is no limit to the number of regions in the network, but every region can support a maximum of 16 MSTIs. Instance 0 is a special instance for a region, known as the Internal Spanning Tree (IST) instance. All other instances are numbered from 1 to 4094. IST is the only spanning-tree instance that sends and receives BPDUs (typically BPDUs are untagged). All other spanning-tree instance information is included in MSTP records (M-records), which are encapsulated within MSTP BPDUs. This means that single BPDU carries information for multiple MSTI which reduces overhead of the protocol.

Any given MSTI is local to an MSTP region and completely independent from an MSTI in other MST regions. Two redundantly connected MST regions will use only a single path for all traffic flows (no load balancing between MST regions or between MST and SST region).

Traditional Layer 2 switches running MSTP protocol assign all VLANs to the IST instance per default. The operator may then “re-assign” individual VLANs to a given MSTI by configuring per VLAN assignment. This means that a SR-Series PE can be considered as the part of the same MST region only if the VLAN assignment to IST and MSTIs is identical to the one of Layer 2 switches in access network.

MSTP in the 7210 SAS Platform

The 7210 SAS platform uses a concept of mVPLS to group different SAPs under a single STP instance. The VLAN range covering SAPs to be managed by a given mVPLS is declared under a specific mVPLS SAP definition. MSTP mode-of-operation is only supported in an mVPLS.

When running MSTP, by default, all VLANs are mapped to the CIST. On the VPLS level VLANs can be assigned to specific MSTIs. When running RSTP, the operator must explicitly indicate, per SAP, which VLANs are managed by that SAP.

Enhancements to the Spanning Tree Protocol

To interconnect 7210 SAS devices (PE devices) across the backbone, service tunnels (SDPs) are used. These service tunnels are shared among multiple VPLS instances. Alcatel-Lucent's implementation of the Spanning Tree Protocol (STP) incorporates some enhancements to make the operational characteristics of VPLS more effective. The implementation of STP on the router is modified in order to guarantee that service tunnels will not be blocked in any circumstance without imposing artificial restrictions on the placement of the root bridge within the network. The modifications introduced are fully compliant with the 802.1D-2004 STP specification.

When running MSTP, spoke SDPs cannot be configured. Also, ensure that all bridges connected by mesh SDPs are in the same region. If not, the mesh will be prevented from becoming active (trap is generated).

In order to achieve this, all mesh SDPs are dynamically configured as either root ports or designated ports. The PE devices participating in each VPLS mesh determine (using the root path cost learned as part of the normal protocol exchange) which of the 7210 SAS devices is closest to the root of the network. This PE device is internally designated as the primary bridge for the VPLS mesh. As a result of this, all network ports on the primary bridges are assigned the designated port role and therefore remain in the forwarding state.

The second part of the solution ensures that the remaining PE devices participating in the STP instance see the SDP ports as a lower cost path to the root rather than a path that is external to the mesh. Internal to the PE nodes participating in the mesh, the SDPs are treated as zero cost paths towards the primary bridge. As a consequence, the path through the mesh are seen as lower cost than any alternative and the PE node will designate the network port as the root port. This ensures that network ports always remain in forwarding state.

A combination of the above mentioned features ensure that network ports are never blocked and maintain interoperability with bridges external to the mesh that are running STP instances.

L2PT Termination

NOTE: 7210 SAS-K does not support L2PT termination.

L2PT is used to transparently transport protocol data units (PDUs) of Layer 2 protocols such as STP, CDP, DTP, VTP, PAGP, and UDLD. This allows running these protocols between customer CPEs without involving backbone infrastructure.

The 7210 SAS routers allow transparent tunneling of PDUs across the VPLS core. However, in some network designs, the VPLS PE is connected to CPEs through a legacy Layer 2 network, rather than having direct connections. In such environments termination of tunnels through such infrastructure is required.

L2PT tunnels protocol PDUs by overwriting MAC destination addresses at the ingress of the tunnel to a proprietary MAC address such as 01-00-0c-cd-cd-d0. At the egress of the tunnel, this MAC address is then overwritten back to MAC address of the respective Layer 2 protocol.

The 7210 SAS nodes support L2PT termination for STP BPDUs. More specifically:

- At ingress of every SAPwhich is configured as L2PT termination, all PDUs with a MAC destination address, 01-00-0c-cd-cd-d0 will be intercepted and their MAC destination address will be overwritten to MAC destination address used for the corresponding protocol. The type of protocol can be derived from LLC and SNAP encapsulation.
- In egress direction, PDUs of the corresponding protocol received on all VPLS ports will be intercepted and L2PT encapsulation will be performed for SAPs configured as L2PT termination points. Because of the implementation reasons, PDU interception and re-direction to CPM can be performed only at ingress. Therefore, to comply with the above requirement, as soon as at least 1 port of a given VPLS service is configured as L2PT termination port, redirection of PDUs to CPM will be set on all other ports (SAPs) of the VPLS service.

L2PT termination can be enabled only if STP is disabled in a context of the given VPLS service.

BPDU Translation

NOTE: 7210 SAS-K does not support BPDU termination.

VPLS networks are typically used to interconnect different customer sites using different access technologies such as Ethernet and bridged-encapsulated ATM PVCs. Typically, different Layer 2 devices can support different types of STP and even if they are from the same vendor. In some cases, it is necessary to provide BPDU translation in order to provide an interoperable e2e solution.

To address these network designs, BPDU format translation is supported on 7210 SAS D, E devices. If enabled on a given SAP, the system will intercept all BPDUs destined to that interface and perform required format translation such as STP-to-PVST or vice versa.

Similarly, BPDU interception and redirection to the CPM is performed only at ingress meaning that as soon as at least 1 port within a given VPLS service has BPDU translation enabled, all BPDUs received on any of the VPLS ports will be redirected to the CPM.

BPDU translation involves all encapsulation actions that the data path would perform for a given outgoing port (such as adding VLAN tags depending on the outer SAP and adding or removing all the required VLAN information in a BPDU payload.

This feature can be enabled on a SAP only if STP is disabled in the context of the given VPLS service.

L2PT and BPDU Translation

L2PT termination for only STP (Spanning Tree Protocol) and PVST (Per VLAN Spanning Tree Protocol) are supported on 7210 SAS-E.

Cisco Discovery Protocol (CDP), Digital Trunking Protocol (DTP), Port Aggregation Protocol (PAgP), Uni-directional Link Detection (UDLD), Virtual Trunk Protocol (VTP), STP (Spanning Tree Protocol) and PVST (per-VLAN Spanning Tree protocol) are supported on 7210 SAS-D.

These protocols automatically pass the other protocols tunneled by L2PT towards the CPM and all carry the same specific Cisco MAC.

The existing L2PT limitations apply.

- The protocols apply only to VPLS.
- The protocols are mutually exclusive with running STP on the same VPLS as soon as one SAP has L2PT/BPDU translation enabled.
- Forwarding occurs on the CPM.

VPLS Access Redundancy

A second application of hierarchical VPLS is using 7210 SAS D, E nodes that are MPLS-enabled which must have Ethernet links to the closest PE node. To protect against failure of the PE node, 7210 SAS D, E can be dual-homed and have two SAPs on two PE nodes.

Listed below are several mechanisms that can be used to resolve a loop in an access network where 7210s are used:

- STP-based access, with or without mVPLS.
- Ethernet APS using G.8032.
- Non-STP-based access using mechanisms such as active/standby links and MC-LAG on the PE.

NOTE: 7210 SAS-K does not support xSTP, G8032 and A/S LAG.

STP-Based Redundant Access to VPLS

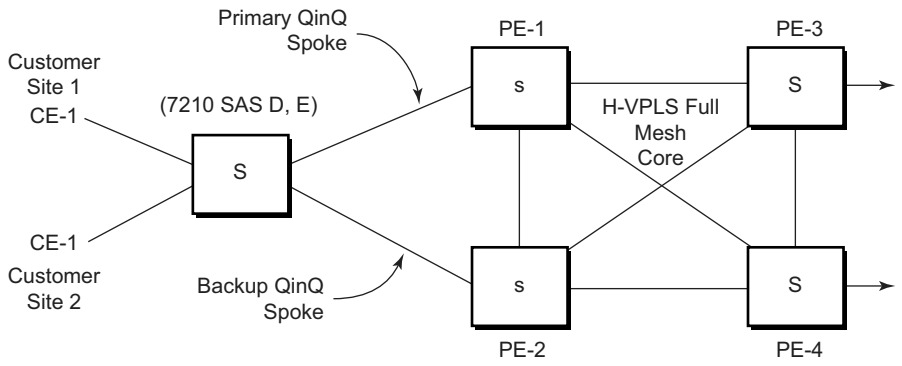


Figure 18: Dual Homed 7210 SAS D, E Acting as MTU-s in Two-Tier Hierarchy H-VPLS

In configuration shown in Figure 18, STP is activated on the MTU and two PEs in order to resolve a potential loop.

In this configuration the scope of STP domain is limited to MTU and PEs, while any topology change needs to be propagated in the whole VPLS domain. When TCN (topology change notification) is received with in the VPLS domain all mACs learned on SAPs are flushed except the SAP on which TCN was received.

VPLS Service Considerations

This section describes various 7210 SAS service features and any special capabilities or considerations as they relate to VPLS services.

SAP Encapsulations

VPLS services are designed to carry Ethernet frame payloads, so it can provide connectivity between any SAPs that pass Ethernet frames. The following SAP encapsulations are supported on the VPLS service on an access port:

- Ethernet null
- Ethernet Dot1q
- Ethernet QinQ (This is supported only on 7210 SAS-D)

The following encapsulations are supported on an access-uplink port:

- Ethernet QinQ

VLAN Processing

The SAP encapsulation definition on Ethernet ingress ports defines which VLAN tags are used to determine the service that the packet belongs:

1. Null encapsulation defined on ingress — Any VLAN tags are ignored and the packet goes to a default service for the SAP.
2. Dot1q encapsulation defined on ingress — Only first VLAN tag is considered.
3. QinQ encapsulation defined on ingress— Both VLAN tags are considered.
   Note that the SAP can be defined with a wildcard for the inner label (for example, “100.*”). In this situation all packets with an outer label of 100 will be treated as belonging to the SAP. If, on the same physical link, there is also a SAP defined with a QinQ encapsulation of 100.1, then traffic with 100.1 will go to that SAP and all other traffic with 100 as the first label will go to the SAP with the *100.* definition.

In situations 2 and 3 above, traffic encapsulated with tags for which there is no definition are discarded.

Support for IP Interface in a VPLS Service

NOTE: 7210 SAS-D and 7210 SAS-K does not support this feature.

The 7210 SAS-E supports host IP interface in a VPLS service. The IP interface is non-rout able and support only IP ping, IP trace-route and management ACLs. SAP ingress QoS policies applied on a SAP in a VPLS service are applicable to the packets destined to the IP interface.

Configuration Notes

1. The system uses the chassis MAC address by default for IP packets originating on the VPLS IP interface. The user is provided with an option to configure a MAC address.
2. The system adds the MAC address for a VPLS IP interface to the Layer 2 forwarding table. The Layer 2 forwarding table is a hash table. In case of hash collisions, the system removes the dynamically learned Layer 2 forwarding entry. If there are multiple such entries installed, the oldest entry is removed. Layer 2 packets will be forwarded as before. If the system is unable to locate a dynamic entry for removal, the IP interface is set to an operational down state. In such a case, the **show router vpls-management interface detail** command, displays **DownReason** as **HashCollision**. Additionally, the system generates a log message of the format MAC address **aa:bb:cc:dd:ee:ff configured for VPLS IP interface <interface-name> resulted in hash collision**. On receiving a log message, it is recommended that the user configure a new MAC address for the IP interface. If the user configured MAC address results in a hash collision, the CLI command fails, allowing the user to try with another MAC address.

Routed VPLS

Routed VPLS (R-VPLS) allows a VPLS instance to be associated with an IES IP interface.

Within an R-VPLS service, traffic with a destination MAC matching that of the associated IP interface is routed based on the IP forwarding table; all other traffic is forwarded based on the VPLS forwarding table.

In access-uplink mode, RVPLS service can be associated with an IPv4 interface and supports only static routing. It is primarily designed for use of in-band management of the node. It allows for inband management of the 7210 nodes in a ring deployment using a single IPv4 subnet, reducing the number of IP subnets needed.

In network mode, RVPLS service can be associated with an IPv4 interface and supports static routing and other routing protocols. It can be used to provide a service to the customer or for inband management of the node.

NOTE: 7210 SAS-E does not support Routed VPLS.

IES IP Interface Binding

A standard IP interface within an existing IES service context may be bound to a service name. A VPLS service only supports binding for a single IP interface.

While an IP interface may only be bound to a single VPLS service, the routing context containing the IP interface (IES) may have other IP interfaces bound to other VPLS service contexts. In other words, Routed VPLS allows the binding of IP interfaces in IES services to be bound to VPLS services.

Assigning a Service Name to a VPLS Service

When a service name is applied to any service context, the name and service ID association is registered with the system. A service name cannot be assigned to more than one service ID. Special consideration is given to a service name that is assigned to a VPLS service that has the "*configure>service>vpls>allow-ip-int-binding*" command is enabled. If a name is applied to the VPLS service while the flag is set, the system scans the existing IES services for an IP interface that is bound to the specified service name. If an IP interface is found, the IP interface is attached to the VPLS service associated with the name. Only one interface can be bound to the specified name.

If the allow-ip-int-binding command is not enabled on the VPLS service, the system does not attempt to resolve the VPLS service name to an IP interface. As soon as the allow-ip-int-binding

flag is configured on the VPLS, the corresponding IP interface is adhered and become operational up. There is no need to toggle the shutdown or no shutdown command.

If an IP interface is not currently bound to the service name used by the VPLS service, no action is taken at the time of the service name assignment.

Service Binding Requirements

In the event that the defined service name is created on the system, the system checks to ensure that the service type is VPLS. If the created service type is VPLS, the IP interface is eligible to enter the operationally upstate. On 7210 SAS-K it is required that the user uses the R-VPLS tag while creating the VPLS service or the service cannot be bound to an IP interface. This is not required for SAS-D.

Bound Service Name Assignment

In the event that a bound service name is assigned to a service within the system, the system first checks to ensure the service type is VPLS. Secondly the system ensures that the service is not already bound to another IP interface through the service name. If the service type is not VPLS or the service is already bound to another IP interface through the service ID, the service name assignment fails.

A single VPLS instance cannot be bound to two separate IP interfaces.

Binding a Service Name to an IP Interface

An IP interface within an IES service context may be bound to a service name at anytime. Only one interface can be bound to a service. When an IP interface is bound to a service name and the IP interface is administratively up, the system scans for a VPLS service context using the name and takes the following actions:

- If the name is not currently in use by a service, the IP interface is placed in an operationally down: Non-existent service name or inappropriate service type state.
- If the name is currently in use by a non-VPLS service or the wrong type of VPLS service, the IP interface is placed in the operationally down: Non-existent service name or inappropriate service type state.
- If the name is currently in use by a VPLS service without the allow-ip-int-binding flag set, the IP interface is placed in the operationally down: VPLS service allow-ip-intbinding flag not set state. There is no need to toggle the shutdown or no shutdown command.

- If the name is currently in use by a valid VPLS service and the allow-ip-int-binding flag is set, the IP interface is eligible to be placed in the operationally up state depending on other operational criteria being met.

IP Interface Attached VPLS Service Constraints

Once a VPLS service has been bound to an IP interface through its service name, the service name assigned to the service cannot be removed or changed unless the IP interface is first unbound from the VPLS service name.

A VPLS service that is currently attached to an IP interface cannot be deleted from the system unless the IP interface is unbound from the VPLS service name.

The allow-ip-int-binding flag within an IP interface attached VPLS service cannot be reset. The IP interface must first be unbound from the VPLS service name to reset the flag.

IP Interface and VPLS Operational State Coordination

When the IP interface is successfully attached to a VPLS service, the operational state of the IP interface is dependent upon the operational state of the VPLS service.

The VPLS service itself remains down until at least one virtual port (SAP, spoke-SDP or Mesh-SDP) is operational.

IP Interface MTU and Fragmentation on 7210 SAS-D

In 7210 SAS-D Access-Uplink mode, VPLS service MTU is not supported. The user must ensure that the port MTU is configured appropriately so that the largest packet traversing through any of the SAPs (virtual ports) of the VPLS service can be forwarded out of any of the SAPs. VPLS services do not support fragmentation and can discard packets larger than the configured port MTU.

When an IP interface is associated with a VPLS service, the IP-MTU is based on either the administrative value configured for the IP interface or an operational value derived from port MTU of all the SAPs configured in the service. The port MTU excluding the Layer 2 Header and tags for all the ports which have SAPs configured in this VPLS service are considered and the minimum value among those are computed (which is called computed MTU). The operational value of the IP interface is set as follows:

- If the configured (administrative) value of IP MTU is greater than the computed MTU, then the operational IP MTU is set to the computed MTU.

- If the configured (administrative) value of IP MTU is lesser than or equal to the computed MTU, then operational IP MTU is set to the configured (administrative) value of IP MTU.

IP Interface MTU and Fragmentation on 7210 SAS-K

The VPLS service is affected by two MTU values; port MTUs and the VPLS service MTU. The MTU on each physical port defines the largest Layer 2 packet (including all DLC headers) that may be transmitted out a port. The VPLS itself has a service level MTU that defines the largest packet supported by the service. The service MTU does not include the local encapsulation overhead for each port (QinQ, Dot1Q, TopQ or SDP service delineation fields and headers) but does include the remainder of the packet. As SAPs are created in the system, the SAPs cannot become operational unless the configured port MTU minus the SAP service delineation overhead is greater than or equal to the configured VPLS service MTU. Thus, an operational SAP is ensured to support the largest packet traversing the VPLS service. The service delineation overhead on each Layer 2 packet is removed before forwarding into a VPLS service. VPLS services do not support fragmentation and must discard any Layer 2 packet larger than the service MTU after the service delineation overhead is removed.

When an IP interface is associated with a VPLS service, the IP-MTU is based on either the administrative value configured for the IP interface or an operational value derived from VPLS service MTU. The operational IP-MTU cannot be greater than the VPLS service MTU minus 14 bytes.

- If the configured (administrative) IP-MTU is configured for a value greater than the normalized IP-MTU, based on the VPLS service-MTU, then the operational IP-MTU is reset to equal the normalized IP-MTU value (VPLS service MTU – 14 bytes).
- If the configured (administrative) IP-MTU is configured for a value less than or equal to the normalized IP-MTU, based on the VPLS service-MTU, then the operational IP-MTU is set to equal the configured (administrative) IP-MTU value.

ARP and VPLS FIB Interactions

Two address-oriented table entries are used when routing into a VPLS service. On the routing side, an ARP entry is used to determine the destination MAC address used by an IP next-hop. In the case where the destination IP address in the routed packet is a host on the local subnet represented by the VPLS instance, the destination IP address itself is used as the next-hop IP address in the ARP cache lookup. If the destination IP address is in a remote subnet that is reached by another router attached to the VPLS service, the routing lookup returns the local IP address on the VPLS service of the remote router is returned. If the next-hop is not currently in the ARP cache, the system generates an ARP request to determine the destination MAC address associated with the

next-hop IP address. IP routing to all destination hosts associated with the next-hop IP address stops until the ARP cache is populated with an entry for the next-hop. The dynamically populated ARP entries age out according to the ARP aging timer.

NOTE: In 7210 SAS-D, static ARP, entries cannot be used. Static ARP is supported on 7210 SAS-K devices.

The second address table entry that affects VPLS routed packets is the MAC destination lookup in the VPLS service context. The MAC associated with the ARP table entry for the IP next-hop may or may not currently be populated in the VPLS Layer 2 FIB table. While the destination MAC is unknown (not populated in the VPLS FIB), the system is flooded with all packets destined to that MAC (routed or bridged) to all SAPs within the VPLS service context. Once the MAC is known (populated in the VPLS FIB), all packets destined to the MAC (routed or bridged) is targeted to the specific SAP where the MAC has been learned. As with ARP entries, static MAC entries may be created in the VPLS FIB. Dynamically learned MAC addresses are allowed to age out or be flushed from the VPLS FIB while static MAC entries always remain associated with a specific virtual port. Dynamic MACs may also be relearned on another VPLS SAP than the current SAP in the FIB. In this case, the system automatically moves the MAC FIB entry to the new VPLS SAP.

NOTES:

- In 7210 SAS-D, whenever a MAC entry is removed from the VPLS FIB (either explicitly by the user or due to MAC aging or mac-move), ARP entries which match this MAC address is removed from the ARP cache. Though the VPLS FIB entries are not removed; an ARP entry ages out and is removed from the ARP cache. This restriction is not applicable to 7210 SAS-K.
- In 7210 SAS-D, if If the VPLS FIB limit is reached and we are no longer able to learn new MAC address, ARP will also not be learnt. This restriction does not apply to 7210 SAS-K.

Routed VPLS Specific ARP Cache Behavior

In typical routing behavior, the system uses the IP route table to select the egress interface, an ARP entry is used forward the packet to the appropriate Ethernet MAC. With routed VPLS, the egress IP interface may be represented by multiple egress (VPLS service SAPs).

The following tables describes how the ARP cache and MAC FIB entry states interact.

Table 16: Routing behavior in RVPLS and interaction ARP Cache and MAC FIB

ARP Cache Entry	MAC FIB Entry	Routing or System behavior
ARP Cache Miss (No Entry)	Known or Unknown	Triggers a request to control plane ARP processing module, to send out an ARP request, out of all the SAPs. (also known as virtual ports) of the VPLS instance.
ARP Cache Hit	Known	Forward to specific VPLS virtual port or SAP.
	Unknown	This behavior cannot happen typically in 7210 SAS-D, as and when a L2 entry is removed from the FDB, the matching MAC address is also removed from the ARP cache. On 7210 SAS-K, the packet is sent out of all the SAPs of the VPLS instance.

The allow-ip-int-binding VPLS Flag

The allow-ip-int-binding flag on a VPLS service context is used to inform the system that the VPLS service is enabled for routing support. The system uses the setting of the flag as a key to determine what type of ports the VPLS service may span.

The system also uses the flag state to define which VPLS features are configurable on the VPLS service to prevent enabling a feature that is not supported when routing support is enabled.

Routed VPLS SAPs only Supported on Standard Ethernet Ports

The allow-ip-int-binding flag is set (routing support enabled) on a VPLS service. SAPs within the service can be created on standard Ethernet ports.

LAG Port Membership Constraints

If a LAG has a non-supported port type as a member, a SAP for the routing-enabled VPLS service cannot be created on the LAG. Once one or more routing enabled VPLS SAPs are associated with a LAG, a non-supported Ethernet port type cannot be added to the LAG membership.

VPLS Feature Support and Restrictions

When the allow-ip-int-binding flag is set on a VPLS service, the following features cannot be enabled (The flag also cannot be enabled while any of these features are applied to the VPLS service). The following restrictions apply to both network mode and access-uplink mode unless called out separately:

- In network mode, SDPs used in spoke or mesh SDP bindings cannot be configured.
- In access-uplink mode, the VPLS service type cannot be M-VPLS.
- In network mode, the VPLS Service type must be 'r-vpls' and any other VPLS service is not allowed.
- MVR from Routed VPLS and to another SAP is not supported.
- Default QinQ SAPs is not supported in R-VPLS service.
- The “allow-ip-int-binding” command cannot be used in a VPLS service which is acting as the G8032 control instance.
- IPv4 filters (ingress and egress) can be used with the R-VPLS SAPs. Additionally IP ingress override filters are supported which affects the behavior of the IP filters attached to the R-VPLS SAPs. Please see below for more information about use of ingress override filters. Ingress override filters are not supported on 7210 SAS-K.
- MAC filters (ingress and egress) are not supported for use with R-VPLS SAPs.
- VPLS IP interface is not allowed in a R-VPLS service. The converse also holds.
- On 7210 SAS-K, during creation of the VPLS service the keyword 'rvpls' must be used. It lets the software know that this is a VPLS service to which an IP interface will be associated.
- In Access-uplink mode, the VPLS service can be configured either access SAP or Access-Uplink SAPs.
- In Access-uplink mode, VPLS service can use the following 'svc-sap-type' values: any, dot1q-preserve and null-star. Only specific SAP combinations are allowed for a given svc-sap-type, except that default QinQ SAPs cannot be used in a R-VPLS service. The allowed SAP combinations are similar to that available in a plain VPLS service and is as given in the table above in the services Chapter (with the exception noted before).
- G8032 or mVPLS/STP based protection mechanism can be used with R-VPLS service. A separate G8032 control instance or a separate mVPLS/STP instance needs to be used and the R-VPLS SAPs needs to be associated with these control instances such that the R-VPLS SAP's forwarding state is driven by the control instance protocols. These protection mechanisms are not supported on 7210 SAS-K.
- IGMP snooping is not supported in a VPLS service. IP multicast is not supported in the R-VPLS service.

- On 7210 SAS-D, DHCP snooping is not supported for the SAPs configured in the routed VPLS service. Instead, DHCP relay can be enabled on the IES service associated with the routed VPLS service. DHCP snooping and DHCP relay is not supported on 7210 SAS-K.
- In network mode, RVPLS SAP drops packets received with extra tags. In other words, if a packet is received on a RVPLS SAP, with number of tags greater than the SAP tags to which it is mapped, then it is dropped. This is true for all supported encapsulations (that is, null, dot1q, and QinQ encapsulations) of the port. For example - Double tagged packets received on a Dot1q SAP configured in a RVPLS service is dropped on ingress.

VPLS SAP Ingress IP Filter Override on 7210 SAS-D

NOTE: 7210 SAS-K does not support Ingress IP filter override.

When an IP Interface is attached to a VPLS service context, the VPLS SAP provisioned IP filter for ingress routed packets may be optionally overridden in order to provide special ingress filtering for routed packets. This allows different filtering for routed packets and non-routed packets. The filter override is defined on the IP interface bound to the VPLS service name. A separate override filter may be specified for IPv4 packet types.

If a filter for a given packet type (IPv4) is not overridden, the SAP specified filter is applied to the packet (if defined).

The following tables lists ACL Lookup behavior with and without Ingress Override filter attached to an IES interface in a R-VPLS service:

Table 17: ACL Lookup behavior with Ingress Override filter attached to an IES interface in a R-VPLS service.

Type of traffic	SAP Ingress IPv4 Filter	SAP Egress IPv4 Filter	Ingress Override IPv4 Filter
Destination MAC != IES IP interface MAC	Yes	Yes	No
Destination MAC = IES IP interface MAC and Destination IP on same subnet as IES interface	No	No	Yes

Table 17: ACL Lookup behavior with Ingress Override filter attached to an IES interface in a R-VPLS service.

Type of traffic	SAP Ingress IPv4 Filter	SAP Egress IPv4 Filter	Ingress Override IPv4 Filter
Destination Mac = IES IP interface mac and destination IP not on same subnet as IES IP interface and route to destination IP does not exist	No	No	No
Destination Mac = IES IP interface mac and destination IP not on same subnet as IES IP interface and route to destination IP exists	No	No	Yes
Destination MAC = IES IP interface MAC and IP TTL = 1	No	No	No
Destination MAC = IES IP interface MAC and IPv4 packet with Options	No	No	No
Destination MAC = IES IP interface MAC and IPv4 Multicast packet	No	No	No

Table 18: ACL Lookup behavior without Ingress Override filter attached to an IES interface in a R-VPLS service

Type of traffic	SAP Ingress IPv4 Filter	SAP Egress IPv4 Filter
Destination MAC != IES IP interface MAC	Yes	Yes
Destination MAC = IES IP interface MAC and Destination IP on same subnet as IES IP interface	Yes	No

Table 18: ACL Lookup behavior without Ingress Override filter attached to an IES interface in a R-VPLS service

Type of traffic	SAP Ingress IPv4 Filter	SAP Egress IPv4 Filter
Destination Mac = IES IP interface mac and destination IP not on same subnet as IES IP interface and route to destination IP does not exist	No	No
Destination Mac = IES IP interface MAC and destination IP not on same subnet as IES IP interface and route to destination IP exists	Yes	No
Destination MAC = IES IP interface MAC and IP TTL = 1	No	No
Destination MAC = IES IP interface MAC and IPv4 packet with Options	No	No
Destination MAC = IES IP interface MAC and IPv4 Multicast packet	No	No

QoS Support for VPLS SAPs and IP interface in a Routed VPLS service

- SAP ingress classification (IPv4 and MAC criteria) is supported for SAPs configured in the service. SAP ingress policies cannot be associated with IES IP interface.
- On 7210 SAS-D, egress port based queuing and shaping are available. It is shared among all the SAPs on the port.
- On 7210 SAS-D, Port based Egress Marking is supported for both routed packets and bridged packets. The existing access egress QoS policy can be used for Dot1p marking and DSCP marking.
- On 7210 SAS-K, per SAP egress queuing, shaping and scheduling is available. Per SAP egress Dot1p marking is supported for both routed packet and bridged packets.
- In Access-Uplink mode, IES IP interface bound to routed VPLS services, IES IP interface on access SAPs and IES IP interface on Access-Uplink SAPs are designed for use with inband management of the node. Consequently, they share a common set of queues for CPU bound management traffic. All CPU bound traffic is policed to pre-defined rates before being queued into CPU queues for application processing. The system uses meters per application or a set of applications. It does not allocate meters per IP interface. The possibility of CPU overloading has been reduced by use of these mechanisms. Users must use appropriate security policies either on the node or in the network to ensure that this does not happen.

Routed VPLS Supported Routing Related Protocols

In network mode and access-uplink mode R-VPLS is supported only in the base routing instance. Only IPv4 addressing support is available for IES interfaces associated with Routed VPLS service. The following lists the support available for routing protocols on IP interfaces bound to a VPLS service in access-uplink mode and network mode.

Table 19: Routing Protocols on IP interfaces bound to a VPLS service.

Services	Access-uplink	Network
Static-routing	Supported	Supported
BGP	Not Supported	Not Supported
OSPF	Not Supported	Supported
ISIS	Not Supported	Supported
BFD	Not Supported	Supported
VRRP	Not Supported	Supported
ARP and Proxy-Arp	ARP is supported	Both are supported

Table 19: Routing Protocols on IP interfaces bound to a VPLS service.

Services	Access-uplink	Network
DHCP Relay (Note-1)	Supported	Supported

NOTE 1: DHCP relay can be configured for the IES interface associated with the Routed VPLS service. DHCP snooping cannot be configured on the VPLS SAPs in the routed VPLS Service.

Spanning Tree and Split Horizon

NOTE: 7210 SAS-K does not support STP (all flavors) protocols.

A routed VPLS context supports all spanning tree and port-based split horizon capabilities that a non-routed VPLS service supports.

Routed VPLS support available and Caveats

Routed VPLS supported functionality and restrictions for both access-uplink and network mode is given below. The following is applicable to both the modes, unless called out explicitly.

- On 7210 SAS-D, static ARP cannot be configured with an IES IP interface that is associated with an R-VPLS, though static MAC can be configured in an R-VPLS service.
- In access-uplink mode, only Static routes are supported. No dynamic routing protocols are supported.
- On 7210 SAS-D, whenever a VPLS FIB entry is removed either due to user action, aging or mac-move, the corresponding ARP entry whose MAC address matches that of the MAC in the FIB is removed from the ARP cache.
- In network mode and access-uplink mode R-VPLS is supported only in the base routing instance. Only IPv4 addressing support is available for IES interfaces associated with Routed VPLS service.
- IPv6 addressing support is not available for IES interface associated with R-VPLS service.
- In network mode, R-VPLS service cannot be bound to an VPRN Service.
- In both network mode and access-uplink mode, multiple SAPs configured on the same port cannot be part of the same R-VPLS Service. In other words, a single service can only be configured with a single SAP on a given port. This restriction does not apply to 7210 SAS-K. In other words, on 7210 SAS-K multiple SAPs configured on the same port can be part of the same service.
- Service MTU configuration is not supported in the R-VPLS service. This does not apply to 7210 SAS-K. In other words, 7210 SAS-K supports service MTU configuration for RVPLS.
- In network mode, in 'any' service (that is, svc-sap-type set to any), null sap accepts only un-tagged packets. Tagged packets received are dropped.
- MPLS protocols (For example: RSVP, LDP) cannot be enabled on R-VPLS IP interface
- MPLS-TP cannot use R-VPLS, IES, and IP interface.
- In network mode, R-VPLS SAPS can be configured on a MC-LAG LAG.

Epipe Emulation using Dot1q VLAN range SAP in VPLS with G8032

NOTE: This feature is supported only on7210 SAS-D (ETR and non-ETR). On the node where the service originates, in addition to the access dot1q range SAP, the service needs to be configured with access-uplink SAPs on the two G.8032 ring ports. G.8032 mechanism is used to for breaking the loop in the ring and VPLS service protection. The intermediate nodes on the ring needs to use VPLS service with access-uplink SAPs on the ring ports and use the same G.8032 instance for protection, as one is used for service protection on the originating node.

The Figure 19 shows how two business offices, served by an operator are connected in a ring network deployment using Dot1q range SAPs and a VPLS service with G.8032 for protection.

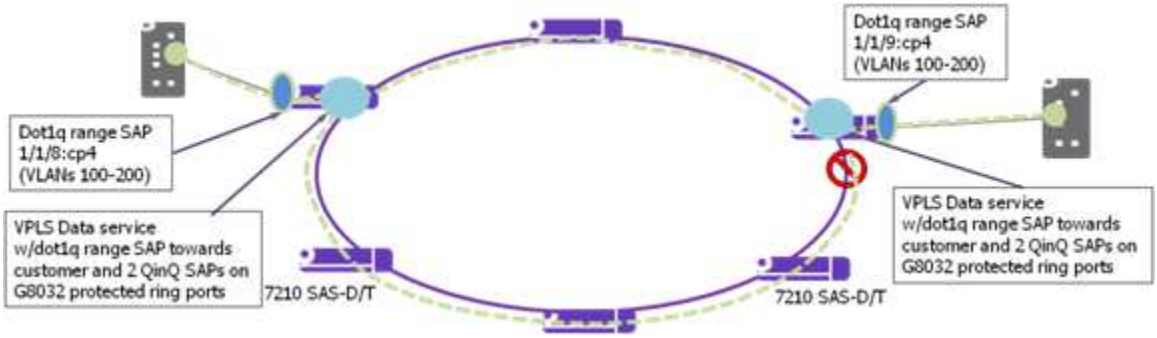


Figure 19: Epipe Emulation in a ring using VPLS with G.8032

The following are the requirements to provide for an Epipe service connectivity between two business sites:

- Transport all the VLANs used by the internal enterprise network of the businesses.
- Support high availability for the service between the business sites by protecting against failure of the links or nodes in the ring.

To achieve connectivity between two business sites in access-uplink/L2 mode is to configure SAPs for each of the individual VLANs used in the enterprise network in a VPLS service and use G.8032 for protection. The number of VLANs that was supported is limited by the number of SAPs supported on the platform.

The 7210 SAS platforms, currently support the use of Dot1q range SAPs with only Epipe services in either network/MPLS mode or access-uplink/L2 mode. Dot1q range SAPs allows operators to transport a range of VLANs by providing similar service treatment (service treatment refers to forwarding decision along with encapsulation used, QoS and ACL processing, accounting, etc.) to

all the VLANs configured in the range. It simplifies service configuration and allows operators to scale the number of VLANs that can be handled by the node. This took care of the need to support hundreds of VLANs using a single SAP or a small number of SAPs. When MPLS the mode is deployed in ring topology, operators have the option of using different redundancy mechanisms such as FRR, primary/secondary LSPs, Active/Standby PWs, to improve Epipe service availability. No such option is available to protect Epipe service in L2 mode when deployed in a ring topology. Additionally many operators prefer G.8032 based ring protection mechanism, since a single control instance on the ring can potentially protect all the VPLS services on the ring.

This feature allows operators to deploy Epipe services in a ring topology when using L2 mode, by emulating an Epipe service using a VPLS service with G8032 protection and at the same time provides the benefits of using dot1q range SAPs. The user should ensure that the VPLS service is a point-to-point service. This is achieved by configuring a VPLS service with an access dot1q range SAP used at the customer handoff on one node in the ring and an access dot1q range SAP in a customer handoff of a VPLS service on another node (that is, at the other end of the Epipe), such that there are only two endpoints for the service in the network.

On the node where the service originates, in addition to the access dot1q range SAP, the service needs to be configured with access-uplink SAPs on the two G.8032 ring ports. G.8032 mechanism is used to for breaking the loop in the ring and VPLS service protection. The intermediate nodes on the ring needs to use VPLS service with access-uplink SAPs on the ring ports and use the same G.8032 instance for protection, as one is used for service protection on the originating node.

Configuration guidelines and restrictions

The VPLS service with dot1-range SAPs use svc-sap-type of dot1q-range and supports limited functionality in comparison to a normal VPLS service, The following paragraph provide more details of the feature functionality, configuration guidelines and restrictions:

- The user can define access dot1q range SAPs, which specifies a group of VLANs which receive similar service treatment, that is, forwarding behavior, SAP ingress QoS treatment and SAP (behavior similar to that available in Epipe service) and allows it to be configured in a VPLS service.
  - → On the node, where the service originates, in addition to the access dot1q range SAP, the service should be configured with Q1.* SAPs on the two G.8032 ring ports. The access or access-uplink Q1.*SAPs can be used, but the access-uplink SAPs are recommended for use.The user cannot configure any other SAPs in the same VPLS service.
  - → There is no special configuration required on intermediate nodes, that is, the ring nodes which do not terminate or originate the service. The nodes should be configured for providing transit VPLS service and the VPLS service must use the same G8032 instance for protection as is used by the service on originating and terminating node.

  - → The Epipe service on 7210, currently does not check if the inner tag received on a Q1.* SAP is within the range of the configured VLANs. VPLS service too has the same behavior.
- Support for SAP Ingress QoS, Ingress and Egress ACLs, accounting, and other services, for dot1q range SAP configured in a VPLS service matches the support available in Epipe service.
- G.8032 mechanism is used for loop detection in ring network and service protection. A separate VPLS service representing the G.8032 control instance must be configured and the state should be associated with this service.
  - → Use of dot1q range SAPs to provide service on the interconnection node, in a G.8032 major-ring/sub-ring deployment, when using the virtual channel, is not supported. This restriction is not applicable when the interconnection node in a G8032 major-ring/sub-ring is configured without a virtual channel.
- mVPLS/xSTP support is available for use with Q1.* SAP on the ring ports to break the loop. This is a add-on to the G.8032 support.
- Broadcast, Unknown Unicast and Multicast (BUM) traffic is flooded in the service.
- Learning is enabled on the service by default, to avoid the need to flood the service traffic out of one of the ring ports, after network MAC addresses are learnt. The user has an option to disable learning per service. Learning enable/disable per SAP is not supported.
- MAC limiting is available per service. MAC limiting per SAP is not supported.
- CFM OAM is supported. The support for UP MEPs on the dot1q range SAP in the service to be used for fault management and performance management using the CFM/Y.1731 OAM tools is available.
  - → Only UP MEP is allowed to be configured only on the dot1q VLAN range SAPs. CFM/Y.1731 tools can be used for trouble shooting and performance measurements. User must pick a VLAN value from the range of VLANs configured for the dot1-range SAP using the CLI command config>eth-cfm>domain>association>bridge-identifier VLAN and enable the use of using the CLI command primary-vlan-enable under the MEP CLI context. It is used as the VLAN tag in the packet header for all the CFM/Y.1731 messages sent out in the context of the UP MEP.
  - → Down MEPs and MIPs are not allowed to be configured.
  - → Fault propagation is not supported with UP MEPs for dot1q range SAP in access-uplink mode.
- CFM support is not available for SAPs on the ring ports.
- IGMP snooping and MVR is not supported.

Configuring a VPLS Service with CLI

This section provides information to configure VPLS services using the command line interface.

Topics in this section include:

Basic Configuration

The following fields require specific input (there are no defaults) to configure a basic VPLS service:

- Customer ID (refer to Configuring Customers on page 59)
- For a local service, configure two SAPs, specifying local access ports and encapsulation values.

The following example displays a sample configuration of a local VPLS service on ALA-1.

The **svc-sap-type** option must be specified at service creation. The default option is **null-star**. The following example displays a configuration of a local VPLS service with a null-star SAP type on ALA-1. This service comprises of a null access SAP and an Uplink LAG SAP.

```
*A:ALA-1>config>service# info
----------------------------------------------
...
       vpls 7 customer 7 create
            stp
                shutdown
            exit
            sap 1/1/21 create
            exit
            sap lag-1:700 create
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-1>config>service#
```

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure both local VPLS services and provides the CLI commands.

For VPLS services:

1. Associate VPLS service with a customer ID
2. Define SAPs:
   - Select node(s) and port(s)
   - Optional — Select QoS policies other than the default (configured in `config>qos` context)
   - Optional — Select filter policies (configured in `config>filter` context)
   - Optional — Select accounting policy (configured in `config>log` context)
3. Modify STP default parameters (optional) (see VPLS and Spanning Tree Protocol on page 175)
4. Enable service

Configuring VPLS Components

Use the CLI syntax displayed below to configure the following entities:

Creating a VPLS Service

Use the following CLI syntax to create a VPLS service (for 7210 SAS-E):

```
config>service# vpls service-id [customer customer-id] [cre-
   ate] [vpn <vpn-id>] [m-vpls] [svc-sap-type {null-
   star|dot1q|dot1q-preserve}] [customer-vid <vlan-id>]
```

The following example displays a VPLS configuration (for 7210 SAS-E):

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
...
        vpls 1000 customer 1 create
            description "This is a VPLS with NULL SAP"
            stp
                shutdown
            exit
            no shutdown
        exit
        vpls 2000 customer 6 svc-sap-type dot1q create
            description "This is a Distributed VPLS with DOT1Q SAP"
            stp
                shutdown
            exit
            no shutdown
        exit
        vpls 3000 customer 8 svc-sap-type dot1q-preserve customer-vid 300 create
            description "This is a VPLS with QinQ Uplink SAP"
            stp
                shutdown
            exit
            no shutdown
        exit
...
----------------------------------------------
*A:ALA-1>config>service>vpls#
```

Use the following CLI syntax to create a VPLS service (for 7210 SAS-D):

CLI Syntax: `config>service# vpls service-id [customer customer-id] [create] [vpn <vpn-id>] [m-vpls] [svc-sap-type {null-star|dot1q-preserve|any }] [customer-vid <vlan-id>]`

The following example displays a VPLS configuration (for 7210 SAS-D):

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
     ...
         vpls 1000 customer 1 create
              description "This is a VPLS with NULL SAP"
              stp
                   shutdown
              exit
              no shutdown
```

```
            exit
            vpls 2000 customer 6 svc-sap-type any create
                 description "This is a Distributed VPLS with ANY SAP"
                 stp
                      shutdown
                 exit
                 no shutdown
            exit
            vpls 3000 customer 8 svc-sap-type dot1q-preserve customer-vid 300 create
                 description "This is a VPLS with QinQ Uplink SAP"
                 stp
                      shutdown
                 exit
                 no shutdown
            exit
       ...
-----------------------------------------------
*A:ALA-1>config>service>vpls#
```

Enabling MAC Move

The **mac-move** feature is useful to protect against undetected loops in your VPLS topology as well as the presence of duplicate MACs in a VPLS service. For example, if two clients in the VPLS have the same MAC address, the VPLS will experience a high re-learn rate for the MAC and will shut down the SAP when the threshold is exceeded.

Use the following CLI syntax to configure **mac-move** parameters.

CLI Syntax: `config>service# vpls service-id [customer customer-id] [vpn vpn-id] [m-vpls]`

```
            mac-move
               move-frequency frequency
               retry-timeout timeout
               no shutdown
```

The following example displays mac-move information.

```
*A:ALA-1# show service id 6 all
....
*A:ALA-1#
-------------------------------------------------------------------------------
Forwarding Database specifics
-------------------------------------------------------------------------------
Service Id        : 1150                Mac Move          : Disabled
Mac Move Rate     : 2                   Mac Move Timeout  : 10
Table Size        : 1000                Total Count       : 1000
Learned Count     : 1000                Static Count      : 0
Remote Age        : 900                 Local Age         : 300
High WaterMark    : 95%                 Low Watermark     : 90%
Mac Learning      : Enabl               Discard Unknown   : Dsabl
Mac Aging         : Enabl               Relearn Only      : True
===============================================================================
....
*A:ALA-1#
```

Configuring STP Bridge Parameters in a VPLS

Modifying some of the Spanning Tree Protocol parameters allows the operator to balance STP between resiliency and speed of convergence extremes. Modifying particular parameters, mentioned below, must be done in the constraints of the following two formulae:

2 x (*Bridge_Forward_Delay* - 1.0 seconds) >= *Bridge_Max_Age*
Bridge_Max_Age >= 2 x (*Bridge_Hello0_Time* + 1.0 seconds)

The following STP parameters can be modified at VPLS level:

- Bridge STP Admin State on page 212
- Mode on page 213
- Bridge Priority on page 213
- Max Age on page 214
- Forward Delay on page 214
- Hello Time on page 215
- MST Instances on page 216
- MST Max Hops on page 216
- MST Name on page 216
- MST Revision on page 216

STP always uses the locally configured values for the first three parameters (Admin State, Mode and Priority).

For the parameters Max Age, Forward Delay, Hello Time and Hold Count, the locally configured values are only used when this bridge has been elected root bridge in the STP domain, otherwise the values received from the root bridge are used. The exception to this rule is: when STP is running in RSTP mode, the Hello Time is always taken from the locally configured parameter. The other parameters are only used when running mode MSTP.

Bridge STP Admin State

The administrative state of STP at the VPLS level is controlled by the shutdown command.

When STP on the VPLS is administratively disabled, any BPDUs are forwarded transparently through the 7210 SAS D, E. When STP on the VPLS is administratively enabled, but the administrative state of a SAP is down, BPDUs received on such a SAP are discarded.

CLI Syntax:
```
config>service>vpls service-id# stp
  no shutdown
```

Mode

To be compatible with the different iterations of the IEEE 802.1D standard, the 7210 SAS D, E support several variants of the Spanning Tree protocol:

- `rstp` — Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1D-2004 - default mode.
- `dot1w` — Compliant with IEEE 802.1w.
- `comp-dot1w` — Operation as in RSTP but backwards compatible with IEEE 802.1w (this mode was introduced for interoperability with some MTU types).
- `mstp` — Compliant with the Multiple Spanning Tree Protocol specified in IEEE 802.1Q REV/D5.0-09/2005. This mode of operation is only supported in an mVPLS.

See section Spanning Tree Operating Modes on page 175 for details on these modes.

CLI Syntax: `config>service>vpls` *`service-id`*`# stp`
`mode {rstp | comp-dot1w | dot1w | mstp}`
Default: `rstp`

Bridge Priority

The **bridge-priority** command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDU between messages received and sent.

All values will be truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

CLI Syntax: `config>service>vpls` *`service-id`*`# stp`
`priority` *`bridge-priority`*
Range: 1 to 65535
Default: 32768
Restore Default: `no priority`

Max Age

The **max-age** command indicates how many hops a BPDU can traverse the network starting from the root bridge. The message age field in a BPDU transmitted by the root bridge is initialized to 0. Each other bridge will take the message_age value from BPDUs received on their root port and increment this value by 1. The message_age thus reflects the distance from the root bridge. BPDUs with a message age exceeding max-age are ignored.

STP uses the max-age value configured in the root bridge. This value is propagated to the other bridges by the BPDUs.
The default value of **max-age** is 20. This parameter can be modified within a range of 6 to 40, limited by the standard STP parameter interaction formulae.

CLI Syntax: `config>service>vpls` *`service-id#`* `stp`
`max-age` *`max-info-age`*
Range: 6 to 40 seconds
Default: 20 seconds
Restore Default: `no max-age`

Forward Delay

RSTP, as defined in the IEEE 802.1D-2004 standards, will normally transition to the forwarding state by a handshaking mechanism (rapid transition), without any waiting times. If handshaking fails (e.g. on shared links, see below), the system falls back to the timer-based mechanism defined in the original STP (802.1D-1998) standard.

A shared link is a link with more than two Ethernet bridges (for example, a shared 10/100BaseT segment). The `port-type` command is used to configure a link as point-to-point or shared (see section SAP Link Type on page 223).

For timer-based transitions, the 802.1D-2004 standard defines an internal variable forward-delay, which is used in calculating the default number of seconds that a SAP spends in the discarding and learning states when transitioning to the forwarding state. The value of the forward-delay variable depends on the STP operating mode of the VPLS instance:

- in `rstp` mode, but only when the SAP has not fallen back to legacy STP operation, the value configured by the **hello-time** command is used;
- in all other situations, the value configured by the **forward-delay** command is used.

CLI Syntax: `config>service>vpls` *`service-id#`* `stp`
`forward-delay` *`seconds`*
Range: 4 to 30 seconds
Default: 15 seconds
Restore Default: `no forward-delay`

Hello Time

The **hello-time** command configures the Spanning Tree Protocol (STP) hello time for the Virtual Private LAN Service (VPLS) STP instance.

The *seconds* parameter defines the default timer value that controls the sending interval between BPDU configuration messages by this bridge, on ports where this bridge assumes the designated role.

The active hello time for the spanning tree is determined by the root bridge (except when the STP is running in RSTP mode, then the hello time is always taken from the locally configured parameter).

The configured hello-time value can also be used to calculate the bridge forward delay, see Forward Delay on page 214.

CLI Syntax: `config>service>vpls` *`service-id#`* `stp`
`hello-time` *`hello-time`*
Range: 1 to 10 seconds
Default: 2 seconds
Restore Default: `no hello-time`

Hold Count

The **hold-count** command configures the peak number of BPDUs that can be transmitted in a period of one second.

CLI Syntax: `config>service>vpls` *`service-id#`* `stp`
`hold-count` *`count-value`*
Range: 1 to 10
Default: 6
Restore Default: `no hold-count`

MST Instances

You can create up to 15 MST-instances. They can range from 1 to 4094. By changing path-cost and priorities, you can make sure that each instance will form it's own tree within the region, thus making sure different VLANs follow different paths.

You can assign non overlapping VLAN ranges to each instance. VLANs that are not assigned to an instance are implicitly assumed to be in instance 0, which is also called the CIST. This CIST cannot be deleted or created.

The parameter that can be defined per instance are mst-priority and vlan-range.

- mst-priority — The bridge-priority for this specific mst-instance. It follows the same rules as bridge-priority. For the CIST, the bridge-priority is used.
- vlan-range — The VLANs are mapped to this specific mst-instance. If no VLAN-ranges are defined in any mst-instances, then all VLANs are mapped to the CIST.

MST Max Hops

The mst-max-hops command defines the maximum number of hops the BPDU can traverse inside the region. Outside the region max-age is used.

MST Name

The MST name defines the name that the operator gives to a region. Together with MST revision and the VLAN to MST-instance mapping, it forms the MST configuration identifier. Two bridges that have the same MST configuration identifier form a region if they exchange BPDUs.

MST Revision

The MST revision together with MST-name and VLAN to MST-instance mapping define the MST configuration identifier. Two bridges that have the same MST configuration identifier form a region if they exchange BPDUs.

Configuring a VPLS SAP

A default QoS policy is applied to each ingress SAP. Additional QoS policies can be configured in the **config**>**qos** context. There are no default filter policies. Filter policies are configured in the **config**>**filter** context and must be explicitly applied to a SAP.

Use the following CLI syntax to create:

- Local VPLS SAPs on page 217

Local VPLS SAPs

To configure a local VPLS service, enter the **sap** *sap-id* command twice with different port IDs in the same service configuration.

```
*A:ALA-1>config>service# info
----------------------------------------------
        vpls 1000 customer 1 create
            description "This is a Local VPLS with NULL SAP"
            stp
                shutdown
            exit
            sap 1/1/1 create
            exit
            sap 1/1/2 create
            exit
            sap 1/1/3:500.* create
            exit
            no shutdown
        exit
        vpls 2000 customer 6 create
            description "This is a Local VPLS with DOT1Q SAP"
            stp
                shutdown
            exit
            sap 1/1/4:100 create
            exit
            sap 1/1/5:200 create
            exit
            sap 1/1/3:900.* create
            exit
            no shutdown
        exit
        vpls 3000 customer 8 create
            description "This is a Local VPLS"
            stp
                shutdown
            exit
            sap 1/1/4:300 create
            exit
            sap 1/1/5:300 create
            exit
            sap 1/1/3:1200 create
            exit
```

```
            no shutdown
        exit
-----------------------------------------------
*A:ALA-1>config>service#
```

Configuring Default QinQ SAPs to Pass all Traffic from Access to Access-uplink Port without any Tag Modifications

The following example displays the VPLS SAP configuration of Default QinQ SAPs:

```
ALA-1>config>service# vpls 9 customer 1 svc-sap-type null-star create
            shutdown
            stp
                shutdown
            exit
            sap 1/1/5:*.* create
                statistics
                    ingress
                        received-count
                    exit
                exit
            exit
            sap 1/1/6:*.* create
                statistics
                    ingress
                        received-count
                    exit
                exit
            exit
        exit
```

Configuring SAP-Specific STP Parameters

When a VPLS has STP enabled, each SAP within the VPLS has STP enabled by default. The operation of STP on each SAP is governed by:

- SAP STP Administrative State on page 220
- SAP Virtual Port Number on page 221
- SAP Priority on page 221
- SAP Path Cost on page 222
- SAP Edge Port on page 222
- SAP Auto Edge on page 223
- SAP Link Type on page 223
- MST Instances on page 223

SAP STP Administrative State

The administrative state of STP within a SAP controls how BPDUs are transmitted and handled when received. The allowable states are:

- SAP Admin Up

  The default administrative state is *up* for STP on a SAP. BPDUs are handled in the normal STP manner on a SAP that is administratively up.

- SAP Admin Down

  An administratively down state allows a service provider to prevent a SAP from becoming operationally blocked. BPDUs will not originate out the SAP towards the customer.

  If STP is enabled on VPLS level, but disabled on the SAP, received BPDUs are discarded. Discarding the incoming BPDUs allows STP to continue to operate normally within the VPLS service while ignoring the down SAP. The specified SAP will always be in an operationally forwarding state.

  NOTE: The administratively down state allows a loop to form within the VPLS.

CLI Syntax: `config>service>vpls>sap>stp#`
`[no] shutdown`
Range: `shutdown` or `no shutdown`
Default: `no shutdown` (SAP admin up)

SAP Virtual Port Number

The virtual port number uniquely identifies a SAP within configuration BPDUs. The internal representation of a SAP is unique to a system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a SAP and identifies it with it's own virtual port number that is unique to every other SAP defined on the VPLS. The virtual port number is assigned at the time that the SAP is added to the VPLS.

Since the order in which SAPs are added to the VPLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance. To achieve consistency after a reboot, the virtual port number can be specified explicitly.

CLI Syntax: `config>service>vpls>sap# stp`
`port-num` *`number`*
Range: 1 — 2047
Default: (automatically generated)
Restore Default: `no port-num`

SAP Priority

SAP priority allows a configurable "tie breaking" parameter to be associated with a SAP. When configuration BPDUs are being received, the configured SAP priority will be used in some circumstances to determine whether a SAP will be designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16 bit value. In the latest STP standard (802.1D-2004) only the upper 4 bits of the port priority field are used to encode the SAP priority. The remaining 4 bits are used to extend the port ID field into a 12 bit virtual port number field. The virtual port number uniquely references a SAP within the STP instance. See SAP Virtual Port Number on page 221 for details on the virtual port number.

STP computes the actual SAP priority by taking the configured priority value and masking out the lower four bits. The result is the value that is stored in the SAP priority parameter. For example, if a value of 0 was entered, masking out the lower 4 bits would result in a parameter value of 0. If a value of 255 was entered, the result would be 240.

The default value for SAP priority is 128. This parameter can be modified within a range of 0 to 255, 0 being the highest priority. Masking causes the values actually stored and displayed to be 0 to 240, in increments of 16.

CLI Syntax: `config>service>vpls>sap>stp#`
`priority` *`stp-priority`*
Range: 0 to 255 (240 largest value, in increments of 16)
Default: 128
Restore Default: `no priority`

SAP Path Cost

The SAP path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremental with the configured path cost for that SAP. When BPDUs are sent out other egress SAPs, the newly calculated root path cost is used.

STP suggests that the path cost is defined as a function of the link bandwidth. Since SAPs are controlled by complex queuing dynamics, in the 7210 SAS D, E the STP path cost is a purely static configuration.

The default value for SAP path cost is 10. This parameter can be modified within a range of 1 to 65535, 1 being the lowest cost.

CLI Syntax: `config>service>vpls>sap>stp#`
`path-cost` *`sap-path-cost`*
Range: 1 to 200000000
Default: 10
Restore Default: `no path-cost`

SAP Edge Port

The SAP `edge-port` command is used to reduce the time it takes a SAP to reach the forwarding state when the SAP is on the edge of the network, and thus has no further STP bridge to handshake with.

The `edge-port` command is used to initialize the internal OPER_EDGE variable. At any time, when OPER_EDGE is false on a SAP, the normal mechanisms are used to transition to the forwarding state (see Forward Delay on page 214). When OPER_EDGE is true, STP assumes that the remote end agrees to transition to the forwarding state without actually receiving a BPDU with an agreement flag set.

The OPER_EDGE variable will dynamically be set to false if the SAP receives BPDUs (the configured edge-port value does not change). The OPER_EDGE variable will dynamically be set to true if auto-edge is enabled and STP concludes there is no bridge behind the SAP.

When STP on the SAP is administratively disabled and re-enabled, the OPER_EDGE is re-initialized to the value configured for edge-port.

Valid values for SAP edge-port are enabled and disabled with disabled being the default.

CLI Syntax: `config>service>vpls>sap>stp#`
`[no] edge-port`
Default: `no edge-port`

SAP Auto Edge

The SAP **edge-port** command is used to instruct STP to dynamically decide whether the SAP is connected to another bridge.

If auto-edge is enabled, and STP concludes there is no bridge behind the SAP, the OPER_EDGE variable will dynamically be set to true. If auto-edge is enabled, and a BPDU is received, the OPER_EDGE variable will dynamically be set to true (see SAP Edge Port on page 222).

Valid values for SAP auto-edge are enabled and disabled with enabled being the default.

CLI Syntax: `config>service>vpls>sap>stp#`
`[no] auto-edge`
Default: `auto-edge`

SAP Link Type

The SAP **link-type** parameter instructs STP on the maximum number of bridges behind this SAP. If there is only a single bridge, transitioning to forwarding state will be based on handshaking (fast transitions). If more than two bridges are connected by a shared media, their SAPs should all be configured as shared, and timer-based transitions are used.

Valid values for SAP link-type are shared and pt-pt with pt-pt being the default.

CLI Syntax: `config>service>vpls>sap>stp#`
`link-type {pt-pt|shared}`
Default: `link-type pt-pt`
Restore Default: `no link-type`

MST Instances

The SAP mst-instance command is used to create MST instances at the SAP level. MST instance at a SAP level can be created only if MST instances are defined at the service level.

The parameters that can be defined per instance are mst-path-cost and mst-port-priority.

- mst-path-cost — Specifies path-cost within a given MST instance. The path-cost is proportional to link speed.
- mst-port-priority — Specifies the port priority within a given MST instance.

STP SAP Operational States

The operational state of STP within a SAP controls how BPDUs are transmitted and handled when received. Defined states are:

- Operationally Disabled on page 224
- Operationally Discarding on page 224
- Operationally Learning on page 224
- Operationally Forwarding on page 225

Operationally Disabled

Operationally disabled is the normal operational state for STP on a SAP in a VPLS that has any of the following conditions:

- VPLS state administratively down
- SAP state administratively down
- SAP state operationally down

If the SAP enters the operationally up state with the STP administratively up and the SAP STP state is up, the SAP will transition to the STP SAP discarding state.

When, during normal operation, the router detects a downstream loop behind a SAP, BPDUs can be received at a very high rate. To recover from this situation, STP will transition the SAP to disabled state for the configured forward-delay duration.

Operationally Discarding

A SAP in the discarding state only receives and sends BPDUs, building the local proper STP state for each SAP while not forwarding actual user traffic. The duration of the discarding state is explained in section Forward Delay on page 214.

Note: in previous versions of the STP standard, the discarding state was called a blocked state.

Operationally Learning

The learning state allows population of the MAC forwarding table before entering the forwarding state. In this state, no user traffic is forwarded.

Operationally Forwarding

Configuration BPDUs are sent out a SAP in the forwarding state. Layer 2 frames received on the SAP are source learned and destination forwarded according to the FIB. Layer 2 frames received on other forwarding interfaces and destined for the SAP are also forwarded.

SAP BPDU Encapsulation State

STP is associated with a VPLS service like PVST is associated per VLAN. The main difference resides in the Ethernet and LLC framing and a type-length-value (TLV) field trailing the BPDU.

IEEE 802.1d (referred as dot1d) and Cisco's per VLAN Spanning Tree (PVST) BPDU encapsulations are supported on a per SAP basis. The STP is associated with a VPLS service like PVST is per VLAN. The difference between the two encapsulations is in the Ethernet and LLC framing and a type-length-value (TLV) field trailing the BPDU.The encapsulation format cannot be configured by the user,the system automatically determines the encapsulation format based on the BPDUs received on the port.

The following table shows differences between Dot1d and PVST Ethernet BPDU encapsulations based on the interface encap-type field:

Table 20: SAP BPDU Encapsulation States

Field	dot1d encap-type null	dot1d encap-type dot1q	PVST encap-type null	PVST encap-type dot1q
Destination MAC	01:80:c2:00:00:00	01:80:c2:00:00:00	N/A	01:00:0c:cc:cc:cd
Source MAC	Sending Port MAC	Sending Port MAC	N/A	Sending Port MAC
EtherType	N/A	0x81 00	N/A	0x81 00
Dot1p and CFI	N/A	0xe	N/A	0xe
Dot1q	N/A	VPLS SAP ID	N/A	VPLS SAP encap value
Length	LLC Length	LLC Length	N/A	LLC Length
LLC DSAP SSAP	0x4242	0x4242	N/A	0xaaaa (SNAP)
LLC CNTL	0x03	0x03	N/A	0x03
SNAP OUI	N/A	N/A	N/A	00 00 0c (Cisco OUI)
SNAP PID	N/A	N/A	N/A	01 0b
CONFIG	Standard 802.1d	Standard 802.1d	N/A	Standard 802.1d

Table 20: SAP BPDU Encapsulation States (Continued)

TLV: Type & Len	N/A	N/A	N/A	58 00 00 00 02
TLV: VLAN	N/A	N/A	N/A	VPLS SAP encap value
Padding	As Required	As Required	N/A	As Required

Each SAP has a Read-Only operational state that shows which BPDU encapsulation is currently active on the SAP. The states are:

- Dot1d — This state specifies that the switch is currently sending IEEE 802.1d standard BPDUs. The BPDUs are tagged or non-tagged based on the encapsulation type of the egress interface and the encapsulation value defined in the SAP. A SAP defined on an interface with encapsulation type Dot1q continues in the dot1d BPDU encapsulation state until a PVST encapsulated BPDU is received. When a PVST-encapsulated BPDU is received, the SAP converts to the PVST encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged, if the interface encapsulation type is defined as dot1q. PVST BPDUs are silently discarded, if received, when the SAP is on an interface defined with encapsulation type null.
- PVST — This state specifies that the switch is currently sending proprietary encapsulated BPDUs. PVST BPDUs are only supported on Ethernet interfaces with the encapsulation type set to dot1q. The SAP continues in the PVST BPDU encapsulation state until a dot1d encapsulated BPDU is received.When a dot1d-encapsulated BPDU is received,the SAP reverts to the dot1d encapsulation state. Each received BPDU must be properly IEEE 802.1q tagged with the encapsulation value defined for the SAP. PVST BPDUs are silently discarded, if received, when the SAP is on an interface defined with a null encapsulation type.

Dot1d is the initial and only SAP BPDU encapsulation state for SAPs defined on Ethernet interface with encapsulation type set to null.

per service

Configuring VPLS Redundancy

This section discusses the following service management tasks:

- Creating a Management VPLS for SAP Protection on page 227

Creating a Management VPLS for SAP Protection

This section provides a brief overview of the tasks that must be performed to configure a management VPLS for SAP protection and provides the CLI commands, see Figure 20. The tasks below should be performed on both nodes providing the protected VPLS service.

1. Create an access uplink SAPs to the peer node.
2. Create a management VPLS.
3. Define a SAP in the m-vpls on the port towards the 7210 SAS D, E. Note that the port must be dot1q. The SAP corresponds to the (stacked) VLAN on the 7210 SAS D, E in which STP is active.
4. Optionally modify STP parameters for load balancing.
5. Create access uplink SAPs in the m-vpls using the access uplink SAPs defined in Step 1.
6. Enable the management VPLS service and verify that it is operationally up.
7. Create a list of VLANs on the port that are to be managed by this management VPLS.
8. Create one or more user VPLS services with SAPs on VLANs in the range defined by Step 6.

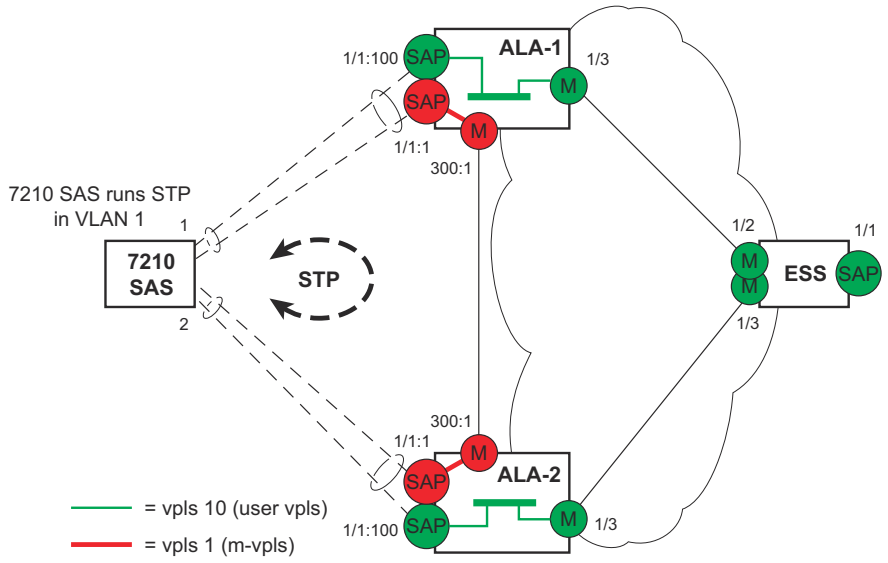


Figure 20: Example Configuration for Protected VPLS SAP

CLI Syntax: `config>service# vpls service-id [customer customer-id] [create] [m-vpls]`

```
            description description-string
            sap sap-id create
               managed-vlan-list
                  range vlan-range
                     stp
                     no shutdown
```

The following example displays a VPLS configuration:

```
*A:ALA-1>config>service# info
----------------------------------------------
        vpls 2000 customer 6 m-vpls create
            stp
                no shutdown
            exit
            sap 1/1/1:100 create
            exit
            sap 1/1/2:200 create
            exit
            sap 1/1/3:300 create
               managed-vlan-list
                  range 1-50
            exit
            no shutdown
        exit
----------------------------------------------
*A:ALA-1>config>service#
```

Configuring Load Balancing with Management VPLS

With the concept of management VPLS, it is possible to load balance the user VPLS services across the two protecting nodes. This is done by creating two management VPLS instances, where both instances have different active QinQ SAPs (by changing the STP path-cost). When different user VPLS services are associated with either the two management VPLS services, the traffic will be split across the two QinQ SAPs. Load balancing can be achieved in SAP protection scenarios.

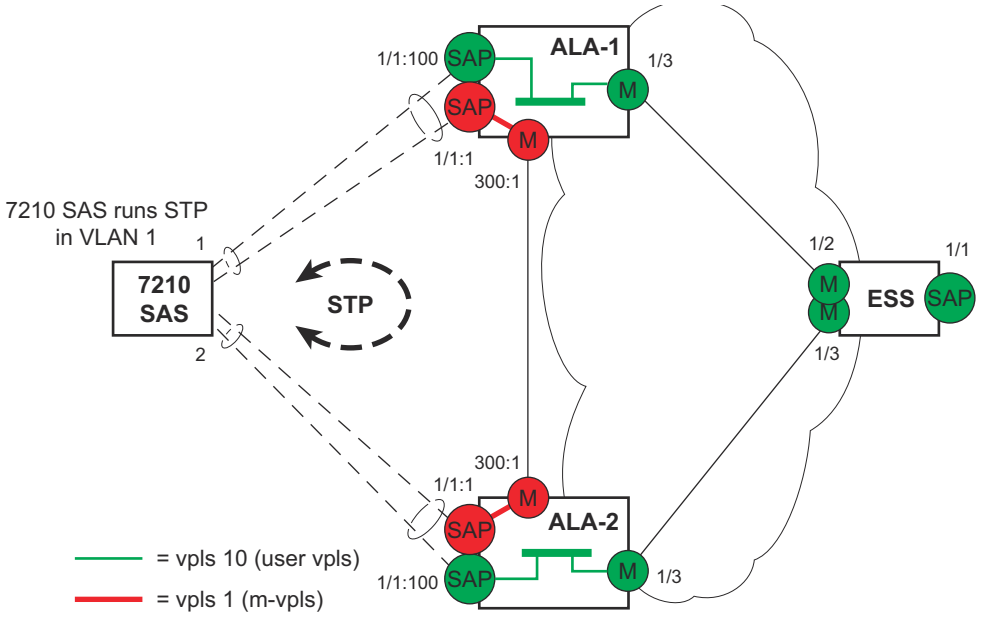


Figure 21: Example Configuration for Load Balancing Across with Management VPLS

Note: the STP path costs in each peer node should be reversed.

CLI Syntax: (for 7210 SAS-E) `config>service# vpls` *`service-id`* `[customer` *`customer-id`*`] [create] [m-vpls] [svc-sap-type {null-star | dot1q | dot1q-preserve}] [customer-vid vlan-id]`

```
            description description-string
            sap sap-id create
               managed-vlan-list
                  range vlan-range
            stp
            no shutdown
```

CLI Syntax: (for 7210 SAS-D)`config>service# vpls service-id [customer customer-id] [create][m-vpls] [svc-sap-type {null-star | any | dot1q-preserve}] [customer-vid vlan-id]`

```
            description description-string
            sap sap-id create
               managed-vlan-list
```

```
                    range vlan-range
                stp
                no shutdown
```

The following example displays a VPLS configuration (for 7210 SAS-E):

```
*A:ALA-1>config>service# info
----------------------------------------------
        vpls 100 customer 1 m-vpls svc-sap-type dot1q create
            stp
                no shutdown
            exit
            sap 1/1/2:100.* create
                managed-vlan-list
                    range 1-10
                exit
                stp
                    path-cost 1
                exit
            exit
            sap 1/1/3:500.* create
                shutdown
                managed-vlan-list
                    range 1-10
                exit
            exit
            no shutdown
        exit
        vpls 200 customer 6 m-vpls svc-sap-type dot1q create
            stp
                no shutdown
            exit
            sap 1/1/2:1000.* create
                managed-vlan-list
                    range 110-200
                exit
            exit
            sap 1/1/3:2000.* create
                managed-vlan-list
                    range 110-200
                exit
                stp
                    path-cost 1
                exit
            exit
            no shutdown
        exit
        vpls 101 customer 1 svc-sap-type dot1q create
            stp
                shutdown
            exit
            sap 1/1/1:100 create
            exit
            sap 1/1/2:1.* create
            exit
            sap 1/1/3:1.* create
            exit
            no shutdown
        exit
        vpls 201 customer 1 svc-sap-type dot1q create
```

```
            stp
                shutdown
            exit
            sap 1/1/1:200 create
            exit
            sap 1/1/2:110.* create
            exit
            sap 1/1/3:110.* create
            exit
            no shutdown
        exit
-----------------------------------------------

*A:ALA-1>config>service#
```

```
PE134>config>service>vpls>bgp-ad#
 [no] pw-template-bi* - Configure pw-template bind policy
 [no] route-target    - Configure route target
 [no] shutdown        - Administratively enable/disable BGP auto-discovery
      vpls-id         - Configure VPLS-ID
 [no] vsi-export      - VSI export route policies
      vsi-id         + Configure VSI-id
 [no] vsi-import      - VSI import route policies
```

Service Management Tasks

This section discusses the following service management tasks:

Modifying VPLS Service Parameters

You can change existing service parameters. The changes are applied immediately.
To display a list of services, use the **show service service-using vpls** command. Enter the parameter such as description SAP and then enter the new information.

The following displays a modified VPLS configuration.

```
*A:ALA-1>config>service>vpls# info
----------------------------------------------
            description "This is a different description."
            disable-learning
            disable-aging
            discard-unknown
            local-age 500
            stp
                shutdown
            exit
            sap 1/1/5:22 create
                description "VPLS SAP"
            exit
            exit
            no shutdown
----------------------------------------------
*A:ALA-1>config>service>vpls#
```

Modifying Management VPLS Parameters

To modify the range of VLANs on an access port that are to be managed by an existing management VPLS, first the new range should be entered and afterwards the old range removed. If the old range is removed before a new range is defined, all customer VPLS services in the old range will become unprotected and may be disabled.

CLI Syntax:
```
config>service# vpls service-id
     sap sap-id
        managed-vlan-list
           [no] range vlan-range
```

Deleting a Management VPLS

As with normal VPLS service, a management VPLS cannot be deleted until SAPs are unbound (deleted), interfaces are shutdown, and the service is shutdown on the service level.

Use the following CLI syntax to delete a management VPLS service:

CLI Syntax:
```
config>service
  [no] vpls service-id
     shutdown
     [no] sap sap-id
        shutdown
```

Disabling a Management VPLS

You can shut down a management VPLS without deleting the service parameters.

When a management VPLS is disabled, all associated user VPLS services are also disabled (to prevent loops). If this is not desired, first un-manage the user's VPLS service by removing them from the managed-vlan-list.

CLI Syntax:
```
config>service
   vpls service-id
      shutdown
```

Example:
```
config>service# vpls 1
config>service>vpls# shutdown
config>service>vpls# exit
```

Deleting a VPLS Service

A VPLS service cannot be deleted until SAPs are unbound (deleted), interfaces are shutdown, and the service is shutdown on the service level.

Use the following CLI syntax to delete a VPLS service:

CLI Syntax:
```
config>service
  [no] vpls service-id
     shutdown
     sap sap-id
     no sap sap-id
        shutdown
```

Disabling a VPLS Service

You can shut down a VPLS service without deleting the service parameters.

CLI Syntax:
```
config>service> vpls service-id
  [no] shutdown
```

Example:
```
config>service# vpls 1
config>service>vpls# shutdown
config>service>vpls# exit
```

Re-Enabling a VPLS Service

To re-enable a VPLS service that was shut down.

CLI Syntax:
```
config>service> vpls service-id
  [no] shutdown
```

Example:
```
config>service# vpls 1
config>service>vpls# no shutdown
config>service>vpls# exit
```

VPLS Services Command Reference

Command Hierarchies

VPLS Service Configuration Commands

Global Commands

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (7210 SAS-E)
  - **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (7210 SAS-D)
  - **vpls** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any|dot1q-range}] [r-vpls] (for 7210 SAS-K)**
  - **no vpls** *service-id*
    - **description** *description-string*
    - **no description**
    - [**no**] **disable-aging**
    - [**no**] **disable-learning**
    - [**no**] **discard-unknown**
    - [**no**] **.fdb-table-high-wmark** *high-water-mark*
    - [**no**] **fdb-table-low-wmark** *low-water-mark*
    - **fdb-table-size** *table-size*
    - **no fdb-table-size** [*table-size*]
    - **local-age** *aging-timer*
    - **no local-age**
    - [**no**] **mac-move**
      - **move-frequency** *frequency*
      - **no move-frequency**
      - **retry-timeout** *timeout*
      - **no retry-timeout**
      - [**no**] **shutdown**
    - **remote-age** *aging-timer*
    - **no remote-age**
    - **service-mtu** *octets* (for 7210 SAS-K only)
    - **no service-mtu**

VPLS service - IP interface (Host only) commands on 7210 SAS-E

NOTE: This is not a Routed VPLS IP interface.

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **no vpls** *service-id*
    - [**no**] **interface** *ip-int-name* [**create**]
      - **address** *ip-address*[/*mask*] [*netmask*]
      - **no address**
      - **arp-timeout** *seconds*
      - **no arp-timeout**
      - **description** *description-string*
      - **no description**
      - **mac** *ieee-address*
      - **no mac**
      - [**no**] **shutdown**
      - **static-arp** *ip-address ieee-address*
      - **no static-arp** *ip-address* [*ieee-address*]

VPLS service xSTP commands

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **no vpls** *service-id*
    - **stp**
      - **forward-delay** *forward-delay*
      - **no forward-delay**
      - **hello-time** *hello-time*
      - **no hello-time**
      - **hold-count** *BDPU tx hold count*
      - **no hold-count**
      - **max-age** *max-age*
      - **no max-age**
      - **mode** {**rstp** | **comp-dot1w** | **dot1w** | **mstp**}
      - **no mode**
      - [**no**] **mst-instance** *mst-inst-number*
        - **mst-port-priority** *bridge-priority*
        - **no mst-port-priority**
        - [**no**] **vlan-range** *vlan-range*
      - **mst-max-hops** *hops-count*
      - **no mst-max-hops**
      - **mst-name** *region-name*
      - **no mst-name**
      - **mst-revision** *revision-number*

— **no mst-revision**
— **priority** *bridge-priority*
— **no priority**
— [**no**] **shutdown**

VPLS Service SAP DHCP Snooping commands

config
— **service**
— **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
— **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
— **vpls** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any|dot1q-range}] [r-vpls] (for 7210 SAS-K)**
— **no vpls** *service-id*
— **sap** *sap-id* [**split-horizon-group** *group-name*] [**eth-ring** *ring-index*]
— **no sap** *sap-id*
— **dhcp**
— **description** *description-string*
— **no description**
— [**no**] **option**
— **action** [*dhcp-action*]
— **no action**
— **[no] circuit-id** [**ascii-tuple** | **vlan-ascii-tuple**]
— [**no**] **remote-id** [**mac** | **string** *string*]
— [**no**] **vendor-specific-option**
— [**no**] **client-mac-address**
— [**no**] **sap-id**
— [**no**] **service-id**
— **string** *text*
— **no string**
— [**no**] **system-id**
— [**no**] **shutdown**
— [**no**] **snoop**

SAP Commands

config
— **service**
— **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
— **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
— **vpls** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any|dot1q-range}] [r-vpls] (for 7210 SAS-K)**
— **no vpls** *service-id*
— **sap** *sap-id* [**split-horizon-group** *group-name*] [**eth-ring** *ring-index*]

— **no sap** *sap-id*
  — **accounting-policy** *acct-policy-id*
  — **no accounting-policy**
  — **bpdu-translation** {**auto** | **pvst** | **stp**}
  — **no bpdu-translation**
  — [**no**] **collect-stats**
  — **description** *description-string*
  — **no description**
  — [**no**] **disable-aging**
  — [**no**] **disable-learning**
  — [**no**] **discard-unknown-source**
  — **eth-cfm**
    — **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** **{**up | down**}**]
    — **no mep** *mep-id* **domain** *md-index* **association** *ma-index*
      — [**no**] **ais-enable**
        — **client-meg-level** [*level* [*level...*]]
        — **no client-meg-level**
        — [**no**] **description**
        — **interval** {**1**| **60**}
        — **no interval**
        — **priority** *priority-value*
        — **no priority**
        — **no send-ais-on-port-down**
        — **send-ais-on-port-down**
      — [**no**] **ccm-enable**
      — **ccm-ltm-priority** *priority*
      — **no ccm-ltm-priority**
      — **description** *description-string*
      — **no description**
      — [**no**] **eth-test-enable**
        — **bit-error-threshold** *bit-errors*
        — **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
        — **no test-pattern**
      — **low-priority-defect** {**allDef** | **macRemErrXcon** | **remErrXcon** | **errXcon** | **xcon** | **noXcon**}
      — **mac-address** *mac-address*
      — **no mac-address**
      — **one-way-delay-threshold** *seconds*
      — [**no**] **shutdown**
  — **l2pt-termination** **[cdp] [dtp] [pagp] [stp] [udld] [vtp]**
  — **no l2pt-termination**
  — **limit-mac-move** [**blockable** | **non-blockable**]
  — **no limit-mac-move**
  — [**no**] **mac-pinning**
  — **max-nbr-mac-addr** *table-size*
  — **no max-nbr-mac-addr**

VPLS SAP Configuration- QoS and Filter commands for 7210 SAS-D and 7210 SAS-E

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**m-vpls**] **[svc-sap-type {null-star|dot1q-preserve|dot1q-range|any}] [customer-vid** *vlan-id***] - SAS-D**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**m-vpls**] **[customer-vid** *vlan-id***] [svc-sap-type {null-star|dot1q-preserve|dot1q}] - SAS-E**
  - **no vpls** *service-id*
    - **sap** *sap-id* **[create] [eth-ring** *ring-index***]**
    - **no sap** *sap-id*
      - **egress**
        - **filter ip** *ip-filter-id*
        - **filter ipv6** *ipv6 -filter-id*
        - **filter mac** *mac-filter-id*
        - **no filter** [**ip** *ip-filter-id*] [**ipv6** *ipv6 -filter-id*] [**mac** *mac-filter-id*]
      - **ingress**
        - **aggregate-meter-rate** *rate-in-kbps* [**burst** *burst-in-kbits*] **- SAS-D**
        - **no aggregate-meter-rate**
        - **filter ip** *ip-filter-id*
        - **filter [ipv6** *ipv6-filter-id***]**
        - **filter mac** *mac-filter-id*
        - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6-filter-id***]** [**mac** *mac-filter-id*]
        - **qos** *policy-id*
        - **no qos**

VPLS SAP Configuration- QoS and Filter commands for 7210 SAS-K

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**m-vpls**] **[svc-sap-type {dot1q-range|any}] [r-vpls]**
  - **no vpls** *service-id*
    - **sap** *sap-id* **[create] [split-horizon-group** *group-name***]**
    - **no sap** *sap-id*
      - **egress**
        - **agg-shaper-rate cir** *cir-rate* **[pir** *pir-rate***]**
        - **no agg-shaper-rate**
        - **dot1p-inner** *dot1p-inner*
        - **no dot1p-inner**
        - **no dot1p-outer**
        - **dot1p-outer** *dot1p-outer*

- — **filter** [**ip** *ip-filter-id*]
- — **filter** **[ipv6** *ipv6 -filter-id***]**
- — **filter** [**mac** *mac-filter-id*] (app
- — **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6 -filter-id***]** [**mac** *mac-filter-id*]
- — **qos** *policy-id*
- — **no qos**

— **ingress**

- — **agg-shaper-rate** **cir** *cir-rate* **[pir** *pir-rate***]**
- — **no agg-shaper-rate**
- — **filter** [**ip** *ip-filter-id*]
- — **filter** **[ipv6** *ipv6-filter-id***]**
- — **filter** [**mac** *mac-filter-id*]
- — **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6-filter-id***]** [**mac** *mac-filter-id*]
- — **qos** *policy-id*
- — **no qos**

VPLS Service SAP IGMP Snooping and MVR commands for 7210 SAS-D and 7210 SAS-E

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **no vpls** *service-id*
    - **sap** *sap-id* [**split-horizon-group** *group-name*] [**eth-ring** *ring-index*]
    - **no sap** *sap-id*
      - **igmp-snooping**
        - [**no**] **fast-leave**
        - **import** *policy-name*
        - **no import**
        - **last-member-query-interval** *interval*
        - **no last-member-query-interval**
        - **max-num-groups** *max-num-groups*
        - **no max-num-groups**
        - **max-num-sources** *max-num-sources*
        - **no max-num-sources**
        - [**no**] **mrouter-port**
        - **mvr**
          - **from-vpls** *service-id*
          - **no from-vpls**
          - **to-sap** *sap-id*
          - **no to-sap**
        - **query-interval** *seconds*
        - **no query-interval**
        - **query-response-interval** *seconds*
        - **no query-response-interval**
        - **robust-count** *count*
        - **no robust-count**
        - [**no**] **send-queries**
        - **static**
          - [**no**] **group** *group-address*
            - [**no**] **source** *ip-address* (applicable only in access-uplink mode)
            - [**no**] **starg**
        - **version** *version*
        - **no version**
      - **mfib-table-high-wmark** *high-water-mark*
      - **no mfib-table-high-wmark**
      - **mfib-table-low-wmark** *low-water-mark*
      - **no mfib-table-low-wmark**
      - **mfib-table-size** *table-size*
      - **no mfib-table-size**

VPLS SAP Meter Override Commands for 7210 SAS-E and 7210 SAS-D

config
— **service**
— **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
— **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
— **vpls** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any|dot1q-range}] [r-vpls] (for 7210 SAS-K)**
— **no vpls** *service-id*
— **sap** *sap-id* [**split-horizon-group** *group-name*] [**eth-ring** *ring-index*]
— **no sap** *sap-id*
— **ingress**
— **meter** *meter-id* **[create]**
— **no meter** *meter-id*
— **adaptation-rule [pir** *adaptation-rule***] [cir** *adaptation-rule***]**
— **cbs** *size-in-kbytes*
— **no cbs**
— **mbs** *size-in-kbits*
— **no mbs**
— **mbs** *mode*
— **no mode**
— **no mode**
— **rate cir** *cir-rate* **[pir** *pir-rate***]**

VPLS SAP Queue Override Commands

config
— **service**
— **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
— **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
— **vpls** *service-id* **[customer** *customer-id***] [create] [svc-sap-type {any|dot1q-range}] [r-vpls] (for 7210 SAS-K)**
— **no vpls** *service-id*
— **sap** *sap-id* [**split-horizon-group** *group-name*] [**eth-ring** *ring-index*]
— **no sap** *sap-id*
— **ingress**
— **queue-override**
— **queue** *queue-id* **[create]**
— **adaptation-rule [pir** ***adaptation-rule***] **[cir** ***adaptation-rule***]
— **no port-parent**
— **port-parent [cir-level** *cir-level***] [pir-weight** *pir-weight***]**
— **queue-mgmt** *name*
— **no queue-mgmt**
— **no rate**
— **rate [cir** ***cir-rate***] **[pir** ***pir-rate***]

VPLS service SAP xSTP commands for 7210 SAS-D and 7210 SAS-E.

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **no vpls** *service-id*
    - **sap** *sap-id* [**split-horizon-group** *group-name*] [**eth-ring** *ring-index*]
    - **no sap** *sap-id*
      - **stp**
        - [**no**] **auto-edge**
        - [**no**] **edge-port**
        - **link-type** {**pt-pt** | **shared**}
        - **no link-type** [**pt-pt** | **shared**]
        - **mst-instance** *mst-inst-number*
          - **mst-path-cost** *inst-path-cost*
          - **no mst-path-cost**
          - **mst-port-priority** *stp-priority*
          - **no mst-port-priority**
        - **path-cost** *sap-path-cost*
        - **no path-cost**
        - [**no**] **port-num** *virtual-port-number*
        - **priority** *stp-priority*
        - **no priority**
        - no **root-guard**
        - **root-guard**
        - [**no**] **shutdown**
      - **tod-suite** *tod-suite-name*
      - **no tod-suite**
      - **managed-vlan-list**
        - [**no**] **default-sap**
        - [**no**] **range** *vlan-range*

VPLS SAP Statistics commands for 7210 SAS-E and 7210 SAS-D

config
- **service**
  - **vpls** *service-id* [**customer** *customer-id*] [**create**] [**vpn** *vpn-id*] [**m-vpls**] [**svc-sap-type** {**null-star** | **dot1q** | **dot1q-preserve**}] [**customer-vid** *vlan-id*] (for 7210 SAS-E)
  - **vpls** *service-id* [customer *customer-id*] [**create**] [**m-vpls**] [**svc-sap-type {null-star|dot1q-preserve|dot1q-range|any**}] [**customer-vid** *vlan-id*] (for 7210 SAS-D)
  - **no vpls** *service-id*
    - **sap** *sap-id* **[split-horizon-group** *group-name***] [eth-ring** *ring-index***] [create]**
    - **no sap** *sap-id*

— **statistics**
  — **egress**
    — [**no**] **packets-forwarded-count** (supported only on 7210 SAS-E)
    — **forwarded-count** (supported only on 7210 SAS-D)
  — **ingress**
    — **counter-mode {in-out-profile-count|forward-drop-count}** {**packet** | **octet**}(supported only on 7210 SAS-E)
    — **counter-mode {in-out-profile-count|forward-drop-count}**(supported only on 7210 SAS-D)
    — **[no] received-count** (supported only on 7210 SAS-D)

Routed VPLS Commands applicable only to 7210 SAS-D and 7210 SAS-K

config
— **service**
  — **vpls** *service-id* **[customer** *customer-id***] [vpn** *vpn-id***] [r-vpls] [create]**
    — **service-name** *service-name*
    — **no service-name**
      — **[no] allow-ip-int-binding**

Show Commands

show
- **service**
  - **fdb-info**
  - **fdb-mac** *ieee-address* [**expiry**]
  - **id** *service-id*
    - **all**
    - **arp** [*ip-address*]|[**mac** *ieee-address*]|[**sap** *sap-id*]|[**interface** *ip-int-name*] | [summary]
    - **base**
    - **dhcp**
      - **statistics** [**sap** *sap-id*] [**interface** *interface-name*]
      - **summary [interface** *interface-name* | **saps]**
    - **fdb** [**sap** *sap-id*]| [**mac** *ieee-address* | **endpoint** *endpoint* | **detail**] [**expiry**]
    - **igmp-snooping**
      - **all**
      - **base**
      - **mrouters**
      - **mvrmrouters** [**detail**]
      - **port-db sap** *sap-id* [**detail**]
      - **port-db sap** *sap-id* **group** *grp-address*
      - **proxy-db** [**detail**]
      - **proxy-db** [**group** *grp-ip-address*]
      - **querier**
      - **static** [**sap** *sap-id*]
      - **statistics**[**sap** *sap-id* | **sdp** *sdp-ic:vc-id*]
    - **l2pt disabled**
    - **l2pt** [**detail**]
    - **mac-move**
    - **mfib** [**brief**]
    - **mfib** [**group** *grp-address* | **mstp-configuration**
    - **sap** [*sap-id* [**detail | stp**]]
    - **stp** [**detail**]
  - **sap-using** [**sap** *sap-id*]
  - **sap-using** [**ingress** | **egress**] **filter** *filter-id*
  - **sap-using** [**ingress**] **qos-policy** *qos-policy-id*
  - **service-using** [**vpls**]

Clear Commands

clear
- — **service**
  - — **id** *service-id*
    - — **fdb** {**all** | **mac** *ieee-address* | **sap** *sap-id* |}
    - — **igmp-snooping**
      - — **port-db** **sap** ***sap-id*** [**group** *grp-address*]
      - — **querier**
    - — **statistics** [**all** | **sap** *sap-id* | **sdp** *sdp-id*:*vc-id*]
      - —
    - — **stp**
      - — **detected-protocols** [**all** | **sap** *sap-id*]
  - — **statistics**
    - — **id** *service-id*
      - — **counters**
      - — **stp**
    - — **sap** *sap-id* {**all** | **counters** | **stp** }

Debug Commands

debug
- — **service**
  - — **id** *service-id*
    - — [**no**] **event-type** {**config-change** | **svc-oper-status-change** | **sap-oper-status-change** | **sdpbind-oper-status-change**}
    - — [**no**] **sap** *sap-id*

VPLS Service Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context config>service>vpls
config>service>vpls>igmp-snooping
config>service>vpls>sap
config>service>vpls>sap>stp
config>service>vpls>stp

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

sap-id

Syntax [**no**] **sap-id**

Context config>service>vpls>sap>dhcp>option>vendor
config>service>ies>sap>dhcp>option>vendor
config>service>vprn>sap>dhcp>option>vendor

Description This command enables the sending of the SAP ID in the vendor specific suboption of the DHCP relay packet.

The **no** form of the command disables the sending of the SAP ID in the vendor specific suboption of the DHCP relay packet.

service-id

Syntax [**no**] **service-id**

Context config>service>vpls>sap>dhcp>option>vendor
config>service>ies>sap>dhcp>option>vendor
config>service>vprn>sap>dhcp>option>vendor

Description This command enables the sending of the service ID in the vendor specific suboption of the DHCP relay packet.

The **no** form of the command disables the sending of the service ID in the vendor specific suboption of the DHCP relay packet.

string

Syntax [**no**] **string** *text*

Context config>service>vpls>sap>dhcp>option>vendor
config>service>ies>sap>dhcp>option>vendor
config>service>vprn>sap>dhcp>option>vendor

Description This command specifies the string in the vendor specific suboption of the DHCP relay packet.

The **no** form of the command returns the default value.

Parameters *text* — The string can be any combination of ASCII characters up to 32 characters in length. If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

system-id

Syntax [**no**] **system-id**

Context config>service>vpls>sap>dhcp>option>vendor
config>service>ies>sap>dhcp>option>vendor
config>service>vprn>sap>dhcp>option>vendor

Description This command specifies whether the system-id is encoded in the vendor specific sub-option of Option 82.

server

Syntax **server** *server1* [*server2*...(up to 8 max)]

Context config>service>ies>if>dhcp
config>service>vprn>if>dhcp

Description This command specifies a list of servers where requests will be forwarded. The list of servers can entered as either IP addresses or fully qualified domain names. There must be at least one server

specified for DHCP relay to work. If there are multiple servers then the request is forwarded to all of the servers in the list.

There can be a maximum of 8 DHCP servers configured.

Default no server

Parameters *server* — Specify the DHCP server IP address.

trusted

Syntax [**no**] **trusted**

Context config>service>ies>if>dhcp
config>service>vprn>if>dhcp

Description This command enables relaying of untrusted packets.

The **no** form of this command disables the relay.

Default not enabled

snoop

Syntax [**no**] **snoop**

Context config>service>vpls>sap>dhcp

Description This command enables DHCP snooping of DHCP messages on the SAP. Enabling DHCP snooping on VPLS interfaces (SAPs) is required where DHCP messages where Option 82 information is to be inserted. This includes interfaces that are in the path to receive messages from either DHCP servers or from subscribers.

Use the **no** form of the command to disable DHCP snooping on the specified VPLS SAP.

Default no snoop

VPLS Service Commands

vpls

Syntax **vpls** *service-id* [**customer** *customer-id*] [**create**] [**m-vpls**] **[svc-sap-type {null-star|dot1q-preserve|dot1q-range|any}] [customer-vid** *vlan-id***] - SAS-D**
vpls*service-id* [**customer** *customer-id*] [**create**] [**m-vpls**] **[customer-vid** *vlan-id***] [svc-sap-type {null-star|dot1q-preserve|dot1q}] - SAS-E**
no vpls *service-id*

Context config>service

Description This command creates or edits a Virtual Private LAN Services (VPLS) instance. The **vpls** command is used to create or maintain a VPLS service. If the *service-id* does not exist, a context for the service is created. If the *service-id* exists, the context for editing the service is entered.

A VPLS service connects multiple customer sites together acting like a zero-hop, Layer 2 switched domain. A VPLS is always a logical full mesh.

When a service is created, the **create** keyword must be specified if the **create** command is enabled in the **environment** context. When a service is created, the **customer** keyword and *customer-id* must be specified and associates the service with a customer. The *customer-id* must already exist having been created using the **customer** command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified will result in an error.

More than one VPLS service may be created for a single customer ID.

By default, no VPLS instances exist until they are explicitly created.

The **no** form of this command deletes the VPLS service instance with the specified *service-id*. The service cannot be deleted until all SAPs defined within the service ID have been shutdown and deleted, and the service has been shutdown.

Parameters *any* — Allows any SAP type. When svc-sap-type is set to **any**, for a NULL SAP, the system processes and forwards only packets with no VLAN tag (that is, untagged). All other packets with one or more VLAN tags (even those with priority tag only) are not processed and dropped. Users can use the service with svc- sap-type set to `null-star' to process and forward packets with one or more tags (including priority tag) on a null SAP.

Default null-star

service-id — The unique service identification number identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7210 SAS on which this service is defined.

Values *service-id*: 1 — 2147483648

customer customer-id — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 — 2147483647

m-vpls — Specifies a management VPLS. Not supported on 7210 SAS-K

create — This keyword is mandatory while creating a VPLS service. Keyword used to create the service instance. The create keyword requirement can be enabled or disabled in the environment>create context.

customer-vid vlan-id — Defines the dot1q VLAN ID to be specified while creating the local Dot1q SAP for svc-sap-type dot1q-preserve.

Values 1 — 4094

dot1q — Specifies that the allowed SAP in the service are Dot1q SAPs and dot1q explicit null SAPs. This is supported only on 7210 SAS-E.

dot1q-preserve — Specifies that the allowed SAP in the service are Dot1q. The Dot1q ID is not stripped after packets matches the SAP. Not supported on 7210 SAS-K

Default null-star

null-star — Specifies that the allowed SAP in the service, which can be null SAPs, Dot1q default, Q.* SAP,0.* SAP or Default QinQ SAP. Not supported on 7210 SAS-K .

svc-sap-type- — Specifies the type of service and allowed SAPs in the service.

dot1q-range — Specifies that the access SAP in the service can use VLAN ranges as the SAP tags. The VLAN ranges are configured using the CLI command *configure> connection-profile*. On ingress of the access dot1q SAP using VLAN ranges, the received tag on the SAP is preserved. A VPLS service with svc-sap-type set to dot1q-range can be used for Epipe emulation with G8032 for protection. For more information about the capabilities and restrictions, see Epipe Emulation using Dot1q VLAN range SAP in VPLS with G8032 on page 202.

r-vpls — Allows this VPLS instance to be associated with an IP interface to provide R-VPLS functionality.Supported on 7210 SAS-D and 7210 SAS-K. **pbb-epipe —** keyword used to create a pbb-epipe.

bpdu-translation

Syntax **bpdu-translation** {**auto** | **pvst** | **stp**}
no bpdu-translation

Context config>service>vpls>sap

Description **Note**: This command is not supported on 7210 SAS-K.

This command enables the translation of BPDUs to a given format, meaning that all BPDUs transmitted on a given SAP will have a specified format.

The **no** form of this command reverts to the default setting.

Default no bpdu-translation

Parameters **auto —** Specifies that appropriate format will be detected automatically, based on type of bpdus received on such port.

pvst — Specifies the BPDU-format as PVST. Note that the correct VLAN tag is included in the payload (depending on encapsulation value of outgoing SAP).

stp — Specifies the BPDU-format as STP.

l2pt-termination

Syntax **l2pt-termination** [cdp] [dtp] [pagp] [stp] [udld] [vtp]
no l2pt-termination

Context config>service>vpls>sap
config>service>vpls>spoke-sdp

Description **Platforms Supported:** 7210 SAS-D and 7210 SAS-E. It is not supported on 7210 SAS-K. See notes below.

This command enables Layer 2 Protocol Tunneling (L2PT) termination on a given SAP. L2PT termination is supported for STP/CDP/DTP/PAGP/UDLD and VTP PDUs.

This feature can be enabled only if STP is disabled in the context of the given VPLS service.

NOTE: CDP, DTP, PAGP, STP, UDID and VTP is supported only on 7210 SAS-D. It is not supported on 7210 SAS-E

Default no l2pt-termination

Parameters *cdp* — Specifies the Cisco discovery protocol.

dtp — Specifies the dynamic trunking protocol.

pagp — Specifies the port aggregation protocol.

stp — Specifies all spanning tree protocols: stp, rstp, mstp, pvst (default).

udld — Specifies unidirectional link detection.

vtp — Specifies the VLAN trunking protocol.

disable-aging

Syntax [**no**] **disable-aging**

Context config>service>vpls
config>service>vpls>sap

Description This command disables MAC address aging across a VPLS service or on a VPLS service SAP.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time).In a VPLS service instance, the local age timer is applicable to both the local learned and remote learned MAC entries in the VPLS forwarding

database (FDB). The disable-aging command at the service level turns off aging for local and remote learned MAC addresses.

When **no disable-aging** is specified for a VPLS, it is possible to disable aging for specifc SAPs by entering the **disable-aging** command at the appropriate level.

When the **disable-aging** command is entered at the VPLS level, the **disable-aging** state of individual SAPs will be ignored.

The **no** form of this command enables aging on the VPLS service.

Default no disable-aging

disable-learning

Syntax [**no**] **disable-learning**

Context config>service>vpls

Description This command disables learning of new MAC addresses in the VPLS forwarding database (FDB) for the service instance.

When **disable-learning** is enabled, new source MAC addresses will not be entered in the VPLS service forwarding database.

When **disable-learning** is disabled, new source MAC addresses will be learned and entered into the VPLS forwarding database.

This parameter is mainly used in conjunction with the **discard-unknown** command.

The **no** form of this command enables learning of MAC addresses.

Default no disable-learning (Normal MAC learning is enabled)

discard-unknown

Syntax [**no**] **discard-unknown**

Context config>service>vpls

Description By default, packets with unknown destination MAC addresses are flooded. If discard-unknown is enabled at the VPLS level, packets with unknown destination MAC address will be dropped instead (even when configured FIB size limits for VPLS or SAP are not yet reached).

The **no** form of this command allows flooding of packets with unknown destination MAC addresses in the VPLS.

Default **no discard-unknown** — Packets with unknown destination MAC addresses are flooded.

.fdb-table-high-wmark

Syntax [**no**] **fdb-table-high-wmark** *high-water-mark*

Context config>service>vpls

Description This command specifies the value to send logs and traps when the threshold is reached.

Parameters *high-water-mark* — Specify the value to send logs and traps when the threshold is reached.

Values 0— 100

Default 95%

fdb-table-low-wmark

Syntax [**no**] **fdb-table-low-wmark** *low-water-mark*

Context config>service>vpls

Description This command specifies the value to send logs and traps when the threshold is reached.

Parameters *low-water-mark* — Specify the value to send logs and traps when the threshold is reached.

Values 0— 100

Default 90%

fdb-table-size

Syntax **fdb-table-size** *table-size*

Context config>service>vpls

Description This command specifies the maximum number of MAC entries in the forwarding database (FDB) for the VPLS instance on this node.

The **fdb-table-size** specifies the maximum number of forwarding database entries for both learned and static MAC addresses for the VPLS instance.

The **no** form of this command returns the maxium FDB table size to default.

Default **250** — Forwarding table of 250 MAC entries.

Parameters *table-size* — Specifies the maximum number of MAC entries in the FDB.

local-age

Syntax **local-age** *aging-timer*
no local-age

Context config>service>vpls

Description Specifies the aging time for locally learned MAC addresses in the forwarding database (FDB) for the Virtual Private LAN Service (VPLS) instance. In a VPLS service, MAC addresses are associated with a Service Access Point (SAP). MACs associated with a SAP are classified as local MACs, and MACs associated with are remote MACsQinQ / access uplink SAPs.

Like in a Layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). The **local-age** timer specifies the aging time for local learned MAC addresses.

The **no** form of this command returns the local aging timer to the default value.

Default **local age 300** — Local MACs aged after 300 seconds.

Parameters *aging-timer* — The aging time for local MACs expressed in seconds.

Values 60 — 86400

mac-move

Syntax [**no**] **mac-move**

Context config>service>vpls

Description This command enables the context to configure MAC move attributes. A sustained high re-learn rate can be a sign of a loop somewhere in the VPLS topology. Typically, STP detects loops in the topology, but for those networks that do not run STP, the mac-move feature is an alternative way to protect your network against loops.

When enabled in a VPLS, **mac-move** monitors the re-learn rate of each MAC. If the rate exceeds the configured maximum allowed limit, it disables the SAP where the source MAC was last seen. The SAP can be disabled permanently (until a **shutdown**/**no shutdown** command is executed) or for a length of time that grows linearly with the number of times the given SAP was disabled. You have the option of marking a SAP as non-blockable in the **config>service>vpls>sap>limit-mac-move** context. This means that when the re-learn rate has exceeded the limit, another (blockable) SAP will be disabled instead.

The **mac-move** command enables the feature at the service level for SAPs, as only those objects can be blocked by this feature.

The operation of this feature is the same on the SAP. For example, if a MAC address moves from SAP to SAP, one will be blocked to prevent thrashing.

mac-move will disable a VPLS port when the number of relearns detected has reached the number of relearns needed to reach the move-frequency in the 5-second interval. For example, when the move-frequency is configured to 1 (relearn per second) mac-move will disable one of the VPLS ports when 5 relearns were detected during the 5-second interval because then the average move-frequency of 1 relearn per second has been reached. This can already occur in the first second if the real relearn rate is 5 relearns per second or higher.

The **no** form of this command disables MAC move.

move-frequency

Syntax **move-frequency** *frequency*
no move-frequency

Context config>service>vpls>mac-move

Description This command indicates the maximum rate at which MAC's can be re-learned in the VPLS service, before the SAP where the moving MAC was last seen is automatically disabled in order to protect the system against undetected loops or duplicate MAC's.

The **no** form of the command reverts to the default value.

Default 2 (when mac-move is enabled). For example, 10 relearns in a 5 second period.

Parameters *frequency* — Specifies the rate, in 5-second intervals for the maximum number of relearns.

Values 1 — 100

retry-timeout

Syntax **retry-timeout** *timeout*
no retry-timeout

Context config>service>vpls>mac-move

Description This indicates the time in seconds to wait before a SAP that has been disabled after exceeding the maximum relearn rate is reenabled.

It is recommended that the retry-timeout value is larger or equal to 5s * cumulative factor of the highest priority port so that the sequential order of port blocking will not be disturbed by re-initializing lower priority ports.

A zero value indicates that the SAP will not be automatically re-enabled after being disabled.
If, after the SAP is reenabled it is disabled again, the effective retry timeout is doubled in order to avoid thrashing.

The **no** form of the command reverts to the default value.

Default 10 (when mac-move is enabled)

Parameters *timeout* — Specifies the time, in seconds, to wait before a SAP that has been disabled after exceeding the maximum relearn rate is reenabled.

Values 0 — 120

mfib-table-high-wmark

Syntax [**no**] **mfib-table-high-wmark** *high-water-mark*

Context config>service>vpls

Description This command specifies the multicast FIB high watermark. When the percentage filling level of the multicast FIB exceeds the configured value, a trap is generated and/or a log entry is added.

Parameters *high-water-mark* — Specifies the multicast FIB high watermark as a percentage.

Values 1 — 100

Default 95%

mfib-table-low-wmark

Syntax [**no**] **mfib-table-low-wmark** *low-water-mark*

Context config>service>vpls

Description This command specifies the multicast FIB low watermark. When the percentage filling level of the Multicast FIB drops below the configured value, the corresponding trap is cleared and/or a log entry is added.

Parameters *low-water-mark* — Specifies the multicast FIB low watermark as a percentage.

Values 1 — 100

Default 90%

mfib-table-size

Syntax **mfib-table-size** *size*
no mfib-table-size

Context config>service>vpls

Description This command specifies the maximum number of (s,g) entries in the multicast forwarding database (MFIB) for this VPLS instance.

The *mfib-table-size* parameter specifies the maximum number of multicast database entries for both learned and static multicast addresses for the VPLS instance. When a table-size limit is set on the mfib of a service which is lower than the current number of dynamic entries present in the mfib then the number of entries remains above the limit.

The **no** form of this command removes the configured maxium MFIB table size.

Default none

Parameters *size* — The maximum number of (s,g) entries allowed in the Multicast FIB.

Values 1 — 2047

remote-age

Syntax **remote-age** *seconds*
no remote-age

Context config>service>vpls

Description Specifies the aging time for remotely learned MAC addresses in the forwarding database (FDB) for the Virtual Private LAN Service (VPLS) instance. In a VPLS service, MAC addresses are associated with a Service Access Point (SAP). MACs associated with a SAP are classified as local MACs.

Like in a layer 2 switch, learned MACs can be aged out if no packets are sourced from the MAC address for a period of time (the aging time). In each VPLS service instance, there are independent aging timers for local learned MAC and remote learned MAC entries in the FDB. The **remote-age** timer specifies the aging time for remote learned MAC addresses. To reduce the amount of signaling required between switches configure this timer larger than the **local-age** timer.

The **no** form of this command returns the remote aging timer to the default value.

Default **remote age 900** — Remote MACs aged after 900 seconds

Parameters *seconds* — The aging time for remote MACs expressed in seconds.

Values 60 — 86400

service-mtu

Syntax **service-mtu** *octets*
no service-mtu

Context config>service>vpls

Description **Platforms Supported:** 7210 SAS-K.

This command configures the service payload (Maximum Transmission Unit – MTU), in bytes, for the service. This MTU value overrides the service-type default MTU. The **service-mtu** defines the payload capabilities of the service. It is used by the system to validate the SAP and SDP binding's operational state within the service.

The service MTU and a SAP's service delineation encapsulation overhead (i.e., 4 bytes for a dot1q tag) is used to derive the required MTU of the physical port or channel on which the SAP was created. If the required payload is larger than the port or channel MTU, then the SAP will be placed in an inoperative state. If the required MTU is equal to or less than the port or channel MTU, the SAP will be able to transition to the operative state.

In the event that a service MTU, port or channel MTU, or path MTU is dynamically or administratively modified, then all associated SAP and SDP binding operational states are automatically re-evaluated.

The **no** form of this command returns the default **service-mtu** for the indicated service type to the default value.

Note: To disable service MTU check execute the command no service-mtu-check. Disabling service MTU check allows the packets to pass to the egress if the packet length is lesser than or equal to the MTU configured on the port.

Default VPLS: 1514

The following table displays MTU values for specific VC types.

VC-Type	Example Service MTU	Advertised MTU
Ethernet	1514	1500
Ethernet (with preserved dot1q)	1518	1504
VPLS	1514	1500
VPLS (with preserved dot1q)	1518	1504
VLAN (dot1p transparent to MTU value)	1514	1500
VLAN (QinQ with preserved bottom Qtag)	1518	1504

The size of the MTU in octets, expressed as a decimal integer.

Values 1 — 9194

root-guard

Syntax [**no**] **root-guard**

Context config>service>vpls>sap>stp

Description This command specifies whether this port is allowed to become an STP root port. It corresponds to the restrictedRole parameter in 802.1Q. If set, it can cause lack of spanning tree connectivity.

Default no root-guard

tod-suite

Syntax **tod-suite** *tod-suite-name*
no tod-suite

Context config>service>vpls>sap

Description This command applies a time-based policy (filter or QoS policy) to the service SAP. The suite name must already exist in the **config>cron** context.

Default no tod-suite

Parameters *tod-suite-name* — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

Values

service-name

Syntax **service-name** *service-name*
no service-name

Context config>service>vpls

Description This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the 7750 SR, 7450 ESS and 7710 SR platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used o identify and reference a given service once it is initially created.

Parameters *service-name* — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).

allow-ip-int-binding

Syntax [no] **allow-ip-int-binding**

Context config>service>vpls

Description The allow-ip-int-binding command that sets a flag on the VPLS service that enables the ability to attach an IES IP interface to the VPLS service in order to make the VPLS service routable. When the allow-ip-int-binding command is not enabled, the VPLS service cannot be attached to an IP interface.

VPLS Configuration Constraints for Enabling allow-ip-int-bindingNOTE: This command is supported only on 7210 SAS-D.

When attempting to set the allow-ip-int-binding VPLS flag, the system first checks to see if the correct configuration constraints exist for the VPLS service and the network ports. In Release 5.0 the following VPLS features must be disabled or not configured for the allow-ip-int-binding flag to set:

- SAP ingress QoS policies applied to the VPLS SAPs cannot have MAC match criteria defined
- The VPLS service type cannot be M-VPLS.
- MVR from Routed VPLS and to another SAP is not supported

Once the VPLS allow-ip-int-binding flag is set on a VPLS service, the above features cannot be enabled on the VPLS service.

VPLS SERVICE NAME BOUND TO IP INTERFACE WITHOUT ALLOW-IP-INT-BINDING FLAG SET

In the event that a service name is applied to a VPLS service and that service name is also bound to an IP interface but the allow-ip-int-binding flag has not been set on the VPLS service context, the system attempt to resolve the service name between the VPLS service and the IP interface will fail. After the allow-ip-int-binding flag is successfully set on the VPLS service, either the service name on the VPLS service must be removed and reapplied or the IP interface must be re-initialized using the shutdown or no shutdown commands. This will cause the system to reattempt the name resolution process between the IP interface and the VPLS service.

The no form of the command resets the allow-ip-int-binding flag on the VPLS service. If the VPLS service currently has an IP interface from an IES service attached, the no allow-ip intbinding command will fail. Once the allow-ip-int-binding flag is reset on the VPLS service, the configuration restrictions associated with setting the flag are removed.

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>service>vpls

Description This command creates a logical IP routing interface for a VPLS service. Once created, attributes such as IP address and service access points (SAP) can be associated with the IP interface.

The interface command, under the context of services, is used to create and maintain IP routing interfaces within the VPLS service IDs. The IP interface created is associated with the VPLS management routing instance.This instance does not support routing.

Interface names are case-sensitive and must be unique within the group of defined IP interfaces defined for the network core router instance. Interface names in the dotted decimal notation of an IP address are not allowed. For example, the name “1.1.1.1” is not allowed, but “int-1.1.1.1” is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. Duplicate interface names can exist in different router instances.

Enter a new name to create a logical router interface. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, no default IP interface names are defined within the system. All VPLS IP interfaces must be explicitly defined in an enabled state.

The no form of this command removes the IP interface and the entire associated configuration. The interface must be administratively shutdown before issuing the no interface command.

For VPLS services, the IP interface must be shutdown before the SAP on that interface is removed.

For VPLS service, ping and traceroute are the only applications supported.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP.

An interface name:

- Should not be in the form of an IP address.
- Can be from 1 to 32 alphanumeric characters.
- If the string contains special characters (such as #,$,spaces), the entire string must be enclosed within double quotes.

If ip-int-name already exists within the service ID, the context changes to maintain that IP interface. If ip-int-name already exists within another service ID, an error occurs and the context does not change to that IP interface. If ip-int-name does not exist, the interface is created and the context is changed to that interface for further command processing.

address

Syntax **address** {*ip-address/mask* | *ip-address netmask*}
address *ip-address mask*

Context config>service>vpls>interface

Description This command assigns an IP address and an IP subnet, to a VPLS IP router interface. Only one IP address can be associated with an IP interface. An IP address must be assigned to each VPLS IP interface. An IP address and a mask are used together to 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 7210 SAS.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created. Use the no form of this command to remove the IP address assignment from the IP interface. When the no address command is entered, the interface becomes operationally down.

Address	Admin State	Oper State
No Address	Up	Down
No Address	Down	Down
1.1.1.1	Up	Up
1.1.1.1	Down	Down

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an adminstratively up state and an address is assigned, it becomes operationally up.

Parameters *ip-address* — The IP address of the IP interface. The ip-address portion of the address command specifies the IP host address that will be used by the IP interface within the subnet.

This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

/ — The forward slash is a parameter delimiter and separates the ip-address portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the ipaddress, the "/" and the mask-length parameter. If a forward slash is not immediately following the ip-address, a dotted decimal mask must follow the prefix.

mask-length — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the ip-address from the mask-length parameter. 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 values allowed are integers in the range 0 – 30. Note that a mask length of 32 is reserved for system IP addresses.

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the ip-address from a traditional dotted decimal mask. The mask parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

Values 1 — 16383

arp-timeout

Syntax **arp-timeout** *seconds*
no arp-timeout

Context config>service>vpls>interface

Description This command configures the minimum time in seconds an ARP entry learned on the IP interface will be 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. If **arp-timeout** is set to a value of zero seconds, ARP aging is disabled.

The default value for **arp-timeout** is 14400 seconds (4 hours).

The **no** form of this command restores **arp-timeout** to the default value.

Default 14400 seconds

Parameters *seconds* — The minimum number of seconds a learned ARP entry will be stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

Values 0 — 65535

mac

Syntax **mac** *ieee-address*
no mac

Context config>service>vpls>interface

Description This command assigns a specific MAC address to a VPLS IP interface.

The **no** form of the command returns the MAC address of the IP interface to the default value.

Default The system chassis MAC address.

Parameters *ieee-address* — 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. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

static-arp

Syntax **static-arp** *ip-address ieee-address*
no static-arp *ip-address* [*ieee-address*]

Context config>service>vpls>interface

Description This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. A static ARP can only be configured if it exists on the network attached to the IP interface.

If an entry for a particular IP address already exists and a new MAC address is configured for the IP address, the existing MAC address will be replaced with the new MAC address.

The **no** form of the command removes a static ARP entry.

Default None

Parameters *ip-address* — Specifies the IP address for the static ARP in dotted decimal notation.

ieee-mac-address — 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. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

VPLS STP Commands

stp

Syntax **stp**

Context config>service>vpls
config>service>vpls>sap

Description This command enables the context to configure the Spanning Tree Protocol (STP) parameters. Alcatel-Lucent's STP is simply the Spanning Tree Protocol (STP) with a few modifications to better suit the operational characteristics of VPLS services. The most evident change is to the root bridge election. Since the core network operating between Alcatel-Lucent's service routers should not be blocked, the root path is calculated from the core perspective.

auto-edge

Syntax **auto-edge**
no auto-edge

Context config>service>vpls>sap>stp

Description This command configures automatic detection of the edge port characteristics of the SAP.

The **no** form of this command returns the auto-detection setting to the default value.

Default auto-edge

edge-port

Syntax [**no**] **edge-port**

Context config>service>vpls>sap>stp

Description This command configures the SAP as an edge or non-edge port. If **auto-edge** is enabled for the SAP, this value will be used only as the initial value.

RSTP, however, can detect that the actual situation is different from what **edge-port** may indicate.

Initially, the value of the SAP parameter is set to edge-port. This value will change if:

- A BPDU is received on that port. This means that after all there is another bridge connected to this port. Then the edge-port becomes disabled.
- If auto-edge is configured and no BPDU is received within a certain period of time, RSTP concludes that it is on an edge and enables the edge-port.

The **no** form of this command returns the edge port setting to the default value.

Default no edge-port

forward-delay

Syntax **forward-delay** *seconds*
no forward-delay

Context config>service>vpls>stp

Description RSTP, as defined in the IEEE 802.1D-2004 standards, will normally transition to the forwarding state via a handshaking mechanism (rapid transition), without any waiting times. If handshaking fails (e.g. on shared links, see below), the system falls back to the timer-based mechanism defined in the original STP (802.1D-1998) standard.

A shared link is a link with more than two nodes (for example, a shared 10/100BaseT segment). The `port-type` command is used to configure a link as point-to-point or shared.

For timer-based transitions, the 802.1D-2004 standard defines an internal variable forward-delay, which is used in calculating the default number of seconds that a SAP spends in the discarding and learning states when transitioning to the forwarding state.

The value of the forward-delay variable depends on the STP operating mode of the VPLS instance:

- in `rstp` or `mstp` mode, but only when the SAP has not fallen back to legacy STP operation, the value configured by the `hello-time` command is used;
- in all other situations, the value configured by the `forward-delay` command is used.

Default 15 seconds

Parameters *seconds* — The forward delay timer for the STP instance in seconds.

Values 4 — 30

hello-time

Syntax **hello-time** *hello-time*
no hello-time

Context config>service>vpls>stp
config>template>vpls-template>stp

Description This command configures the Spanning Tree Protocol (STP) hello time for the Virtual Private LAN Service (VPLS) STP instance.

The hello time parameter defines the default timer value that controls the sending interval between BPDU configuration messages by this bridge, on ports where this bridge assumes the designated role.

The active hello time for the spanning tree is determined by the root bridge (except when the STP is running in RSTP mode, then the hello time is always taken from the locally configured parameter).

The configured hello-time can also be used to calculate the forward delay. See auto-edge on page 269.

The **no** form of this command returns the hello time to the default value.

Default 2 seconds

Parameters *hello-time* — The hello time for the STP instance in seconds.

hold-count

Syntax **hold-count** *BDPU tx hold count*
no hold-count

Context config>service>vpls>stp

Description This command configures the peak number of BPDUs that can be transmitted in a period of one second.

The **no** form of this command returns the hold count to the default value

Default 6

Parameters *BDPU tx hold count* — The hold count for the STP instance in seconds.

Values 1 — 10

link-type

Syntax **link-type** {**pt-pt** | **shared**}
no link-type

Context config>service>vpls>sap>stp

Description This command instructs STP on the maximum number of bridges behind this SAP. If there is only a single bridge, transitioning to forwarding state will be based on handshaking (fast transitions). If more than two bridges are connected via a shared media, their SAP should all be configured as shared, and timer-based transitions are used.

The **no** form of this command returns the link type to the default value.

Default pt-pt

mst-instance

Syntax **mst-instance** *mst-inst-number*

Context config>service>vpls>sap>stp

Description This command enables the context to configure MSTI related parameters at SAP level. This context can be open only for existing mst-instances defined at the service level.

Default none

Parameters *mst-inst-number* — Specifies an existing Multiple Spanning Tree Instance number.

Values 1 — 4094

mst-path-cost

Syntax **mst-path-cost** *inst-path-cost*
no mst-path-cost

Context config>service>vpls>sap>stp>mst-instance

Description This commands specifies path-cost within a given instance. If a loop occurs, this parameter indicates the probability of a given port being assigned a forwarding state. (The highest value expresses lowest priority).

The **no** form of this command sets port-priority to its default value.

Default The path-cost is proportional to link speed.

Parameters *inst-path-cost* — Specifies the contribution of this port to the MSTI path cost.

Values 1 — 200000000

mst-port-priority

Syntax **mst-port-priority** *stp-priority*
no mst-port-priority

Context config>service>vpls>sap>stp>mst-instance

Description This commands specifies the port priority within a given instance. If a loop occurs, this parameter indicates the probability of a given port being assigned a forwarding state.

The **no** form of this command sets port-priority to its default value.

Default 128

Parameters *stp-priority* — Specifies the value of the port priority field.

max-age

Syntax **max-age** *seconds*
no max-age

Context config>service>vpls>stp

Description This command indicates how many hops a BPDU can traverse the network starting from the root bridge. The message age field in a BPDU transmitted by the root bridge is initialized to 0. Each other bridge will take the message_age value from BPDUs received on their root port and increment this value by 1. The message_age thus reflects the distance from the root bridge. BPDUs with a message age exceeding max-age are ignored.

STP uses the max-age value configured in the root bridge. This value is propagated to the other bridges via the BPDUs.

The **no** form of this command returns the max ageto the default value.

Default 20 seconds

Parameters *seconds* — The max info age for the STP instance in seconds. Allowed values are integers in the range 6 to 40.

mode

Syntax **mode** {**rstp** | **comp-dot1w** | **dot1w** | **mstp**}
no mode

Context config>service>vpls>stp

Description This command specifies the version of Spanning Tree Protocol the bridge is currently running.

See section Spanning Tree Operating Modes on page 175 for details on these modes.

The **no** form of this command returns the STP variant to the default.

Default rstp

Parameters **rstp —** Corresponds to the Rapid Spanning Tree Protocol specified in IEEE 802.1D/D4-2003.

dot1w — Corresponds to the mode where the Rapid Spanning Tree is backward compatible with IEEE 802.1w.

compdot1w — Corresponds to the Rapid Spanning Tree Protocol fully conformant to IEEE 802.1w.

mstp — Sets MSTP as the STP mode of operation. Corresponds to the Multiple Spanning Tree Protocol specified in 802.1Q REV/D5.0-09/2005

mst-instance

Syntax [**no**] **mst-instance** *mst-inst-number*

Context config>service>vpls>stp

Description This command creates the context to configure Multiple Spanning Tree Instance (MSTI) related parameters. MSTP supports “16” instances. The instance “0” is mandatory (by protocol) and cannot be created by the CLI. The software automatically maintains this instance.

Default none

Parameters *mst-inst-number* — Specifies the Multiple Spanning Tree instance.

Values 1 — 4094

mst-priority

Syntax **mst-priority** *bridge-priority*
no mst-priority

Context config>service>vpls>stp>mst-instance

Description This command specifies the bridge priority for this specific Multiple Spanning Tree Instance for this service. The *bridge-priority* value reflects likelihood that the switch will be chosen as the regional root switch (65535 represents the least likely). It is used as the highest 4 bits of the Bridge ID included in the MSTP BPDU's generated by this bridge.

The values of the priority are only multiples of 4096 (4k). If a value is specified that is not a multiple of 4K, the value is replaced by the closest multiple of 4K(lower than the value entered).

The **no** form of this command sets the bridge-priority to its default value.

Default 32768 — All instances that are created by the **vlan-range** command do not have explicit definition of bridge-priority and will inherit the default value.

Parameters *bridge-priority* — Specifies the priority of this specific Multiple Spanning Tree Instance for this service.

Values 0 — 65535

vlan-range

Syntax [**no**] **vlan-range** [*vlan-range*]

Context config>service>vpls>stp>mst-instance

Description This command specifies a range of VLANs associated with a certain MST-instance. This range applies to all SAPs of the mVPLS.

Every VLAN range that is not assigned within any of the created **mst-instance** is automatically assigned to mst-instance 0. This instance is automatically maintained by the software and cannot be modified. Changing the VLAN range value can be performed only when the given mst-instance is shutdown.

The **no** form of this command removes the **vlan-range** from given **mst-instance**.

Parameters *vlan-range* — The first VLAN range specifies the left-bound (i.e., minimum value) of a range of VLANs that are associated with the mVPLS SAP. This value must be smaller than (or equal to) the second VLAN range value. The second VLAN range specifies the right-bound (i.e., maximum value) of a range of VLANs that are associated with the mVPLS SAP.

Values 1— 4094

mst-max-hops

Syntax **mst-max-hops** *hops-count*
no mst-max-hops

Context config>service>vpls>stp

Description This command specifies the number of hops in the region before BPDU is discarded and the information held for the port is aged out. The root bridge of the instance sends a BPDU (or M-record) with remaining-hop-count set to configured <*max-hops*>. When a bridge receives the BPDU (or M-record), it decrements the received remaining-hop-count by 1 and propagates it in BPDU (or M-record) it generates.

The **no** form of this command sets the *hops-count* to its default value.

Default 20

Parameters *hops-count* — Specifies the maximum number of hops.

Values 1 — 40

mst-name

Syntax **mst-name** *region-name*
no mst-name

Context config>service>vpls>stp

Description This command defines an MST region name. Two bridges are considered as a part of the same MST region as soon as their configuration of the MST region name, the MST-revision and VLAN-to-instance assignment is identical.

The **no** form of this command removes *region-name* from the configuration.

Default no mst-name

Parameters *region-name* — Specifies an MST-region name up to 32 characters in length.

mst-revision

Syntax **mst-revision** *revision-number*

Context config>service>vpls>stp

Description This command defines the MST configuration revision number. Two bridges are considered as a part of the same MST region if their configured MST-region name, MST-revision, and VLAN-to-instance are identical.

The **no** form of this command returns MST configuration revision to its default value.

Default 0

Parameters *revision-number* — Specifies the MSTP region revision number to define the MSTP region.

Values 0 — 65535

path-cost

Syntax **path-cost** *sap-path-cost*
no path-cost

Context config>service>vpls>sap>stp

Description This command configures the Spanning Tree Protocol (STP) path cost for the SAP.

The path cost is used by STP to calculate the path cost to the root bridge. The path cost in BPDUs received on the root port is incremented with the configured path cost for that SAP. When BPDUs are sent out other egress SAPs , the newly calculated root path cost is used.

STP suggests that the path cost is defined as a function of the link bandwidth. Since SAPs are controlled by complex queuing dynamics, in the 7210 SAS the STP path cost is a purely static configuration.

The **no** form of this command returns the path cost to the default value.

path-cost — The path cost for the SAP.

Values 1 — 200000000 (1 is the lowest cost)

Default 10

port-num

Syntax [**no**] **port-num** *virtual-port-number*

Context config>service>vpls>sap>stp

Description This command configures the virtual port number which uniquely identifies a SAP within configuration bridge protocol data units (BPDUs). The internal representation of a SAP is unique to a system and has a reference space much bigger than the 12 bits definable in a configuration BPDU. STP takes the internal representation value of a SAP and identifies it with it's own virtual port number that is unique to every other SAP defined on the TLS. The virtual port number is assigned at the time that the SAP is added to the TLS. Since the order that the SAP was added to the TLS is not preserved between reboots of the system, the virtual port number may change between restarts of the STP instance.

The virtual port number cannot be administratively modifed.

priority

Syntax **priority** *bridge-priority*
no priority

Context config>service>vpls>stp

Description The bridge-priority command is used to populate the priority portion of the bridge ID field within outbound BPDUs (the most significant 4 bits of the bridge ID). It is also used as part of the decision process when determining the best BPDU between messages received and sent. All values will be truncated to multiples of 4096, conforming with IEEE 802.1t and 802.1D-2004.

The **no** form of this command returns the bridge priority to the default value.

Default By default, the bridge priority is configured to 4096 which is the highest priority.

Parameters *bridge-priority* — The bridge priority for the STP instance.

Values Allowed values are integers in the range of 4096 — 65535 with 4096 being the highest priority. The actual bridge priority value stored/used is the number entered

with the lowest 12 bits masked off which means the actual range of values is 4096 to 61440 in increments of 4096.

priority

Syntax **priority** *stp-priority*
no priority

Context config>service>vpls>sap>stp

Description This command configures the Alcatel-Lucent Spanning Tree Protocol (STP) priority for the SAP.

STP priority is a configurable parameter associated with a SAP. When configuration BPDUs are received, the priority is used in some circumstances as a tie breaking mechanism to determine whether the SAPwill be designated or blocked.

In traditional STP implementations (802.1D-1998), this field is called the port priority and has a value of 0 to 255. This field is coupled with the port number (0 to 255 also) to create a 16 bit value. In the latest STP standard (802.1D-2004) only the upper 4 bits of the port priority field are used to encode the SAPpriority. The remaining 4 bits are used to extend the port ID field into a 12 bit virtual port number field. The virtual port number uniquely references a SAP within the STP instance.

STP computes the actual priority by taking the input value and masking out the lower four bits.The result is the value that is stored in the priority parameter. For instance, if a value of 0 is entered, masking out the lower 4 bits results in a parameter value of 0. If a value of 255 is entered, the result is 240.

The **no** form of this command returns the STP priority to the default value.

Default 128

Parameters *stp-priority* — The STP priority value for the SAP . Allowed values are integer in the range of 0 to 255, 0 being the highest priority. The actual value used for STP priority (and stored in the configuration) will be the result of masking out the lower 4 bits, thus the actual value range is 0 to 240 in increments of 16.

Default 128

root-guard

Syntax **[no] root-guard**

Context config>service>vpls>sap>stp

Description This command specifies whether this port is allowed to become an STP root port. It corresponds to the restricted. Role parameter in 802.1Q. If set, it can cause lack of spanning tree connectivity.

Default no root-guard

VPLS SAP Commands

sap

Syntax **sap** *sap-id* [**eth-ring** *ring-index*]
no sap *sap-id*

Context config>service>vpls

Description This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the 7210 SAS. Each SAP must be unique.

A physical port can have only one SAP to be part of one service. Multiple SAPS can be defined over a physical port but each of these SAPs should belong to a different service.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access port using the **config interface** *port-type port-id* **mode access** command.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted. For Internet Enhanced Service (IES), the IP interface must be shutdown before the SAP on that interface may be removed.

This command is also used to create a Ring APS Control SAP or a Data SAP whose traffic is protected by a Ring APS Instance.

No SAPs are defined.

Special Cases A default SAP has the following format: port-id:*. This type of SAP is supported only on Ethernet MDAs and its creation is allowed only in the scope of Layer 2 services (Epipe and VPLS).The 7210 SAS does not support explicit null encapsulation for VPLS service.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

create — Keyword used to create a SAP instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

eth-ring — The keyword to create an instance of a Ring APS Control SAP or a Data SAP whose traffic is protected by a Ring APS Instance.

ring-index — Specifies the ring index of the Ethernet ring.

discard-unknown-source

Syntax [**no**] **discard-unknown-source**

Context config>service>vpls>sap

Description When this command is enabled, packets received on a SAP or with an unknown source MAC address will be dropped only if the maximum number of MAC addresses for that SAP (see max-nbr-mac-addr on page 285) has been reached. If max-nbr-mac-addr has not been set for the SAP, enabling discard-unknown-source has no effect.

When disabled, the packets are forwarded based on the destination MAC addresses.

The **no** form of this command causes packets with an unknown source MAC addresses to be forwarded by destination MAC addresses in VPLS.

Default **no discard-unknown-source**

config>service>vpls

ETH-CFM Service Commands

eth-cfm

Syntax **eth-cfm**

Context config>service>vpls>sap

Description This command enables the context to configure ETH-CFM parameters.

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**direction** {up | **down**}]
no mep *mep-id* **domain** *md-index* **association** *ma-index*

Context config>service>vpls>sap>eth-cfm

Description This command configures the ETH-CFM maintenance endpoint (MEP).

mep-id — Specifies the maintenance association end point identifier.

Values 1 — 8191

md-index — Specifies the maintenance domain (MD) index value.

Values 1 — 4294967295

ma-index — Specifies the MA index value.

Values 1 — 4294967295

direction up| down — Indicates the direction in which the maintenance association (MEP) faces on the bridge port. Direction is not supported when a MEP is created directly under the vpls>eth-cfm construct (vMEP).

down — Sends ETH-CFM messages away from the MAC relay entity.

up — Sends ETH-CFM messages towards the MAC relay entity.

ais-enable

Syntax [**no**] **ais-enable**

Context

Description This command enables the generation and the reception of AIS messages.

client-meg-level

Syntax **client-meg-level** [[*level* [*level* ...]]
no client-meg-level

Context

Description This command configures the client maintenance entity group (MEG) level(s) to use for AIS message generation. Up to 7 levels can be provisioned with the restriction that the client MEG level must be higher than the local MEG level.

Parameters *level* — Specifies the client MEG level.

Values 1 — 7

Default 1

interval

Syntax **interval** {**1** | **60**}
no interval

Context

Description This command specifies the transmission interval of AIS messages in seconds.

Parameters **1** | **60 —** The transmission interval of AIS messages in seconds.

Default 1

priority

Syntax **priority** *priority-value*
no priority

Context

Description This command specifies the priority of AIS messages originated by the node.

Parameters *priority-value* — Specify the priority value of the AIS messages originated by the node.

Values 0 — 7

Default 1

ccm-enable

Syntax [**no**] **ccm-enable**

Context config>service>vpls>sap>eth-cfm>mep

Description This command enables the generation of CCM messages.

The **no** form of the command disables the generation of CCM messages.

ccm-ltm-priority

Syntax **ccm-ltm-priority** *priority*
no ccm-ltm-priority

Context config>service>vpls>sap>eth-cfm>mep

Description This command specifies the priority value for CCMs and LTMs transmitted by the MEP.

The **no** form of the command removes the priority value from the configuration.

Default The highest priority on the bridge-port.

Parameters *priority* — Specifies the priority of CCM and LTM messages.

Values 0 — 7

eth-test-enable

Syntax [**no**] **eth-test-enable**

Context config>service>vpls>sap>eth-cfm>mep

Description For ETH-test to work, operators need to configure ETH-test parameters on both sender and receiver nodes. The ETH-test then can be done using the following OAM commands:

oam eth-cfm eth-test *mac-address* mep *mep-id* domain *md-index* association *ma-index* [priority *priority*] [data-length *data-length*]

A check is done for both the provisioning and test to ensure the MEP is an Y.1731 MEP (MEP provisioned with domain format none, association format icc-based). If not, the operation fails. An error message in the CLI and SNMP will indicate the problem.

test-pattern

Syntax **test-pattern** {**all-zeros** | **all-ones**} [**crc-enable**]
no test-pattern

Context config>service>vpls>sap>eth-cfm>mep>eth-test-enable

Description This command configures the test pattern for eth-test frames.

The **no** form of the command removes the values from the configuration.

Parameters **all-zeros** — Specifies to use all zeros in the test pattern.

all-ones — Specifies to use all ones in the test pattern.

crc-enable — Generates a CRC checksum.

Default all-zeros

bit-error-threshold

Syntax **bit-error-threshold** <errors>
no bit-error-threshold

Context config>service>vpls>sap>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>mep

Description This command is used to specify the threshold value of bit errors.

fault-propagation-enable

Syntax **fault-propagation-enable {use-if-tlv | suspend-ccm}**
no fault-propagation-enable

Context config>service>epipe>sap>eth-cfm>mep
config>service>epipe>spoke-sdp>eth-cfm>mep

Description This command configures the fault propagation for the MEP.

Parameters *use-if-tlv* — Specifies to use the interface TLV.

suspend-ccm — Specifies to suspend the continuity check messages.

low-priority-defect

Syntax **low-priority-defect** {**allDef**|**macRemErrXcon**|**remErrXcon**|**errXcon**|**xcon**|**noXcon**}

Context

Description This command specifies the lowest priority defect that is allowed to generate a fault alarm.

Default macRemErrXcon

Values

allDef	DefRDICCM, DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
macRemErrXcon	Only DefMACstatus, DefRemoteCCM, DefErrorCCM, and DefXconCCM
remErrXcon	Only DefRemoteCCM, DefErrorCCM, and DefXconCCM
errXcon	Only DefErrorCCM and DefXconCCM
xcon	Only DefXconCCM; or
noXcon	No defects DefXcon or lower are to be reported

mac-address

Syntax **mac-address** *mac-address*
no mac-address

Context config>service>vpls>sap>eth-cfm>mep

Description This command specifies the MAC address of the MEP.

The **no** form of this command reverts the MAC address of the MEP back to that of the port (if the MEP is on a SAP) or the bridge (if the MEP is on a spoke).

Parameters *mac-address* — Specifies the MAC address of the MEP.

Values 6-byte mac-address in the form of xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx of the MEP. Must be unicast. Using the all zeros address is equivalent to the no form of this command.

one-way-delay-threshold

Syntax **one-way-delay-threshold** *seconds*

Context config>service>vpls>sap>eth-cfm>mep

Description This command enables/disables eth-test functionality on MEP.

Parameters *seconds* — Specifies the one way delay threshold, in seconds.

Values 0..600

Default 3

limit-mac-move

Syntax **limit-mac-move** [**blockable** | **non-blockable**]
no limit-mac-move

Context config>service>vpls>sap

Description This command indicates whether or not the mac-move agent, when enabled using **config>service>vpls>mac-move** or **config>service>epipe>mac-move**, will limit the MAC re-learn (move) rate on this SAP.

Default **blockable**

Parameters **blockable —** The agent will monitor the MAC re-learn rate on the SAP, and it will block it when the re-learn rate is exceeded.

non-blockable — When specified, this SAP will not be blocked, and another blockable SAP will be blocked instead.

mac-pinning

Syntax [**no**] **mac-pinning**

Context config>service>vpls>sap

Description Enabling this command will disable re-learning of MAC addresses on other SAPs within the VPLS. The MAC address will remain attached to a given SAP for duration of its age-timer.
The age of the MAC address entry in the FIB is set by the age timer. If mac-aging is disabled on a given VPLS service, any MAC address learned on a SAP with mac-pinning enabled will remain in the FIB on this SAP forever. Every event that would otherwise result in re-learning will be logged (MAC address; original-SAP; new-SAP).

max-nbr-mac-addr

Syntax **max-nbr-mac-addr** *table-size*
no max-nbr-mac-addr

Context config>service>vpls>sap
config>service>vpls>spoke-sdp
config>service>vpls>endpoint

Description This command specifies the maximum number of FDB entries for both learned and static MAC addresses for this SAP.

When the configured limit has been reached, and discard-unknown-source has been enabled for this SAP, packets with unknown source MAC addresses will be discarded.

The **no** form of the command restores the global MAC learning limitations for the SAP.

Default no max-nbr-mac-addr

Parameters *table-size* — Specifies the maximum number of learned and static entries allowed in the FDB of this service.

Values 1 — 8191

statistics

Syntax **statistics**

Context config>service>vpls>sap

Description This command enables the context to configure the counters associated with SAP ingress and egress.

egress

Syntax **egress**

Context config>service>vpls>sap>statistics

Description This command enables the context to configure the egress SAP statistics counter and set the mode of the counter.

This counter counts the number of packets forwarded through the SAP.

ingress

Syntax **ingress**

Context config>service>epipe>sap>statistics

Description This command enables the context to configure the ingress SAP statistics counter.

For 7210 E, by default, SAP ingress counters are associated with a SAP and cannot be disabled.

In 7210 SAS-D devices, for access-uplink SAPs the ingress counters are not enabled by default. For access SAPs if the ingress counter is enabled by default, it can be disabled.

The two types of ingress SAP counters are:

- A counter that counts the total packets or octets received on the SAP
- A counter associated with meters defined in the QoS policy of the SAP. This counter counts the in-profile and out-of-profile packets or octets received on the SAP.

forwarded-count

Syntax [**no**] **forwarded-count**

Context config>service>vpls>sap>statistics>egress
config>service>vpls>sap>statistics>egress
config>service>ies>sap>statistics>egress

Platform supported: 7210 SAS-D

Description This command associates a counter with the SAP. The counter counts the number of packets forwarded through the SAP.

A limited amount of such counters are available for use with access SAPs and access-uplink SAPs.

Use this command before enabling applicable accounting record collection on the SAP to associate a counter with the SAP.

The **no** form of this command disables the packet count.

packets-forwarded-count

Syntax [**no**] **packets-forwarded-count**

Context config>service>vpls>sap>statistics>egress

Platform supported: 7210 SAS-E

Description This command associates a counter with the SAP. The counter counts the number of packets forwarded through the SAP.

A limited amount of such counters are available for use with access SAPs and access-uplink SAPs.

Use this command before enabling applicable accounting record collection on the SAP to associate a counter with the SAP.

The **no** form of this command disables the packet count.

static-mac

Syntax [**no**] **static-mac** *ieee-mac-address* [**create**]

Context config>service>vpls>sap

Description This command creates a local static MAC entry in the Virtual Private LAN Service (VPLS) forwarding database (FDB) associated with the Service Access Point (SAP).

In a VPLS service, MAC addresses are associated with a Service Access Point (SAP). MACs associated with a SAP are classified as local MACs.

Local static MAC entries create a permanent MAC address to SAP association in the forwarding database for the VPLS instance so that MAC address will not be learned on the edge device.

Note that static MAC definitions on one edge device are not propagated to other edge devices participating in the VPLS instance, that is, each edge device has an independent forwarding database for the VPLS.

Only one static MAC entry (local or remote) can be defined per MAC address per VPLS instance.

By default, no static MAC address entries are defined for the SAP.

The **no** form of this command deletes the static MAC entry with the specified MAC address associated with the SAP from the VPLS forwarding database.

Parameters *ieee-mac-address* — 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. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

create — This keyword is mandatory when specifying a static MAC address.

managed-vlan-list

Syntax **managed-vlan-list**

Context config>service>vpls>sap

Description This command enables the context to configure VLAN ranges to be managed by a management VPLS. The list indicates, for each SAP, the ranges of associated VLANs that will be affected when the SAP changes state.

This command is only valid when the VPLS in which it is entered was created as a management VPLS.

default-sap

Syntax [**no**] **default-sap**

Context config>service>vpls>sap>managed-vlan-list

Description This command adds a default SAP to the managed VLAN list.

The **no** form of the command removes the default SAP to the managed VLAN list.

range

Syntax [**no**] **range** *vlan-range*

Context config>service>vpls>sap>managed-vlan-list

Description This command configures a range of VLANs on an access port that are to be managed by an existing management VPLS.

This command is only valid when the VPLS in which it is entered was created as a management VPLS, and when the SAP in which it was entered was created on an Ethernet port with encapsulation type of dot1q or qinq, or on a Sonet/SDH port with encapsulation type of bcp-dot1q.

To modify the range of VLANs, first the new range should be entered and afterwards the old range removed. See Modifying VPLS Service Parameters on page 232.

Default None

Parameters *vlan-range* — Specify the VLAN start value and VLAN end value. The end-vlan must be greater than start-vlan. The format is <start-vlan>-<end-vlan>

Values start-vlan: 0 — 4094
end-vlan: 0 — 4094

VPLS Filter and QoS Policy Commands

egress

Syntax **egress**

Context config>service>vpls>sap
config>service>ies>sap

Description This command enables the context to configure egress filter policies.

If **no** egress filter is defined, no filtering is performed.

ingress

Syntax **ingress**

Context config>service>vpls>sap
config>service>ies>sap

Description This command enables the context to configure ingress SAP Quality of Service (QoS) policies and filter policies.

If no sap-ingress QoS policy is defined, the system default sap-ingress QoS policy is used for ingress processing. If no ingress filter is defined, no filtering is performed.

filter

Syntax **filter ip** *ip-filter-id*
filter ipv6 *ipv6-filter-id*
filter mac *mac-filter-id*

Context config>service>vpls>sap>egress
config>service>vpls>sap>ingress
config>service>ies>sap>egress
config>service>ies>sap>ingress

Description This command associates an IP filter policy or MAC filter policy with an ingress or egress Service Access Point (SAP) or IP interface.

Filter policies control the forwarding and dropping of packets based on IP or MAC matching criteria. There are two types of filter policies: IP and MAC. Only one type may be applied to a SAP at a time.

The **filter** command is used to associate a filter policy with a specified filter ID with an ingress or egress SAP. The filter ID must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to IP match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID itself is not removed from the system.

Special Cases **VPLS —** Both MAC and IP filters are supported on a VPLS service SAP.

Parameters **ip** *ip-filter-id* **—** Specifies IP filter policy. The filter ID must already exist within the created IP filters.

Values 1 — 65535

ipv6 *ipv6-filter-id* — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters.

Values 1 — 65535

mac *mac-filter-id* **—** Specifies the MAC filter policy. The specified filter ID must already exist within the created MAC filters. The filter policy must already exist within the created MAC filters.

Values 1 — 65535

qos

Syntax **qos** *policy-id*
no qos

Context config>service>vpls>sap>ingress

Description This command associates a Quality of Service (QoS) policy with an ingress Service Access Point (SAP) or IP interface.

QoS ingress policies are important for the enforcement of SLA agreements. The policy ID must be defined prior to associating the policy with a SAP. If the *policy-id* does not exist, an error will be returned.

The **qos** command is used to associate ingress apolicies. The **qos** command only allows ingress policies to be associated on SAP ingress. Attempts to associate a QoS policy of the wrong type returns an error.

Only one ingress QoS policy can be associated with a SAP at one time. Attempts to associate a second QoS policy of a given type will return an error.

By default, if no specific QoS policy is associated with the SAP for ingress , so the default QoS policy is used.

The **no** form of this command removes the QoS policy association from the SAP, and the QoS policy reverts to the default.

policy-id — The ingress policy ID to associate with SAP on ingress. The policy ID must already exist.

Values 1 — 65535

aggregate-meter-rate

Syntax **aggregate-meter-rate** *rate-in-kbps* [**burst** *burst-in-kbits*]
no aggregate-meter-rate

Context config>service> vpls> sap> ingress
config>service>epipe> sap> ingress
config>service> ies> sap> ingress
config>service>vprn> sap> ingress

Description This command allows the user to configure the SAP aggregate policer. The rate of the SAP aggregate policer must be specified by the user. The user can optionally specify the burst size for the SAP aggregate policer. The aggregate policer monitors the traffic on different FCs and determines the destination of the packet. The packet is either forwarded to an identified profile or dropped.

Note: The sum of CIR of the individual FCs configured under the SAP cannot exceed the PIR rate configured for the SAP. Though the 7210 SAS software does not block this configuration, it is not recommended for use.

The table below provides information about the final disposition of the packet based on the operating rate of the per FC policer and the per SAP aggregate policer:

Per FC meter Operating Rate	Per FC Assigned Color	SAP aggre-gate meter Operating Rate	SAP aggre-gate meter color	Final Packet Color
Within CIR	Green	Within PIR	Green	Green or In-profile
Within CIR*	Green	Above PIR	Red	Green or In-profile
Above CIR, Within PIR	Yellow	Within PIR	Green	Yellow or Out-of-Profile
Above CIR, Within PIR	Yellow	Above PIR	Red	Red or Dropped
Above PIR	Red	Within PIR	Green	Red or Dropped
Above PIR	Red	Above PIR	Red	Red or Dropped

Table 21: Final Disposition of the packet based on per FC and per SAP policer or meter.

Note*: The row number 2 in the above table is not recommended for use. For more information on this, see the Note in the "**aggregate-meter-rate**" description.

When the SAP aggregate policer is configured, per FC policer can be only configured in "trtcm2" mode (RFC 4115).

Note: The meter modes "srtcm" and "trtcm1" are used in the absence of an aggregate meter.

The SAP ingress meter counters increment the packet or octet counts based on the final disposition of the packet.

If ingress Frame-based accounting is used, the SAP aggregate meter rate accounts for the Ethernet frame overhead. The system accounts for 12 bytes of IFG and 8 bytes of start delimiter.

The **no** form of the command removes the aggregate policer from use.

Default no aggregate-meter-rate

Parameters *rate-in-kbps* — Specifies the rate in kilobits per second.

Values 0 — 20000000 | max

Default max

burst <*burst-in-kilobits*> — Specifies the burst size for the policer in kilobits. The burst size cannot be configured without configuring the rate.

Values 4 —2146959

Default 512

accounting-policy

Syntax **accounting-policy** *acct-policy-id*
no accounting-policy

Context config>service>vpls>sap

Note: This command is not applicable for access uplink SAPs.

Description This command creates the accounting policy context that can be applied to a SAP.
An accounting policy must be defined before it can be associated with a SAP.
If the *policy-id* does not exist, an error message is generated.
A maximum of one accounting policy can be associated with a SAP at one time. Accounting policies are configured in the **config**>**log** context.

The **no** form of this command removes the accounting policy association from the SAP, and the acccounting policy reverts to the default.

Default Default accounting policy.

Parameters *acct-policy-id* — Enter the accounting *policy-id* as configured in the **config>log>accounting-policy** context.

Values 1 — 99

collect-stats

Syntax [**no**] **collect-stats**

Context config>service>vpls>sap

Note: This command is not applicable for access uplink SAPs.

Description This command enables accounting and statistical data collection for either the SAP, network port, or IP interface. When applying accounting policies the data, by default, is collected in the appropriate records and written to the designated billing file.

When the **no collect-stats** command is issued the statistics are still accumulated by the cards. However, the CPU will not obtain the results and write them to the billing file. If a subsequent **collect-stats** command is issued then the counters written to the billing file include all the traffic while the **no collect-stats** command was in effect.

Default no collect-stats

IGMP Snooping Commands

fast-leave

Syntax [**no**] **fast-leave**

Context config>service>vpls>sap>igmp-snooping

Description This command enables fast leave. When IGMP fast leave processing is enabled, the 7210 SAS E will immediately remove a SAP from the multicast group when it detects an IGMP “leave” on that SAP. Fast leave processing allows the switch to remove a SAP that sends a 'leave' from the forwarding table without first sending out group-specific queries to the SAP, and thus speeds up the process of changing channels ('zapping').

Fast leave should only be enabled when there is a single receiver present on the SAP.
When fast leave is enabled, the configured last-member-query-interval value is ignored.

Default no fast-leave

from-vpls

Syntax **from-vpls** *service-id*
no from-vpls

Context config>service>vpls>sap>igmp-snooping>mvr

Description This command configures the VPLS from which multicast traffic is copied upon receipt of an IGMP join request. IGMP snooping must be enabled on the MVR VPLS.

Default no from-vpls

Parameters *service-id* — Specifies the MVR VPLS from which multicast channels should be copied into this SAP.

Values *service-id*: 1 — 2147483648

group

Syntax [**no**] **group** *grp-address*

Context config>service>vpls>sap>igmp-snooping>static

Description This command adds a static multicast group as a (*, g). When a static IGMP group is added, multicast data for that (*,g) or (s,g) is forwarded to the specific SAP without receiving any membership report from a host.

Default none

Parameters *grp-address* — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

group-policy

Syntax **group-policy** *policy-name*
no group-policy

Context config>service>vpls>igmp-snooping>mvr

Description This command identifies filter policy of multicast groups to be applied to this VPLS entity. The sources of the multicast traffic must be a member of the VPLS.

The **no** form of the command removes the policy association from the VPLS configuration.

Default No group policy is specified.

Parameters *policy-name* — The group policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Routing policies are configured in the config>router>policy-options context. The router policy must be defined before it can be imported.

igmp-snooping

Syntax **igmp-snooping**

Context config>service>vpls
config>service>vpls>sap

Description This command enables the Internet Group Management Protocol (IGMP) snooping context.

Default none

max-num-sources

Syntax **max-num-sources** *max-num-sources*
no max-num-sources

Context config>service>vpls>sap>igmp-snooping

Description This command configures the maximum number of multicast sources allowed per group.

The **no** form of the command removes the value from the configuration.

Parameters *max-num-sources* — Specifies the maximum number of multicast sources allowed per group.

Values 1 — 2047

import

Syntax **import** *policy-name*
no import

Context config>service>vpls>sap>igmp-snooping

Description This command specifies the import routing policy to be used for IGMP packets to be used on this SAP. Only a single policy can be imported on a single SAP at any time.

The **no** form of the command removes the policy association from the SAP.

Default **no import** — No import policy is specified.

Parameters *policy-name* — The import policy name. Values can be string up to 32 characters long of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. These policies are configured in the **config**>**router**> **policy-options** context The router policy must be defined before it can be imported.

last-member-query-interval

Syntax **last-member-query-interval** *tenths-of-seconds*
no last-member-query-interval

Context config>service>vpls>sap>igmp-snooping

Description This command configures the maximum response time used in group-specific queries sent in response to 'leave'messages, and is also the amount of time between 2 consecutive group-specific queries. 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 configured last-member-query-interval is ignored when fast-leave is enabled on the SAP.

Default 10

Parameters *seconds* — Specifies the frequency, in tenths of seconds, at which query messages are sent.

Values 1 — 50

max-num-groups

Syntax **max-num-groups** *count*
no max-num-groups

Context config>service>vpls>sap>igmp-snooping

Description This command defines the maximum number of multicast groups that can be joined on this SAP. If the node receives an IGMP join message that would exceed the configured number of groups, the request is ignored.

Default no max-num-groups

Parameters *count* — Specifies the maximum number of groups that can be joined on this SAP.

Values 1 — 2047

mrouter-port

Syntax [**no**] **mrouter-port**

Context config>service>vpls>sap>igmp-snooping

Description This command specifies whether a multicast router is attached behind this SAP.

Configuring a SAP or SDP as an mrouter-port will have a double effect. Firstly, all multicast traffic received on another SAP or SDP will be copied to this SAP or SDP. Secondly, IGMP reports generated by the system as a result of someone joining or leaving a multicast group, will be sent to this SAP or SDP.

If two multicast routers exist in the network, one of them will become the active querier. While the other multicast router (non-querier) stops sending IGMP queries, it should still receive reports to keep its multicast trees up to date. To support this, the mrouter-port should be enabled on all SAPs or SDPs connecting to a multicast router.

Note that the IGMP version to be used for the reports (v1or v2) can only be determined after an initial query has been received. Until such time no reports are sent on the SAP, even if mrouter-port is enabled.

If the **send-queries** command is enabled on this SAP or SDP, the mrouter-port parameter can not be set.

Default no mrouter-port

mvr

Syntax mvr

Context config>service>vpls>igmp-snooping
config>service>vpls>sap>igmp-snooping

Description This command enables the context to configure Multicast VPLS Registration (MVR) parameters.

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context config>service>vpls>igmp-snooping
config>service>vpls>sap>igmp-snooping

Description This command configures the IGMP query interval. If the **send-queries** command is enabled, this parameter specifies the interval between two consecutive general queries sent by the system on this SAP. The configured query-interval must be greater than the configured query-response-interval. If send-queries is not enabled on this SAP, the configured query-interval value is ignored.

Default 125

Parameters *seconds* — The time interval, in seconds, that the router transmits general host-query messages.

Values

config>service>vpls>igmp-snooping:	1 - 65535
config>service>vpls>sap>igmp-snooping:	2 - 1024

query-src-ip

Syntax **query-src-ip** *ip-address*
no query-src-ip

Context config>service>vpls>igmp-snooping

Description This command configures the IP source address used in IGMP queries.

query-response-interval

Syntax **query-response-interval** *seconds*

Context config>service>vpls>sap>igmp-snooping

Description This command configures the IGMP query response interval. If the **send-queries** command is enabled, this parameter specifies the maximum response time advertised in IGMP queries.

The configured query-response-interval must be smaller than the configured query-interval.

If send-queries is not enabled on this SAP, the configured query-response-interval value is ignored.

Default 10

Parameters *seconds* — Specifies the length of time to wait to receive a response to the host-query message from the host.

Values 1 — 1023

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context config>service>vpls>igmp-snooping
config>service>vpls>sap>igmp-snooping

Description If the **send-queries** command is enabled, this parameter allows tuning for the expected packet loss on a SAP. The robust-count variable allows tuning for the expected packet loss on a subnet and is comparable to a retry count. If this SAP is expected to be 'lossy', this parameter may be increased. IGMP snooping on this SAP is robust to (robust-count-1) packet losses.

If send-queries is not enabled, this parameter will be ignored.

Default 2

Parameters *robust-count* — Specifies the robust count for the SAP.

Values **config>service>vpls>sap>igmp-snooping**: 2— 7
config>service>vpls>igmp-snooping: 1 — 255

send-queries

Syntax [**no**] **send-queries**

Context config>service>vpls>sap>igmp-snooping

Description This command specifies whether to send IGMP general query messages on the SAP.

When send-queries is configured, all type of queries generate ourselves are of the configured version. If a report of a version higher than the configured version is received, the report will get dropped and a new wrong version counter will get incremented. If send-queries is not configured, the version command has no effect. The version used will be the version of the querier.

Default no send-queries

source

Syntax [**no**] **source** *ip-address*

Context config>service>vpls>sap>igmp-snooping>static>group

Description This command adds a static (s,g) entry, to allow multicast traffic for a multicast group from a specified source. For a multicast group, more than one source address can be specified. Static (s,g) entries cannot be added, if a starg is previously created.

The **no** form of the command removes the source from the configuration.

Default none

Parameters *ip-address* — Specifies the IPv4 unicast address.

starg

Syntax [**no**] **starg**

Context config>service>vpls>sap>igmp-snooping>static>group

Description This command adds a static (*,g) entry to allow multicast traffic for the corresponding multicast group from any source. This command can only be enabled if no existing source addresses for this group are specified.

The **no** form of the command removes the starg entry from the configuration.

Default no starg

static

Syntax **static**

Context config>service>vpls>sap>igmp-snooping

Description This command enables access to the context to configure static group addresses. Static group addresses can be configured on a SAP. When present either as a (*, g) entry, multicast packets matching the configuration will be forwarded even if no join message was registered for the specific group.

Default none

version

Syntax **version** *version*
no version

Context config>service>vpls>sap>igmp-snooping

Description This command specifies the version of IGMP which is running on this SAP. This object can be used to configure a router capable of running either value. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN.

When the **send-query** command is configured, all type of queries generate ourselves are of the configured **version**. If a report of a version higher than the configured version is received, the report gets dropped and a new “wrong version” counter is incremented.

If the **send-query** command is not configured, the **version** command has no effect. The version used on that SAP orwill be the version of the querier.

Parameters *version* — Specify the IGMP version.

Values 1, 2, 3

to-sap

Syntax **to-sap** *sap-id*
no to-sap

Context config>service>vpls>sap>igmp-snooping>mvr

Description This command configures the SAP to which the multicast data needs to be copied.

In some scenarios, the multicast traffic should not be copied from the MVR VPLS to the SAP on which the IGMP message was received (standard MVR behaviour) but to another SAP.

Default no to-sap

Parameters *sap-id* — Specifies the SAP to which multicast channels should be copied.

Internet Enhanced Service

In This Chapter

This chapter provides information about Internet Enhanced Services , the process overview, and implementation notes.NOTE: IES is designed for in-band management of the node.

Topics in this chapter include:

IES Service Overview

NOTE: IES service (standalone, without being associated with Routed VPLS) is not supported on 7210 SAS-K.

Internet Enhanced Service (IES) is a routed connectivity service where the subscriber communicates with an IP router interface to send and receive Internet traffic. An IES has one or more logical IP routing interfaces each with a SAP which acts as the access point to the subscriber's network.

NOTE: In access-uplink mode, IES is primarily designed for in-band management of the node.

IES allows IP interfaces to participate in the same routing instance used for service network core routing connectivity. IES services require that the IP addressing scheme used by the subscriber be unique between other provider addressing schemes and potentially the entire Internet. While IES is part of the routing domain, the usable IP address space may be limited. This allows a portion of the service provider address space to be reserved for service IP provisioning, and be administered by a separate, but subordinate address authority.

IP interfaces defined within the context of an IES service must have a SAP associated as the uplink access point to the subscriber network. Multiple IES services are created to segregate subscriber owned IP interfaces.

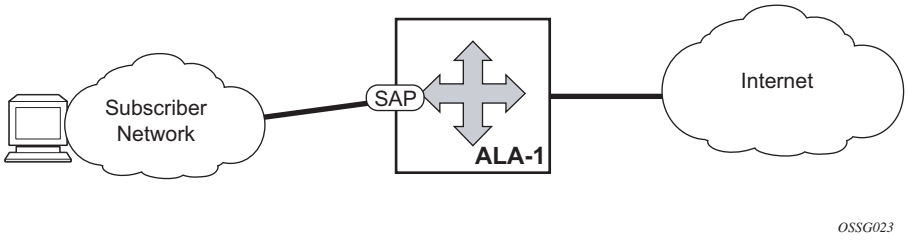


Figure 22: Internet Enhanced Service

The IES service provides in-band management connectivity. Other features include:

- Multiple IES services are created to separate IP interfaces.
- More than one IES service can be created for a single customer ID.
- More than one IP interface can be created within a single IES service ID. All IP interfaces created within an IES service ID belong to the same customer.

In access-uplink mode, the IES services provide IP connectivity to the node for in-band management of the node. Most of the management tasks supported with the out-of-band management port are supported with in-band management.

IES Features

This section describes various general service features and any special capabilities or considerations as they relate to IES services.

IP Interfaces

IES customer IP interfaces can be configured with most of the options found on the core IP interfaces. The advanced configuration options supported are:

- ICMP Options

IPv6 support for IES IP interfaces associated with Access-Uplink SAPs

In access-uplink mode, IES IP interfaces associated with access-uplink SAPs support IPv6 addressing. IPv6 can be used for in-band management of the node using the IES IP interface.

NOTE: IPv6 IES IP interfaces on access-uplink SAPs is supported only on 7210 SAS-D. It is not supported for 7210 SAS-E and 7210 SAS-K.

In 7210 SAS-D, IPv4 and IPv6 route table lookup entries are shared. Before adding routes for IPv6 destinations, route entries in the routed lookup table needs to be allocated for IPv6 addresses. This can be done using the CLI command *config> system> resource-profile> router> max-ipv6-routes*. This command allocates route entries for /64 IPv6 prefix route lookups. The system does not allocate any IPv6 route entries by default and user needs to allocate some resources before using IPv6. For the command to take effect, the node must be rebooted after making the change. For more information, see the example below and the 7210 SAS Basic System Configuration Guide.A separate route table is used for IPv6 /128-bit prefix route lookup. A limited amount of IPv6 /128 prefixes route lookup entries is supported on 7210 SAS-D. The software enables lookups in this table by default (in other words no user configuration is required to enable IPv6 / 128-bit route lookup).

NOTE: In 7210 SAS-D, IPv6 interfaces are allowed to be created without allocating IPv6 route entries.

Following features and restrictions is applicable for IPv6 IES IP interfaces:

- IPv6 interfaces supports only static routing.
- Only port-based ingress QoS policies are supported.
- IPv6 filter policies can be used on SAP ingress and egress.
- Routing protocols, such as OSPFv3, and others are not supported.

A limited amount of IPv6 /128 prefixes route lookup entries is supported on 7210 SAS-D .

SAPs

Encapsulations

In 7210 SAS-D the following Access SAP encapsulation is supported on IES services in both network mode and access-uplink mode:

- Ethernet null
- Ethernet dot1q
- Ethernet QinQ

NOTE: 7210 SAS-E does not support access SAP based IES interfaces.

In 7210 SAS-D and 7210 SAS-E, the following access-uplink SAP encapsulations are supported:

- Etherent QinQ (access-uplink QinQ SAP)

CPE Connectivity Check

NOTE: This service is supported only in 7210 SAS-D.

Static routes are used within many IES services. Unlike dynamic routing protocols, there is no way to change the state of routes based on availability information for the associated CPE. CPE connectivity check adds flexibility so that unavailable destinations will be removed from the service provider's routing tables dynamically and minimize wasted bandwidth.

The availability of the far-end static route is monitored through periodic polling. The polling period is configured. If the poll fails a specified number of sequential polls, the static route is marked as inactive.

An ICMP ping mechanism is used to test the connectivity. If the connectivity check fails and the static route is de-activated, the router will continue to send polls and re-activate any routes that are restored.

QoS Policies

When applied to 7210 SAS IES services, service ingress QoS policies only create the unicast meters defined in the policy. The multipoint meters are not created on the service. With IES services, service egress QoS policies function as with other services where the class-based queues are created as defined in the policy.

On 7210 SAS ingress, only meters are supported on all the platforms.

Note: QoS policies only create the unicast meters defined in the policy if PIM is not configured on the associated IP interface; if PIM is configured, the multipoint meters are applied as well.

In access-uplink mode, IES IP interface associated with an access SAP supports use of service ingress QoS policies. IES IP interface associated with an access-uplink SAP does not support use of service ingress QoS policies. IES IP interfaces associated with an access-uplink SAP share the port based ingress and egress QoS policies.

Note that both MAC and IPv4 criteria can be used in the QoS policies for traffic classification in an IES.

CPU QoS for IES interfaces in access-uplink mode

In access-uplink mode, IES IP interface bound to routed VPLS services, IES IP interface on access SAPs and IES IP interface on Access-Uplink SAPs are designed for use with inband management of the node. Consequently, they share a common set of queues for CPU bound management traffic. All CPU bound traffic is policed to pre-defined rates before being queued into CPU queues for application processing. The system uses meters per application or a set of applications. It does not allocate meters per IP interface. The possibility of CPU overloading has been reduced by use of these mechanisms. Users must use appropriate security policies either on the node or in the network to ensure that this does not happen.

Filter Policies

In access-uplink mode, only IP filter policies can be applied to IES service when either access SAP or access-uplink SAP is associated with the service.

Configuring an IES Service with CLI

This section provides information to configure IES services using the command line interface.

Topics in this section include:

Basic Configuration

The most basic IES service configuration has the following entities:

- Customer ID (refer to Configuring Customers on page 59)
- An interface to create and maintain IP routing interfaces within IES service ID.
- A SAP on the interface specifying the access port and encapsulation values.

The following example displays a sample configuration of an IES service on ALA-48 on an access-uplink SAP (applicable for access-uplink mode only).

```
*A:ALA-48>config>service# info
----------------------------------------------
     ies 1000 customer 50 create
             description "to internet"
             interface "to-web" create
                 address 10.1.1.1/24
                 sap 1/1/5:0.* create
                 exit
             exit
             no shutdown
----------------------------------------------
*A:ALA-48>config>service#
```

The following example displays a sample configuration of an IES service on ALA-50.

```
*A:ALA-50>config>service# info
----------------------------------------------
ies 1000 customer 50 vpn 1000 create
     description "to internet"
     interface "to-web" create
          address 10.1.1.1/24
               sap 1/1/10:100 create
          exit
     exit
     no shutdown
----------------------------------------------
*A:ALA-50>config>service#
```

The following example displays a basic IES service configuration for IPv6, along with the use of max-ipv6-routes.

The following displays an example of allocation of IPv6 routes on the node.

```
*A:7210SAS>config>system>res-prof# info
----------------------------------------------
             max-ipv6-routes 1000
----------------------------------------------
```

NOTE: The node must be rebooted after the above change.

```
*A:7210SAS>config>service# info
----------------------------------------------
     ies 1000 customer 50 vpn 1000 create
          description "to inband-mgmt"
          interface "to-mgmt" create
               ipv6
                    address 10::1/24
                         sap 1/1/10:100 create
                    exit
          exit
     no shutdown
----------------------------------------------
*A:7210SAS>config>service#
```

Common Configuration Tasks

This section provides a brief overview of the tasks that must be performed to configure IES services and provides the CLI commands.

1. Associate an IES service with a customer ID.
2. Associate customer ID with the service.
3. Assign an IP address.
4. Create an interface.
5. Define SAP parameters on the interface
   - → Select node(s) and port(s).
   - → Optional — select filter policies (configured in the **config>filter** context).
6. Enable service.

Configuring IES Components

Use the CLI syntax to configure the following entities:

- Configuring an IES Service on page 317
- Configuring IES Interface Parameters on page 318
  - → Configuring SAP Parameters on page 319
  - → Configuring VRRP on page 581

Configuring an IES Service

Use the following CLI syntax to create an IES service:

The following example displays a basic IES service configuration.

```
A:ALA-48>config>service#
-----------------------------------------------
...
     ies 1001 customer 1730 create
             description "to-internet"
             no shutdown
     exit
-----------------------------------------------
A:ALA-48>config>service#
```

Configuring IES Interface Parameters

The following example displays an IES configuration with interface parameters in access-uplink mode:

```
*A:7210-SAS>config>service>ies>if# info
----------------------------------------------
     arp-timeout 10000
     allow-directed-broadcasts
     icmp
          ttl-expired 120 38
     exit
     ip-mtu 1000
----------------------------------------------
*A:7210-SAS>config>service>ies>if#
```

Configuring SAP Parameters

A SAP is a combination of a port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique within a router.

When configuring IES access SAP parameters, a default QoS policy is applied to each SAP ingress . Additional QoS policies must be configured in the config>qos context. Filter policies are configured in the config>filter context and must be explicitly applied to a SAP. There are no default filter policies.

Only in 7210 SAS-D, SAP ingress Qos policy is supported only for access SAPs. It is not supported for access-uplink SAP. Access-uplink SAPs (on both 7210 SAS-E and 7210 SAS-D) use the port based ingress and egress QoS policies.

This example displays an IES SAP configuration.

```
-----------------------------------------------
*A:ALA-A>config>service>ies>if# info
-----------------------------------------------
     address 10.10.36.2/24
     sap 1/1/3:100 create
          ingress
               qos 101
          exit
     exit
-----------------------------------------------
*A:ALA-A>config>service>ies>if#
```

Service Management Tasks

This section discusses the following service management tasks:

- Modifying IES Service Parameters on page 320
- Deleting an IES Service on page 321

Modifying IES Service Parameters

Existing IES service parameters in the CLI or NMS can be modified, added, removed, enabled or disabled. The changes are applied immediately to all services when the charges are applied.

To display a list of customer IDs, use the **show service customer** command.
Enter the parameter(s) (such as description and SAP information) and then enter the new information.

The following displays the modified service:

```
*A:ALA-A>config>service>ies# info
----------------------------------------------
     ies 1000 customer 50 create
           description "This is a new description"
           interface "to-web" create
               address 10.1.1.1/24
               mac 00:dc:98:1d:00:00
               sap 1/1/5:0.* create
               exit
           exit
           no shutdown
     exit
----------------------------------------------
*A:ALA-A>config>service#
```

Deleting an IES Service

An IES service cannot be deleted until SAPs and interfaces are shut down *and* deleted and the service is shutdown on the service level.

Use the following CLI syntax to delete an IES service:

CLI Syntax:

```
config>service#
         [no] ies service-id
         shutdown
            [no] interface ip-int-name
            shutdown
               [no] sap sap-id
               shutdown
```

Disabling an IES Service

An IES service can be shut down without deleting the service parameters.

CLI Syntax:`config>service> ies` *`service-id`*
`shutdown`

Re-Enabling an IES Service

To re-enable an IES service that was shut down.

CLI Syntax:`config>service> ies` *`service-id`*
`[no] shutdown`

Example:

```
config>service# ies 2000
config>service>ies# no shutdown
config>service>ies# exit
```

IES Services Command Reference

Command Hierarchies

Global Commands

```
config
    — service
        — ies service-id [customer customer-id] [create] [vpn vpn-id]
        — no ies service-id
            — description description-string
            — no description
            — interface
            — no interface
            — service-name service-name
            — no service-name
            — [no] shutdown
```

Interface Commands

```
config
    — service
        — ies service-id [customer customer-id] [create] [vpn vpn-id]
            — [no] interface ip-int-name [create]
                — address {ip-address/mask | ip-address netmask}
                — no address
                — [no] allow-directed-broadcasts
                — arp-timeout seconds
                — no arp-timeout
                — dhcp
                    — description description-string
                    — no description
                    — gi-address ip-address [src-ip-addr]
```

```
                    — no gi-address
                    — [no] option
                        — action {replace|drop|keep}
                        — no action
                        — [no] circuit-id [ascii-tuple|ifindex|sap-id|vlan-ascii-
                          tuple]
                        — [no] remote-id [mac | string string]
                        — [no] vendor-specific-option
                            — [no] client-mac-address
                            — [no] sap-id
                            — [no] service-id
                            — string text
                            — no string
                            — [no] system-id
                    — no server
                    — server server1 [server2...(upto 8 max)]
                    — [no] shutdown
                    — [no] trusted
                — delayed-enable seconds (supported only on 7210 SAS-D)
                — no delayed-enable
                — description description-string
                — no description
                — icmp
                    — mask-reply (supported only on 7210 SAS-D)
                    — no mask-reply
                    — redirects [number seconds]
                    — no redirects
                    — ttl-expired [number seconds]
                    — no ttl-expired
                    — unreachables [number seconds]
                    — no unreachables
                — ip-mtu octets (Supported only on 7210 SAS-D)
                — no ip-mtu
                — [no] loopback
                — [no] shutdown
                — [no] static-arp ip-address
```

Routed VPLS Commands (for devices configured in Access-uplink mode)

```
config
    — service
        — ies service-id [customer customer-id] [vpn vpn-id]
            — interface ip-interface-name [create]
            — no interface-interface-name
                — vpls service-name
                — no vpls
                    — ingress
                        — v4-routed-override-filter ip-filter-id
                        — no v4-routed-override-filter
```

Interface SAP Commands for 7210 SAS-D

config
- **service**
  - **ies** *service-id* [**customer** *customer-id*] [**create**]
    - [**no**] **interface** *ip-int-name*
      - [**no**] **sap** *sap-id* [**create**]
        - **accounting-policy** *acct-policy-id*
        - **no accounting-policy**
        - **collect-stats**
        - **no collect-stats**
        - **description** *description-string*
        - **no description**
        - **ingress**
          - **meter** *meter-id* **[create]**
          - **no meter** *meter-id*
            - **adaptation-rule [pir** *adaptation-rule***] [cir** *adaptation-rule***]**
            - **cbs** *size-in-kbytes*
            - **no cbs**
            - **mbs** *size-in-kbits*
            - **no mbs**
            - **mbs** *mode*
            - **no mode**
            - **no mode**
            - **rate cir** *cir-rate* **[pir** *pir-rate***]**
          - **[no] qos** *policy-id* **(only supported on 7210-D access SAPs)**
        - **statistics**
          - **egress**
            - [**no**] **forwarded-count** (**only supported in 7210 SAS-D)**
          - **ingress**
            - **counter-mode** {in-out-profile-count|forward-drop-count}
            - [**no**] **received-count**
        - **[no] tod-suite** *tod-suite-name*
        - [**no**] **shutdown**

IES SAP Configuration - QoS and Filter Commands for 7210 SAS-D and SAS-E

config
- **service**
  - **ies** *service-id* [**customer** *customer-id*] [**vpn** *vpn-id*] [**create**]
    - [**no**] **interface** *ip-int-name*
      - [**no**] **sap** *sap-id* [**create**]
        - **egress**
          - **filter ip** *ip-filter-id*
          - **filter ipv6** *ipv6 -filter-id*
          - **no filter** [**ip** *ip-filter-id*] [**ipv6** *ipv6 -filter-id*]
        - **ingress**
          - **filter ip** *ip-filter-id*
          - **filter [ipv6** *ipv6-filter-id***] - SAS-D**
          - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6-filter-id***]**
          - **qos** *policy-id* **- SAS-D**
          - **no qos**

IES SAP Configuration - QoS and Filter Commands for 7210 SAS-K

config
- **service**
  - **ies** *service-id* [**customer** *customer-id*] [**vpn** *vpn-id*] [**create**]
    - [**no**] **interface** *ip-int-name*
      - [**no**] **sap** *sap-id* [**create**]
        - **egress**
          - **agg-shaper-rate** **cir** *cir-rate* **[pir** *pir-rate***]**
          - **no agg-shaper-rate**
          - **filter** [**ip** *ip-filter-id*]
          - **filter** **[ipv6** *ipv6 -filter-id***]**
          - **filter** [**mac** *mac-filter-id*] (app
          - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6 -filter-id***]** [**mac** *mac-filter-id*]
          - **qos** *policy-id*
          - **no qos**
        - **ingress**
          - **agg-shaper-rate** **cir** *cir-rate* **[pir** *pir-rate***]**
          - **no agg-shaper-rate**
          - **filter** **ip** *ip-filter-id*
          - **filter** **[ipv6** *ipv6-filter-id***]**
          - **no filter** [**ip** *ip-filter-id*] **[ipv6** *ipv6-filter-id***]**
          - **qos** *policy-id*
          - **no qos**

Interface IPv6 commands (applicable only to 7210 SAS-D and supported only for access-uplink SAPs)

config
- **service**
  - **ies** *service-id* [**customer** *customer-id*] [**create**]
    - [**no**] **interface** *ip-int-name* [**create**]
      - **ipv6**
      - **no ipv6**
        - **[no] address** *ipv6-address/prefix-length [eui-64] [preferred]*
        - **icmp6**
          - **[no] packet-too-big** *number seconds*
          - **[no] param-problem** *number seconds*
          - **[no] redirects** *number seconds*
          - **[no] time-exceeded** *number seconds*
          - **[no] unreachables** *number seconds*
        - **[no] link-local-address** *ipv6-address* **[preferred]**
        - **[no] local-proxy-nd**
        - **[no] neighbor** *ipv6-address mac-address*
        - **[no] proxy-nd-policy** *policy-name* **[policy-name...(upto 5 max)]**

Show Commands

show
- **service**
  - **customer** [*customer-id*] [**site** *customer-site-name*]
  - **sap-using** [**sap** *sap-id*]
  - **sap-using interface** [*ip-address* | *ip-int-name*]
  - **sap-using** [**ingress** | **egress**] **filter** *filter-id*
  - **sap-using** [**ingress**] **qos-policy** *qos-policy-id*
  - **service-using** [**ies**] [**customer** *customer-id*]
  - **id** *service-id*
    - **all**
    - **arp** [*ip-address*]|[**mac** *ieee-address*]|[**sap** *sap-id*]|[**interface** *ip-int-name*]
    - **base**
    - **dhcp**
      - **statistics** [**sap** *sap-id*] [**interface** *interface-name*]
      - **summary [interface** *interface-name* | **saps]**
    - **interface** [*ip-address* | *ip-int-name*] [**detail** |summary]

IES Service Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context config>service>ies
config>service>ies>if

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state. Default administrative states for services and service entities is described below in Special Cases.

The **no** form of this command places the entity into an administratively enabled state.

Special Cases **IES —** The default administrative status of an IES service is down. While the service is down, all its associated virtual router interfaces will be operationally down. The administrative state of the service is not reflected in the administrative state of the virtual router interface.

For example if: 1) An IES service is operational and an associated interface is shut down.
2) The IES service is administratively shutdown and brought back up.
3) The interface shutdown will remain in administrative shutdown state.

A service is regarded as operational provided that one IP Interface is operational.

IES IP Interfaces — When the IP interface is shutdown, it enters the administratively and operationally down states. For a SAP bound to the IP interface, no packets are transmitted out the SAP and all packets received on the SAP will be dropped while incrementing the packet discard counter.

description

Syntax **description** *long description-string*
no description

Context config>service>ies

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the content in the configuration file.

The **no** form of this command removes the string from the configuration.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

IES Global Commands

ies

Syntax **ies** *service-id* **customer** *customer-id* [**create**] [**vpn** *vpn-id*]
no ies *service-id*

Context config>service

Description This command creates or edits an IES service instance.

The **ies** command is used to create or maintain an Internet Enhanced Service (IES). If the *service-id* does not exist, a context for the service is created. If the *service-id* exists, the context for editing the service is entered.

IP interfaces defined within the context of an IES service ID must have a SAP created.

When a service is created, the **customer** keyword and *customer-id* must be specified and associates the service with a customer. The *customer-id* must already exist having been created using the **customer** command in the service context. Once a service has been created with a customer association, it is not possible to edit the customer association. The service must be deleted and recreated with a new customer association.

Once a service is created, the use of the **customer** *customer-id* is optional for navigating into the service configuration context. Attempting to edit a service with the incorrect *customer-id* specified will result in an error.

More than one IP interface may be created within a single IES service ID.

By default, no IES service instances exist until they are explicitly created.

The **no** form of this command deletes the IES service instance with the specified *service-id*. The service cannot be deleted until all the IP interfaces defined within the service ID have been shutdown and deleted.

Parameters *service-id* — The unique service identification number or string identifying the service in the service domain. This ID must be unique to this service and may not be used for any other service of any type. The *service-id* must be the same number used for every 7750 SR, 7450 ESS and 7710 SR on which this service is defined.

Values *service-id*: 1 — 2147483648

customer *customer-id* — Specifies the customer ID number to be associated with the service. This parameter is required on service creation and optional for service editing or deleting.

Values 1 — 2147483647

vpn *vpn-id* — Specifies the VPN ID assigned to the service.

Values 1 — 2147483647

service-name

Syntax **service-name** *service-name*
no service-name

Context config>service>ies

Description This command configures an optional service name, up to 64 characters in length, which adds a name identifier to a given service to then use that service name in configuration references as well as display and use service names in show commands throughout the system. This helps the service provider/administrator to identify and manage services within the 7750 SR, 7450 ESS and 7710 SR platforms.

All services are required to assign a service ID to initially create a service. However, either the service ID or the service name can be used o identify and reference a given service once it is initially created.

Parameters *service-name* — Specifies a unique service name to identify the service. Service names may not begin with an integer (0-9).

IES Interface IPv6 Commands

ipv6

Syntax [**no**] **ipv6**

Context config>service>ies>if
config>service>vprn>if

Description This command enables the context to configure IPv6 for an IES interface.

address

Syntax **address** *ipv6-address/prefix-length* [**eui-64**]
no address *ipv6-address/prefix-length*

Context config>service>ies>if>ipv6
config>service>vprn>if>ipv6

Description This command assigns an IPv6 address to the IES interface.

Parameters *ipv6-address/prefix-length* — Specify the IPv6 address on the interface.

Values

ipv6-address/prefix:	ipv6-address	x:x:x:x:x:x:x:x (eight 16-bit pieces)
		x:x:x:x:x:x:d.d.d.d
		x [0 — FFFF]H
		d [0 — 255]D
	prefix-length	1 — 128

eui-64 — When the **eui-64** keyword is specified, a complete IPv6 address from the supplied prefix and 64-bit interface identifier is formed. The 64-bit interface identifier is derived from MAC address on Ethernet interfaces. For interfaces without a MAC address, for example ATM interfaces, the Base MAC address of the chassis is used.

icmp6

Syntax **icmp6**

Context config>service>ies>if>ipv6
config>service>vprn>if>ipv6

Description This command configures ICMPv6 parameters for the IES interface.

packet-too-big

Syntax **packet-too-big** [*number seconds*]
no packet-too-big

Context config>service>ies>if>ipv6>icmp6
config>service>vprn>if>ipv6>icmp6

Description This command specifies whether “packet-too-big” ICMPv6 messages should be sent. When enabled, ICMPv6 “packet-too-big” messages are generated by this interface.

The **no** form of the command disables the sending of ICMPv6 “packet-too-big” messages.

Default 100 10

Parameters *number* — Specifies the number of “packet-too-big” ICMPv6 messages to send in the time frame specified by the *seconds* parameter.

Values 10 — 1000

Default 100

seconds — Specifies the time frame in seconds that is used to limit the number of “packet-too-big” ICMPv6 messages issued.

Values 1 — 60

Default 10

param-problem

Syntax **param-problem** [*number seconds*]
no packet-too-big

Context config>service>ies>if>ipv6>icmp6
config>service>vprn>if>ipv6>icmp6

Description This command specifies whether “parameter-problem” ICMPv6 messages should be sent. When enabled', “parameter-problem” ICMPv6 messages are generated by this interface.

The **no** form of the command disables the sending of “parameter-problem” ICMPv6 messages.

Default 100 10

number — Specifies the number of “parameter-problem” ICMPv6 messages to send in the time frame specified by the *seconds* parameter.

Values 10 — 1000

Default 100

seconds — Specifies the time frame in seconds that is used to limit the number of “parameter-problem” ICMPv6 messages issued.

Values 1 — 60

Default 10

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context config>service>ies>if>ipv6>icmp6
config>service>vprn>if>ipv6>icmp6

Description This command configures ICMPv6 redirect messages. When enabled, ICMPv6 redirects are generated when routes are not optimal on this router and another router on the same subnetwork has a better route in order to alert that node that a better route is available.

When disabled, ICMPv6 redirects are not generated.

Default 100 10

number — Specifies the number of version 6 redirects are to be issued in the time frame specified by the *seconds* parameter.

Values 10 — 1000

Default 100

seconds — Specifies the time frame in seconds that is used to limit the number of version 6 redirects issued.

Values 1 — 60

Default 10

time-exceeded

Syntax **time-exceeded** [*number seconds*]
no time-exceeded

Context config>service>ies>if>ipv6>icmp6
config>service>vprn>if>ipv6>icmp6

Description This command specifies whether “time-exceeded” ICMPv6 messages should be sent. When enabled, ICMPv6 “time-exceeded” messages are generated by this interface.

When disabled, ICMPv6 “time-exceeded” messages are not sent.

Default 100 10

number — Specifies the number of “time-exceeded” ICMPv6 messages are to be issued in the time frame specified by the *seconds* parameter.

Values 10 — 1000

Default 100

seconds — Specifies the time frame in seconds that is used to limit the number of “time-exceeded” ICMPv6 message to be issued.

Values 1 — 60

Default 10

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>service>ies>if>ipv6>icmp6
config>service>vprn>if>ipv6>icmp6

Description This command specifies that ICMPv6 host and network unreachable messages are generated by this interface.

When disabled, ICMPv6 host and network unreachable messages are not sent.

Default 100 10

number — Specifies the number of destination unreachable ICMPv6 messages are issued in the time frame specified by the *seconds* parameter.

Values 10 — 1000

Default 100

seconds — Specifies the time frame in seconds that is used to limit the number of destination unreachable ICMPv6 messages to be issued.

Values 1 — 60

Default 10

link-local-address

Syntax **link-local-address** *ipv6-address* [preferred]
no link-local-address

Context config>service>ies>if>ipv6
config>service>vprn>if>ipv6

Description This command configures the IPv6 link local address.

local-proxy-nd

Syntax [**no**] **local-proxy-nd**

Context config>service>ies>if>ipv6
config>service>vprn>if>ipv6

Description This command enables local proxy neighbor discovery on the interface.

The **no** form of the command disables local proxy neighbor discovery.

proxy-nd-policy

Syntax **proxy-nd-policy** *policy-name* [*policy-name*...(up to 5 max)]
no proxy-nd-policy

Context config>service>ies>if>ipv6
config>service>vprn>if>ipv6

Description This command applies a proxy neighbor discovery policy for the interface.

Parameters *policy-name* — Specifies an existing neighbor discovery policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. The specified policy name(s) must already be defined.

neighbor

Syntax **neighbor** *ipv6-address mac-address*
no neighbor *ipv6-address*

Context config>service>ies>if>ipv6
config>service>vprn>if>ipv6

Description This command configures IPv6-to-MAC address mapping on the IES interface.

Default none

Parameters *ipv6-address* — The IPv6 address of the interface for which to display information.

Values x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0 — FFFF]H
d: [0 — 255]D
prefix-length [1..128]

mac-address — Specifies the 48-bit MAC address for the IPv6-to-MAC address mapping 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. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

IES Interface Commands

interface

Syntax **interface** *ip-int-name* [**create**]
no interface *ip-int-name*

Context config>service>ies

Description This command creates a logical IP routing interface for an Internet Enhanced Service (IES). Once created, attributes like an IP address and service access point (SAP) can be associated with the IP interface.

The **interface** command, under the context of services, is used to create and maintain IP routing interfaces within IES service IDs. The **interface** command can be executed in the context of an IES service ID. The IP interface created is associated with the service core network routing instance and default routing.

Interface names are case sensitive and must be unique within the group of defined IP interfaces defined for **config service ies interface** (that is, the network core router instance). Interface names must not be in the dotted decimal notation of an IP address. For example, the name "1.1.1.1" is not allowed, but "int-1.1.1.1" is allowed. Show commands for router interfaces use either interface names or the IP addresses. Use unique IP address values and IP address names to maintain clarity. It could be unclear to the user if the same IP address and IP address name values are used. Although not recommended, duplicate interface names can exist in different router instances.

When a new name is entered, a new logical router interface is created. When an existing interface name is entered, the user enters the router interface context for editing and configuration.

By default, there are no default IP interface names defined within the system. All IES IP interfaces must be explicitly defined. Interfaces are created in an enabled state.

The **no** form of this command removes IP the interface and all the associated configuration. The interface must be administratively shutdown before issuing the **no interface** command.

For IES services, the IP interface must be shutdown before the SAP on that interface may be removed.

Parameters *ip-int-name* — Specifies the name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be from 1 to 32 alphanumeric characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If *ip-int-name* already exists within the service ID, the context will be changed to maintain that IP interface. If *ip-int-name* already exists within another service ID, an error will occur and context will not be changed to that IP interface. If *ip-int-name* does not exist, the interface is created and context is changed to that interface for further command processing.

address

Syntax **address** {*ip-address/mask* | *ip-address netmask*} [**broadcast** [**all-ones** | **host-ones**}]
address *ip-address mask*
no address

Context config>service>ies>if

Description This command assigns an IP address and IP subnet, to an IES IP router interface. Only one IP address can be associated with an IP interface. An IP address must be assigned to each IES IP interface. An IP address and a mask are used together to 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 7210 SAS.

The IP address for the interface can be entered in either CIDR (Classless Inter-Domain Routing) or traditional dotted decimal notation. The show commands display CIDR notation and is stored in configuration files.

By default, no IP address or subnet association exists on an IP interface until it is explicitly created.

Use the **no** form of this command to remove the IP address assignment from the IP interface. When the **no address** command is entered, the interface becomes operationally down.

Address	Admin state	Oper state
No address	up	down
No address	down	down
1.1.1.1	up	up
1.1.1.1	down	down

The operational state is a read-only variable and the only controlling variables are the address and admin states. The address and admin states are independent and can be set independently. If an interface is in an adminstratively up state and an address is assigned, it becomes operationally up.

ip-address — The IP address of the IP interface. The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation. Allowed values are IP addresses in the range 1.0.0.0 – 223.255.255.255 (with support of /31 subnets).

/ — The forward slash is a parameter delimiter and separates the *ip-address* portion of the IP address from the mask that defines the scope of the local subnet. No spaces are allowed between the *ip-address*, the "/" and the *mask-length* parameter. If a forward slash is not immediately following the *ip-address*, a dotted decimal mask must follow the prefix.

mask-length — The subnet mask length when the IP prefix is specified in CIDR notation. When the IP prefix is specified in CIDR notation, a forward slash (/) separates the *ip-address* from the *mask-length* parameter. 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. Allowed values are integers in the range 0 – 30. Note that a mask length of 32 is reserved for system IP addresses.

mask — The subnet mask in dotted decimal notation. When the IP prefix is not specified in CIDR notation, a space separates the *ip-address* from a traditional dotted decimal mask. The *mask*

parameter indicates the complete mask that will be used in a logical 'AND' function to derive the local subnet of the IP address. Allowed values are dotted decimal addresses in the range 128.0.0.0 – 255.255.255.252. Note that a mask of 255.255.255.255 is reserved for system IP addresses.

broadcast - — Specifies the broadcast format.

Values all-ones, host-ones

allow-directed-broadcasts

Syntax [**no**] **allow-directed-broadcasts**

Context config>service>ies>if

Description This command enables the forwarding of directed broadcasts out of the IP interface.

A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address on another IP interface. The **allow-directed-broadcasts** command on an IP interface enables or disables the transmission of packets destined to the subnet broadcast address of the egress IP interface.

When enabled, a frame destined to the local subnet on this IP interface will be sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts as it is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface will be counted in the normal discard counters for the egress SAP.

By default, directed broadcasts are not allowed and will be discarded at this egress IP interface.

The **no** form of this command disables the forwarding of directed broadcasts out of the IP interface.

Default **no allow-directed-broadcasts —** Directed broadcasts are dropped.

arp-timeout

Syntax **arp-timeout** *seconds*
no arp-timeout

Context config>service>ies>if

Description This command configures the minimum time in seconds an ARP entry learned on the IP interface will be 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. If **arp-timeout** is set to a value of zero seconds, ARP aging is disabled.

The **no** form of this command restores **arp-timeout** to the default value.

Default 14400 seconds

Parameters *seconds* — The minimum number of seconds a learned ARP entry will be stored in the ARP table, expressed as a decimal integer. A value of zero specifies that the timer is inoperative and learned ARP entries will not be aged.

Values 0 — 65535

Values

allow-directed-broadcasts

Syntax **[no] allow-directed-broadcasts**

Context config>service>ies>if

Description This command enables the forwarding of directed broadcasts out of the IP interface. A directed broadcast is a packet received on a local router interface destined for the subnet broadcast address on another IP interface. The allow-directed-broadcasts command on an IP interface enables or disables the transmission of packets destined to the subnet broadcast address of the egress IP interface.

When enabled, a frame destined to the local subnet on this IP interface will be sent as a subnet broadcast out this interface. Care should be exercised when allowing directed broadcasts as it is a well-known mechanism used for denial-of-service attacks.

When disabled, directed broadcast packets discarded at this egress IP interface will be counted in the normal discard counters for the egress SAP.

By default, directed broadcasts are not allowed and will be discarded at this egress IP interface.

The no form of this command disables the forwarding of directed broadcasts out of the IP interface.

Default no allow-directed-broadcasts — Directed broadcasts are dropped.

delayed-enable

Syntax **delayed-enable seconds [init-only]**
no delayed-enable

Context config>service>ies>if

Description This command delays making interface operational by the specified number of seconds. In environments with many subscribers, it can take time to synchronize the subscriber state between peers when the subscriber-interface is enabled (perhaps, after a reboot). To ensure that the state has time to be synchronized, the delayed-enable timer can be specified. The optional parameter init-only can be added to use this timer only after a reboot.

Default no delayed-enable

Parameters *seconds* — Specifies the number of seconds to delay before the interface is operational.

Values 1 — 1200

ip-mtu

Note: This command is supported only on 7210 SAS-D devices. The ip-mtu command for 7210 SAS-

E devices can be enabled using the CLI "**config>port>ethernet>ip-mtu** *mtu-bytes* ".

Syntax **ip-mtu** *octets*
no ip-mtu

Context config>service>ies>if

Description This command configures the maximum IP transmit unit (packet) for the interface.

The MTU that is advertized from the IES size is:

MINIMUM((SdpOperPathMtu - EtherHeaderSize), (Configured ip-mtu))

By default (for Ethernet network interface) if no ip-mtu is configured, the packet size is (1568 - 14) = 1554.

The **no** form of the command returns the default value.

Default no ip-mtu

Parameters *octets* — pecifies the number of octets in the IP-MTU.

Values 512 — 9000

loopback

Syntax [**no**] **loopback**

Context config>service>ies>if

Description This command specifies that the associated interface is a loopback interface that has no associated physical interface. As a result, the associated IES interface cannot be bound to a SAP.

Note that you can configure an IES interface as a loopback interface by issuing the **loopback** command instead of the **sap** command. The loopback flag cannot be set on an interface where a SAP is already defined and a SAP cannot be defined on a loopback interface.

Default none

static-arp

Syntax **static-arp** *ip-address ieee-address*
no static-arp *ip-address*

Context config>service>ies>if

Description This command configures a static address resolution protocol (ARP) entry associating a subscriber IP address with a MAC address for the core router instance. This static ARP appears in the core routing ARP table. A static ARP can only be configured if it exists on the network attached to the IP interface.

If an entry for a particular IP address already exists and a new MAC address is configured for the IP

address, the existing MAC address will be replaced with the new MAC address.

The **no** form of the command removes a static ARP entry.

Default None

Parameters *ip-address* — Specifies the IP address for the static ARP in IP address dotted decimal notation.

ieee-address — 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. Allowed values are any non-broadcast, non-multicast MAC and non-IEEE reserved MAC addresses.

vpls

Syntax vpls *service-name*

Context config>service
config>service>ies>if

Description The vpls command, within the IP interface context, is used to bind the IP interface to the specified service name.

The system does not attempt to resolve the service name provided until the IP interface is placed into the administratively up state (no shutdown). Once the IP interface is administratively up, the system scans the available VPLS services that have the allow-ip-int-binding flag set for a VPLS service associated with the name. If the service name is bound to the service name when the IP interface is already in the administratively up state, the system will immediately attempt to resolve the given name.

If a VPLS service is found associated with the name and with the allow-ip-int-binding flag set, the IP interface will be attached to the VPLS service allowing routing to and from the service virtual ports once the IP interface is operational.

A VPLS service associated with the specified name that does not have the allow-ip-int-binding flag set or a non-VPLS service associated with the name will be ignored and will not be attached to the IP interface.

If the service name is applied to a VPLS service after the service name is bound to an IP interface and the VPLS service allow-ip-int-binding flag is set at the time the name is applied, the VPLS service is automatically resolved to the IP interface if the interface is administratively up or when the interface is placed in the administratively up state.

If the service name is applied to a VPLS service without the allow-ip-int-binding flag set, the system does not attempt to resolve the applied service name to an existing IP interface bound to the name. To rectify this condition, the flag must first be set and then the IP interface must enter or reenter the administratively up state.

While the specified service name may be assigned to only one service context in the system, it is possible to bind the same service name to more than one IP interface. If two or more IP interfaces are bound to the same service name, the first IP interface to enter the administratively up state (if currently administratively down) or to reenter the administratively up state (if currently administratively up) when a VPLS service is configured with the name and has the allow-ip-intbinding flag set will be attached to the VPLS service. Only one IP interface is allowed to attach to a VPLS service context. No error is generated for the remaining non-attached IP interfaces using the service name.

Once an IP interface is attached to a VPLS service, the name associated with the service cannot be removed or changed until the IP interface name binding is removed. Also, the allow-ip-int-binding flag cannot be removed until the attached IP interface is unbound from the service name. Unbinding the service name from the IP interface causes the IP interface to detach from the VPLS service context. The IP interface may then be bound to another service name or a SAP or SDP binding may be created for the interface using the sap or spoke-sdp commands on the interface.

Default none

Parameters *service-name* — The service-name parameter is required when using the IP interface vpls command and specifies the service name that the system will attempt to resolve to an allow-ip-int-binding enabled VPLS service associated with the name. The specified name is expressed as an ASCII string comprised of up to 32 characters. It does not need to already be associated with a service and the system does not check to ensure that multiple IP interfaces are not bound to the same name.

ingress

Syntax ingress

Context config>service>ies>if>vpls

Description The ingress node in this context under the vpls binding is used to define the routed ip-filter-id optional filter overrides.

v4-routed-override-filter

Syntax v4-routed-override-filter *ip-filter-id*
no v4-routed-override-filter

Context config>service>ies>if>vpls>ingress

Description **Platforms supported:** 7210 SAS-D. Not supported on 7210 SAS-K.

The v4-routed-override-filter command is used to specify an IP filter ID that is applied to all ingress packets entering the VPLS service. The filter overrides any existing ingress IP filter applied to SAPs or SDP bindings for packets associated with the routing IP interface. The override filter is optional and when it is not defined or it is removed, the IP routed packets uses the any existing ingress IP filter on the VPLS virtual port.

The no form of the command is used to remove the IP routed override filter from the ingress IP interface. When removed, the IP ingress routed packets within a VPLS service attached to the IP interface uses the IP ingress filter applied to the packets virtual port when defined.

Default none

Parameters *ip-filter-id* — Specifies the ID for the IP filter policy. Allowed values are an integer in the range of 1 and 65535 that corresponds to a previously created IP filter policy in the **configure**>**filter**>**ip-filter** context.

Values 1 — 65535

IES Interface ICMP Commands

icmp

Syntax **icmp**

Context config>service>ies>if

Description This command enables the context to configure Internet Control Message Protocol (ICMP) parameters on an IES service

mask-reply

Syntax **[no] mask-reply**

Context config>service>ies>if>icmp

Description This command enables responses to Internet Control Message Protocol (ICMP) mask requests on the router interface.

If a local node sends an ICMP mask request to the router interface, the **mask-reply** command configures the router interface to reply to the request.

By default, the router instance will reply to mask requests.

The no form of this command disables replies to ICMP mask requests on the router interface.

Default mask-reply — Reply to ICMP mask requests.

redirects

Syntax **redirects** [*number seconds*]
no redirects

Context config>service>ies>if>icmp

Description This commad configures the rate for Internet Control Message Protocol (ICMP) redirect messages issued on the router interface.

When routes are not optimal on this router and another router on the same subnetwork has a better route, the router can issue an ICMP redirect to alert the sending node that a better route is available.

The **redirects** command enables the generation of ICMP redirects on the router interface. The rate at which ICMP redirects is issued can be controlled with the optional *number* and *seconds* parameters by indicating the maximum number of redirect messages that can be issued on the interface for a given time interval.

By default, generation of ICMP redirect messages is enabled at a maximum rate of 100 per 10 second time interval. (*Default: redirects 100 10*)

The **no** form of this command disables the generation of icmp redirects on the router interface.

Default **redirects 100 10** — Maximum of 100 redirect messages in 10 seconds

Parameters *number* — The maximum number of ICMP redirect messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP redirect messages that can be issued.

Values 1 — 60

ttl-expired

Syntax **ttl-expired** *number seconds*
no ttl-expired

Context config>service>ies>if>icmp

Description This command configures the rate Internet Control Message Protocol (ICMP) TTL expired messages are issued by the IP interface.

By default, generation of ICMP TTL expired messages is enabled at a maximum rate of 100 per 10 second time interval.

The **no** form of this command disables the limiting the rate of TTL expired messages on the router interface.

Default ttl-expired 100 10

Parameters *number* — The maximum number of ICMP TTL expired messages to send, expressed as a decimal integer. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP TTL expired messages that can be issued, expressed as a decimal integer.

Values 1 — 60

unreachables

Syntax **unreachables** [*number seconds*]
no unreachables

Context config>service>ies>if>icmp

Description This command configures the rate for ICMP host and network destination unreachable messages issued on the router interface.

The **unreachables** command enables the generation of ICMP destination unreachables on the router interface. The rate at which ICMP unreachables is issued can be controlled with the optional *number* and *time* parameters by indicating the maximum number of destination unreachable messages which can be issued on the interface for a given time interval.

By default, generation of ICMP destination unreachable messages is enabled at a maximum rate of 10 per 60 second time interval.

The **no** form of this command disables the generation of icmp destination unreachable messages on the router interface.

Default **unreachables 100 10**

Parameters *number* — The maximum number of ICMP unreachable messages to send. This parameter must be specified with the *seconds* parameter.

Values 10 — 1000

seconds — The time frame in seconds used to limit the *number* of ICMP unreachable messages that can be issued.

Values 1 — 60

IES SAP Commands

sap

Syntax **sap** *sap-id* [**create**]
no sap *sap-id*

Context config>service>ies>if

Description This command creates a Service Access Point (SAP) within a service. A SAP is a combination of port and encapsulation parameters which identifies the service access point on the interface and within the router. Each SAP must be unique.

All SAPs must be explicitly created. If no SAPs are created within a service or on an IP interface, a SAP will not exist on that object.

Enter an existing SAP without the **create** keyword to edit SAP parameters. The SAP is owned by the service in which it was created.

A SAP can only be associated with a single service. A SAP can only be defined on a port that has been configured as an access uplink port using the **configure port** *port number* **ethernet mode access uplink** command.

If a port is shutdown, all SAPs on that port become operationally down. When a service is shutdown, SAPs for the service are not displayed as operationally down although all traffic traversing the service will be discarded. The operational state of a SAP is relative to the operational state of the port on which the SAP is defined.

The **no** form of this command deletes the SAP with the specified port. When a SAP is deleted, all configuration parameters for the SAP will also be deleted.

Default No SAPs are defined.

Special Cases **IES —** A SAP is defined within the context of an IP routed interface. Each IP interface is limited to a single SAP definition. Attempts to create a second SAP on an IP interface will fail and generate an error; the original SAP will not be affected.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

port-id — Specifies the physical port ID in the *slot/mda/port* format.

If the card in the slot has Media Dependent Adapters (MDAs) installed, the *port-id* must be in the slot_number/MDA_number/port_number format. For example 1/1/1 specifies port 1 on MDA 1 in slot 1.

The *port-id* must reference a valid port type. The port must be configured as an uplink access port.

create — Keyword used to create a SAP instance. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

IES Filter Commands

filter

Syntax **filter ipv6** *ipv6-filter-id*
filter ip *ip-filter-id* **ipv6** *ipv6-filter-id*
no filter

Context config>service>ies>if>sap>egress
config>service>ies>if>sap>ingress

Description This command associates a filter policy with an ingress or egress Service Access Point (SAP). Filter policies control the forwarding and dropping of packets based on the matching criteria.

The **filter** command is used to associate a filter policy with a specified *ip-filter-id* with an ingress or egress SAP. The filter policy must already be defined before the **filter** command is executed. If the filter policy does not exist, the operation will fail and an error message returned.

In general, filters applied to SAPs (ingress or egress) apply to all packets on the SAP. One exception is non-IP packets are not applied to the match criteria, so the default action in the filter policy applies to these packets.

The **no** form of this command removes any configured filter ID association with the SAP. The filter ID itself is not removed from the system.

Special Cases **IES —** Only IP filters are supported on an IES IP interface, and the filters only apply to routed traffic.

Parameters **ip —** Keyword indicating the filter policy is an IP filter.

ipv6 — Keyword indicating the filter policy is an IPv6 filter.

ip-filter-id — Specifies the ID for the IP filter policy. Allowed values are an integer in the range of 1 and 65535 that corresponds to a previously created IP filter policy in the **configure**>**filter**>**ip-filter** context.

Values 1 — 65535

ipv6 ipv6-filter-id — Specifies the IPv6 filter policy. The filter ID must already exist within the created IPv6 filters (applicable only for 7210 SAS-D).

Values 1 — 65535

egress

Syntax **egress**

Context config>service>ies>if>sap

Description This command enables the context to apply egress policies.

ingress

Syntax **ingress**

Context config>service>ies>if>sap

Description This command enables the context to apply ingress policies

statistics

Syntax **statistics**

Context config>service>>ies>sap

Description This command enables the context to configure the counters associated with SAP ingress and egress.

egress

Syntax **egress**

Context config>service>>ies>sap>statistics

Description This command enables the context to configure the egress SAP statistics counter and set the mode of the counter.

This counter counts the number of packets forwarded through the SAP.

ingress

Syntax **ingress**

Description config>service>>ies>sap>statistics

Description This command enables the context to configure the ingress SAP statistics counter.

By default, SAP ingress counters are associated with a SAP and cannot be disabled.

The IES service supports a counter that counts the total packets or octets received on the SAP.

packets-forwarded-count

Syntax [**no**] **packets-forwarded-count**

Context config>service>>ies>sap>statistics>egress

Description This command associates a counter with the SAP. The counter counts the number of packets forwarded through the SAP.

The **no** form of this command disables the packet count.

counter-mode

Syntax **counter-mode** {in-out-profile-count|forward-drop-count}

Context config>service>ies>sap>statistics>ingress

Description This command sets the mode of ingress counters associated with the SAP to either octets or packets. On IES SAPs, collect stats cannot be enabled so the mode of the counter can be changed without any reference. Changing the mode of the counter results in loss of previously collected counts and resets the counter. The **no** form of this command is not supported.

Default in-out-profile-count

Parameters **in-out-profile-count —** If the counter mode is specified as "in-out-profile-count", one counter counts the total in-profile packets and octets received on ingress of a SAP and another counts the total out-of-profile packets and octets received on ingress of a SAP. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. Dropped counts are not maintained in hardware when this mode is used. It is obtained by subtracting the sum of in-profile count and out-of-profile count from the total SAP ingress received count and displayed.

forward-drop-count — If the counter mode is specified as "forward-drop-count", one counter counts the forwarded packets and octets received on ingress of a SAP and another counts the dropped packets. The forwarded count is the sum of in-profile and out-of-profile packets/octets received on SAP ingress. The dropped count is count of packets/octets dropped by the policer. A packet is determined to be in-profile or out-of-profile based on the meter rate parameters configured. A packet is dropped by the policer if it exceeds the configured PIR rate. The in-profile count and out-of-profile count is not individually available when operating in this mode.

tod-suite

Syntax **tod-suite** *tod-suite-name*
no tod-suite

Context config>service>ies>if>sap

Description This command applies a time-based policy (filter or QoS policy) to the service SAP. The suite name must already exist in the **config**>**cron** context.

Default no tod-suite

Parameters *tod-suite-name* — Specifies collection of policies (ACLs, QoS) including time-ranges that define the full or partial behavior of a SAP. The suite can be applied to more than one SAP.

Service Global Commands

In This Chapter

This section provides show command descriptions and output.

Show, Clear, Debug, Commands

Services Show Commands

Service Commands

customer

Syntax **customer** [*customer-id*] [**site** *customer-site-name*]]

Context show>service

Description This command displays service customer information.

Parameters *customer-id* — Displays only information for the specified customer ID.

Default All customer IDs display.

Values 1 — 2147483647

site *customer-site-name* — Specifies the customer site which is an anchor point for an ingress and egress virtual scheduler hierarchy.

Output **Show Customer Command Output —** The following table describes show customer command output fields:

Label	Description
Customer-ID	The ID that uniquely identifies a customer.
Contact	The name of the primary contact person.
Description	Generic information about the customer.
Phone	The phone/pager number to reach the primary contact person.
Total Customers	The total number of customers configured.
Site	Multi-service site name. A multi-service customer site is a group of SAPs with common origination and termination points.
Description	Displays information about a specific customer's multi-service site.
Assignment	The port ID, MDA, or card number, where the SAP's that are members of this multi- service site are defined.
I. Sched Pol	The ingress QoS scheduler policy assigned to this multi-service site.
E. Sched Pol	The egress QoS scheduler policy assigned to this multi-service site.

Service-ID	The ID that uniquely identifies a service.
SAP	Specifies the SAP assigned to the service.

Sample Output

```
*A:ALA-12# show service customer
===========================================================
Customers
===========================================================
Customer-ID : 1
Contact     : Manager
Description : Default customer
Phone       : (123) 555-1212

Customer-ID : 2
Contact     : Tech Support
Description : TiMetra Networks
Phone       : (234) 555-1212

Customer-ID : 3
Contact     : Test
Description : TiMetra Networks
Phone       : (345) 555-1212

Customer-ID : 6
Contact     : Test1
Description : Epipe Customer
Phone       : (456) 555-1212

Customer-ID : 7
Contact     : Test2
Description : VPLS Customer
Phone       : (567) 555-1212

Customer-ID : 8
Contact     : Customer Service
Description : IES Customer
Phone       : (678) 555-1212

Customer-ID : 274
Contact     : TestA
Description : ABC Company
Phone       : 650 123-4567

Customer-ID : 94043
Contact     : Test Engineer on Duty
Description : TEST Customer
Phone       : (789) 555-1212
-------------------------------------------------------
Total Customers : 8
-----------------------------------------------------------
*A:ALA-12#
*A:ALA-12# show service customer 274
===============================================================================
Customer  274
===============================================================================
```

```
Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567
-------------------------------------------------------------------------------
Multi Service Site
-------------------------------------------------------------------------------
Site        : west
Description : (Not Specified)
===============================================================================
*A:ALA-12#
```

fdb-mac

Syntax **fdb-mac** [*ieee-address*] [**expiry**]

Context show>service

Description This command displays the FDB entry for a given MAC address.

Parameters *ieee-address* — Specifies the 48-bit MAC address 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.

expiry — shows amount of time until MAC is aged out.

Sample Output

```
*A:ALA-48# show service fdb-mac
===============================================================================
Service Forwarding Database
===============================================================================
ServId    MAC               Source-Identifier     Type/Age  Last Change
-------------------------------------------------------------------------------
103       12:34:56:78:90:0f sap:1/1/7:0           Static    02/02/2009 09:27:57
700       90:30:ff:ff:ff:8f cpm                   Host      02/02/2009 09:27:57
-------------------------------------------------------------------------------
No. of Entries: 2
===============================================================================
*A:ALA-48#


*A:ALA-48# show service fdb-mac expiry
===============================================================================
Service Forwarding Database
===============================================================================
ServId    MAC               Source-Identifier     Type/     Last Change
                                                  Expiry
-------------------------------------------------------------------------------
103       12:34:56:78:90:0f sap:1/1/7:0           Static    02/02/2009 09:27:57
700       90:30:ff:ff:ff:8f cpm                   Host      02/02/2009 09:27:57
-------------------------------------------------------------------------------
No. of Entries: 2
===============================================================================
*A:ALA-48#
```

LSP

service-using

Syntax **service-using** [**epipe**][**ies**] [**vpls**] [**mirror**] [**i-vpls**] [**m-vpls**] [**customer** *customer-id*]

Context show>service

Description This command displays the services matching certain usage properties. If no optional parameters are specified, all services defined on the system are displayed.

Parameters **epipe —** Displays matching Epipe services.

ies — Displays matching IES instances.

vpls — Displays matching VPLS instances.

mirror — Displays matching mirror services.

customer *customer-id* **—** Displays services only associated with the specified customer ID.

Default Services associated with a customer.

Values 1 — 2147483647

Output **Show Service Service-Using —** The following table describes show command output fields.

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The desired state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Service name	The name of the service.

Sample Output

```
*7210SAS>show>service# service-using customer 1

===============================================================================
Services  Customer 1
===============================================================================
ServiceId    Type      Adm  Opr  CustomerId Service Name
-------------------------------------------------------------------------------
1            VPLS      Up   Up   1
2            VPLS      Up   Up   1
3            VPLS      Up   Up   1
4            VPLS      Up   Up   1
2147483648   IES       Up   Down 1          _tmnx_InternalIesService
2147483649   intVpls   Up   Down 1          _tmnx_InternalVplsService
-------------------------------------------------------------------------------
Matching Services : 6
-------------------------------------------------------------------------------
```

```
===============================================================================
*7210SAS>show>service#
```

id

Syntax **id** *<service-id>*

Context show>service

Description This command displays vpls-template used to instantiate this service and m-vpls that controls this service.

eth-ring

Syntax ***eth-ring*** *[status]*
eth-ring *[ring-index] hierarchy*
eth-ring *ring-index [path {a|b}]*

Context show

Description This command displays the Ethernet rings information.

Parameters *status* — Displays the status information of the Ethernet rings configured on the system.

hierarchy — Displays eth-ring hierarical relationships.

path {a|b} — Displays information related to the configured Ethernet rings.

Output **Show Ethernet Ring Status —** The following table describes show command output fields.

Label	Description
`Ring Id`	The ring identifier
`Admin State`	Displays the administrative state
`Oper State`	Displays the operational state
Path Information	
`Path`	Displays the path information
`Tag`	Displays the tag information
`State`	Displays the state of the path
MEP Information	
`Ctrl-MEP`	Displays the Ctrl-MEP information
`CC-Intvl`	Displays the Ctrl-Interval information

Label	Description (Continued)
Defects	Displays the defects

```
*A:NS1015C0821>show# eth-ring status

===============================================================================
Ethernet Ring (Status information)
===============================================================================
Ring   Admin  Oper       Path Information                MEP Information
ID     State  State  Path         Tag       State     Ctrl-MEP CC-Intvl Defects
-------------------------------------------------------------------------------
1      Up     Up     a - 1/1/1    100       Up        Yes      100ms     -----
                      b - 1/1/2    100       Up        Yes      100ms     -----
10     Down   Down   a - N/A                 -        -        -         -----
                      b - N/A                 -        -        -         -----
===============================================================================
Ethernet Tunnel MEP Defect Legend:
R = Rdi, M = MacStatus, C = RemoteCCM, E = ErrorCCM, X = XconCCM
*A:NS1015C0821>show#
```

Output **Show Ethernet Ring —** The following table describes show command output fields.

Label	Description
Description	The ring description
Admin State	Displays the administrative state
Oper State	Displays the operational state
Node ID	Displays the node identifier
Guard Time	Displays the configured guard time
Max Revert time	Displays the configured maximum revert time
CCM Hold down time	Displays the configured CCM Hold down time
APS TX PDU	Displays the APS TX PDU information
Defect Status	Displays the defect status
RPL Node	Displays the RPL node information
Time to revert	Displays the configured time to revert
CCM Hold Up Time	Displays the configured CCM Hold up time
Sub-Ring Type	Displays the sub-ring type information, the sub-ring type can be virtual link or on-virtual link.

Label	Description (Continued)
Interconnect-ID	Displays the interconnect ID. The ID can be a ring-index ID or VPLS service ID.
Compatible Version	Displays the Ethernet ring version information.

```
*A:NS1015C0821>show# eth-ring 10

===============================================================================
Ethernet Ring 10 Information
===============================================================================
Description        : (Not Specified)
Admin State        : Down               Oper State       : Down
Node ID            : 00:25:ba:03:48:04
Guard Time         :    5 deciseconds   RPL Node         : rplNone
Max Revert Time    :  300 seconds       Time to Revert   : N/A
CCM Hold Down Time :    0 centiseconds  CCM Hold Up Time :   20 deciseconds
APS Tx PDU         : N/A
Defect Status      :

-------------------------------------------------------------------------------
Ethernet Ring Path Summary
-------------------------------------------------------------------------------
Path Port     Raps-Tag     Admin/Oper      Type            Fwd State
-------------------------------------------------------------------------------
  a  -        -                 -/-         -               -
  b  -        -                 -/-         -               -
===============================================================================
*A:NS1015C0821>show#
```

ETH-CFM Show Commands

eth-cfm

Syntax **eth-cfm**

Context show

Description This command enables the context to display eth-cfm information.

association

Syntax **association** [*ma-index*] [**detail**]

Context show>eth-cfm

Description This command displays eth-cfm association information.

Parameters *ma-index* — Specifies the maintenance association (MA) index.

Values 1— 4294967295

detail — Displays detailed information for the eth-cfm association.

Output **Show eth-cfm Association Command Output —** The following table describes show eth-cfm association command output fields:

Label	Description
`Md-index`	Displays the the maintenance domain (MD) index.
`Ma-index`	Displays the the maintenance association (MA) index.
`Name`	Displays the part of the maintenance association identifier which is unique within the maintenance domain name.
`CCM-interval`	Displays the CCM transmission interval for all MEPs in the association.
`Bridge-id`	Displays the bridge-identifier value for the domain association.
`MHF Creation`	Displays the MIP half function (MHF) for the association.
`Primary VLAN`	Displays the primary bridge-identifier VLAN ID.
`Num Vids`	Displays the number of VIDs associated with the VLAN.
`Remote Mep Id`	Displays the remote maintenance association end point (MEP) identifier

Sample Output

```
*A:ALU-IPD#  show eth-cfm association
=====================================================================
CFM Association Table
=====================================================================
Md-index   Ma-index   Name                      CCM-interval Bridge-id
---------------------------------------------------------------------
1          1          abcabcabcabc1             1            1
1          2          abcabcabcabc2             1            2
1          3          abcabcabcabc3             1            3
1          4          abcabcabcabc4             1            4
=====================================================================
*A:ALU-IPD#
```

cfm-stack-table

Syntax

cfm-stack-table [{all-ports}] [level <0..7>**] [direction <down>]**

Context show>eth-cfm

Description This command displays stack-table information. This stack-table is used to display the various management points MEPs and MIPs that are configured on the system. These can be Service based or facility based. The various option allow the operator to be specific. If no parameters are include then the entire stack-table will be displayed.

Parameters **port** *port-id* **—** Displays the bridge port or aggregated port on which MEPs or MHFs are configured.

vlan *vlan-id* **—** Displays the associated VLAN ID.

level — Display the MD level of the maintenance point.

Values 0 — 7

direction down — Displays the direction in which the MP faces on the bridge port.

facility — Displays the CFM stack table information for facility MEPs. The base command will display all the facility MEPs. Options may be included in order to further parse the table for specific facility MEP information.

Output **Show eth-cfm CFM Stack Table Command Output —** The following table describes show eth-cfm CFM stack table command output fields:

Label	Description
Sap	Displays associated SAP IDs.
Level Dir	Displays the MD level of the maintenance point.
Md-index	Displays the the maintenance domain (MD) index.
Ma-index	Displays the the maintenance association (MA) index.

Label	Description
Mep-id	Displays the integer that is unique among all the MEPs in the same MA.
Mac-address	Displays the MAC address of the MP.

Sample Output

```
*A:ALU-IPD#   show eth-cfm cfm-stack-table
===========================================================================
CFM SAP Stack Table
===========================================================================
Sap            Level Dir  Md-index   Ma-index   Mep-id Mac-address
---------------------------------------------------------------------------
lag-1:1.1      0     Down 2          1          10     00:f3:f0:98:97:1b
lag-1:1.1      6     Down 1          1          1      00:f3:f0:98:97:1b
lag-1:2.2      0     Down 2          2          20     00:f3:f0:98:97:1b
lag-1:2.2      6     Down 1          2          2      00:f3:f0:98:97:1b
===========================================================================
===========================================================================
CFM Ethernet Tunnel Stack Table
===========================================================================
Eth-tunnel     Level Dir  Md-index   Ma-index   Mep-id Mac-address
---------------------------------------------------------------------------
===========================================================================
===========================================================================
CFM SDP Stack Table
===========================================================================
Sdp            Level Dir  Md-index   Ma-index   Mep-id Mac-address
---------------------------------------------------------------------------
No Matching Entries
===========================================================================
===========================================================================
CFM Virtual Stack Table
===========================================================================
Service        Level Dir  Md-index   Ma-index   Mep-id Mac-address
---------------------------------------------------------------------------
No Matching Entries
===========================================================================
*A:ALU-IPD#
```

domain

Syntax **domain** [*md-index*] [**association** *ma-index* | **all-associations**] [**detail**]

Context show>eth-cfm

Description This command displays domain information.

Parameters *md-index* — Displays the index of the MD to which the MP is associated, or 0, if none.

association *ma-index* — Displays the index to which the MP is associated, or 0, if none.

all-associations — Displays all associations to the MD.

detail — Displays detailed domain information.

Output **Show eth-cfm Domain Command Output —** The following table describes show eth-cfm domain command output fields:

Label	Description
Md-index	Displays the Maintenance Domain (MD) index value.
Level	Displays an integer identifying the Maintenance Domain Level (MD Level). Higher numbers correspond to higher Maintenance Domains, those with the greatest physical reach, with the highest values for customers' CFM PDUs. Lower numbers correspond to lower Maintenance Domains, those with more limited physical reach, with the lowest values for CFM PDUs protecting single bridges or physical links.
Name	Displays a generic Maintenance Domain (MD) name.
Format	Displays the type of the Maintenance Domain (MD) name. Values include **dns**, **mac**, and *string*.

Sample Output

```
*A:7210-2#  show eth-cfm domain
===============================================================================
CFM Domain Table
===============================================================================
Md-index   Level Name                                          Format
-------------------------------------------------------------------------------
1          6                                                   none
2          0                                                   none
===============================================================================
*A:7210-2#
```

mep

Syntax **mep** *mep-id* **domain** *md-index* **association** *ma-index* [**loopback**] [**linktrace**]
mep *mep-id* **domain** *md-index* **association** *ma-index* **remote-mepid** *mep-id* | **all-remote-mepids**
mep *mep-id* **domain** *md-index* **association** *ma-index* **eth-test-results** [**remote-peer** *mac-address*]
mep *mep-id* **domain** *md-index* **association** *ma-index* **one-way-delay-test** [**remote-peer** *mac-address*]
mep*mep-id* **domain** *md-index* **association** *ma-index* **two-way-delay-test** [**remote-peer** *mac-address*]
mep *mep-id* **domain** *md-index* **association** *ma-index* **two-way-slm-test [remote-peer** *macaddress***]**

Context show>eth-cfm

Description This command displays Maintenance Endpoint (MEP) information.

NOTES:

- The show eth-cfm mep mep-id domain md-id association ma-id command does not display CCM ERROR, CCM XCON frames in the output.
- The show eth-cfm mep mep-id domain md-id association ma-id remote-mep rmep-id command does not display some TLVs details.

Parameters *mep-id* — Displays the integer that is unique among all the MEPs in the same MA.

domain *md-index* **—** Displays the index of the MD to which the MP is associated, or 0, if none.

association *ma-index* — Displays the index to which the MP is associated, or 0, if none.

loopback — Displays loopback information for the specified MEP.

linktrace — Displays linktrace information for the specified MEP.

remote-mepid *mep-id* **—** Includes specified remote mep-id information for specified the MEP.

all-remote-mepids — Includes all remote mep-id information for the specified MEP.

eth-test-results — Includes eth-test-result information for the specified MEP.

one-way-delay-test — Includes one-way-delay-test information for the specified MEP.

two-way-delay-test — Includes two-way-delay-test information for the specified MEP.

two-way-slm-test — Includes two-way-slm-test information for the specified MEP.

remote-peer *mac-address* — Includes specified remote mep-id information for the specified MEP.

Sample Output

```
*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 linktrace
-------------------------------------------------------------------------------
Mep Information
-------------------------------------------------------------------------------
Md-index           : 1                        Direction         : Down
```

```
Ma-index           : 1                        Admin             : Enabled
MepId              : 1                        CCM-Enable        : Enabled
IfIndex            : 1342177281               PrimaryVid        : 65537
FngState           : fngReset                 ControlMep        : False
LowestDefectPri    : macRemErrXcon            HighestDefect     : none
Defect Flags       : None
Mac Address        : 00:f3:f0:98:97:1b        CcmLtmPriority    : 7
CcmTx              : 531                      CcmSequenceErr    : 0
Eth-1Dm Threshold  : 3(sec)
Eth-Ais:           : Disabled
Eth-Tst:           : Enabled                  Eth-Tst Pattern:  : allZerosNoCrc
Eth-Tst dataLength : 64                       Eth-Tst Priority: : 7
Eth-Tst Threshold  : 1(bitError)
CcmLastFailure Frame:
    None
XconCcmFailure Frame:
    None
-------------------------------------------------------------------------------
Mep Linktrace Message Information
-------------------------------------------------------------------------------
LtRxUnexplained    : 0                        LtNextSequence    : 2
LtStatus           : False                    LtResult          : False
TargIsMepId        : False                    TargMepId         : 0
TargMac            : 00:00:00:00:00:00        TTL               : 64
EgressId           : 00:00:00:f3:f0:98:97:1b  SequenceNum       : 1
LtFlags            : useFDBonly
-------------------------------------------------------------------------------
Mep Linktrace Replies
-------------------------------------------------------------------------------
SequenceNum        : 1                        ReceiveOrder      : 1
Ttl                : 63                       Forwarded         : False
LastEgressId       : 00:00:00:f3:f0:98:97:1b  TerminalMep       : True
NextEgressId       : 00:00:00:e0:b1:99:cb:46  Relay             : n/a
ChassisIdSubType   : unknown value (0)
ChassisId:
    None
ManAddressDomain:
    None
ManAddress:
    None
IngressMac         : 00:e0:b1:99:cb:46        Ingress Action    : ingOk
IngrPortIdSubType  : unknown value (0)
IngressPortId:
    None
EgressMac          : 00:00:00:00:00:00        Egress Action     : egrNoTlv
EgrPortIdSubType   : unknown value (0)
EgressPortId:
    None
Org Specific TLV:
    None
-------------------------------------------------------------------------------
*A:7210-2#


*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 loopback
-------------------------------------------------------------------------------
Mep Information
-------------------------------------------------------------------------------
Md-index           : 1                        Direction         : Down
```

```
Ma-index           : 1                        Admin             : Enabled
MepId              : 1                        CCM-Enable        : Enabled
IfIndex            : 1342177281               PrimaryVid        : 65537
FngState           : fngReset                 ControlMep        : False
LowestDefectPri    : macRemErrXcon            HighestDefect     : none
Defect Flags       : None
Mac Address        : 00:f3:f0:98:97:1b        CcmLtmPriority    : 7
CcmTx              : 566                      CcmSequenceErr    : 0
Eth-1Dm Threshold  : 3(sec)
Eth-Ais:           : Disabled
Eth-Tst:           : Enabled                  Eth-Tst Pattern:  : allZerosNoCrc
Eth-Tst dataLength : 64                       Eth-Tst Priority: : 7
Eth-Tst Threshold  : 1(bitError)
CcmLastFailure Frame:
    None
XconCcmFailure Frame:
    None
-------------------------------------------------------------------------------
Mep Loopback Information
-------------------------------------------------------------------------------
LbRxReply          : 1                        LbRxBadOrder      : 0
LbRxBadMsdu        : 0                        LbTxReply         : 0
LbSequence         : 2                        LbNextSequence    : 2
LbStatus           : False                    LbResultOk        : True
DestIsMepId        : False                    DestMepId         : 0
DestMac            : 00:00:00:00:00:00        SendCount         : 0
VlanDropEnable     : True                     VlanPriority      : 7
Data TLV:
    None
-------------------------------------------------------------------------------
*A:7210-2#


*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 remote-mepid 10
===============================================================================
Eth-CFM Remote-Mep Table
===============================================================================
R-mepId Rx CC  Rx Rdi Port-Tlv If-Tlv Peer Mac Addr     CCM status since
-------------------------------------------------------------------------------
10      True   False  Absent   Absent 00:e0:b1:99:cb:46 05/20/2010 12:59:55
===============================================================================
*A:7210-2#


*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 eth-test-results
===============================================================
Eth CFM ETH-Test Result Table
===============================================================
                                Current        Accumulate
                 FrameCount     ErrBits        ErrBits
Peer Mac Addr    ByteCount      CrcErrs        CrcErrs
---------------------------------------------------------------
00:e0:b1:99:cb:46 1             0              0
                 64             0              0
===============================================================


*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 eth-test-results remote-peer
00:e0:b1:99:cb:46
```

```
===============================================================
Eth CFM ETH-Test Result Table
===============================================================
                                 Current        Accumulate
                  FrameCount     ErrBits        ErrBits
Peer Mac Addr     ByteCount      CrcErrs        CrcErrs
---------------------------------------------------------------
00:e0:b1:99:cb:46 1              0              0
                  64             0              0
===============================================================
*A:7210-2#


*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 one-way-delay-test
====================================================================
Eth CFM One-way Delay Test Result Table
====================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
--------------------------------------------------------------------
00:e0:b1:99:cb:46     10000               10000
====================================================================


*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 one-way-delay-test remote-peer
00:e0:b1:99:cb:46
====================================================================
Eth CFM One-way Delay Test Result Table
====================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
--------------------------------------------------------------------
00:e0:b1:99:cb:46     10000               10000
====================================================================
*A:7210-2#


*A:7210-2#  show eth-cfm mep 1 domain 1 association 1 two-way-delay-test
====================================================================
Eth CFM Two-way Delay Test Result Table
====================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
--------------------------------------------------------------------
00:e0:b1:99:cb:46     10000               10000
====================================================================
*A:7210-2#


*A:7210-2# # show eth-cfm mep 1 domain 1 association 1 two-way-delay-test remote-peer
00:e0:b1:99:cb:46
====================================================================
Eth CFM Two-way Delay Test Result Table
====================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
--------------------------------------------------------------------
00:e0:b1:99:cb:46     10000               10000
====================================================================
*A:7210-2#
A:dut-b# show eth-cfm mep 1 domain 1 association 1 linktrace
-------------------------------------------------------------------------------
Mep Information
```

```
-------------------------------------------------------------------------------
Md-index           : 1                        Direction         : Down
Ma-index           : 1                        Admin             : Enabled
MepId              : 1                        CCM-Enable        : Enabled
IfIndex            : 35946496                 PrimaryVid        : 1
FngState           : fngReset                 ControlMep        : False
LowestDefectPri    : macRemErrXcon            HighestDefect     : none
Defect Flags       : None
Mac Address        : 00:25:ba:01:c3:6a        CcmLtmPriority    : 7
CcmTx              : 0                        CcmSequenceErr    : 0
Eth-1Dm Threshold  : 3(sec)
Eth-Ais:           : Disabled
Eth-Tst:           : Disabled
CcmLastFailure Frame:
    None
XconCcmFailure Frame:
    None
-------------------------------------------------------------------------------
Mep Linktrace Message Information
-------------------------------------------------------------------------------
LtRxUnexplained    : 0                        LtNextSequence    : 2
LtStatus           : False                    LtResult          : False
TargIsMepId        : False                    TargMepId         : 0
TargMac            : 00:00:00:00:00:00        TTL               : 64
EgressId           : 00:00:00:25:ba:01:c3:6a  SequenceNum        : 1
LtFlags            : useFDBonly
-------------------------------------------------------------------------------
Mep Linktrace Replies
-------------------------------------------------------------------------------
SequenceNum        : 1                        ReceiveOrder      : 1
Ttl                : 63                       Forwarded         : False
LastEgressId       : 00:00:00:25:ba:01:c3:6a  TerminalMep       : True
NextEgressId       : 00:00:00:25:ba:00:5e:bf  Relay             : rlyHit
ChassisIdSubType   : unknown value (0)
ChassisId:
    None
ManAddressDomain:
    None
ManAddress:
    None
IngressMac         : 00:25:ba:00:5e:bf        Ingress Action    : ingOk
IngrPortIdSubType  : unknown value (0)
IngressPortId:
    None
EgressMac          : 00:00:00:00:00:00        Egress Action     : egrNoTlv
EgrPortIdSubType   : unknown value (0)
EgressPortId:
    None
Org Specific TLV:
    None
A:dut-b#
A:dut-b#

A:dut-b# show eth-cfm mep 1 domain 1 association 1 loopback
-------------------------------------------------------------------------------
Mep Information
-------------------------------------------------------------------------------
Md-index           : 1                        Direction         : Down
Ma-index           : 1                        Admin             : Enabled
```

```
MepId              : 1                        CCM-Enable        : Enabled
IfIndex            : 35946496                 PrimaryVid        : 1
FngState           : fngReset                 ControlMep        : False
LowestDefectPri    : macRemErrXcon            HighestDefect     : none
Defect Flags       : None
Mac Address        : 00:25:ba:01:c3:6a        CcmLtmPriority    : 7
CcmTx              : 0                        CcmSequenceErr    : 0
Eth-1Dm Threshold  : 3(sec)
Eth-Ais:           : Disabled
Eth-Tst:           : Disabled
CcmLastFailure Frame:
    None
XconCcmFailure Frame:
    None
-------------------------------------------------------------------------------
Mep Loopback Information
-------------------------------------------------------------------------------
LbRxReply          : 1                        LbRxBadOrder      : 0
LbRxBadMsdu        : 0                        LbTxReply         : 0
LbSequence         : 2                        LbNextSequence    : 2
LbStatus           : False                    LbResultOk        : True
DestIsMepId        : False                    DestMepId         : 0
DestMac            : 00:00:00:00:00:00        SendCount         : 0
VlanDropEnable     : True                     VlanPriority      : 7
Data TLV:
    None
A:dut-b#


*A:dut-b# show eth-cfm mep 1 domain 4 association 4 two-way-delay-test remote-peer
00:25:ba:00:5e:bf

===================================================================
Eth CFM Two-way Delay Test Result Table
===================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
-------------------------------------------------------------------
00:25:ba:00:5e:bf     507                 507
===================================================================
*A:dut-b#
*A:dut-b# show eth-cfm mep 1 domain 4 association 4 two-way-delay-test

===================================================================
Eth CFM Two-way Delay Test Result Table
===================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
-------------------------------------------------------------------
00:25:ba:00:5e:bf     507                 507
===================================================================
*A:dut-b#
*A:dut-a# show eth-cfm mep 2 domain 4 association 4  eth-test-results remote-peer
00:25:ba:01:c3:6a

===============================================================
Eth CFM ETH-Test Result Table
===============================================================
                                 Current        Accumulate
                  FrameCount     ErrBits        ErrBits
Peer Mac Addr     ByteCount      CrcErrs        CrcErrs
```

```
-------------------------------------------------------------
00:25:ba:01:c3:6a 6              0              0
                  384            0              0
=============================================================
*A:dut-a#
*A:dut-a# show eth-cfm mep 2 domain 4 association 4  eth-test-results

=============================================================
Eth CFM ETH-Test Result Table
=============================================================
                                 Current        Accumulate
                  FrameCount     ErrBits        ErrBits
Peer Mac Addr     ByteCount      CrcErrs        CrcErrs
-------------------------------------------------------------
00:25:ba:01:c3:6a 6              0              0
                  384            0              0
=============================================================
*A:dut-a# show eth-cfm mep 2 domain 4 association 4 one-way-delay-test remote-peer
00:25:ba:01:c3:6a

===================================================================
Eth CFM One-way Delay Test Result Table
===================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
-------------------------------------------------------------------
00:25:ba:01:c3:6a     402                 402
===================================================================
*A:dut-a#

*A:dut-a# show eth-cfm mep 2 domain 4 association 4 one-way-delay-test

===================================================================
Eth CFM One-way Delay Test Result Table
===================================================================
Peer Mac Addr         Delay (us)          Delay Variation (us)
-------------------------------------------------------------------
00:25:ba:01:c3:6a     402                 402
===================================================================
*A:dut-a#
```

Show output for two-way-slm-test

```
*A:7210SAS# show eth-cfm mep 1 domain 7 association 100 two-way-slm-test

===============================================================================

Eth CFM Two-way SLM Test Result Table (Test-id: 1)

===============================================================================

Peer Mac Addr      Remote MEP       Count     In Loss    Out Loss         Unack

-------------------------------------------------------------------------------

00:25:ba:0d:1e:12           2           1           0           0            0

===============================================================================

*A:7210SAS#
```

connection-profile

Syntax **connection-profile [conn-prof-id] [associations]**

Context show

Description This command displays connection profile information.

Parameters *conn-prof-id* — Specifies the connection profile ID.

Values 1 — 8000

associations — Displays the SAP and the service ID that use this connection profile.

Output **The following table describes show connection-profile command output fields**

Label	Description
CP Index	Identifies the connection-profile.
Number of Members	Indicates the number of ATM connection profile members not applicable for 7210.
HasRange	Indicates whether VLAN range is configured or not

Sample Output

Show output for connection-profile

```
*7210SAS>show# connection-profile

===============================================================================
Connection Profile Summary Information
===============================================================================
CP Index  Number of HasRange
          Members
-------------------------------------------------------------------------------
1         0         Yes
2         0         Yes
3         0         Yes
5         0         Yes
6         0         Yes
100       0         Yes
200       0         Yes
300       0         Yes
400       0         Yes
500       0         Yes
600       0         Yes
700       0         Yes
800       0         Yes
900       0         Yes
===============================================================================
*7210SAS>show#
```

Show output for connection-profile associations

```
*A:7210SAS>show# connection-profile associations

===============================================================================
Connection Profile Summary Information
===============================================================================
CP Index  Number of HasRange
          Members
-------------------------------------------------------------------------------
1         0         No
===============================================================================
*A:7210SAS>show#
```

VLL Show Commands

sap-using

Syntax **sap-using** [**sap** *sap-id*]
sap-using [**ingress**] **filter** *filter-id*
sap-using [**ingress**] **qos-policy** *qos-policy-id*

Context show>service

Description This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

Parameters **ingress —** Specifies matching an ingress policy.

ingress — Specifies matching an ingress policy.

ingress — Specifies matching an ingress policy.

qos-policy *qos-policy-id* **—** The ingress QoS Policy ID for which to display matching SAPs.

Values 1 — 65535

filter *filter-id* **—** The ingress or egress filter policy ID for which to display matching SAPs.

Values 1 — 65535

sap *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

Output **Show Service SAP —** The following table describes show service SAP output fields:

Label	Description
Port ID	The ID of the access port where the SAP is defined.
Svc ID	The service identifier.
MTU	The port MTU value.
Ing. QoS	The SAP ingress QoS policy number specified on the ingress SAP.
Ing Fltr	The MAC or IP filter policy ID applied to the ingress SAP.
Egr. QoS	The SAP egress QoS policy number specified on the egress SAP.
Egr. Fltr	The MAC or IP filter policy ID applied to the egress SAP.
Adm	The administrative state of the SAP.
Opr	The operational state of the SAP.

Label	Description (Continued)

Sample Output

```
*A:Dut-B# show service sap-using sap 1/1/3
===============================================================================
Service Access Points
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.   Adm  Opr
                                           QoS   Fltr    Fltr
-------------------------------------------------------------------------------
1/1/3                           2          1     none    none   Up   Down
-------------------------------------------------------------------------------
Number of SAPs : 1
===============================================================================
*A:Dut-B#
```

service-using

Syntax **service-using** [**epipe**] [**ies**] [**vpls**] [**mirror**] [**customer** *customer-id*]

Context show>service

Description This command displays the services matching certain usage properties.

If no optional parameters are specified, all services defined on the system are displayed.

Parameters [**service**] — Displays information for the specified service type.

customer *customer-id* **—** Displays services only associated with the specified customer ID.

Default Services associated with any customer.

Values 1 — 2147483647

Output **Show service-using output —** The following table describes the command output fields:

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The desired state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

Sample Output

```
*A:ALA-12# show service service-using customer 10
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            VPLS      Up     Up         10                09/05/2006 13:24:15
100          IES       Up     Up         10                09/05/2006 13:24:15
300          Epipe     Up     Up         10                09/05/2006 13:24:15
-------------------------------------------------------------------------------
Matching Services : 3
===============================================================================
*A:ALA-12#


*A:ALA-12# show service service-using
================================================================================
Services
```

```
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            uVPLS     Up     Up         1                 10/26/2006 15:44:57
2            Epipe     Up     Down       1                 10/26/2006 15:44:57
10           mVPLS     Down   Down       1                 10/26/2006 15:44:57
11           mVPLS     Down   Down       1                 10/26/2006 15:44:57
100          mVPLS     Up     Up         1                 10/26/2006 15:44:57
101          mVPLS     Up     Up         1                 10/26/2006 15:44:57
102          mVPLS     Up     Up         1                 10/26/2006 15:44:57
999          uVPLS     Down   Down       1                 10/26/2006 16:14:33
-------------------------------------------------------------------------------
Matching Services : 8
-------------------------------------------------------------------------------
*A:ALA-12#
```

id

Syntax **id** *service-id* {**all** | **arp** | **base**| **fdb** |**sap stp** | **interface** | **mstp-configuration** | **interface** | **igmp-snooping**}

Context show>service

Description This command displays information for a particular service-id.

Parameters *service-id* — The service identification number that identifies the service in the domain.

Values service-id: 1 — 214748364
svc-name: A string up to 64 characters in length.

all — Display detailed information about the service.

arp — Display ARP entries for the service.

base — Display basic service information.

fdb — Display FDB information.

igmp-snooping — Display IGMP snooping information

interface — Display service interfaces.

mstp-configuration — Display MSTP information.

sap — Display SAPs associated to the service.

stp — Display STP information.

all

Syntax **all**

Context show>service>id

Description This command displays detailed information for all aspects of the service.

Output **Show service ID Output —** The following table describes the output fields when the **all** option is specified:

Label	Description
`Service Id`	The service identifier.
`VPN Id`	The number which identifies the VPN.
`Service Type`	Specifies the type of service.
`VLL Type`	Specifies the VLL type.
`SDP Id`	The SDP identifier.
`Description`	Generic information about the service.
`Customer Id`	The customer identifier.

Label	Description (Continued)
Last Mgmt Change	The date and time of the most recent management-initiated change.
Endpoint	Specifies the name of the service endpoint.
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown, PortOperDown, L2OperDown, SapIngressQoSMismatch, SapEgressQoSMismatch,RelearnLimitExceeded, RxProtSrcMac, ParentIfAdminDown, NoSapIpipeCeIpAddr, TodResourceUnavail, TodMssResourceUnavail, SapParamMismatch, CemSapNoEcidOrMacAddr, StandByForMcRing, SapIngressNamedPoolMismatch, SapEgressNamedPoolMismatch, NoSapEpipeRingNode.
SAP Count	The number of SAPs specified for this service.
SDP Bind Count	The number of SDPs bound to this service.
Service Destination Points (SDPs)	
SDP Id	The SDP identifier.
Type	Indicates whether this Service SDP binding is a spoke or a mesh.
Admin Path MTU	The desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The operational state of this SDP.
Jitter Buffer (packets)	Indicates the jitter buffer length in number of packet buffers.
Playout Threshold (packets)	Indicates the playout buffer packets threshold in number of packet buffers.
Playout Threshold (packets)	Indicates the current packet depth of the jitter buffer.

Label	Description (Continued)
Peer Pw Bits	Indicates the bits set by the LDP peer when there is a fault on its side of the pseudowire. LAC failures occur on the SAP that has been configured on the pipe service, PSN bits are set by SDP-binding failures on the pipe service. The pwNotForwarding bit is set when none of the above failures apply, such as an MTU mismatch failure. This value is only applicable if the peer is using the pseudowire status signalling method to indicate faults. pwNotForwarding — Pseudowire not forwarding lacIngressFault Local — Attachment circuit RX fault lacEgresssFault Local — Attachment circuit TX fault psnIngressFault Local — PSN-facing PW RX fault psnEgressFault Local — PSN-facing PW TX fault pwFwdingStandby — Pseudowire in standby mode
Signaling Over-ride	Indicates the overriding signaled pseudowire type, as configured under the **signaled-vc-type-override** option for Apipes. This field is only displayed if **signaled-vc-type-override** is configured.
LLF Admin State	Displays the Link Loss Forwarding administrative state.
LLF Oper State	Displays the Link Loss Forwarding operational state.

Sample Output

```
*A:7210-E# show service id 2 all
===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 2                   Vpn Id            : 0
Service Type      : Epipe
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 05/31/2002 19:26:08
Last Mgmt Change  : 06/09/2002 18:53:34
Admin State       : Down                Oper State        : Down
SAP Count         : 1
Uplink Type:      : L2
SAP Type:         : Null-star           Customer vlan:    : n/a
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
SAP 1/1/1
-------------------------------------------------------------------------------
Service Id         : 2
SAP                : 1/1/1                    Encap             : null
Description        : (Not Specified)
Admin State        : Up                       Oper State        : Down
Flags              : ServiceAdminDown
                     PortOperDown
Last Status Change : 05/31/2002 19:26:08
Last Mgmt Change   : 06/09/2002 18:53:49
Dot1Q Ethertype    : 0x8100                   QinQ Ethertype    : 0x8100
```

```
LLF Admin State    : Down                      LLF Oper State    : Clear
Admin MTU          : 1514                      Oper MTU          : 1514
Ingr IP Fltr-Id    : n/a                       Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                       Egr Mac Fltr-Id   : n/a
tod-suite          : None
Ing Agg Rate Limit : max                       Egr Agg Rate Limit: max
Endpoint           : N/A
Q Frame-Based Acct : Disabled

Acct. Pol          : None                      Collect Stats     : Disabled
-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1
I. Sched Pol       : (Not Specified)
E. Sched Pol       : (Not Specified)
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 16                     Meters Allocated   : 8
Classifiers Used     : 1                      Meters Used        : 1
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Stats:          0                       0
Egress Stats:           0                       0
Ingress Drop Stats:     0                       0
Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats (in/out coiunter mode)
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Meter 1 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0
-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
No Endpoints found.
===============================================================================
*A:7210-E>

*A:ces-A# show service id 1 all

===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 1                   Vpn Id            : 0
Service Type      : Cpipe               VLL Type          : SAToPT1
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 07/06/2010 19:21:14
Last Mgmt Change  : 07/06/2010 19:21:14
Admin State       : Up                  Oper State        : Up
MTU               : 1514
Vc Switching      : False
SAP Count         : 1                   SDP Bind Count    : 1
-------------------------------------------------------------------------------
Service Destination Points(SDPs)
-------------------------------------------------------------------------------
```

```
-------------------------------------------------------------------------------
 Sdp Id 12:1  -(2.2.2.2)
-------------------------------------------------------------------------------
Description     : (Not Specified)
SDP Id            : 12:1                    Type              : Spoke
VC Type           : SAToPT1                 VC Tag            : 0
Admin Path MTU    : 0                       Oper Path MTU     : 9190
Far End           : 2.2.2.2                 Delivery          : MPLS

Admin State       : Up                      Oper State        : Up
Acct. Pol         : None                    Collect Stats     : Disabled
Ingress Label     : 131064                  Egress Label      : 131064
Admin ControlWord  : Preferred              Oper ControlWord  : True
Admin BW(Kbps)    : 0                       Oper BW(Kbps)     : 0
Last Status Change : 07/06/2010 19:21:14    Signaling         : TLDP
Last Mgmt Change  : 07/06/2010 19:21:14
Endpoint          : N/A                     Precedence        : 4
Flags             : None
Peer Pw Bits      : None
Peer Fault Ip     : None
Peer Vccv CV Bits  : lspPing
Peer Vccv CC Bits  : pwe3ControlWord mplsRouterAlertLabel

KeepAlive Information :
Admin State       : Enabled                 Oper State        : Alive
Hello Time        : 10                      Hello Msg Len     : 0
Max Drop Count    : 3                       Hold Down Time    : 10

Statistics           :
I. Fwd. Pkts.     : 141578                  I. Fwd. Octs.     : 31430316
E. Fwd. Pkts.     : 141583                  E. Fwd. Octets    : 31431426

Associated LSP LIST :
Lsp Name          : to_b_1_2
Admin State       : Up                      Oper State        : Up
Time Since Last Tr*: 04h08m22s
```

Sample output (Meter-override)

```
A:7210SAS>show>service# id 1101 sap 1/2/1:1 detail
Ingress Meter Override
-------------------------------------------------------------------------------

Meter Id          : 1
Admin PIR         : 12000                   Admin CIR         : 10000
Oper PIR          : 12000                   Oper CIR          : 10000
PIR Rule          : closest*                CIR Rule          : closest*
MBS               : max*                    CBS               : max*
Mode              : Trtcm2*

* means the value is inherited
-------------------------------------------------------------------------------
A:7210SAS>show>service#
```

base

Syntax **base**

Context show>service>id

Description Displays basic information about the service ID including service type, description, SAPs.

Output **Show Service-ID Base —** The following table describes show service-id base output fields:

Label	Description
`Service Id`	The service identifier.
`Vpn Id`	Specifies the VPN ID assigned to the service.
`Service Type`	The type of service: Epipe, VPLS, IES.
`Description`	Generic information about the service.
`Customer Id`	The customer identifier.
`Last Mgmt Change`	The date and time of the most recent management-initiated change to this customer.
`Adm`	The desired state of the service.
`Oper`	The operating state of the service.
`Mtu`	The largest frame size (in octets) that the service can handle.
`Def. Mesh VC Id`	This object is only valid in services that accept mesh SDP bindings. It is used to validate the VC ID portion of each mesh SDP binding defined in the service.
`SAP Count`	The number of SAPs defined on the service.
`SDP Bind Count`	The number of SDPs bound to the service.
`Identifier`	Specifies the service access (SAP) points.
`Type`	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received.
`AdmMTU`	Specifies the desired largest service frame size (in octets) that can be transmitted through this SAP, without requiring the packet to be fragmented.
`PBB Tunnel Point`	Specifies the endpoint in the B-VPLS environment where the Epipe terminates.
`Admin MTU`	Specifies the B-VPLS admin MTU.
`Backbone-Flooding`	Specifies whether or not the traffic is flooded in the B-VPLS for the detination instead of unicast. If the backbone destination MAC is in the B-VPLS FDB, then it will be unicast.

Label	Description (Continued)
ISID	The 24 bit field carrying the service instance identifier associated with the frame. It is used at the destination PE as a demultiplexor field.

Sample Output

```
A:ALU-7210#  show service id 6 base
===============================================================================
Service Basic Information
===============================================================================
Service Id        : 6                   Vpn Id            : 0
Service Type      : Epipe
Customer Id       : 1
Last Status Change: 07/05/2005 14:37:19
Last Mgmt Change  : 07/12/2005 18:05:12
Admin State       : Down                Oper State        : Down
SAP Count         : 2
Uplink Type:      : L2
SAP Type:         : Null-star           Customer vlan:    : n/a
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                               Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
sap:1/1/2                                null         1514    1514    Up   Down
sap:1/1/10                               null         1514    1514    Up   Down
===============================================================================
A:ALU-7210#
```

endpoint

Syntax **endpoint** [*endpoint-name*]

Context show>service>id

Description This command displays service endpoint information.

Parameters *endpoint-name* — Specifies the name of an existing endpoint for the service.

Sample Output

```
*A:ALU_SIM2>config>service>epipe# show service  id 200 base
===============================================================================
Service Basic Information
===============================================================================
Service Id        : 200                 Vpn Id            : 0
Service Type      : Epipe
Customer Id       : 1
Last Status Change: 11/14/2008 02:39:05
Last Mgmt Change  : 11/14/2008 02:31:21
Admin State       : Up                  Oper State        : Up
SAP Count         : 2
Uplink Type:      : L2
```

```
SAP Type:         : Dot1q Preserve      Customer vlan:    : 200
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                                Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
sap:1/1/1:200                             q-tag        1518    1518    Up   Up
sap:1/1/3:100.200                         qinq         1522    1522    Up   Up
===============================================================================
*A:ALU_SIM2>config>service>epipe#
```

sap

Syntax **sap** *sap-id* [**detail**]

Context show>service>id

Description This command displays information for the SAPs associated with the service. If no optional parameters are specified, a summary of all associated SAPs is displayed.

Parameters *sap-id* — The ID that displays SAPs for the service in the form *slot*/*mda*/*port*[**.***channel*]. See Common CLI Command Descriptions on page 483 for command syntax.

detail — Displays detailed information for the SAP.

stp — - Displays the stp information of the SAP.

Output **Show Service-ID SAP —** The following table describes show service SAP fields:

Label	Description
Service Id	The service identifier.
SAP	The SAP and qtag.
Encap	The encapsulation type of the SAP.
Ethertype	Specifies an Ethernet type II Ethertype value.
Admin State	The administrative state of the SAP.
Oper State	The operating state of the SAP.
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown, PortOperDown, PortMTUTooSmall, L2OperDown, SapIngressQoSMismatch, SapEgressQoSMismatch,RelearnLimitExceeded, RxProtSrcMac, ParentIfAdminDown, NoSapIpipeCeIpAddr, TodResourceUnavail, TodMssResourceUnavail, SapParamMismatch, ServiceMTUTooSmall, SapIngressNamedPoolMismatch, SapEgressNamedPoolMismatch, NoSapEpipeRingNode.
Last Status Change	The time of the most recent operating status change to this SAP.

Label	Description (Continued)
Last Mgmt Change	The time of the most recent management-initiated change to this SAP.
Admin MTU	The desired largest service frame size (in octets) that can be transmitted through the port to the far-end router, without requiring the packet to be fragmented.
Oper MTU	The actual largest service frame size (in octets) that can be transmitted through the port to the far-end router, without requiring the packet to be fragmented.
Ingress qos-policy	The ingress QoS policy ID assigned to the SAP.
Ingress Filter-Id	The ingress filter policy ID assigned to the SAP.
Egress Filter-Id	The egress filter policy ID assigned to the SAP.
Acct. Pol	The accounting policy ID assigned to the SAP.
Collect Stats	Specifies whether collect stats is enabled.
Ignore Oper Down	Displays whether user has enabled or disabled ignore-oper-down parameter.
The labels and description listed below are not supported on 7210 SAS-E devices:	
Loopback Mode	Displays the Ethernet port loop back mode
Loopback Src Addr	Displays the configured loopback source address
Loopback Dst Addr	Displays the configured loopback destination address
No-svc-port used	Displays the port ID of the port on which no service is configured. This port is used for the port loop back with MAC swap functionality.

Sample Output

```
*A:Dut-R# show service id 500 sap 1/1/5:*
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 500
SAP                : 1/1/5:*                   Encap             : q-tag
Dot1Q Ethertype    : 0x8100                    QinQ Ethertype    : 0x8100

Admin State        : Up                        Oper State        : Up
Flags              : None
Last Status Change : 01/06/2009 12:02:23
Last Mgmt Change   : 01/06/2009 12:01:23Loopback Mode : Internal No-svc-port used :
1/1/13
Loopback Src Addr : 00:00:00:22:22:22
Loopback Dst Addr : 00:00:00:11:11:11
Admin MTU          : 1518                      Oper MTU          : 1518
Ingress qos-policy : 1                         Egress qos-policy : 1
Shared Q plcy      : n/a                       Multipoint shared : Disabled
```

```
Ingr IP Fltr-Id    : n/a                       Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                       Egr Mac Fltr-Id   : n/a
tod-suite          : None                      qinq-pbit-marking : both
Egr Agg Rate Limit : max                       Endpoint          : N/A
Vlan-translation   : None

Acct. Pol          : None                      Collect Stats     : Disabled
Ignore Oper Down : Disabled
===============================================================================
*A:Dut-R#


*A:Dut-R# show service id 500 sap 1/1/5:*  detail
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 500
SAP                : 1/1/5:*                   Encap             : q-tag
Dot1Q Ethertype    : 0x8100                    QinQ Ethertype    : 0x8100

Admin State        : Up                        Oper State        : Up
Flags              : None
Last Status Change : 01/06/2009 12:02:23
Last Mgmt Change   : 01/06/2009 12:01:23
Admin MTU          : 1518                      Oper MTU          : 1518
Ingress qos-policy : 1                         Egress qos-policy : 1
Shared Q plcy      : n/a                       Multipoint shared : Disabled
Ingr IP Fltr-Id    : n/a                       Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                       Egr Mac Fltr-Id   : n/a
tod-suite          : None                      qinq-pbit-marking : both
Egr Agg Rate Limit : max                       Endpoint          : N/A
Vlan-translation   : None

Acct. Pol          : None                      Collect Stats     : Disabled
Ignore Oper Down : Disabled
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets
Ingress Packets rcvd:   0
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Meter 1 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0
===============================================================================
*A:Dut-R#
```

The following output displays LLF information.

```
*A:SIM6>config>service# show service id 2 sap 1/1/3 detail
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 2
SAP                : 1/1/3                     Encap             : null
Dot1Q Ethertype    : 0x8100                    QinQ Ethertype    : 0x8100
```

```
Admin State        : Up                        Oper State        : Down
Flags              : PortOperDown
Last Status Change : 01/21/2010 17:40:16
Last Mgmt Change   : 01/21/2010 17:40:16
Admin MTU          : 1514                      Oper MTU          : 1514
LLF Admin State    : Up                        LLF Oper State    : Clear
Ingress qos-policy : 1
Ingr IP Fltr-Id    : n/a                       Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                       Egr Mac Fltr-Id   : n/a
tod-suite          : None
Egr Agg Rate Limit : max                       Endpoint          : N/A

Acct. Pol          : None                      Collect Stats     : Disabled
Ignore Oper Down : Disabled
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets
Ingress Packets rcvd:   0
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                        Packets                 Octets

Ingress Meter 1 (Unicast)
Ingress Meter 1 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0
===============================================================================*A:SI
M6>config>service#
```

stp

Syntax **stp** [**detail**]

Context show>service>id

Description This command displays information for the spanning tree protocol instance for the service.

Parameters **detail** — Displays detailed information.

Output **Show Service-ID STP Output —** The following table describes show service-id STP output fields:

Label	Description
RSTP Admin State	Indicates the administrative state of the Rapid Spanning Tree Protocol instance associated with this service.
Core Connectivity	Indicates the connectivity status to the core.
RSTP Oper State	Indicates the operational state of the Rapid Spanning Tree Protocol instance associated with this service. This field is applicable only when STP is enabled on the router.

Label	Description (Continued)
Bridge-id	Specifies the MAC address used to identify this bridge in the network.
Hold Time	Specifies the interval length during which no more than two Configuration BPDUs shall be transmitted by this bridge.
Bridge fwd delay	Specifies how fast a bridge changes its state when moving toward the forwarding state.
Bridge Hello time	Specifies the amount of time between the transmission of Configuration BPDUs.
Bridge max age	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded. This is the actual value that this bridge is currently using.
Bridge priority	Defines the priority of the Spanning Tree Protocol instance associated with this service.
Topology change	Specifies whether a topology change is currently in progress.
Last Top. change	Specifies the time (in hundredths of a second) since the last time a topology change was detected by the Spanning Tree Protocol instance associated with this service.
Top. change count	Specifies the total number of topology changes detected by the Spanning Tree Protocol instance associated with this service since the management entity was last reset or initialized.
Root bridge-id	Specifies the bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol instance associated with this service. This value is used as the Root Identifier parameter in all Configuration BPDUs originated by this node.
Root path cost	Specifies the cost of the path to the root bridge as seen from this bridge.
Root forward delay	Specifies how fast the root changes its state when moving toward the forwarding state.
Rcvd hello time	Specifies the amount of time between the transmission of configuration BPDUs.
Root max age	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded.
Root priority	This object specifies the priority of the bridge that is currently selected as root-bridge for the network.
Root port	Specifies the port number of the port which offers the lowest cost path from this bridge to the root bridge.
SAP Identifier	The ID of the access port where this SAP is defined.
RSTP State	The operational state of RSTP.

Label	Description (Continued)
STP Port State	Specifies the port identifier of the port on the designated bridge for this port's segment.
BPDU encap	Specifies the type of encapsulation used on BPDUs sent out and received on this SAP.
Port Number	Specifies the value of the port number field which is contained in the least significant 12 bits of the 16-bit port ID associated with this SAP.
Port Priority	Specifies the value of the port priority field which is contained in the most significant 4 bits of the 16-bit port ID associated with this SAP.
Port Path Cost	Specifies the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
Fast Start	Specifies whether Fast Start is enabled on this SAP.
Designated Port	Specifies the port identifier of the port on the designated bridge for this port's segment.
Designated Bridge	Specifies the bridge identifier of the bridge which this port considers to be the designated bridge for this port's segment.

```
*A:ALU_SIM2>config>service>vpls>sap# show service id 1 stp
===============================================================================
Stp info, Service 1
===============================================================================
Bridge Id          : 00:00.00:45:67:32:10:ab  Top. Change Count : 2
Root Bridge        : This Bridge              Stp Oper State    : Up
Primary Bridge     : N/A                      Topology Change   : Inactive
Mode               : Rstp                     Last Top. Change  : 1d 18:34:36
Vcp Active Prot.   : N/A
Root Port          : N/A                      External RPC      : 0
===============================================================================
Stp port info
===============================================================================
Sap Id             Oper-     Port-      Port-       Port-  Oper-  Link-  Active
                   State     Role       State       Num    Edge   Type   Prot.
-------------------------------------------------------------------------------
1/1/21:1           Up        Designated Forward     2048   True   Pt-pt  Rstp
lag-1:1.1          Up        Designated Forward     2049   False  Pt-pt  Rstp
lag-2:1.1          Up        Designated Forward     2050   False  Pt-pt  Rstp
===============================================================================
*A:ALU_SIM2>config>service>vpls>sap#


*A:ALU_SIM2>config>service>vpls>sap#  show service id 1 stp detail
===============================================================================
Spanning Tree Information
===============================================================================
-------------------------------------------------------------------------------
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
VPLS oper state    : Up
Stp Admin State    : Up                       Stp Oper State    : Up
```

```
Mode               : Rstp                      Vcp Active Prot.  : N/A

Bridge Id          : 00:00.00:45:67:32:10:ab  Bridge Instance Id: 0
Bridge Priority    : 0                         Tx Hold Count     : 6
Topology Change    : Inactive                  Bridge Hello Time : 2
Last Top. Change   : 1d 18:35:18               Bridge Max Age    : 20
Top. Change Count  : 2                         Bridge Fwd Delay  : 15

Root Bridge        : This Bridge
Primary Bridge     : N/A

Root Path Cost     : 0                         Root Forward Delay: 15
Rcvd Hello Time    : 2                         Root Max Age      : 20
Root Priority      : 0                         Root Port         : N/A
-------------------------------------------------------------------------------
Spanning Tree Sap Specifics
-------------------------------------------------------------------------------
SAP Identifier     : 1/1/21:1                  Stp Admin State   : Up
Port Role          : Designated                Port State        : Forwarding
Port Number        : 2048                      Port Priority     : 128
Port Path Cost     : 10                        Auto Edge         : Enabled
Admin Edge         : Disabled                  Oper Edge         : True
Link Type          : Pt-pt                     BPDU Encap        : Dot1d
Root Guard         : Disabled                  Active Protocol   : Rstp
Last BPDU from     : N/A
CIST Desig Bridge  : This Bridge               Designated Port   : 34816
Forward transitions: 2                         Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                         Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                         TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                         RST BPDUs tx      : 79126
MST BPDUs rcvd     : 0                         MST BPDUs tx      : 0

SAP Identifier     : lag-1:1.1                 Stp Admin State   : Up
Port Role          : Designated                Port State        : Forwarding
Port Number        : 2049                      Port Priority     : 128
Port Path Cost     : 10                        Auto Edge         : Enabled
Admin Edge         : Disabled                  Oper Edge         : False
Link Type          : Pt-pt                     BPDU Encap        : Dot1d
Root Guard         : Disabled                  Active Protocol   : Rstp
Last BPDU from     : 10:00.00:f3:f0:98:97:00
CIST Desig Bridge  : This Bridge               Designated Port   : 34817
Forward transitions: 1                         Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                         Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                         TCN BPDUs tx      : 0
RST BPDUs rcvd     : 5                         RST BPDUs tx      : 79128
MST BPDUs rcvd     : 0                         MST BPDUs tx      : 0

SAP Identifier     : lag-2:1.1                 Stp Admin State   : Up
Port Role          : Designated                Port State        : Forwarding
Port Number        : 2050                      Port Priority     : 128
Port Path Cost     : 10                        Auto Edge         : Enabled
Admin Edge         : Disabled                  Oper Edge         : False
Link Type          : Pt-pt                     BPDU Encap        : Dot1d
Root Guard         : Disabled                  Active Protocol   : Rstp
Last BPDU from     : 20:00.00:e0:b1:99:cb:2a
CIST Desig Bridge  : This Bridge               Designated Port   : 34818
Forward transitions: 1                         Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                         Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                         TCN BPDUs tx      : 0
RST BPDUs rcvd     : 6                         RST BPDUs tx      : 78760
MST BPDUs rcvd     : 0                         MST BPDUs tx      : 0
```

```
===============================================================================
*A:ALU_SIM2>config>service>vpls>sap#
```

VLL Clear Commands

id

Syntax **id** *service-id*

Context clear>service
clear>service>statistics

Description This command clears commands for a specific service.

Parameters *service-id* — The ID that uniquely identifies a service.

Values service-id: 1 — 214748364
svc-name: A string up to 64 characters in length.

sap

Syntax **sap** *sap-id* {**all** | **counters** | **stp**}

Context clear>service>statistics

Description This command clears SAP statistics for a SAP.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

all — Clears all SAP queue statistics and STP statistics.

counters — Clears all queue statistics associated with the SAP.

stp — Clears all STP statistics associated with the SAP.

l2pt — Clears all L2PT statistics associated with the SDP.

counters

Syntax **counters**

Context clear>service>statistics>id

Description This command clears all traffic queue counters associated with the service ID.

stp

Syntax **stp**

Context clear>service>statistics>id

Description Clears all spanning tree statistics for the service ID.

VLL Debug Commands

id

Syntax **id** *service-id*

Context debug>service

Description This command debugs commands for a specific service.

Parameters *service-id* — The ID that uniquely identifies a service.

sap

Syntax [**no**] **sap** *sap-id*

Context debug>service>id

Description This command enables debugging for a particular SAP.

Parameters *sap-id* — Specifies the SAP ID.

VPLS Show Commands

fdb-info

Syntax **fdb-info**

Context show>service

Description Displays global FDB usage information.

Output **Show FDB-Info Command Output —** The following table describes show FDB-Info command output.

Label	Description
`Service ID`	The value that identifies a service.
`Mac Move`	Indicates the administrative state of the MAC movement feature associated with the service.
`Mac Move Rate`	The maximum rate at which MAC's can be re-learned in this TLS service, before the SAP where the moving MAC was last seen is automatically disabled in order to protect the system against undetected loops or duplicate MAC's. The rate is computed as the maximum number of re-learns allowed in a 5 second interval. The default rate of 10 re-learns per second corresponds to 50 re-learns in a 5 second period.
`Mac Move Timeout`	Indicates the time in seconds to wait before a SAP that has been disabled after exceeding the maximum re-learn rate is re-enabled. A value of zero indicates that the SAP will not be automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled in order to avoid thrashing.
`Table Size`	The maximum number of learned and static entries allowed in the FDB.
`Total Count`	The current number of entries (both learned and static) in the FDB of this service.
`Learned Count`	The current number of learned entries in the FDB of this service.
`Static Count`	The current number of static entries in the FDB of this service.
`Remote Age`	The number of seconds used to age out FDB entries learned on an SDP. These entries correspond to MAC addresses learned on remote SAPs.
`Local Age`	The seconds used to age out FDB entries learned on local SAPs.
`High WaterMark`	The utilization of the FDB table of this service at which a ‘table full’ alarm is raised by the agent.

Label	Description (Continued)
Low WaterMark	The utilization of the FDB table of this service at which a ‘table full’ alarm is cleared by the agent.
Mac Learning	Specifies whether the MAC learning process is enabled in this service.
Discard Unknown	Specifies whether frames received with an unknown destination MAC are discarded in this service.
MAC Aging	Specifies whether the MAC aging process is enabled in this service.
MAC Pinning	Specifies whether MAC pinning is enabled in this service.
Relearn Only	When enabled, indicates that either the FDB table of this service is full or that the maximum system-wide number of MAC's supported by the agent has been reached, and thus MAC learning is temporary disabled, and only MAC re-learns can take place.
Total Service FDB	The current number of service FDBs configured on this node.
Total FDB Configured Size	The sum of configured FDBs.
Total FDB Entries In Use	The total number of entries (both learned and static) in use.

Sample Output

```
A:7210-SASE# show service fdb-info
===============================================================================
Forwarding Database(FDB) Information
===============================================================================================
============ Service Id : 1 Mac Move : Disabled
Primary Factor : 3 Secondary Factor : 2
Mac Move Rate : 2 Mac Move Timeout : 10
Mac Move Retries : 3
Table Size : 250 Total Count : 1
Learned Count : 0 Static Count : 0
Host-learned Count: 1
Remote Age : 900 Local Age : 300
High Watermark : 95% Low Watermark : 90%
Mac Learning : Enabled Discard Unknown : Disabled
Mac Aging : Enabled Relearn Only : False
Mac Subnet Len : 48
-------------------------------------------------------------------------------
Total Service FDBs : 1
Total FDB Configured Size : 250
Total FDB Entries In Use : 1
PBB MAC Address Indices In Use : 0
-------------------------------------------------------------------------------
===============================================================================
A:7210-SASE#
```

fdb-mac

Syntax **fdb-mac** *ieee-address* [**expiry**]

Context show>service

Description This command displays the FDB entry for a given MAC address.

Parameters *ieee-address* — The 48-bit MAC address for which to display the FDB entry 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.

expiry — Shows the time until the MAC is aged out.

Output **Show FDB-MAC Command Output —** The following table describes the show FDB MAC command output fields:

Label	Description
Service ID	The service ID number.
MAC	The specified MAC address
Source-Identifier	The location where the MAC is defined.
Type/Age	Static — FDB entries created by management. Learned — Dynamic entries created by the learning process. OAM — Entries created by the OAM process. H — Host, the entry added by the system for a static configured subscriber host. D or DHCP — DHCP-installed MAC. Learned addresses can be temporarily frozen by the DHCP snooping application for the duration of a DHCP lease. P — Indicates the MAC is protected by the MAC protection feature.

Sample Output

```
*A:ALA-12# show service fdb-mac 00:99:00:00:00:00
===============================================================================
Services Using Forwarding Database Mac 00:99:00:00:00:00
===============================================================================
ServId  MAC                     Source-Identifier       Type/Age Last Change
-------------------------------------------------------------------------------
1       00:99:00:00:00:00             sap:1/2/7:0               Static
===============================================================================
*A:ALA-12#
```

sap-using

Syntax **sap-using** [**ingress** | **egress**] **filter** *filter-id*
sap-using [**sap** *sap-id*]

show>service **Context**

Description This command displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs.

The optional parameters restrict output to only SAPs matching the specified properties.

Parameters **ingress** — Specifies matching an ingress policy.

egress — Specifies matching an egress policy.

filter *filter-id* — The ingress or egress filter policy ID for which to display matching SAPs.

Values 1 — 65535

sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

Output **Show Service SAP —** The following table describes show service SAP output fields:

Label	Description
Port ID	The ID of the access port where the SAP is defined.
Svc ID	The service identifier.
I.QoS	The SAP ingress QoS policy number specified on the ingress SAP.
I.MAC/IP	The MAC or IP filter policy ID applied to the ingress SAP.
Egr. Fltr	The filter policy ID applied to the egress SAP.
A.Pol	The accounting policy ID assigned to the SAP.
Adm	The administrative state of the SAP.
Opr	The actual state of the SAP.

Sample Output

```
*A:ALU_SIM2>config>service>vpls# show service sap-using
===============================================================================
Service Access Points
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.   Adm  Opr
                                           QoS   Fltr    Fltr
-------------------------------------------------------------------------
1/1/1:10                        1          1     none     none   Up   Up
1/1/3:500.*                     1          1     none     none   Up   Up
1/1/1:200                       200        1     none     none   Up   Up
1/1/3:100.200                   200        1     none     none   Up   Up
1/1/1:300                       300        1     none     none   Up   Up
```

```
-------------------------------------------------------------------------------
Number of SAPs : 5
-------------------------------------------------------------------------------
*A:ALU_SIM2>config>service>vpls#
```

service-using

Syntax **service-using** [**epipe**] [**ies**] [**vpls**] [**mirror**] [**customer** *customer-id*]

Context show>service

Description This command displays the services matching certain usage properties. If no optional parameters are specified, all services defined on the system are displayed.

Parameters **epipe —** Displays matching Epipe services.

ies — Displays matching IES instances.

vpls — Displays matching VPLS instances.

mirror — Displays matching mirror services.

customer *customer-id* **—** Displays services only associated with the specified customer ID.

Default Services associated with a customer.

Values 1 — 2147483647

Output **Show Service Service-Using —** The following table describes show service service-using output fields:

Label	Description
Service Id	The service identifier.
Type	Specifies the service type configured for the service ID.
Adm	The administrative state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

Sample Output

```
*A:ALA-12# show service service-using customer 10
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
1            VPLS      Up     Up         10                09/05/2006 13:24:15
100          IES       Up     Up         10                09/05/2006 13:24:15
300          Epipe     Up     Up         10                09/05/2006 13:24:15
```

```
-------------------------------------------------------------------------------
Matching Services : 3
===============================================================================
*A:ALA-12#


*A:ALA-12# show service service-using epipe
===============================================================================
Services [epipe]
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
6            Epipe     Up     Up         6                 09/22/2006 23:05:58
7            Epipe     Up     Up         6                 09/22/2006 23:05:58
8            Epipe     Up     Up         3                 09/22/2006 23:05:58
103          Epipe     Up     Up         6                 09/22/2006 23:05:58
-------------------------------------------------------------------------------
Matching Services : 4
===============================================================================
*A:ALA-12#


*A:ALA-14# show service service-using
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
10           mVPLS     Down   Down       1                 10/26/2006 15:44:57
11           mVPLS     Down   Down       1                 10/26/2006 15:44:57
100          mVPLS     Up     Up         1                 10/26/2006 15:44:57
101          mVPLS     Up     Up         1                 10/26/2006 15:44:57
102          mVPLS     Up     Up         1                 10/26/2006 15:44:57
-------------------------------------------------------------------------------
Matching Services : 5
-------------------------------------------------------------------------------
*A:ALA-14#


*A:SetupCLI# show service service-using
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
23           mVPLS     Up     Down       2                 09/25/2007 21:45:58
100          Epipe     Up     Down       2                 09/25/2007 21:45:58
101          Epipe     Up     Down       2                 09/25/2007 21:45:58
102          Epipe     Up     Down       2                 09/25/2007 21:45:58
105          Epipe     Up     Down       2                 09/25/2007 21:45:58
110          Epipe     Up     Down       1                 09/25/2007 21:45:58
990          IES       Up     Down       1                 09/25/2007 21:45:58
1000         Mirror    Up     Down       1                 09/25/2007 21:45:59
1001         Epipe     Up     Down       1                 09/25/2007 21:45:58
1002         Epipe     Up     Down       1                 09/25/2007 21:45:58
1003         Epipe     Up     Down       1                 09/25/2007 21:45:58
1004         Epipe     Up     Down       1                 09/25/2007 21:45:58
2000         Mirror    Up     Down       1                 09/25/2007 21:45:59
...
-------------------------------------------------------------------------------
Matching Services : 27
```

```
-------------------------------------------------------------------------------
*A:SetupCLI#


*A:SetupCLI# show service service-using
===============================================================================
Services
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
23           mVPLS     Up     Down       2                 09/25/2007 21:45:58
100          Epipe     Up     Down       2                 09/25/2007 21:45:58
101          Epipe     Up     Down       2                 09/25/2007 21:45:58
102          Epipe     Up     Down       2                 09/25/2007 21:45:58
105          Epipe     Up     Down       2                 09/25/2007 21:45:58
110          Epipe     Up     Down       1                 09/25/2007 21:45:58
990          IES       Up     Down       1                 09/25/2007 21:45:58
1000         Mirror    Up     Down       1                 09/25/2007 21:45:59
1001         Epipe     Up     Down       1                 09/25/2007 21:45:58
1002         Epipe     Up     Down       1                 09/25/2007 21:45:58
1003         Epipe     Up     Down       1                 09/25/2007 21:45:58
...
-------------------------------------------------------------------------------
Matching Services : 27
-------------------------------------------------------------------------------
*A:SetupCLI#
```

id

Syntax **id** *service-id*

Context show>service

Description This command displays information for a particular service-id.

Parameters *service-id* — The unique service identification number that identifies the service in the service domain.

Values service-id: 1 — 214748364
svc-name: A string up to 64 characters in length.

all — Display detailed information about the service.

arp — Display ARP entries for the service.

base — Display basic service information.

fdb — Display FDB entries.

igmp-snooping — Display IGMP snooping information.

interface — Display service interfaces.

mstp-configuration — - Display MSTP information.

sap — Display SAPs associated to the service.

stp — Display STP information.

all

Syntax **all**

Context show>service>id

Description This command displays detailed information for all aspects of the service.

Output **Show service ID all output —** The following table describes the command output fields.

Label	Description
`Service Id`	The service identifier.
`VPN Id`	The number which identifies the VPN.
`Service Type`	Specifies the type of service.
`SDP Id`	The SDP identifier.
`Description`	Generic information about the service.
`Customer Id`	The customer identifier.
`Last Mgmt Change`	The date and time of the most recent management-initiated change to this customer.

Label	Description (Continued)
SAP Count	The number of SAPs specified for this service.
SDP Bind Count	The number of SDPs bound to this service.
Split Horizon Group	Name of the split horizon group for this service.
Description	Description of the split horizon group.
Last Changed	The date and time of the most recent management-initiated change to this split horizon group.
SDP Id	The SDP identifier.
Type	Indicates whether this service SDP binding is a spoke or a mesh.
Admin Path MTU	The desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDPSAP.
Oper State	The operational state of this SDPSAP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.
Ingress Filter	The ID of the ingress filter policy.
Egress Filter	The ID of the egress filter policy.
Far End	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Last Changed	The date and time of the most recent change to this customer.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.

Label	Description (Continued)
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
SDP Delivery Mechanism	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the Far End field.
Number of SDPs	The total number SDPs applied to this service ID.
Service Id	The service identifier.
Port Id	The ID of the access port where this SAP is defined.
Description	Generic information about the SAP.
Encap Value	The value of the label used to identify this SAP on the access port.
Admin State	The administrative state of the SAP.
Oper State	The operating state of the SAP.
Last Changed	The date and time of the last change.
Admin MTU	The desired largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Oper MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Ingress qos-policy	The SAP ingress QoS policy ID.
Egress qos-policy	The SAP egress QoS policy ID.
Ingress Filter-Id	The SAP ingress filter policy ID.
Egress Filter-Id	The SAP egress filter policy ID.
Multi Svc Site	Indicates the multi-service site that the SAP is a member.
Ingress sched-policy	Indicates the ingress QoS scheduler for the SAP.
Egress sched-policy	Indicates the egress QoS scheduler for the SAP.
Acct. Pol	Indicates the accounting policy applied to the SAP.
Collect Stats	Specifies whether accounting statistics are collected on the SAP.
Dropped	The number of packets or octets dropped.
Offered Hi Priority	The number of high priority packets, as determined by the SAP ingress QoS policy.
Offered Low Priority	The number of low priority packets, as determined by the SAP ingress QoS policy.

Label	Description (Continued)
Offered Low Priority	The number of low priority packets, as determined by the SAP ingress QoS policy.
Forwarded In Profile	The number of in-profile packets or octets (rate below CIR) forwarded.
Forwarded Out Profile	The number of out-of-profile packets or octets (rate above CIR) forwarded.
Dropped In Profile	The number of in-profile packets or octets discarded.
Dropped Out Profile	The number of out-of-profile packets or octets discarded.
Forwarded In Profile	The number of in-profile packets or octets (rate below CIR) forwarded.
Forwarded Out Profile	The number of out-of-profile packets or octets (rate above CIR) forwarded.
Ingress Queue 1	The index of the ingress QoS queue of this SAP.
High priority offered	The packets or octets count of the high priority traffic for the SAP.
High priority dropped	The number of high priority traffic packets/octets dropped.
Low priority offered	The packets or octets count of the low priority traffic.
Low priority dropped	The number of low priority traffic packets/octets dropped.
In profile forwarded	The number of in-profile packets or octets (rate below CIR) forwarded.
Out profile forwarded	The number of out-of-profile octets (rate above CIR) forwarded.
Egress Queue 1	The index of the egress QoS queue of the SAP.
In profile forwarded	The number of in-profile packets or octets (rate below CIR) forwarded.
In profile dropped	The number of in-profile packets or octets dropped for the SAP.
Out profile forwarded	The number of out-of-profile packets or octets (rate above CIR) forwarded.
Out profile dropped	The number of out-of-profile packets or octets discarded.
State	Specifies whether DHCP Relay is enabled on this SAP.
Info Option	Specifies whether Option 82 processing is enabled on this SAP.
Action	Specifies the Option 82 processing on this SAP or interface: keep, replace or drop.

Label	Description (Continued)
Circuit ID	Specifies whether the If Index is inserted in Circuit ID sub-option of Option 82.
Remote ID	Specifies whether the far-end MAC address is inserted in Remote ID sub-option of Option 82.
Managed by Service	Specifies the service-id of the management VPLS managing this SAP.
Managed by MSTI	Specifies the MST instance inside the management VPLS managing this SAP.
Last BPDU from	The bridge ID of the sender of the last BPDU received on this SAP.
Managed by SAP	Specifies the sap-id inside the management VPLS managing this SAP.
Prune state	Specifies the STP state inherited from the management VPLS.
Managed by Service	Specifies the service-id of the management VPLS managing this SAP.
Last BPDU from	The bridge ID of the sender of the last BPDU received on this SAP.
Managed by Spoke	Specifies the sap-id inside the management VPLS managing this spoke SDP.
Prune state	Specifies the STP state inherited from the management VPLS.

Sample Output

```
*A:7210-E> show service id 1 all
===============================================================================
Service Detailed Information
===============================================================================
Service Id        : 1                   Vpn Id            : 0
Service Type      : VPLS
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 05/31/2002 19:26:08
Last Mgmt Change  : 06/07/2002 18:14:58
Admin State       : Down                Oper State        : Down
SAP Count         : 1
Uplink Type:      : L2
SAP Type:         : Null-star           Customer vlan:    : n/a
-------------------------------------------------------------------------------
Service Access Points
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
SAP 1/1/1
-------------------------------------------------------------------------------
Service Id         : 1
SAP                : 1/1/1                    Encap             : null
Description        : (Not Specified)
Admin State        : Up                       Oper State        : Down
Flags              : ServiceAdminDown
                     PortOperDown
Last Status Change : 05/31/2002 19:26:08
Last Mgmt Change   : 06/07/2002 18:15:31
Dot1Q Ethertype    : 0x8100                   QinQ Ethertype    : 0x8100
```

```
Max Nbr of MAC Addr: No Limit                 Total MAC Addr    : 0
Learned MAC Addr   : 0                        Static MAC Addr   : 0
Admin MTU          : 1514                     Oper MTU          : 1514
Ingr IP Fltr-Id    : n/a                      Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                      Egr Mac Fltr-Id   : n/a
tod-suite          : None
Ing Agg Rate Limit : max                      Egr Agg Rate Limit: max
Q Frame-Based Acct : Disabled
Mac Learning       : Enabled                  Discard Unkwn Srce: Disabled
Mac Aging          : Enabled                  Mac Pinning       : Disabled
BPDU Translation   : Disabled
L2PT Termination   : Disabled

Acct. Pol          : None                     Collect Stats     : Disabled
-------------------------------------------------------------------------------
Stp Service Access Point specifics
-------------------------------------------------------------------------------
Stp Admin State    : Up                       Stp Oper State    : Down
Core Connectivity  : Down
Port Role          : N/A                      Port State        : Discarding
Port Number        : 2048                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : N/A
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : N/A
Last BPDU from     : N/A
CIST Desig Bridge  : N/A                      Designated Port   : N/A

Forward transitions: 0                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 0
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0
-------------------------------------------------------------------------------
ARP host
-------------------------------------------------------------------------------
Admin State        : outOfService
Host Limit         : 1                        Min Auth Interval : 15 minutes
-------------------------------------------------------------------------------
QOS
-------------------------------------------------------------------------------
Ingress qos-policy : 1
I. Sched Pol       : (Not Specified)
E. Sched Pol       : (Not Specified)
-------------------------------------------------------------------------------
Ingress QoS Classifier Usage
-------------------------------------------------------------------------------
Classifiers Allocated: 16                    Meters Allocated   : 8
Classifiers Used     : 2                     Meters Used        : 2
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Stats:          0                       0
Egress Stats:           0                       0
Ingress Drop Stats:     0                       0
Extra-Tag Drop Stats:   n/a                     n/a
-------------------------------------------------------------------------------
Sap per Meter stats (forward/drop counter mode)
-------------------------------------------------------------------------------
```

```
                        Packets                 Octets
Ingress Meter 1 (Unicast)
Total Forwarded       : 0                       0
Total Dropped         : 0                       0

Ingress Meter 11 (Multipoint)
Total Forwarded       : 0                       0
Total Dropped         : 0                       0

-------------------------------------------------------------------------------
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
VPLS oper state    : Down                     Core Connectivity : Down
Stp Admin State    : Down                     Stp Oper State    : Down
Mode               : Rstp                     Vcp Active Prot.  : N/A

Bridge Id          : 80:00.00:a0:ff:43:21:cb  Bridge Instance Id: 0
Bridge Priority    : 32768                    Tx Hold Count     : 6
Topology Change    : Inactive                 Bridge Hello Time : 2
Last Top. Change   : 0d 00:00:00              Bridge Max Age    : 20
Top. Change Count  : 0                        Bridge Fwd Delay  : 15
MST region revision: 0                        Bridge max hops   : 20
MST region name    :

Root Bridge        : N/A
Primary Bridge     : N/A

Root Path Cost     : 0                        Root Forward Delay: 15
Rcvd Hello Time    : 2                        Root Max Age      : 20
Root Priority      : 32768                    Root Port         : N/A
-------------------------------------------------------------------------------
Forwarding Database specifics
-------------------------------------------------------------------------------
Service Id : 1 Mac Move : Disabled
Primary Factor : 3 Secondary Factor : 2
Mac Move Rate : 2 Mac Move Timeout : 10
Mac Move Retries : 3
Table Size : 250 Total Count : 1
Learned Count : 0 Static Count : 0
Host-learned Count: 1
Remote Age : 900 Local Age : 300
High Watermark : 95% Low Watermark : 90%
Mac Learning : EnabledDiscard Unknown : Disabled
Mac Aging : Enabled Relearn Only : False
Mac Subnet Len : 48
-------------------------------------------------------------------------------
IGMP Snooping Base info
-------------------------------------------------------------------------------
Admin State : Down
Querier     : No querier found
-------------------------------------------------------------------------------
Sap                    Oper    MRtr Send    Max  Max  Num
Id                     State   Port Queries Grps Srcs Grps
-------------------------------------------------------------------------------
sap:1/1/1              Down    No   No      None None 0
-------------------------------------------------------------------------------
Service Endpoints
-------------------------------------------------------------------------------
No Endpoints found.
===============================================================================
*A:7210-E>
```

```
Ignore Standby Sig : False                    Block On Mesh Fail: False
```

arp

Syntax **arp** [*ip-address*] | [**mac** *ieee-address*] | [**sap** *sap-id*] | [**interface** *ip-int-name*]

Context show>service>id

Description This command displays the ARP table for the VPLS instance. The ARP entries for a subscriber interface are displayed uniquely. Each MAC associated with the subscriber interface child group-interfaces is displayed with each subscriber interface ARP entry for easy lookup.

Parameters *ip-address* — All IP addresses.

mac ieee-address — Displays only ARP entries in the ARP table with the specified 48-bit MAC address. The MAC address is 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.

Default All MAC addresses.

sap *sap-id* **—** Displays SAP information for the specified SAP ID.

interface **—** Specifies matching service ARP entries associated with the IP interface.

ip-address — The IP address of the interface for which to display matching ARP entries.

Values 1.0.0.0 — 223.255.255.255

ip-int-name — The IP interface name for which to display matching ARPs.

Output **Show Service-ID ARP** **—** The following table describes show service-id ARP output fields.

Label	Description
IP Address	The IP address.
MAC Address	The specified MAC address.
	Type Static — FDB entries created by management.
	Learned — Dynamic entries created by the learningprocess.
	Other — Local entries for the IP interfaces created.
Expiry	The age of the ARP entry.
Interface	The interface applied to the service.
SAP	The SAP ID.

base

Syntax **base** [**msap**]

Context show>service>id

Description This command displays basic information about the service ID including service type, description, and SAPs.

Output **Show Service-ID Base —** The following table describes show service-id base output fields:

Label	Description
Service Id	The service identifier.
`Service Type`	Displays the type of service.
`Description`	Generic information about the service.
`Customer Id`	The customer identifier.
`Last Mgmt Change`	The date and time of the most recent management-initiated change to this customer.
`Adm`	The administrative state of the service.
`Oper`	The operational state of the service.
`Mtu`	The largest frame size (in octets) that the port can handle.
`Adm`	The largest frame size (in octets) that the SAP can handle.
`SAP Count`	The number of SAPs defined on the service.
`SAP Type`	The type of SAPs allowed in the service. It also describes the applied processing by the node to the packets received on these SAPs.
`Identifier`	Specifies the service access (SAP).
`OprMTU`	Specifies the actual largest service frame size (in octets) that can be transmitted through this port, without requiring the packet to be fragmented.
`Opr`	The operating state of the SAP

Sample Output

```
A:ALU-7210>config>service>vpls# show service id 700 base
===============================================================================
Service Basic Information
===============================================================================
Service Id        : 700                 Vpn Id            : 0
```

```
Service Type      : VPLS
Customer Id       : 1
Last Status Change: 09/19/2005 16:25:28
Last Mgmt Change  : 09/21/2005 14:07:07
Admin State       : Down                Oper State        : Down
SAP Count         : 1
Uplink Type:      : L2
SAP Type:         : Null-star           Customer vlan:    : n/a
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                                Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
sap:1/1/2                                 null         1514    1514    Up   Down
===============================================================================
A:ALU-7210>config>service>vpls#
*A:ALU_SIM2>config>service>vpls# show service  id 600 base
===============================================================================
Service Basic Information
===============================================================================
Service Id        : 600                 Vpn Id            : 0
Service Type      : uVPLS
Customer Id       : 1
Last Status Change: 11/17/2008 00:12:16
Last Mgmt Change  : 11/14/2008 03:36:21
Admin State       : Up                  Oper State        : Down
SAP Count         : 3
Uplink Type:      : L2
SAP Type:         : Dot1q               Customer vlan:    : n/a
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                                Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
sap:1/1/1:950                             q-tag        1518    1518    Down Down
sap:1/1/2:1450                            q-tag        1518    1518    Down Down
sap:1/1/3:3000.*                          qinq         1522    1522    Down Down
===============================================================================
*A:ALU_SIM2>config>service>vpls#

*A:7210SAS-D>show>service# id 15 base

===============================================================================
Service Basic Information
===============================================================================
Service Id        : 15                  Vpn Id            : 0
Service Type      : Epipe
Description       : (Not Specified)
Customer Id       : 40
Last Status Change: 01/01/1970 00:00:14
Last Mgmt Change  : 01/11/1970 23:34:24
Admin State       : Down                Oper State        : Down
SAP Count         : 1
Uplink Type:      : L2
SAP Type:         : Any                 Customer vlan:    : n/a

-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                                Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
```

```
sap:1/1/1                                null         1514    1514    Up   Down
===============================================================================
*A:SAS-D>show>service#
*A:7210SAS# show service id 10 base

===============================================================================
Service Basic Information
===============================================================================
Service Id        : 10                  Vpn Id            : 0
Service Type      : VPLS
Name              : (Not Specified)
Description       : (Not Specified)
Customer Id       : 1
Last Status Change: 02/06/2106 06:28:12
Last Mgmt Change  : 01/10/1970 01:55:31
Admin State       : Down                Oper State        : Down
MTU               : Not Applicable      Def. Mesh VC Id   : 10
SAP Count         : 0
Uplink Type:      : L2
SAP Type:         : Dot1q Range         Customer vlan:    : n/a

-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                               Type         AdmMTU  OprMTU  Adm  Opr
-------------------------------------------------------------------------------
No Matching Entries
===================================================================
*A:7210SAS# show service id 10 base
```

fdb

Syntax **fdb** [**sap** *sap-id* [**expiry**]] | [**mac** *ieee-address* [**expiry**]] | [**detail**] [**expiry**]

Context show>service>id
show>service>fdb-mac

Description This command displays FDB entries for a given MAC address.

Parameters **sap** *sap-id* — Specifies the physical port identifier portion of the SAP. See Common CLI Command Descriptions on page 483 for command syntax.

detail — Displays detailed information.

expiry — Displays time until MAC is aged out.

Show FDB Information — The following table describes service FDB output fields.

Label	Description
`ServID`	Displays the service ID.
`MAC`	Displays the associated MAC address.
`Mac Move`	Displays the administrative state of the MAC movement feature associated with this service.
`Primary Factor`	Displays a factor for the primary ports defining how many MAC-relearn periods should be used to measure the MAC-relearn rate.
`Secondary Factor`	Displays a factor for the secondary ports defining how many MAC-relearn periods should be used to measure the MAC-relearn rate.
`Mac Move Rate`	Displays the maximum rate at which MAC's can be re-learned in this service, before the SAP where the moving MAC was last seen is automatically disabled in order to protect the system against undetected loops or duplicate MAs. The rate is computed as the maximum number of re-learns allowed in a 5 second interval: for example, the default rate of 2 re-learns per second corresponds to 10 re-learns in a 5 second period.
`Mac Move Timeout`	Displays the time in seconds to wait before a SAP that has been disabled after exceeding the maximum re-learn rate is re-enabled. A value of zero indicates that the SAP will not be automatically re-enabled after being disabled. If after the SAP is re-enabled it is disabled again, the effective retry timeout is doubled in order to avoid thrashing.
`Mac Move Retries`	Displays the number of times retries are performed for reen-abling the SAP.

Label	Description
Table Size	Specifies the maximum number of learned and static entries allowed in the FDB of this service.
Total Count	Displays the total number of learned entries in the FDB of this service.
Learned Count	Displays the current number of learned entries in the FDB of this service.
Static Count	Displays the current number of static entries in the FDB of this service.
OAM-learned Count	Displays the current number of OAM entries in the FDB of this service.
DHCP-learned Count	Displays the current number of DHCP-learned entries in the FDB of this service.
Host-learned Count	Displays the current number of host-learned entries in the FDB of this service.
Remote Age	Displays the number of seconds used to age out FDB entries learned on an SAP. These entries correspond to MAC addresses learned on remote SAPs.
Local Age	Displays the number of seconds used to age out FDB entries learned on local SAPs.
High Watermark	Displays the utilization of the FDB table of this service at which a table full alarm will be raised by the agent.
Low Watermark	Displays the utilization of the FDB table of this service at which a table full alarm will be cleared by the agent.
Mac Learning	Specifies whether the MAC learning process is enabled
Discard Unknown	Specifies whether frames received with an unknown destination MAC are discarded.
Mac Aging	Indicates whether the MAC aging process is enabled.
Relearn Only	Displays, that when enabled, either the FDB table of this service is full, or that the maximum system-wide number of MA's supported by the agent has been reached, and thus MAC learning is temporary disabled, and only MAC re-learns can take place.
Mac Subnet Len	Displays the number of bits to be considered when performing MAC-learning or MAC-switching.
Source-Identifier	The location where the MAC is defined.
Type/Age	Type — Specifies the number of seconds used to age out TLS FDB entries learned on local SAPs.

Label	Description
	`Age` — Specifies the number of seconds used to age out TLS FDB entrieslearned on an SDP. These entries correspond to MAC addresses learned on remote SAPs.

Label	Description
	L — Learned - Dynamic entries created by the learning process.
	OAM — Entries created by the OAM process.
	H — Host, the entry added by the system for a static configured subscriber host.
	D or DHCP — DHCP-installed MAC. Learned addresses can be temporarily frozen by the DHCP snooping application for the duration of a DHCP lease.
	P — Indicates the MAC is protected" by the MAC protection feature.
	Static — Statically configured.
Last Change	Indicates the time of the most recent state changes.

```
A:ALU-7210# show service id 1 fdb
===============================================================================
Forwarding Database, Service 1
===============================================================================
Service Id : 1     Mac Move : Disabled
Primary Factor : 3 Secondary Factor : 2
Mac Move Rate : 2 Mac Move Timeout : 10
Mac Move Retries : 3
Table Size : 250 Total Count : 1
Learned Count : 0 Static Count : 0
Host-learned Count: 1
Remote Age : 900 Local Age : 300
High Watermark : 95% Low Watermark : 90%
Mac Learning : Enabled Discard Unknown : Disabled
Mac Aging : Enabled Relearn Only : False
Mac Subnet Len : 48
===============================================================================
A:ALU-7210#
```

l2pt

Syntax **l2pt disabled**
l2pt [**detail**]

Context show>service>id

Description This command displays Layer 2 Protocol Tunnel (L2-PT) route information associated with this service.

Parameters **disabled —** Displays only entries with termination disabled. This helps identify configuration errors.

detail — Displays detailed information.

Output **Show L2PT Fields —** The following table describes show L2PT output fields:

Label	Description
Service id	Displays the 24 bit (0..16777215) service instance identifier for the service.
L2pt-term enabled	Indicates if L2-PT-termination and/or Bpdu-translation is in use in this service by at least one SAP or spoke SDP binding. If in use, at least one of L2PT-termination or Bpdu-translation is enabled. When enabled it is not possible to enable STP on this service.
L2pt-term disabled	Indicates that L2-PT-termination is disabled.
Bpdu-trans auto	Specifies the number of L2-PT PDU's are translated before being sent out on a port or sap.
Bpdu-trans disabled	Indicates that Bpdu-translation is disabled.
SAPs	Displays the number of SAPs with L2PT or BPDU translation enabled or disabled.
SDPs	Displays the number of SDPs with L2PT or BPDU translation enabled or disabled.
Total	Displays the column totals of L2PT entities.
SapId	The ID of the access point where this SAP is defined.
L2pt-termination	Indicates whether L2pt termination is enabled or disabled.
Admin Bpdu-translation	Specifies whether Bpdu translation is administratively enabled or disabled.
Oper Bpdu-translation	Specifies whether Bpdu translation is operationally enabled or disabled.
SdpId	Specifies the SAP ID.

Sample:

```
*A:7210SAS>show>service# id 1 l2pt detail

===============================================================================
L2pt details, Service id 1
===============================================================================

Service Access Points
-------------------------------------------------------------------------------
SapId                       L2pt-                       Admin Bpdu-  Oper Bpdu-
                            termination                 translation  translation
-------------------------------------------------------------------------------
1/1/1                       stp cdp vtp dtp pagp udld  disabled     disabled
-------------------------------------------------------------------------------
Number of SAPs : 1
```

```
===============================================================================

===============================================================================
L2pt summary, Service id 1
===============================================================================
       L2pt-term   L2pt-term   Bpdu-trans  Bpdu-trans  Bpdu-trans  Bpdu-trans
       enabled     disabled    auto        disabled    pvst        stp
-------------------------------------------------------------------------------
SAP's  1           0           0           1           0           0
SDP's  0           0           0           0           0           0
-------------------------------------------------------------------------------
Total  1           0           0           1           0           0
===============================================================================
*A:7210SAS>show>service#
```

mac-move

Syntax **mac-move**

Context show>service>id

Description This command displays MAC move related information about the service.

sap

Syntax **sap** *sap-id* [*sap-id* [**detail**|**stp**]]

Context show>service>id

Description This command displays information for the SAPs associated with the service.

If no optional parameters are specified, a summary of all associated SAPs is displayed.

Parameters **sap** *sap-id* — The ID that displays SAPs for the service in the *slot*/*mda*/*port*[**.***channel*] form. See Common CLI Command Descriptions on page 483 for command syntax.

detail — Displays detailed information for the SAP.

stp - — Displays the stp information of the SAP.

Show Service-ID SAP — The following table describes show service SAP fields:

Label	Description
Service Id	The service identifier.
SAP	The SAP and qtag.
Encap	The encapsulation type of the SAP.
Ethertype	Specifies an Ethernet type II Ethertype value.
Admin State	The administrative state of the SAP.

Label	Description (Continued)
Oper State	The operational state of the SAP.
Flags	Specifies the conditions that affect the operating status of this SAP. Display output includes: ServiceAdminDown, SapAdminDown, InterfaceAdminDown, PortOperDown, L2OperDown, SapIngressQoSMismatch, SapEgressQoSMismatch,RelearnLimitExceeded, ParentIfAdminDown, NoSapIpipeCeIpAddr, TodResourceUnavail, TodMssResourceUnavail, SapParamMismatch, CemSapNoEcidOrMacAddr, StandByForMcRing, SapIngressNamedPoolMismatch, SapEgressNamedPoolMismatch, NoSapEpipeRingNode.
Last Status Change	Specifies the time of the most recent operating status change to this SAP
Last Mgmt Change	Specifies the time of the most recent management-initiated change to this SAP.
Ingress qos-policy	The ingress QoS policy ID assigned to the SAP.
Ingress Filter-Id	The ingress filter policy ID assigned to the SAP.
Egress Filter-Id	The egress filter policy ID assigned to the SAP.
Acct. Pol	The accounting policy ID assigned to the SAP.
Collect Stats	Specifies whether collect stats is enabled.
SAP per Meter stats	
Ingress Meter	Specifies the meter ID.
For. InProf	The number of in-profile packets and octets (rate below CIR) forwarded.
For. OutProf	The number of out-of-profile packets and octets. (rate above CIR and below PIR) forwarded by the ingress meter.
Ingress TD Profile	The profile ID applied to the ingress SAP.
Egress TD Profile	The profile ID applied to the egress SAP.
Alarm Cell Handling	The indication that OAM cells are being processed.
AAL-5 Encap	The AAL-5 encapsulation type.
The labels and description listed below are not supported on 7210 SAS-E devices:	
Loopback Mode	Displays the Ethernet port loopback mode
Loopback Src Addr	Displays the configured loopback source address

Label	Description (Continued)
Loopback Dst Addr	Displays the configured loopback destination address
No-svc-port used	Displays the port ID of the port on which no service is configured. This port is used for the port loop back with MAC swap functionality.

Sample Output

```
*A:ALU_SIM2>config>service# show service  id 1  sap 1/1/3:500.*  detail
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 1
SAP                : 1/1/3:500.*              Encap             : qinq
QinQ Dot1p         : Default
Dot1Q Ethertype    : 0x8100                   QinQ Ethertype    : 0x8100

Admin State        : Up                       Oper State        : Down
Flags              : PortOperDown
Last Status Change : 11/17/2008 00:26:56
Last Mgmt Change   : 11/14/2008 02:45:15
Loopback Mode : Internal                 No-svc-port used : 1/1/13
Loopback Src Addr : 00:00:00:22:22:22
Loopback Dst Addr : 00:00:00:11:11:11
Max Nbr of MAC Addr: No Limit                 Total MAC Addr    : 0
Learned MAC Addr   : 0                        Static MAC Addr   : 0
Ingress qos-policy : 1                        Egress qos-policy : 1
Shared Q plcy      : n/a                      Multipoint shared : Disabled
Ingr IP Fltr-Id    : n/a                      Egr IP Fltr-Id    : n/a
Ingr Mac Fltr-Id   : n/a                      Egr Mac Fltr-Id   : n/a
tod-suite          : TodResourceUnavail       qinq-pbit-marking : both
Egr Agg Rate Limit : max
Mac Learning       : Enabled                  Discard Unkwn Srce: Disabled
Mac Aging          : Enabled                  Mac Pinning       : Disabled
L2PT Termination   : Disabled                 BPDU Translation  : Disabled
Vlan-translation   : None

Acct. Pol          : None                     Collect Stats     : Disabled

Anti Spoofing      : None                     Nbr Static Hosts  : 0
-------------------------------------------------------------------------------
Stp Service Access Point specifics
-------------------------------------------------------------------------------
Mac Move           : Blockable
Stp Admin State    : Up                       Stp Oper State    : Up
Core Connectivity  : Down
Port Role          : Disabled                 Port State        : Discarding
Port Number        : 2049                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : False
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : Rstp
Last BPDU from     : N/A
CIST Desig Bridge  : This Bridge              Designated Port   : 34817

Forward transitions: 1                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
```

```
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                        RST BPDUs tx      : 124267
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0
-------------------------------------------------------------------------------
Sap Statistics
-------------------------------------------------------------------------------
                        Packets
Ingress Packets rcvd:   0
-------------------------------------------------------------------------------
Sap per Meter stats
-------------------------------------------------------------------------------
                        Packets                 Octets
Ingress Meter 1 (Unicast)
For. InProf           : 0                       0
For. OutProf          : 0                       0

Ingress Meter 11 (Multipoint)
For. InProf           : 0                       0
For. OutProf          : 0                       0
===============================================================================
*A:ALU_SIM2>config>service#


*A:PE-A# show service id 10 sap 2/2/5:10 mrp
===============================================================================
Service Access Points(SAP)
===============================================================================
Service Id         : 10
SAP                : 2/2/5:10                 Encap             : q-tag
Description        : Default sap description for service id 10
Admin State        : Up                       Oper State        : Up
Flags              : None
Multi Svc Site     : None
Last Status Change : 01/16/2008 09:37:57
Last Mgmt Change   : 01/16/2008 09:37:41
-------------------------------------------------------------------------------
SAP MRP Information
-------------------------------------------------------------------------------
Join Time          : 0.2 secs                 Leave Time        : 1.0 secs
Leave All Time     : 10.0 secs                Periodic Time     : 1.0 secs
Periodic Enabled   : false
Rx Pdus            : 11                       Tx Pdus           : 12
Dropped Pdus       : 0                        Tx Pdus           : 12
Rx New Event       : 0                        Rx Join-In Event  : 150
Rx In Event        : 10                       Rx Join Empty Evt : 10
Rx Empty Event     : 10                       Rx Leave Event    : 0
Tx New Event       : 0                        Tx Join-In Event  : 140
Tx In Event        : 0                        Tx Join Empty Evt : 20
Tx Empty Event     : 10                       Tx Leave Event    : 0
-------------------------------------------------------------------------------
SAP MMRP Information
-------------------------------------------------------------------------------
MAC Address       Registered        Declared
-------------------------------------------------------------------------------
01:1e:83:00:00:65 Yes               Yes
01:1e:83:00:00:66 Yes               Yes
01:1e:83:00:00:67 Yes               Yes
01:1e:83:00:00:68 Yes               Yes
01:1e:83:00:00:69 Yes               Yes
01:1e:83:00:00:6a Yes               Yes
01:1e:83:00:00:6b Yes               Yes
```

```
01:1e:83:00:00:6c Yes               Yes
01:1e:83:00:00:6d Yes               Yes
01:1e:83:00:00:6e Yes               Yes
-------------------------------------------------------------------------------
Number of MACs=10 Registered=10 Declared=10
-------------------------------------------------------------------------------
*A:PE-A#
```

stp

Syntax **stp** [**detail**]

Context show>service>id

Description This command displays information for the spanning tree protocol instance for the service.

Parameters **detail** — Displays detailed information.

Output **Show Service-ID STP Output —** The following table describes show service-id STP output fields:

Label	Description
`Bridge-id`	Specifies the MAC address used to identify this bridge in the network.
`Bridge fwd delay`	Specifies how fast a bridge changes its state when moving toward the forwarding state.
`Bridge Hello time`	Specifies the amount of time between the transmission of Configuration BPDUs.
`Bridge max age`	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded. This is the actual value that this bridge is currently using.
`Bridge priority`	Defines the priority of the Spanning Tree Protocol instance associated with this service.
`Topology change`	Specifies whether a topology change is currently in progress.
`Last Top. change`	Specifies the time (in hundredths of a second) since the last time a topology change was detected by the Spanning Tree Protocol instance associated with this service.
`Top. change count`	Specifies the total number of topology changes detected by the Spanning Tree Protocol instance associated with this service since the management entity was last reset or initialized.
`Root bridge-id`	Specifies the bridge identifier of the root of the spanning tree as determined by the Spanning Tree Protocol instance associated with this service. This value is used as the Root Identifier parameter in all Configuration BPDUs originated by this node.
`Root path cost`	Specifies the cost of the path to the root bridge as seen from this bridge.

Label	Description (Continued)
Root forward delay	Specifies how fast the root changes its state when moving toward the forwarding state.
Rcvd hello time	Specifies the amount of time between the transmission of configuration BPDUs.
Root max age	Specifies the maximum age of Spanning Tree Protocol information learned from the network on any port before it is discarded.
Root priority	This object specifies the priority of the bridge that is currently selected as root-bridge for the network.
Root port	Specifies the port number of the port which offers the lowest cost path from this bridge to the root bridge.
SAP Identifier	The ID of the access port where this SAP is defined.
BPDU encap	Specifies the type of encapsulation used on BPDUs sent out and received on this SAP.
Port Number	Specifies the value of the port number field which is contained in the least significant 12 bits of the 16-bit port ID associated with this SAP.
Port Priority	Specifies the value of the port priority field which is contained in the most significant 4 bits of the 16-bit port ID associated with this SAP.
Port Path Cost	Specifies the contribution of this port to the path cost of paths towards the spanning tree root which include this port.
Designated Port	Specifies the port identifier of the port on the designated bridge for this port's segment.
Designated Bridge	Specifies the bridge identifier of the bridge which this port considers to be the designated bridge for this port's segment.

Sample Output

```
*A:ALU_SIM2>config>service>vpls>sap# show service id 1 stp
===============================================================================
Stp info, Service 1
===============================================================================
Bridge Id          : 00:00.00:45:67:32:10:ab  Top. Change Count : 2
Root Bridge        : This Bridge              Stp Oper State    : Up
Primary Bridge     : N/A                      Topology Change   : Inactive
Mode               : Rstp                     Last Top. Change  : 1d 18:34:36
Vcp Active Prot.   : N/A
Root Port          : N/A                      External RPC      : 0
===============================================================================
Stp port info
===============================================================================
Sap Id             Oper-     Port-      Port-       Port-  Oper-  Link-  Active
                   State     Role       State       Num    Edge   Type   Prot.
-------------------------------------------------------------------------------
1/1/21:1           Up        Designated Forward     2048   True   Pt-pt  Rstp
```

```
lag-1:1.1          Up        Designated Forward     2049   False  Pt-pt  Rstp
lag-2:1.1          Up        Designated Forward     2050   False  Pt-pt  Rstp
===============================================================================
*A:ALU_SIM2>config>service>vpls>sap#


*A:ALU_SIM2>config>service>vpls>sap#  show service id 1 stp detail
===============================================================================
Spanning Tree Information
===============================================================================
-------------------------------------------------------------------------------
VPLS Spanning Tree Information
-------------------------------------------------------------------------------
VPLS oper state    : Up
Stp Admin State    : Up                        Stp Oper State    : Up
Mode               : Rstp                      Vcp Active Prot.  : N/A

Bridge Id          : 00:00.00:45:67:32:10:ab  Bridge Instance Id: 0
Bridge Priority    : 0                         Tx Hold Count     : 6
Topology Change    : Inactive                  Bridge Hello Time : 2
Last Top. Change   : 1d 18:35:18               Bridge Max Age    : 20
Top. Change Count  : 2                         Bridge Fwd Delay  : 15

Root Bridge        : This Bridge
Primary Bridge     : N/A

Root Path Cost     : 0                         Root Forward Delay: 15
Rcvd Hello Time    : 2                         Root Max Age      : 20
Root Priority      : 0                         Root Port         : N/A
-------------------------------------------------------------------------------
Spanning Tree Sap Specifics
-------------------------------------------------------------------------------
SAP Identifier     : 1/1/21:1                  Stp Admin State   : Up
Port Role          : Designated                Port State        : Forwarding
Port Number        : 2048                      Port Priority     : 128
Port Path Cost     : 10                        Auto Edge         : Enabled
Admin Edge         : Disabled                  Oper Edge         : True
Link Type          : Pt-pt                     BPDU Encap        : Dot1d
Root Guard         : Disabled                  Active Protocol   : Rstp
Last BPDU from     : N/A
CIST Desig Bridge  : This Bridge               Designated Port   : 34816
Forward transitions: 2                         Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                         Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                         TCN BPDUs tx      : 0
RST BPDUs rcvd     : 0                         RST BPDUs tx      : 79126
MST BPDUs rcvd     : 0                         MST BPDUs tx      : 0

SAP Identifier     : lag-1:1.1                 Stp Admin State   : Up
Port Role          : Designated                Port State        : Forwarding
Port Number        : 2049                      Port Priority     : 128
Port Path Cost     : 10                        Auto Edge         : Enabled
Admin Edge         : Disabled                  Oper Edge         : False
Link Type          : Pt-pt                     BPDU Encap        : Dot1d
Root Guard         : Disabled                  Active Protocol   : Rstp
Last BPDU from     : 10:00.00:f3:f0:98:97:00
CIST Desig Bridge  : This Bridge               Designated Port   : 34817
Forward transitions: 1                         Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                         Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                         TCN BPDUs tx      : 0
RST BPDUs rcvd     : 5                         RST BPDUs tx      : 79128
MST BPDUs rcvd     : 0                         MST BPDUs tx      : 0
```

```
SAP Identifier     : lag-2:1.1                Stp Admin State   : Up
Port Role          : Designated               Port State        : Forwarding
Port Number        : 2050                     Port Priority     : 128
Port Path Cost     : 10                       Auto Edge         : Enabled
Admin Edge         : Disabled                 Oper Edge         : False
Link Type          : Pt-pt                    BPDU Encap        : Dot1d
Root Guard         : Disabled                 Active Protocol   : Rstp
Last BPDU from     : 20:00.00:e0:b1:99:cb:2a
CIST Desig Bridge  : This Bridge              Designated Port   : 34818
Forward transitions: 1                        Bad BPDUs rcvd    : 0
Cfg BPDUs rcvd     : 0                        Cfg BPDUs tx      : 0
TCN BPDUs rcvd     : 0                        TCN BPDUs tx      : 0
RST BPDUs rcvd     : 6                        RST BPDUs tx      : 78760
MST BPDUs rcvd     : 0                        MST BPDUs tx      : 0
===============================================================================
*A:ALU_SIM2>config>service>vpls>sap#
```

mstp-configuration

Syntax **mstp-configuration**

Context show>service>id

Description This command displays the MSTP specific configuration data. This command is only valid on a management VPLS.

Output **Show Output —** The following table describes the show all command output fields:

Label	Description
Region Name	Displays the MSTP region name.
Region Revision	Displays the MSTP region revision.
MST Max Hops	Displays the MSTP maximum hops specified.
Instance	Displays the MSTP instance number.
Priority	Displays the MSTP priority.
Vlans mapped	Displays the VLAN range of the MSTP instance.

```
Sample output with MSTP information for 7210 SAS-E:

A:7210-SASE>show>service>id# stp mst-instance 1

===============================================================================
MSTP specific info for service 1 MSTI 1
===============================================================================
Regional Root      : 80:01.00:25:ba:02:8a:30  Root Port         : 2048
Internal RPC       : 20                       Remaining Hopcount: 18

===================================================================
MSTP port info for MSTI 1
===================================================================
```

```
Sap Id             Oper-     Port-      Port-       Port-  Same
                   State     Role       State       Num    Region
-------------------------------------------------------------------
1/1/1:0.*          Up        Root       Forward     2048   True
1/1/5:0.*          Up        Designated Forward     2049   True
1/1/10:0.*         Up        Designated Forward     2050   True
1/1/17:0.*         Up        Designated Forward     2051   True
===================================================================
A:7210-SASE>show>service>id#

Sample output with MSTP information for 7210 SAS-D:

A:SASD1>show>service>id# stp mst-instance 1

===============================================================================
MSTP specific info for service 1 MSTI 1
===============================================================================
Regional Root      : This Bridge              Root Port         : N/A
Internal RPC       : 0                        Remaining Hopcount: 20

===================================================================
MSTP port info for MSTI 1
===================================================================
Sap Id             Oper-     Port-      Port-       Port-  Same
                   State     Role       State       Num    Region
-------------------------------------------------------------------
1/1/2:0.*          Up        Designated Forward     2048   True
1/1/5:0.*          Up        Alternate  Discard     2049   False
1/1/6:0.*          Up        Master     Forward     2050   False
===================================================================
A:SASD1>show>service>id#
```

dhcp

Syntax **dhcp**

Context show>service>id

Description This command enables the context to display DHCP information for the specified service.

statistics

Syntax **statistics** [**sap** *sap-id*]
statistics [**interface** *interface-name*]

Context show>service>id>dhcp

Description Displays DHCP statistics information.

Parameters **sap** *sap-id* — Specifies the physical port identifier portion of the SAP definition.

interface *interface-name* — Displays information for the specified IP interface.

Output **Show DHCP Statistics Output —** The following table describes the output fields for DHCP statistics.

Label	Description
`Received Packets`	The number of packets received from the DHCP clients. Includes DHCP packets received from both DHCP client and DHCP server.
`Transmitted Packets`	The number of packets transmitted to the DHCP clients. Includes DHCP packets transmitted from both DHCP client and DHCP server.
`Received Malformed Packets`	The number of corrupted/invalid packets received from the DHCP clients. Includes DHCP packets received from both DHCP client and DHCP server
`Received Untrusted Packets`	The number of untrusted packets received from the DHCP clients. In this case, a frame is dropped due to the client sending a DHCP packet with Option 82 filled in before “trust” is set under the DHCP interface command.
`Client Packets Discarded`	The number of packets received from the DHCP clients that were discarded.
`Client Packets Relayed`	The number of packets received from the DHCP clients that were forwarded.
`Client Packets Snooped`	The number of packets received from the DHCP clients that were snooped.
`Server Packets Discarded`	The number of packets received from the DHCP server that were discarded.

Label	Description
Server Packets Relayed	The number of packets received from the DHCP server that were forwarded.
Server Packets Snooped	The number of packets received from the DHCP server that were snooped.

```
*A:7210SAS>show>service>id>dhcp# statistics

===================================================================
DHCP Global Statistics, service 1
===================================================================
Rx Packets                           : 416554
Tx Packets                           : 206405
Rx Malformed Packets                 : 0
Rx Untrusted Packets                 : 0
Client Packets Discarded             : 0
Client Packets Relayed               : 221099
Client Packets Snooped               : 0
Client Packets Proxied (RADIUS)      : 0
Client Packets Proxied (Lease-Split) : 0
Server Packets Discarded             : 0
Server Packets Relayed               : 195455
Server Packets Snooped               : 0
DHCP RELEASEs Spoofed                : 0
DHCP FORCERENEWs Spoofed             : 0
===================================================================
*A:7210SAS>show>service>id>dhcp#
```

summary

Syntax **summary [interface** *interface-name]*

Context show>service>id>dhcp

Description Displays DHCP configuration summary information.

Parameters *interface interface-name* — Displays information for the specified IP interface.

Output **Show DHCP Summary Output —** The following table describes the output fields for DHCP summary.

Label	Description
Interface Name	Name of the router interface.
Arp Populate	Specifies whether or not ARP populate is enabled. 7210 SAS does not support ARP populate.
Used/Provided	7210 SAS does not maintain lease state.
Info Option	Indicates whether Option 82 processing is enabled on the interface.
Admin State	Indicates the administrative state.

Sample Output

```
A:7210SAS# show service id 1 dhcp summary
DHCP Summary, service 1
=====================================================================

Interface Name                    Arp      Used/                 Info    Admin
  SapId/Sdp                       Populate Provided              Option  State
-------------------------------------------------------------------------------
egr_1                             No       0/0                   Replace Up
i_1                               No       0/0                   Replace Up
-------------------------------------------------------------------------------
Interfaces: 2
=====================================================================

*A:7210SAS>show>service>id>dhcp#
```

IGMP Snooping Show Commands

igmp-snooping

Syntax **igmp-snooping**

Context show>service>id

Description This command enables the context to display IGMP snooping information.

all

Syntax **all**

Context show>service>id>igmp-snooping

Description This command displays detailed information for all aspects of IGMP snooping on the VPLS service.

Output **Show All Service-ID —** The following table describes the show all service-id command output fields:

Label	Description
`Admin State`	The administrative state of the IGMP instance.
`Querier`	Displays the address of the IGMP querier on the IP subnet to which the interface is attached.
`Sap Id`	Displays the SAP IDs of the service ID.
`Oper State`	Displays the operational state of the SAP IDs of the service ID.
`Mrtr Port`	Specifies if the port is a multicast router port.
`Send Queries`	Specifies whether the send-queries command is enabled or disabled.
`Max Num Groups`	Specifies the maximum number of multicast groups that can be joined on this SAP.
`MVR From VPLS`	Specifies MVR from VPLS.
`Num MVR Groups`	Specifies the actual number of multicast groups that can be joined on this SAP.
`MVR From VPLS Cfg Drops`	Displays the from VPLS drop count.
`MVR To SAP Cfg Drops`	Displays the to SAP drop count.
`MVR Admin State`	Displays the administrative state of MVR.

Label	Description (Continued)
MVR Policy	The MVR policy name.

Sample Output

```
*A:7210-2>show>service>id>snooping# all
===============================================================================
IGMP Snooping info for service 900
===============================================================================
IGMP Snooping Base info
-------------------------------------------------------------------------------
Admin State : Up
Querier     : 5.5.5.5 on SAP 1/1/14:100
-------------------------------------------------------------------------------
Sap                       Oper    MRtr  Send      Max Num   Num
Id                        State   Port  Queries   Groups    Groups
-------------------------------------------------------------------------------
sap:1/1/13:100            Up      No    Disabled  No Limit  0
sap:1/1/14:100            Up      No    Disabled  No Limit  0
sap:1/1/17:100            Up      No    Disabled  No Limit  1
sap:1/1/18:100            Up      No    Disabled  No Limit  1
-------------------------------------------------------------------------------
IGMP Snooping Querier info
-------------------------------------------------------------------------------
Sap Id                  : 1/1/14:100
IP Address              : 10.10.10.2
Expires                 : 254s
Up Time                 : 0d 00:02:42
Version                 : 2

General Query Interval  : 125s
Query Response Interval : 10.0s
Robust Count            : 2
-------------------------------------------------------------------------------
IGMP Snooping Multicast Routers
-------------------------------------------------------------------------------
MRouter          Sap Id                 Up Time        Expires   Version
-------------------------------------------------------------------------------
10.10.10.2       1/1/14:100             0d 00:02:44    254s      2
-------------------------------------------------------------------------------
Number of mrouters: 1
-------------------------------------------------------------------------------
IGMP Snooping Proxy-reporting DB
-------------------------------------------------------------------------------
Group Address    Up Time
-------------------------------------------------------------------------------
226.6.6.6        0d 00:02:17
229.9.9.9        0d 00:02:56
-------------------------------------------------------------------------------
Number of groups: 2
-------------------------------------------------------------------------------
IGMP Snooping SAP 1/1/13:100 Port-DB
-------------------------------------------------------------------------------
Group Address  Type  From-VPLS Up Time    Expires
-------------------------------------------------------------------------------
Number of groups: 0
-------------------------------------------------------------------------------
```

```
IGMP Snooping SAP 1/1/14:100 Port-DB
-------------------------------------------------------------------------------
Group Address   Type    From-VPLS  Up Time       Expires
===============================================================================
*A:7210-2>show>service>id>snooping#
```

mfib

Syntax **mfib** [**brief**]
mfib [**group** *grp-address*]

Context show>service>id

Description This command displays the multicast FIB on the VPLS service.

Parameters **brief** — Displays a brief output.

group grp *grp-address* — Displays the multicast FIB for a specific multicast group address.

Output **Show Output** — The following table describes the command output fields:

Label	Description
Group Address	IPv4 multicast group address.
SAP ID	Indicates the SAP to which the corresponding multicast stream will be forwarded/blocked.
Forwarding/Block-ing	Indicates whether the corresponding multicast stream will be blocked/forwarded.
Number of Entries	Specifies the number of entries in the MFIB.
Forwarded Packets	Indicates the number of multicast packets forwarded for the corresponding source/group.
Forwarded Octets	Indicates the number of octets forwarded for the corresponding source/group.
Svc ID	Indicates the service to which the corresponding multicast stream will forwarded/blocked. Local means that the multicast stream will be forwarded/blocked to a SAP local to the service.

Sample Output

```
*A:SAS# show service id 1 mfib

===============================================================================
Multicast FIB, Service 1
===============================================================================
Group Address         Sap/Sdp Id               Svc Id   Fwd/Blk
-------------------------------------------------------------------------------
224.4.4.4             sap:1/1/1                Local    Fwd
-------------------------------------------------------------------------------
Number of entries: 1
===============================================================================
*A:7210-2# show service id 5 mfib
===============================================================================
Multicast FIB, Service 5
===============================================================================
Source Address  Group Address         Sap Id                   Svc Id   Fwd/Blk
```

```
-------------------------------------------------------------------------------
*               234.5.34.1            sap:lag-1:5.*            Local    Fwd
5.5.5.1         234.5.34.1            sap:lag-1:5.*            Local    Blk
                                      sap:lag-2:5.*            Local    Fwd
*               234.5.34.2            sap:lag-1:5.*            Local    Fwd
5.5.5.1         234.5.34.2            sap:lag-1:5.*            Local    Blk
                                      sap:lag-2:5.*            Local    Fwd
*               234.5.34.3            sap:lag-1:5.*            Local    Fwd
5.5.5.1         234.5.34.3            sap:lag-1:5.*            Local    Blk
                                      sap:lag-2:5.*            Local    Fwd
*               234.5.34.4            sap:lag-1:5.*            Local    Fwd
5.5.5.1         234.5.34.4            sap:lag-1:5.*            Local    Blk
                                      sap:lag-2:5.*            Local    Fwd
*               234.5.34.5            sap:lag-1:5.*            Local    Fwd
5.5.5.1         234.5.34.5            sap:lag-1:5.*            Local    Blk
                                      sap:lag-2:5.*            Local    Fwd
-------------------------------------------------------------------------------
Number of entries: 10
===============================================================================
*A:7210-2
```

mrouters

Syntax **mrouters** [**detail**]

Context show>service>id>igmp-snooping

Description This command displays all multicast routers.

Parameters **detail —** Displays detailed information.

Sample Output

```
*A:7210-2 show service id 3 igmp-snooping mrouters
===============================================================================
IGMP Snooping Multicast Routers for service 3
===============================================================================
MRouter          Sap Id                 Up Time        Expires   Version
-------------------------------------------------------------------------------
10.20.1.2        lag-2:3.*              0d 02:30:39    197s      3
-------------------------------------------------------------------------------
Number of mrouters: 1
===============================================================================
*A:SNPG-1#


*A:7210-2# show service id 3 igmp-snooping mrouters detail
===============================================================================
IGMP Snooping Multicast Routers for service 3
===============================================================================
-------------------------------------------------------------------------------
MRouter 10.20.1.2
-------------------------------------------------------------------------------
Sap Id                  : lag-2:3.*
Expires                 : 181s
Up Time                 : 0d 02:30:55
Version                 : 3
```

```
General Query Interval  : 125s
Query Response Interval : 10.0s
Robust Count            : 2
-------------------------------------------------------------------------------
Number of mrouters: 1
===============================================================================
*A:7210-2#
```

mvr

Syntax **mvr**

Context show>service>id>igmp-snooping

Description This command displays Multicast VPLS Registration (MVR) information.

port-db

Syntax **port-db sap** *sap-id* [**detail**]
port-db sap *sap-id* **group** *grp-address*

show>service>id>igmp-snooping **Context**

Description This command displays information on the IGMP snooping port database for the VPLS service.

Parameters **group** *grp-ip-address* — Displays the IGMP snooping port database for a specific multicast group address.

sap *sap-id* — Displays the IGMP snooping port database for a specific SAP. See Common CLI Command Descriptions on page 483 for command syntax.

group *grp-address* — Displays IGMP snooping statistics matching the specified group address.

source *ip-address* — Displays IGMP snooping statistics matching one particular source within the multicast group.

Output **Show Output** — The following table describes the show output fields:

Label	Description
Group Address	The IP multicast group address for which this entry contains information.

Label	Description
Mode	Specifies the type of membership report(s) received on the interface for the group. In the include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter of the IGMP membership report. In exclude' mode, reception of packets sent to the given multicast address is requested from all IP source addresses except those listed in the source-list parameter.
Type	Indicates how this group entry was learned. If this group entry was learned by IGMP, the value is set to dynamic. For statically configured groups, the value is set to static.
Compatibility mode	Specifies the IGMP mode. This is used in order for routers to be compatible with older version routers. IGMPv3 hosts must operate in Version 1 and Version 2 compatibility modes. IGMPv3 hosts must keep state per local interface regarding the compatibility mode of each attached network. A host's compatibility mode is determined from the host compatibility mode variable which can be in one of three states: IGMPv1, IGMPv2 or IGMPv3. This variable is kept per interface and is dependent on the version of general queries heard on that interface as well as the older version querier present timers for the interface.
V1 host expires	The time remaining until the local router will assume that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv2 leave messages for this group that it receives on this interface.
V2 host expires	The time remaining until the local router will assume that there are no longer any IGMP Version 2 members on the IP subnet attached to this interface. Upon hearing any IGMPv2 membership report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv3 leave messages for this group that it receives on this interface.
Source address	The source address for which this entry contains information.
Up Time	The time since the source group entry was created.
Expires	The amount of time remaining before this entry will be aged out.
Number of sources	Indicates the number of IGMP group and source specific queries received on this SAP.
Forwarding/Blocking	Indicates whether this entry is on the forward list or block list.
Number of groups	Indicates the number of groups configured for this SAP.

Sample Output

```
*A:7210-2>show>service>id>snooping# port-db sap 1/1/18:100
===============================================================================
IGMP Snooping SAP 1/1/18:100 Port-DB for service 900
===============================================================================
Group Address   Type    From-VPLS  Up Time        Expires

-------------------------------------------------------------------------------
226.6.6.6       dynamic local      0d 00:12:35    260s
-------------------------------------------------------------------------------
Number of groups: 1
===============================================================================
*A:7210-2>show>service>id>snooping#
*A:7210-2# show service id 5 igmp-snooping port-db sap lag-1:5.*
===============================================================================
IGMP Snooping SAP lag-1:5.* Port-DB for service 5
===============================================================================
Group Address   Mode    Type    Up Time        Expires  Num
                                                        Src
-------------------------------------------------------------------------------
234.5.34.1      exclude dynamic 0d 00:23:38    216s     1
234.5.34.2      exclude dynamic 0d 00:23:38    216s     1
234.5.34.3      exclude dynamic 0d 00:23:38    216s     1
234.5.34.4      exclude dynamic 0d 00:23:38    216s     1
234.5.34.5      exclude dynamic 0d 00:23:38    216s     1
-------------------------------------------------------------------------------
Number of groups: 5
===============================================================================
*A:7210-2#

*A:7210-2>show>service>id>snooping# port-db sap 1/1/18:100 detail
===============================================================================
IGMP Snooping SAP 1/1/18:100 Port-DB for service 900
-------------------------------------------------------------------------------
IGMP Group 226.6.6.6
-------------------------------------------------------------------------------
Type             : dynamic
Up Time          : 0d 00:12:39          Expires          : 259s
Compat Mode      : IGMP Version 2
V1 Host Expires  : 0s                   V2 Host Expires  : 259s
-------------------------------------------------------------------------------
Number of groups: 1
===============================================================================
*A:7210-2>show>service>id>snooping#
```

proxy-db

Syntax **proxy-db** [**detail**]
proxy-db group *grp-address*

Context show>service>id>igmp-snooping

Description This command displays information on the IGMP snooping proxy reporting database for the VPLS service.

Parameters **group** *grp-ip-address* — Displays the IGMP snooping proxy reporting database for a specific multicast group address.

Output **Show Output —** The following table describes the show output fields:

Label	Description
Group Address	The IP multicast group address for which this entry contains information.
Mode	Specifies the type of membership report(s) received on the interface for the group. In the include mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter of the IGMP membership report. In the "exclude" mode, reception of packets sent to the given multicast address is requested from all IP source addresses except those listed in the source-list parameter.
Up Time	The total operational time in seconds.
Num Sources	Indicates the number of IGMP group and source specific queries received on this interface.
Number of groups	Number of IGMP groups.
Source Address	The source address for which this entry contains information.

Sample Output

```
*A:7210-2 show service id 5 igmp-snooping proxy-db
===============================================================================
IGMP Snooping Proxy-reporting DB for service 5
===============================================================================
Group Address    Mode     Up Time        Num Sources
-------------------------------------------------------------------------------
234.5.34.1       exclude  0d 00:25:54    0
234.5.34.2       exclude  0d 00:25:54    0
234.5.34.3       exclude  0d 00:25:54    0
234.5.34.4       exclude  0d 00:25:54    0
234.5.34.5       exclude  0d 00:25:54    0
-------------------------------------------------------------------------------
Number of groups: 5
===============================================================================
*A:7210-2

*A:7210-2>show>service>id>snooping# proxy-db detail
===============================================================================
IGMP Snooping Proxy-reporting DB for service 900
-------------------------------------------------------------------------------
IGMP Group 226.6.6.6
-------------------------------------------------------------------------------
Up Time : 0d 00:15:17
------------------------------
Source Address  Up Time
```

```
------------------------------
No sources.
-------------------------------------------------------------------------------
IGMP Group 229.9.9.9
-------------------------------------------------------------------------------
Up Time : 0d 00:15:56
------------------------------
Source Address  Up Time
------------------------------
No sources.
-------------------------------------------------------------------------------
Number of groups: 2
===============================================================================
*A:7210-2>show>service>id>snooping#
```

querier

Syntax **querier**

Context show>service>id>igmp-snooping

Description This command displays information on the IGMP snooping queriers for the VPLS service.

Output **Show Output —** The following table describes the show output fields:

Label	Description
SAP Id	Specifies the SAP ID of the service.
IP address	Specifies the IP address of the querier.
Expires	The time left, in seconds, that the query will expire.
Up time	The length of time the query has been enabled.
Version	The configured version of IGMP.
General Query Interval	The frequency at which host-query packets are transmitted.
Query Response Interval	The time to wait to receive a response to the host-query message from the host.
Robust Count	Specifies the value used to calculate several IGMP message intervals.

Sample Output

```
*A:7210-2# show service id 3 igmp-snooping querier
===============================================================================
IGMP Snooping Querier info for service 3
===============================================================================
```

```
Sap Id                  : lag-2:3.*
IP Address              : 10.20.1.2
Expires                 : 226s
Up Time                 : 0d 02:30:11
Version                 : 3

General Query Interval  : 125s
Query Response Interval : 10.0s
Robust Count            : 2
===============================================================================
*A:7210-2#
```

static

Syntax **static** [**sap** *sap-id*]

Context show>service>id>igmp-snooping

Description This command displays information on static IGMP snooping source groups for the VPLS service.

Parameters **sap** *sap-id* — Displays static IGMP snooping source groups for a specific SAP. See Common CLI Command Descriptions on page 483 for command syntax.

Output **Show Output** — The following table describes the show output fields:

Label	Description
Source	Displays the IP source address used in IGMP queries.
Group	Displays the static IGMP snooping source groups for a specified SAP.

Sample Output

```
*A:7210-2# show service id 4093 igmp-snooping static
===============================================================================
IGMP Snooping Static Source Groups for service 4093
===============================================================================
-------------------------------------------------------------------------------
IGMP Snooping Static Source Groups for SAP 1/1/5:4093
-------------------------------------------------------------------------------
Source           Group
-------------------------------------------------------------------------------
93.93.93.1       239.93.39.1
93.93.93.1       239.93.39.2
93.93.93.1       239.93.39.3
93.93.93.1       239.93.39.4
93.93.93.1       239.93.39.5
-------------------------------------------------------------------------------
Static (*,G)/(S,G) entries: 5
-------------------------------------------------------------------------------
IGMP Snooping Static Source Groups for SAP lag-3:4093
-------------------------------------------------------------------------------
Source           Group
-------------------------------------------------------------------------------
93.93.93.1       239.93.39.1
93.93.93.1       239.93.39.2
93.93.93.1       239.93.39.3
93.93.93.1       239.93.39.4
93.93.93.1       239.93.39.5
-------------------------------------------------------------------------------
Static (*,G)/(S,G) entries: 5
===============================================================================
*A:7210-2#
```

statistics

Syntax **statistics** [**sap** *sap-id*]

Context show>service>id>igmp-snooping

Description This command displays IGMP snooping statistics for the VPLS service.

Parameters **sap** *sap-id* — Displays IGMP snooping statistics for a specific SAP. See Common CLI Command Descriptions on page 483 for command syntax.

```
*A:7210-2# show service id 5 igmp-snooping statistics
===============================================================================
IGMP Snooping Statistics for service 5
===============================================================================
Message Type            Received      Transmitted   Forwarded
-------------------------------------------------------------------------------
General Queries         0             228           0
Group Queries           0             0             0
Group-Source Queries    0             0             0
V1 Reports              0             0             0
V2 Reports              0             0             0
V3 Reports              282           0             0
V2 Leaves               0             0             0
Unknown Type            0             N/A           0
-------------------------------------------------------------------------------
Drop Statistics
-------------------------------------------------------------------------------
Bad Length               : 0
Bad IP Checksum          : 0
Bad IGMP Checksum        : 0
Bad Encoding             : 0
No Router Alert          : 0
Zero Source IP           : 0
Wrong Version            : 0

Send Query Cfg Drops     : 0
Import Policy Drops      : 0
Exceeded Max Num Groups  : 0
Exceeded Max Num Sources : 0
===============================================================================
*A:7210-2#
```

VPLS Clear Commands

id

Syntax **id** *service-id*

Context clear>service
clear>service>statistics

Description This command clears commands for a specific service.

Parameters *service-id* — The ID that uniquely identifies a service.

Values service-id: 1 — 214748364
svc-name: A string up to 64 characters in length.

fdb

Syntax **fdb** {**all** | **mac** *ieee-address* | **sap** *sap-id*]

Context clear>service>id

Description This command clears FDB entries for the service.

Parameters **all —** Clears all FDB entries.

mac *ieee-address* **—** Clears only FDB entries in the FDB table with the specified 48-bit MAC address. The MAC address can be expressed 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.

sap-id — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

sap

Syntax **sap** *sap-id* {**all** | **counters** | **stp**}

Context clear>service>statistics

Description This command clears statistics for the SAP bound to the service.

Parameters *sap-id* — See Common CLI Command Descriptions on page 483 for command syntax.

all — Clears all queue statistics and STP statistics associated with the SAP.

counters — Clears all queue statistics associated with the SAP.

counters

Syntax **counters**

Context clear>service>statistics>id

Description This command clears all traffic queue counters associated with the service ID.

stp

Syntax **stp**

Context clear>service>statistics>id

Description Clears all spanning tree statistics for the service ID.

detected-protocols

Syntax **detected-protocols** {**all** | **sap** *sap-id*}

Context clear>service>id>stp

Description RSTP automatically falls back to STP mode when it receives an STP BPDU. The **clear detected-protocols** command forces the system to revert to the default RSTP mode on the SAP.

Parameters **all —** Clears all detected protocol statistics.

sap-id — Clears the specified lease state SAP information. See Common CLI Command Descriptions on page 483 for command syntax.

port-db

Syntax **port-db** [**sap** *sap-id*] [**group** *grp-address*]

Context clear>service>id>igmp-snooping

Description This command clears the information on the IGMP snooping port database for the VPLS service.

Parameters **sap** *sap-id* — Clears IGMP snooping statistics matching the specified SAP ID and optional encapsulation value. See Common CLI Command Descriptions on page 483 for command syntax.

group *grp-address* — Clears IGMP snooping statistics matching the specified group address.

querier

Syntax **querier**

Context clear>service>id>igmp-snooping

Description This command clears the information on the IGMP snooping queriers for the VPLS service.

statistics

Syntax **statistics** { **all** | **sap** *sap-id*}

Context clear>service>id>snooping

Description This command clears IGMP snooping statistics.

Parameters **all** — Clears all statistics for the service ID.

sap *sap-id* — Clears statistics for the specified SAP ID.

VPLS Debug Commands

id

Syntax **id** *service-id*

Context debug>service

Description This command debugs commands for a specific service.

Parameters *service-id* — The ID that uniquely identifies a service.

Values service-id: 1 — 214748364
svc-name: A string up to 64 characters in length.

event-type

Syntax [**no**] **event-type** {**config-change** | **svc-oper-status-change** | **sap-oper-status-change**}

Context debug>service>id

Description This command enables a particular debugging event type.
The **no** form of the command disables the event type debugging.

Parameters **config-change** — Debugs configuration change events.

svc-oper-status-change — Debugs service operational status changes.

sap-oper-status-change — Debugs SAP operational status changes.

sap

Syntax [**no**] **sap** *sap-id*

Context debug>service>id

Description This command enables debugging for a particular SAP.

Parameters *sap-id* — Specifies the SAP ID.

stp

Syntax **stp**

Context debug>service>id

Description This command enables the context for debugging STP.

all-events

Syntax **all-events**

Context debug>service>id>stp

Description This command enables STP debugging for all events.

bpdu

Syntax [**no**] **bpdu**

Context debug>service>id>stp

Description This command enables STP debugging for received and transmitted BPDUs.

exception

Syntax [**no**] **exception**

Context debug>service>id>stp

Description This command enables STP debugging for exceptions.

fsm-state-changes

Syntax [**no**] **fsm-state-changes**

Context debug>service>id>stp

Description This command enables STP debugging for FSM state changes.

fsm-timers

Syntax [**no**] **fsm-timers**

Context debug>service>id>stp

Description This command enables STP debugging for FSM timer changes.

port-role

Syntax [**no**] **port-role**

Context debug>service>id>stp

Description This command enables STP debugging for changes in port roles.

port-state

Syntax [**no**] **port-state**

Context debug>service>id>stp

Description This command enables STP debugging for port states.

sap

Syntax [**no**] **sap** *sap-id*

Context debug>service>id>stp

Description This command enables STP debugging for a specific SAP.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

IES Show Commands

customer

Syntax **customer** [*customer-id*] [**site** *customer-site-name*]

Context show>service

Description This command displays service customer information.

Parameters *customer-id* — Displays only information for the specified customer ID.

Default All customer IDs display

Values 1 — 2147483647

site *customer-site-name* — Specifies the customer site which is an anchor point for an ingress and egress virtual scheduler hierarchy.

Output **Show Customer Command Output —** The following table describes show customer command output fields:

Label	Description
`Customer-ID`	The ID that uniquely identifies a customer.
`Contact`	The name of the primary contact person.
`Description`	Generic information about the customer.
`Phone`	The phone/pager number to reach the primary contact person.
`Total Customers`	The total number of customers configured.
`Multi-service site`	
`Site`	Multi-service site name. A multi-service customer site is a group of SAPs with common origination and termination points.
`Description`	Information about a specific customer's multi-service site.
`Assignment`	The port ID, MDA, or card number, where the SAP's that are members of this multi- service site are defined.
`I. Sched Pol`	The ingress QoS scheduler policy assigned to this multi-service site.
`E. Sched Pol`	The egress QoS scheduler policy assigned to this multi-service site.
`Service Association`	
`Service-ID`	The ID that uniquely identifies a service.
`SAP`	Specifies the SAP assigned to the service.

Sample Output

```
*A:ALA-12# show service customer
===========================================================
Customers
===========================================================
Customer-ID : 1
Contact     : Manager
Description : Default customer
Phone       : (123) 555-1212

Customer-ID : 2
Contact     : Tech Support
Description : TiMetra Networks
Phone       : (234) 555-1212

Customer-ID : 3
Contact     : Fred
Description : TiMetra Networks
Phone       : (345) 555-1212

Customer-ID : 6
Contact     : Ethel
Description : Epipe Customer
Phone       : (456) 555-1212

Customer-ID : 7
Contact     : Lucy
Description : ABC Customer
Phone       : (567) 555-1212

Customer-ID : 8
Contact     : Customer Service
Description : IES Customer
Phone       : (678) 555-1212

Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567

Customer-ID : 94043
Contact     : Test Engineer on Duty
Description : TEST Customer
Phone       : (789) 555-1212

-------------------------------------------------------
Total Customers : 8
-------------------------------------------------------------
*A:ALA-12#


*A:ALA-12# show service customer 274
===============================================================================
Customer  274
===============================================================================
Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567
```

```
-------------------------------------------------------------------------------
Multi Service Site
-------------------------------------------------------------------------------
Site        : west
Description : (Not Specified)
===============================================================================
*A:ALA-12#


*A:ALA-12# show service customer 274 site west
===============================================================================
Customer  274
===============================================================================
Customer-ID : 274
Contact     : Mssrs. Beaucoup
Description : ABC Company
Phone       : 650 123-4567
-------------------------------------------------------------------------------
Multi Service Site
-------------------------------------------------------------------------------
Site        : west
Description : (Not Specified)
Assignment  : Card 5
I. Sched Pol: SLA1
E. Sched Pol: (Not Specified)
-------------------------------------------------------------------------------
Service Association
-------------------------------------------------------------------------------
No Service Association Found.
===============================================================================
*A:ALA-12#
```

sap-using

Syntax **sap-using** [**sap** *sap-id*]
sap-using interface [*ip-address* | *ip-int-name*]
sap-using [**ingress** | **egress**] **filter** *filter-id*
sap-using [**ingress**] **qos-policy** *qos-policy-id*

Context show>service

Description Displays SAP information.

If no optional parameters are specified, the command displays a summary of all defined SAPs. The optional parameters restrict output to only SAPs matching the specified properties.

Parameters **sap *sap-id* —** Specifies the physical port identifier portion of the SAP definition. See Common CLI Command Descriptions on page 483 for command syntax.

ingress — Specifies matching an ingress policy.

egress — Specifies matching an egress policy.

filter *filter-id* **—** The ingress or egress filter policy ID for which to display matching SAPs.

Values 1 — 65535

interface — Specifies matching SAPs with the specified IP interface.

ip-addr — The IP address of the interface for which to display matching SAPs.

Values 1.0.0.0 — 223.255.255.255

ip-int-name — The IP interface name for which to display matching SAPs.

Output **Show Service SAP —** The following table describes show service SAP output fields:

Label	Description
Port ID	The ID of the access port where the SAP is defined.
Svc ID	The value that identifies the service.
SapMTU	The SAP MTU value.
Igr.QoS	The SAP ingress QoS policy number specified on the ingress SAP.
Ing.Fltr	The MAC or IP filter policy ID applied to the ingress SAP.
E.QoS	The SAP egress QoS policy number specified on the egress SAP.
Egr.Fltr	The MAC or IP filter policy ID applied to the egress SAP.
A.Pol	The accounting policy ID assigned to the SAP.
Adm	The administrative state of the SAP.
Opr	The actual state of the SAP.

Sample Output

```
*A:DUT-B# show service sap-using sap 1/1/3:100.*
===============================================================================
Service Access Points
===============================================================================
PortId                          SvcId      Ing.  Ing.    Egr.   Adm  Opr
                                           QoS   Fltr    Fltr
-------------------------------------------------------------------------------
1/1/1                           6          1     none    none   Up   Down
1/1/2                           700        1     none    none   Up   Down
-------------------------------------------------------------------------------
Number of SAPs : 2
===============================================================================
*A:DUT-B#
```

service-using

Syntax **service-using** [**ies**] [**customer** *customer-id*]

Context show>service

Description This command displays the services matching certain usage properties. If no optional parameters are specified, all services defined on the system are displayed.

Parameters **ies** — Displays matching IES services.

customer *customer-id* — Displays services only associated with the specified customer ID.

Default Services associated with an customer.

Values 1 — 2147483647

Output **Show Service Service-Using —** The following table describes show service service-using output fields:

Label	Description
Service Id	The value that identifies the service.
Type	Specifies the service type configured for the service ID.
Adm	The administrative state of the service.
Opr	The operating state of the service.
CustomerID	The ID of the customer who owns this service.
Last Mgmt Change	The date and time of the most recent management-initiated change to this service.

Sample Output

```
A:ALA-48# show service service-using ies
===============================================================================
Services [ies]
===============================================================================
ServiceId    Type      Adm    Opr        CustomerId        Last Mgmt Change
-------------------------------------------------------------------------------
88           IES       Up     Down       8                 07/25/2006 15:46:28
89           IES       Up     Down       8                 07/25/2006 15:46:28
104          IES       Up     Down       1                 07/25/2006 15:46:28
200          IES       Up     Down       1                 07/25/2006 15:46:28
214          IES       Up     Down       1                 07/25/2006 15:46:28
321          IES       Up     Down       1                 07/25/2006 15:46:28
322          IES       Down   Down       1                 07/25/2006 15:46:28
1001         IES       Up     Down       1730              07/25/2006 15:46:28
-------------------------------------------------------------------------------
Matching Services : 8
-------------------------------------------------------------------------------
A:ALA-48#
```

id

Syntax **id** *service-id* {**all** | **arp** | **base** | **sap** }

Context show>service

Description This command displays information for a particular service-id.

Parameters *service-id* — The unique service identification number to identify the service in the service domain.

all — Display detailed information about the service.

arp — Display ARP entries for the service.

base — Display basic service information.

sap — Display SAPs associated to the service.

all

Syntax **all**

Context show>service>id

Description This command displays detailed information for all aspects of the service.

Output **Show All Service-ID Output —** The following table describes the show all service-id command output fields:

Label	Description
Service Detailed Information	
`Service Id`	The service identifier.
`VPN Id`	The number which identifies the VPN.
`Service Type`	Specifies the type of service.
`SDP Id`	The SDP identifier.
`Description`	Generic information about the service.
`Customer Id`	The customer identifier.
`Last Mgmt Change`	The date and time of the most recent management-initiated change to this customer.
`SAP Count`	The number of SAPs specified for this service.
`SDP Bind Count`	The number of SDPs bound to this service.
Service Destination Points (SDPs)	
`SDP Id`	The SDP identifier.
`Type`	Indicates whether this Service SDP binding is a spoke or a mesh.

Label	Description (Continued)
Admin Path MTU	The largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Oper Path MTU	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
Delivery	Specifies the type of delivery used by the SDP: MPLS.
Admin State	The administrative state of this SDP.
Oper State	The operational state of this SDP.
Ingress Label	The label used by the far-end device to send packets to this device in this service by this SDP.
Egress Label	The label used by this device to send packets to the far-end device in this service by this SDP.
Ingress Filter	The ID of the ingress filter policy.
Egress Filter	The ID of the egress filter policy.
Far End	Specifies the IP address of the remote end of the MPLS tunnel defined by this SDP.
Last Changed	The date and time of the most recent change to this customer.
Signaling	Specifies the signaling protocol used to obtain the ingress and egress labels used in frames transmitted and received on this SDP.
Admin State	Specifies the operating status of the service.
Oper State	The current status of the service.
Hello Time	Specifies how often the SDP echo request messages are transmitted on this SDP.
Hello Msg Len	Specifies the length of the SDP echo request messages transmitted on this SDP.
Max Drop Count	Specifies the maximum number of consecutive SDP Echo Request messages that can be unacknowledged before the keepalive protocol reports a fault.
Hold Down Time	Specifies the amount of time to wait before the keepalive operating status is eligible to enter the alive state.
SDP Delivery Mechanism	When the SDP type is MPLS, a list of LSPs used to reach the far-end router displays. All the LSPs in the list must terminate at the IP address specified in the far-end field.
Number of SDPs	The total number SDPs applied to this service ID.

Label	Description (Continued)
Service Access Points	
`Service Id`	The service identifier.
`Port Id`	The ID of the access port where this SAP is defined.
`Description`	Generic information about the SAP.
`Encap`	The value of the label used to identify this SAP on the access port.
`Admin State`	The desired state of the SAP.
`Oper State`	The operating state of the SAP.
`Last Changed`	The date and time of the last change.
`Admin MTU`	The largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
`Oper MTU`	The actual largest service frame size (in octets) that can be transmitted through this SDP to the far-end router, without requiring the packet to be fragmented.
`Ingress qos-policy`	The SAP ingress QoS policy ID.
`Egress qos-policy`	The SAP egress QoS policy ID.
`Ingress Filter-Id`	The SAP ingress filter policy ID.
`Egress Filter-Id`	The SAP egress filter policy ID.
`Multi Svc Site`	Indicates the multi-service site that the SAP is a member.
`Ingress sched-policy`	Indicates the ingress QoS scheduler for the SAP.
`Egress sched-policy`	Indicates the egress QoS scheduler for the SAP.
`Acct. Pol`	Indicates the accounting policy applied to the SAP.
`Collect Stats`	Specifies whether accounting statistics are collected on the SAP.
SAP Statistics	
`Dropped`	The number of packets or octets dropped.
`Offered Hi Priority`	The number of high priority packets, as determined by the SAP ingress QoS policy.
`Offered Low Priority`	The number of low priority packets, as determined by the SAP ingress QoS policy.
`Forwarded In Profile`	The number of in-profile packets or octets (rate below CIR) forwarded.

Label	Description (Continued)
`Forwarded Out Profile`	The number of out-of-profile packets or octets (rate above CIR) forwarded.

arp

Syntax **arp** [*ip-address*] | [**mac** *ieee-address*] | [**sap** *sap-id*] | [**interface** *ip-int-name*]

Context show>service>id

Description Displays the ARP table for the IES instance. The ARP entries for a subscriber interface are displayed uniquely. Each MAC associated with the subscriber interface child group-interfaces are displayed with each subscriber interface ARP entry. They do not reflect actual ARP entries but are displayed along the interfaces ARP entry for easy lookup.

Parameters *ip-address* — Displays only ARP entries in the ARP table with the specified IP address.

Default All IP addresses.

mac *ieee-address* **—** Displays only ARP entries in the ARP table with the specified 48-bit MAC address. The MAC address can be expressed 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.

Default All MAC addresses.

sap *sap-id* **—** Displays SAP information for the specified SAP ID. See Common CLI Command Descriptions on page 483 for command syntax.

port-id — **interface —** Specifies matching service ARP entries associated with the IP interface.

ip-address — The IP address of the interface for which to display matching ARP entries.

Values 1.0.0.0 — 223.255.255.255

ip-int-name — The IP interface name for which to display matching ARPs.

Output **Show Service-ID ARP —** The following table describes show service-id ARP output fields.

Label	Description
IP Address	The IP address.
MAC Address	The specified MAC address.
Type	Static — FDB entries created by management. Learned — Dynamic entries created by the learning process. Other — Local entries for the IP interfaces created.
Expiry	The age of the ARP entry.
Interface	The interface applied to the service.
SAP	The SAP ID.

Sample Output

```
*A:DUT-B# show service id 100 arp
===============================================================================
ARP Table
===============================================================================
IP Address      MAC Address         Type       Expiry    Interface         SAP
```

```
-------------------------------------------------------------------------------
192.168.1.2     00:00:01:00:00:01  Other     00h00m00s   HW                1/1/1:10*
195.168.1.1     32:67:01:01:00:03  Other     00h00m00s   to7x              1/1/3:10*
195.168.1.2     32:68:01:01:00:02  Dynamic   03h59m58s   to7x              1/1/3:10*
===============================================================================
*A:DUT-B#
```

base

Syntax **base**

Context show>service>id

Description This command displays basic information about this IES service.

Sample Output

```
*A:ALA-A# show service id 100 base
-----------------------------------------------------------------
Service Basic Information
-----------------------------------------------------------------
Service Id        : 100                 Vpn Id            : 100
Service Type      : IES
Description       : Default Ies description for service id 100
Customer Id       : 1
Last Status Change: 08/29/2006 17:44:28
Last Mgmt Change  : 08/29/2006 17:44:28
Admin State       : Up                  Oper State        : Up
SAP Count         : 2
-------------------------------------------------------------------------------
Service Access & Destination Points
-------------------------------------------------------------------------------
Identifier                        Type         AdmMTU  OprMTU  Adm     Opr
-------------------------------------------------------------------------------
sap:1/1/3                         null         1514    1514    Up      Up
sap:1/1/4                         null         1514    1514    Up      Up
===============================================================================
*A:ALA-A#
```

interface

Syntax **interface** [*ip-address* | *ip-int-name*] [**detail | summary**]

Context show>service>id

Description This command displays information for the IP interfaces associated with the IES service. If no optional parameters are specified, a summary of all IP interfaces associated to the service are displayed.

Parameters *ip-address* — The IP address of the interface for which to display information.

Values ipv4-address: a.b.c.d (host bits must be 0)

ip-int-name — Specifies the IP interface name for which to display information.

Values 32 characters maximum

detail — Displays detailed IP interface information.

Default IP interface summary output.

summary — Displays the summary of IP interface information.

Output **Show Service-ID —** The following table describes show service-id output fields.

Label	Description
`If Name`	The name used to refer to the IES interface.
`Type`	Specifies the interface type.
`IP-Address`	Specifies the IP address/IP subnet/broadcast address of the interface.
`Adm`	The administrative state of the interface.
`Opr`	The operational state of the interface.
`Admin State`	The administrative state of the interface.
`Oper State`	The operational state of the interface.
`IP Addr/mask`	Specifies the IP address/IP subnet/broadcast address of the interface.
`If Index`	The index corresponding to this IES interface. The primary index is 1; all IES interfaces are defined in the base virtual router context.
`If Type`	Specifies the interface type.
`SAP Id`	Specifies the SAP's port ID.
`SNTP B.Cast`	Specifies whether SNTP broadcast client mode is enabled or disabled.
`Arp Timeout`	Specifies the timeout for an ARP entry learned on the interface.

Label	Description (Continued)
MAC Address	Specifies the 48-bit IEEE 802.3 MAC address.
ICMP Mask Reply	Specifies whether ICMP mask reply is enabled or disabled.
Cflowd	Specifies whether Cflowd collection and analysis on the interface is enabled or disabled.
Redirects	Specifies the rate for ICMP redirect messages.
Unreachables	Specifies the rate for ICMP unreachable messages.
TTL Expired	Specifies the rate for ICMP TTL messages.

Sample Output

```
A:ALA-49# show service id 88 interface
===============================================================================
Interface Table
===============================================================================
Interface-Name                   Adm         Opr         Type    Port/SapId
   IP-Address
-------------------------------------------------------------------------------
Sector A                         Up          Down/Down   IES     1/1/1.2.2
   -                                                                 -
test                             Up          Down/Down   IES     1/1/2:0
   1.1.1.1/31                                                        n/a
   1.1.1.1/31                                                        n/a
   1.1.2.1/31                                                        n/a
test27                           Up          Up/--       IES Sub subscriber
   192.168.10.21/24                                                  n/a
grp-if                           Up          Down/--     IES Grp 1/2/2
Interfaces : 4
===============================================================================
A:ALA-49#
A:ALA-49# show service id 88 interface
===============================================================================
Interface Table
===============================================================================
Interface-Name Adm Opr(v4/v6) Type Port/SapId
IP-Address PfxState
-------------------------------------------------------------------------------
Sector A Up Down/Down IES 1/1/1.2.2
- -
test Up Down/Down IES 1/1/2:0
1.1.1.1/31 n/a
1.1.1.1/31 n/a
1.1.2.1/31 n/a
test27 Up Up/-- IES Sub subscriber
192.168.10.21/24 n/a
grp-if Up Down/-- IES Grp 1/2/2
Interfaces : 4
===============================================================================
A:ALA-49#
```

Appendix: Port-Based Split Horizon

In This Chapter

This section provides Port-Based Split Horizon configuration information.

Overview

NOTE: Port-based SHG is not supported on 7210 SAS-K.

The port-based split horizon feature can be used to disable local switching on the 7210 SAS. A loop-free topology can be achieved using split horizon on 7210 SAS switches.

Traffic arriving on an access or an access-uplink port within a split horizon group will not be copied to other access and an access-uplink ports in the same split horizon group, but will be copied to an access-uplink ports in other split horizon groups.

Since split horizon is a per port feature in 7210 SAS, all SAPs associated with the port becomes part of split horizon group configured on that port.

Topology

Figure illustrates an example of split horizon groups used to prevent communication between two access SAPs and between two access-uplink SAPs.

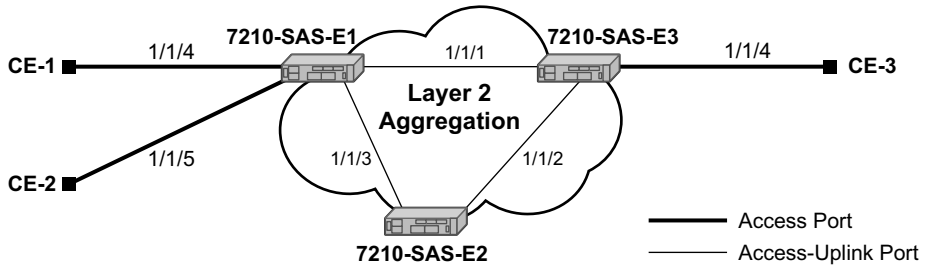


Figure 23: Split Horizon Group Example

Using 7210-SAS-1 as an example:

1. Split horizon group “access” is created to prevent any communication between the SAP’s part of port 1/1/4 and port 1/1/5 (configured as access port) within the same VPLS.
2. Split horizon group “access uplink” is created to prevent any communication between SAP’s part of port 1/1/1 and port 1/1/3 (configured as an access-uplink) within the same VPLS.
3. VPLS 100 is created on 7210 SAS-1 with SAPs 1/1/1, 1/1/3, and SAPs on 1/1/4 and 1/1/5 as part of this VPLS. CE1, CE2 and CE3 are the customer sites.
4. With this configuration, any communication between ports 1/1/4 and 1/1/5 gets blocked, similarly communication between ports 1/1/1 and 1/1/3 gets blocked but any traffic received on ports (SAPs) part of split horizon group “access uplink” will be switched to ports (SAPs) part of split horizon group “access” and vice versa based on the FDB entries

for VPLS 100.

Configuration Guidelines

The following configuration guidelines must be followed to configure a split horizon group.

1. Create a split horizon group in the config prompt. The group name must be unique across the system.

```
7210-SAS1>config#info
#--------------------------------------------------
echo "Split-horizon-group Configuration"
#--------------------------------------------------
    split-horizon-group access create
        description “Block access between access Ports”
    split-horizon-group access-uplink create
        description "Block access between access-uplink Ports"
    exit
#--------------------------------------------------
7210-SAS1>config#
```

2. Associate ports 1/1/4 and 1/1/5 with split horizon group “access” By default all ports are access ports. The default Ethernet encapsulation for access port is “null”.

```
7210-SAS1>config#info
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
    port 1/1/4
        split-horizon-group access
        ethernet
        exit
        no shutdown
exit
    port 1/1/5
        split-horizon-group access
        ethernet
        exit
        no shutdown
  exit
#--------------------------------------------------
7210-SAS1>config#
```

3. Configure ports 1/1/1 and 1/1/3 as access uplink and associate these ports with split horizon group “access-uplink” default Ethernet encapsulation for access uplink port is “qinq”.

```
7210-SAS1>config# info
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
```

```
    port 1/1/1
        split-horizon-group access-uplink
        ethernet
               mode access uplink
        exit
        no shutdown
exit
    port 1/1/3
        split-horizon-group access-uplink
        ethernet
               mode access uplink
        exit
        no shutdown
  exit
#--------------------------------------------------
7210-SAS1>config#
```

4. Create a VPLS instance 100.

```
#--------------------------------------------------
echo "Service Configuration"
#--------------------------------------------------
    service
          customer 2 create
          exit
         vpls 100 customer 2 create
            stp
                shutdown
            exit
            sap 1/1/1:100.* create
            exit
            sap 1/1/3:100.* create
            exit
            sap 1/1/4 create
            exit
            sap 1/1/5 create
            exit
            no shutdown
    exit
...
#--------------------------------------------------
```

Note: A split horizon on a port must be configured before creating any SAPs associated with that port.

Verification

The following output verifies the split horizon configuration on a 7210 SAS:

```
7210-SAS1# show split-horizon-group
===============================================================================
Port: Split Horizon Group
===============================================================================
Name                                Description
-------------------------------------------------------------------------------
access                               Block access between access Ports
access-uplink                        Block access between access-uplink Ports

No. of Split Horizon Groups: 2
===============================================================================
7210-SAS1#
```

Execute the below mentioned command to verify the port association with split horizon groups:

```
7210-SAS1# show split-horizon-group access
===============================================================================
Port: Split Horizon Group
===============================================================================
Name                                Description
-------------------------------------------------------------------------------
access                               Block access between access Ports
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Port1/1/4                            10/100/Gig Ethernet SFP
Port1/1/5                            10/100/Gig Ethernet SFP

Ports Associated : 2
===============================================================================
7210-SAS1#


7210-SAS1# show split-horizon-group access-uplink
===============================================================================
Port: Split Horizon Group
===============================================================================
Name                                Description
-------------------------------------------------------------------------------
Access-uplink                       Block access between access-uplink Ports
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Port1/1/1                            10/100/Gig Ethernet SFP
Port1/1/3                            10/100/Gig Ethernet SFP

Ports Associated : 2
===============================================================================
7210-SAS1#
```

Appendix: DHCP Management

In This Chapter

This chapter provides information about using DHCP, including theory, supported features and configuration process overview.

The topics in this chapter include:

DHCP Principles

In a Triple Play network, client devices (such as a routed home gateway, a session initiation protocol (SIP) phone or a set-top box) use Dynamic Host Configuration Protocol (DHCP) to dynamically obtain their IP address and other network configuration information. 7210 autoinit procedure also uses DHCP to dynamically obtain the BOF file used for first-time booting of the system (along with IP address required to retrieve the BOF file, the configuration file and the Timos software image from the network). DHCP is defined and shaped by several RFCs and drafts in the IETF DHC working group including the following

- RFC 2131, Dynamic Host Configuration Protocol
- RFC 3046, DHCP Relay Agent Information Option

The DHCP operation is illustrated in Figure 24.

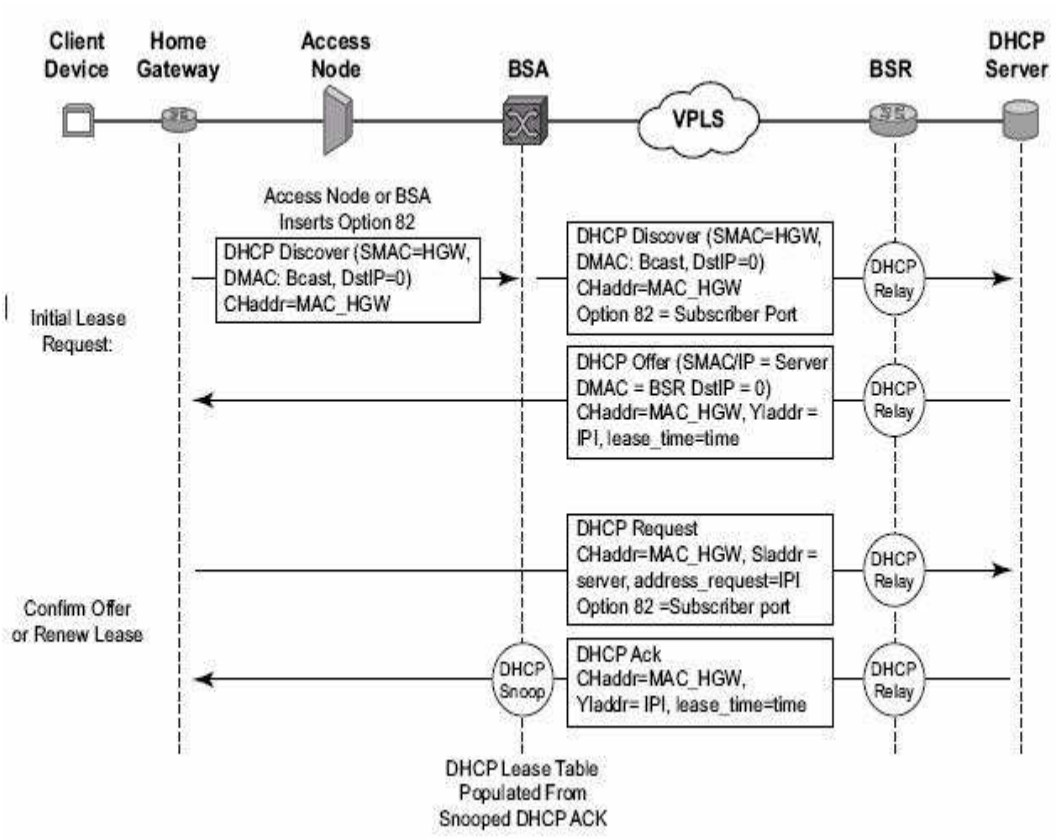


Figure 24: IP Address Assignment with DHCP

1. During boot-up, the client device sends a DHCP discover message to get an IP address from the DHCP Server. The message contains:
   - → Destination MAC address — broadcast
   - → Source MAC address — MAC of client device
   - → Client hardware address — MAC of client device

If this message passes through a DSLAM or other access node (possibly a 7210 SAS device), typically the Relay information option (Option 82) field is added, indicating shelf, slot, port, VPI, VCI and other fields, to identify the subscriber.

DHCP relay is enabled on the first IP interface in the upstream direction. Depending on the scenario, the DSLAM, BSA or the BSR will relay the discover message as a unicast packet towards the configured DHCP server. DHCP relay is configured to insert the giaddr in order to indicate to the DHCP server in which subnet an address should be allocated.

2. The DHCP server will lookup the client MAC address and Option 82 information in its database. If the client is recognized and authorized to access the network, an IP address will be assigned and a DHCP offer message returned. The BSA or BSR will relay this back to the client device.
3. It is possible that the discover reached more than one DHCP server, and thus that more than one offer was returned. The client selects one of the offered IP addresses and confirms it wants to use this in a DHCP request message, sent as unicast to the DHCP server that offered it.
4. The DHCP server confirms that the IP address is still available, updates its database to indicate it is now in use, and replies with a DHCP ACK message back to the client. The ACK also contains the Lease Time of the IP address.

DHCP Features

Using Option 82 Field

Option 82, or the relay information option is specified in RFC 3046, DHCP Relay Agent Information Option, allows the router to append some information to the DHCP request that identifies where the original DHCP request arrives from.

There are two sub-options under Option 82:

- Agent Circuit ID Sub-option (RFC 3046, section 3.1): This sub-option specifies data which must be unique to the box that is relaying the circuit.
- Remote ID Sub-option (RFC 3046 section 3.2): This sub-option identifies the host at the other end of the circuit. This value must be globally unique.

Both sub-options are supported by the Alcatel-Lucent 7210 SAS and can be used separately or together.

Inserting Option 82 information is supported independently of DHCP relay.

When the circuit id sub-option field is inserted by the 7210 SAS, it can take following values:

- *sap-id*: The SAP index (only under a IES or VPRN service)
- *ifindex*: The index of the IP interface (only under a IES or VPRN service)
- *ascii-tuple*: An ASCII-encoded concatenated tuple, consisting of [system-name|serviceid|interface-name] (for VPRN or IES) or [system-name|service-id|sap-id] (for VPLS).
- *vlan-ascii-tuple*: An ASCII-encoded concatenated tuple, consisting of the ascii-tuple followed by Dot1p bits and Dot1q tags.

Note that for VPRN the ifindex is unique only within a VRF. The DHCP relay function automatically prepends the VRF ID to the ifindex before relaying a DHCP Request.

When a DHCP packet is received with Option 82 information already present, the system can do one of three things. The available actions are:

- *Replace* — On ingress the existing information-option is replaced with the information-option parameter configured on the 7210 SAS. On egress (towards the customer) the information-option is stripped (per the RFC).

- *Drop* — The DHCP packet is dropped and a counter is incremented.
- *Keep* — The existing information is kept on the packet and the router does not add any additional information. On egress the information option is not stripped and is sent on to the downstream node.

In accordance with the RFC, the default behavior is to keep the existing information; except if the giaddr of the packet received is identical to a local IP address on the router, then the packet is dropped and an error incremented regardless of the configured action.

The maximum packet size for a DHCP relay packet is 1500 bytes. If adding the Option 82 information would cause the packet to exceed this size, the DHCP relay request will be forwarded without the Option 82 information. This packet size limitation exists to ensure that there will be no fragmentation on the end Ethernet segment where the DHCP server attaches.

In the downstream direction, the inserted Option 82 information should not be passed back towards the client (as per RFC 3046, DHCP Relay Agent Information Option). To enable downstream stripping of the option 82 field, DHCP snooping should be enabled on the SDP or SAP connected to the DHCP server.

Trusted and Untrusted

There is a case where the relay agent could receive a request where the downstream node added Option 82 information without also adding a giaddr (giaddr of 0). In this case the default behavior is for the router to drop the DHCP request. This behavior is in line with the RFC.

The 7210 SAS supports a command trusted, which allows the router to forward the DHCP request even if it receives one with a giaddr of 0 and Option 82 information attached. This could occur with older access equipment. In this case the relay agent would modify the request's giaddr to be equal to the ingress interface. This only makes sense when the action in the information option is keep, and the service is IES or VPRN. In the case where the Option 82 information gets replaced by the relay agent, either through explicit configuration or the VPLS DHCP Relay case, the original Option 82 information is lost, and the reason for enabling the trusted option is lost.

DHCP Snooping

To support DHCP based address assignment in L2 aggregation network, 7210 supports DHCP snooping. 7210 can copy packets designated to the standard UDP port for DHCP (port 67) to its control plane for inspection, this process is called DHCP snooping.

DHCP snooping can be performed in two directions:

1. From the client to the DHCP server (Discover or Request messages) to insert Option 82 information; For these applications, DHCP snooping must be enabled on the SAP towards the subscriber.
2. From the DHCP server (ACK messages), to remove the Option 82 field towards the client. For these applications, DHCP snooping must be enabled on both the SAP towards the network and the SAP towards the subscriber.

Common Configuration Guidelines

The topic in this section are:

- Configuration Guidelines for DHCP relay and snooping on page 481
- Configuring Option 82 Handling on page 481

Configuration Guidelines for DHCP relay and snooping

The following configuration guidelines must be followed to configure DHCP relay and snooping.

- 7210 SAS devices does not support the ARP populate based on the DHCP lease, assigned to the DHCP client
- 7210 SAS devices does not maintain the DHCP lease assigned to the client
- 7210 SAS devices do not perform IP spoofing checks and MAC spoofing checks based on the DHCP parameters assigned to the client
- MAC learning must be enabled in the VPLS service, for DHCP snooping.
- DHCP snooping is not supported for B-SAPs in B-VPLS services and I-SAPs in I-VPLS services.
- Ingress ACLs cannot be used to drop DHCP control packet.
- DHCP packets received over a SDP cannot be identified and option-82 inserted by the node cannot be removed by the node, in the downstream direction. If this behavior is not needed user should not enable DHCP snooping in the VPLS service, if the DHCP server is reachable over the SDP (either spoke-sdp or mesh-sdp).

Configuring Option 82 Handling

Option 82, or “Relay Information Option” is a field in DHCP messages used to identify the subscriber. The Option 82 field can already be filled in when a DHCP message is received at the router, or it can be empty. If the field is empty, the router shoulMAC learning must be enabled in the VPLS service, for DHCP snooping.d add identifying information (circuit ID, remote ID or both). If the field is not empty, the router can decide to replace it.

The following example displays an example of a partial BSA configuration with Option 82 adding on a VPLS service. Note that snooping must be enabled explicitly on a SAP.

```
*A:7210SAS>config>service#
-----------------------------------------------

vpls 2 customer 1 create
            shutdown
            stp
```

```
                shutdown
            exit
sap 1/1/12:100 create
                dhcp                    //Configuration example to add option 82
                    option
                        action replace
                        circuit-id
                        no remote-id
                    exit
                    no shutdown
                exit
            exit
            no shutdown
        exit
----------------------------------------------

*A:7210SAS>config>service#
```

The following example displays an example of a partial BSA configuration to remove the Option 82 on a VPLS service.

```
vpls 2 customer 1 create
            stp
                shutdown
            exit
            sap 1/1/14:100 create      //Configuration example to remove option 82
                dhcp
                    snoop
                    no shutdown
                exit
            exit
```

Common CLI Command Descriptions

In This Chapter

This section provides information about common Command Line Interface (CLI) syntax and command usage.

Topics in this chapter include:

Common Service Commands

sap

Syntax [**no**] **sap** *sap-id*

Description This command specifies the physical port identifier portion of the SAP definition.

Parameters *sap-id* — Specifies the physical port identifier portion of the SAP definition.

The *sap-id* can be configured in one of the following formats:

Type	Syntax	Example
port-id	*slot*/*mda*/*port*[.*channel*]	1/1/5
null	[*port-id* | *lag-id*]	*port-id*: 1/1/3 *lag-id*: lag-3
dot1q	[*port-id* | *lag-id*]:qtag1	*port-id*:qtag1: 1/1/3:100 *lag-id*:qtag1:lag-3:102 *cp*.conn-prof-id: 1/2/1:cp.2
qinq	[*port-id* | *lag-id*]:*qtag1*.*qtag2*	*port-id*:qtag1.qtag2: 1/1/3:100.10 *lag-id*:qtag1.qtag2: lag-10:

The values depends on the encapsulation type configured for the interface. The following table describes the allowed values for the port and encapsulation types.

Port Type	Encap-Type	Allowed Values	Comments
Ethernet	Null	0	The SAP is identified by the port.
Ethernet	Dot1q	0 — 4094	The SAP is identified by the 802.1Q tag on the port. Note that a 0 qtag1 value also accepts untagged packets on the dot1q port.
Ethernet	QinQ	qtag1: 0 — 4094 qtag2: 0 — 4094	The SAP is identified by two 802.1Q tags on the port. Note that a 0 qtag1 value also accepts untagged packets on the Dot1q port.

Standards and Protocol Support

Standards Compliance

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
IANA-IFType-MIB
IEEE8023-LAG-MIB
ITU-T G.8032 Ethernet Ring Protection Switching (version 2)
IEEE 802.3af and 802.3at (Power over Ethernet) – Only on 7210 SAS-T ETR

Protocol Support

DHCP
RFC 2131 Dynamic Host Configuration Protocol
RFC 3046 DHCP Relay Agent Information Option (Option 82)

DIFFERENTIATED SERVICES
RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
RFC 3140 Per-Hop Behavior Identification Codes
RFC 4115 A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic [Only for 7210 SAS-D]

IPv6
RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2462 IPv6 Stateless Address Auto configuration
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
RFC 3587 IPv6 Global Unicast Address Format
RFC 4007 IPv6 Scoped Address Architecture
RFC 4193 Unique Local IPv6 Unicast Addresses
RFC 4291 IPv6 Addressing Architecture
RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

Multicast
RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

NETWORK MANAGEMENT
ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASEDACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 Simple Network Management Protocol (SNMP) Applications
RFC 3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 SNMP MIB draft-ietf-disman-alarm-mib-04.txt
RFC 3418 SNMP MIB

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

TCP/IP

RFC 768 UDP
RFC 1350 The TFTP Protocol
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer Size option

Timing (Only on 7210 SAS-D ETR)

ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008
ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.
GR-1244-CORE Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005
ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.
ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.
ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.
IEEE Std 1588™-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

Proprietary MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib
TIMETRA-CAPABILITY-7210-SAS-E-V5v0.mib (Only for 7210 SAS-E)
TIMETRA-CAPABILITY-7210-SAS-D-V5v0.mib (Only for 7210 SAS-D)
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-ALARM-INPUT-MIB.mib [Only for 7210 SAS-E]
TIMETRA-SAS-FILTER-MIB.mib
TIMETRA-SAS-IEEE8021-CFM-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-LOG-MIB.mib.mib
TIMETRA-SAS-MIRROR-MIB.mib
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRTR-MIB.mib

INDEX