



Alcatel-Lucent 7705

SERVICE AGGREGATION ROUTER OS | RELEASE 4.0
QUALITY OF SERVICE GUIDE

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

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

Copyright 2010 Alcatel-Lucent.
All rights reserved.

Disclaimers

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

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

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

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

Table of Contents

Preface	27
Getting Started	31
Alcatel-Lucent 7705 SAR QoS Configuration Process	31
Notes on 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F	32
QoS Policies	35
QoS Overview	37
Egress and Ingress Traffic Direction	39
Forwarding Classes	40
Traffic Classification at the Access Ingress	41
Traffic Classification Types	42
Access Ingress Queues	44
Ingress Queuing and Scheduling	45
Profiled Scheduling	45
Queue-Type-Based Scheduling	46
Profiled Scheduling and Queue-Type-Based Scheduling Combined	47
Ingress Queuing and Scheduling for BMU Traffic	49
Ingress Shaping to Fabric (Access and Network)	49
BMU Support	49
Configurable Ingress Shaping to Fabric (Access and Network)	51
Traffic Flow Across the Fabric	54
BMU Traffic at Network Egress	55
Network Egress Queuing Aggregation	56
Network Egress Scheduling	56
Network Egress Scheduling on the T1/E1 ASAP Adapter Cards, 2-port OC3/STM1 Channelized Adapter Card, 4-port OC3/STM1 Clear Channel Adapter Card, and 4-port DS3/E3 Adapter Card	56
Network Egress Scheduling on 8-port Ethernet Adapter Cards	58
Network Egress Shaping	58
Network Egress Marking and Re-Marking	59
Network Egress Marking and Re-Marking on Ethernet ports	59
Network Ingress Classification	59
Network Ingress Queuing	60
Network Ingress Queuing for BMU Traffic	61
Network Ingress Scheduling	62
Network Ingress Scheduling on the T1/E1 ASAP Adapter Cards, 2-port OC3/STM1 Channelized Adapter Card, 4-port OC3/STM1 Clear Channel Adapter Card, and 4-port DS3/E3 Adapter Card	62
Network Ingress Scheduling on 8-port Ethernet Adapter Cards	63
Access Egress Queuing and Scheduling	64
Access Egress Scheduling and Queuing for BMU Traffic	64
ATM Access Egress Queuing and Scheduling	64
Ethernet Access Egress Queuing and Scheduling	67
Access Egress Marking/Re-Marking	68
QoS Policies Overview	69
Service Ingress QoS Policies	72
Service Egress QoS Policies	74

Table of Contents

MC-MLPPP SAP Egress QoS Policies	76
Network and Service QoS Policies	77
Network QoS Policies	78
Network Queue QoS Policies	83
WRED and RED Slope Policies	91
WRED MinThreshold and MaxThreshold Computation	92
ATM Traffic Descriptor Profiles	93
Fabric Profiles	93
QoS Policy Entities	93
Configuration Notes	95
Reference Sources	95
Network QoS Policies	97
Overview	98
Basic Configuration	99
Creating a Network QoS Policy	99
Applying Network Policies	101
Default Network Policy Values	102
Service Management Tasks	107
Deleting QoS Policies	107
Copying and Overwriting Network Policies	107
Editing QoS Policies	108
Network QoS Policy Command Reference	109
Command Hierarchies	109
Command Descriptions	111
Configuration Commands	112
Operational Commands	128
Show Commands	129
Network Queue QoS Policies	141
Overview	142
Basic Configuration	143
Creating a Network Queue QoS Policy	143
Applying Network Queue Policies	145
Adapter Cards	145
Network Ports	146
Default Network Queue Policy Values	147
Service Management Tasks	152
Deleting QoS Policies	152
Copying and Overwriting QoS Policies	152
Editing QoS Policies	154
Network Queue QoS Policy Command Reference	155
Command Hierarchies	155
Command Descriptions	157
Configuration Commands	158
Operational Commands	173
Show Commands	174

Service Egress and Ingress QoS Policies	177
Overview	178
Basic Configuration	179
Creating Service Egress and Ingress QoS Policies	179
Creating a Service Egress QoS Policy	179
Creating a Service Ingress QoS Policy	183
Creating an MC-MLPPP SAP Egress QoS Policy	187
Applying Service Egress and Ingress Policies	190
Default Service Egress and Ingress Policy Values	192
Service Egress Policy Defaults	192
Service Ingress Policy Defaults	193
Service Management Tasks	195
Deleting QoS Policies	195
Removing a QoS Policy from a Service SAP	195
Removing a Policy from the QoS Configuration	196
Copying and Overwriting QoS Policies	197
Editing QoS Policies	198
Service Egress and Ingress QoS Policy Command Reference	199
Command Hierarchies	199
Command Descriptions	204
Configuration Commands	205
Operational Commands	237
Show Commands	238
Slope QoS Policies	251
Overview	252
Basic Configuration	253
Creating a Slope QoS Policy	253
Applying Slope Policies	254
Default Slope Policy Values	255
Service Management Tasks	256
Deleting QoS Policies	256
Removing a Policy from the QoS Configuration	256
Copying and Overwriting QoS Policies	256
Editing QoS Policies	258
Slope QoS Policy Command Reference	259
Command Hierarchies	259
Command Descriptions	261
Configuration Commands	262
Operational Commands	268
Show Commands	269
ATM QoS Traffic Descriptor Profiles	273
ATM Traffic Descriptor Profiles	274
ATM Traffic Management	274
ATM Service Categories	274
ATM Traffic Descriptors and QoS Parameters	274
ATM Policing	275
Shaping	276
ATM Queuing and Scheduling	276

Table of Contents

Congestion Avoidance	277
Basic Configuration	278
Creating an ATM Traffic Descriptor Profile QoS Policy	278
Applying ATM Traffic Descriptor Profile Policies	279
ATM VLL (Apipe) SAPs	279
Default ATM Traffic Descriptor Profile Policy Values	280
Service Management Tasks	281
Removing an ATM Traffic Descriptor Profile from the QoS Configuration	281
Copying and Overwriting an ATM Traffic Descriptor Profile	281
Editing QoS Policies	281
ATM QoS Policy Command Reference	283
Command Hierarchies	283
Command Descriptions	284
Configuration Commands	285
Operational Commands	294
Show Commands	295
QoS Fabric Profiles	299
Basic Configuration	300
Creating a QoS Fabric Profile	300
Default Fabric Profile Values	302
Service Management Tasks	303
Removing a Fabric Profile from the QoS Configuration	303
Copying and Overwriting a Fabric Profile	303
Editing QoS Policies	303
QoS Fabric Profile Command Reference	305
Command Hierarchies	305
Command Descriptions	306
Configuration Commands	307
Operational Commands	311
Show Commands	312
Standards and Protocol Support	315

List of Tables

Getting Started	31
Table 1: Configuration Process	31
Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison	32
QoS Policies	35
Table 3: Default Forwarding Classes	40
Table 4: Traffic Classification Types	42
Table 5: Fabric Profile Modes Options and Capabilities	52
Table 6: Default Network Ingress QoS Policy	60
Table 7: Scheduler Weight Values (WRR) based on MIR for the 16-port T1/E1 ASAP Adapter Card, 32-port T1/E1 ASAP Adapter Card, and 2-port OC3/STM1 Channelized Adapter Card	65
Table 8: Scheduler Weight Values (WRR) based on MIR for the 4-port OC3/STM1 Clear Channel Adapter Card	66
Table 9: ATM Scheduling and Relative Priorities	66
Table 10: QoS Policy Types and Descriptions	71
Table 11: Forwarding Class and Enqueuing Priority Classification Hierarchy Based on Rule Type	73
Table 12: Default Service Ingress Policy ID 1 Definition	74
Table 13: Default Service Egress Policy ID 1 Definition	75
Table 14: MC-MLPPP Class Priorities	76
Table 15: Packet Forwarding Class to MLPPP Class Mapping	77
Table 16: Default Network QoS Policy Egress Marking	79
Table 17: Default Network QoS Policy DSCP to Forwarding Class Mappings	80
Table 18: Default Network QoS Policy LSP EXP to Forwarding Class Mappings	81
Table 19: Applications and Support for Configurable DSCP or dot1p Markings	82
Table 20: Default Network Queue Policy Definition	84
Network QoS Policies	97
Table 21: Network Policy Defaults	102
Table 22: Valid DSCP Names	119
Table 23: DSCP Name to Value Mappings Command Output Fields	130
Table 24: Network Policy Command Output Fields	134
Table 25: Application QoS Output Fields	137
Table 26: DSCP-to-FC Mapping Output Fields	139
Network Queue QoS Policies	141
Table 27: Default Network Queue Policy Definition	147
Table 28: CBS Forwarding Class Defaults	165
Table 29: High-prio-only Forwarding Class Defaults	166

List of Tables

Table 30:	MBS Forwarding Class Defaults	167
Table 31:	Network Queue Policy Command Output	175
Service Egress and Ingress QoS Policies		177
Table 32:	Service Egress Policy Defaults	193
Table 33:	Service Ingress Policy Defaults	194
Table 34:	Valid DSCP Names	212
Table 35:	SAP Ingress Command Output	239
Table 36:	SAP Egress Command Output	244
Table 37:	Buffer Pool Command Output	250
Slope QoS Policies		251
Table 38:	Slope Policy Defaults	255
Table 39:	Slope Policy Command Output Fields	270
ATM QoS Traffic Descriptor Profiles		273
Table 40:	ATM Traffic Descriptors	274
Table 41:	ATM-TD-Profile Defaults	280
Table 42:	Service Category Descriptor Type Default Values	288
Table 43:	Traffic Descriptor Type Command Parameters	288
Table 44:	ATM Service Categories	290
Table 45:	Default Shaping Values	290
Table 46:	Service Category Traffic Descriptor Parameters	291
Table 47:	ATM Traffic Parameter Defaults	292
Table 48:	ATM Traffic Descriptor Profile Command Output	296
Table 49:	SAP Command Output	297
QoS Fabric Profiles		299
Table 50:	Fabric Profile Defaults	302
Table 51:	QoS Fabric Profile Command Output	314

List of Figures

QoS Policies	35
Figure 1: Egress and Ingress Traffic Direction	39
Figure 2: Profiled and Queue-Type-Based Scheduling Combined	48
Figure 3: Fabric Shapers in Per Destination Mode	53
Figure 4: Fabric Shapers in Aggregate Mode	54
Figure 5: Traffic Queuing Model for Three Queues and Three Classes	72
Figure 6: WRED for High-Priority and Low-Priority Traffic on the Same Queue	92

List of Acronyms

Acronym	Expansion
2G	second generation wireless telephone technology
3DES	triple DES (data encryption standard)
3G	third generation mobile telephone technology
5620 SAM	5620 Service Aware Manager
7705 SAR	7705 Service Aggregation Router
7710 SR	7710 Service Router
7750 SR	7750 Service Router
9500 MPR	9500 Microwave Packet Radio
ABR	available bit rate area border router
AC	alternating current attachment circuit
ACK	acknowledge
ACL	access control list
ACR	adaptive clock recovery
ADP	automatic discovery protocol
AFI	authority and format identifier
AIS	alarm indication signal
ANSI	American National Standards Institute
Apipe	ATM VLL
APS	automatic protection switching
ARP	address resolution protocol
A/S	active/standby
AS	autonomous system

Acronym	Expansion
ASAP	any service, any port
ASBR	autonomous system boundary router
ASN	autonomous system number
ATM	asynchronous transfer mode
ATM PVC	ATM permanent virtual circuit
B3ZS	bipolar with three-zero substitution
Batt A	battery A
B-bit	beginning bit (first packet of a fragment)
Bellcore	Bell Communications Research
BFD	bidirectional forwarding detection
BGP	border gateway protocol
BITS	building integrated timing supply
BMCA	best master clock algorithm
BMU	<p>broadcast, multicast, and unknown traffic</p> <p>Traffic that is not unicast. Any nature of multipoint traffic:</p> <ul style="list-style-type: none"> • broadcast (that is, all 1s as the destination IP to represent all destinations within the subnet) • multicast (that is, traffic typically identified by the destination address, uses special destination address); for IP, the destination must be 224.0.0.0 to 239.255.255.255 • unknown (that is, the destination is typically a valid unicast address but the destination port/interface is not yet known; therefore, traffic needs to be forwarded to all destinations; unknown traffic is treated as broadcast)
BOF	boot options file
BPDU	bridge protocol data unit
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
BSTA	Broadband Service Termination Architecture

Acronym	Expansion
BTS	base transceiver station
CAS	channel associated signaling
CBN	common bonding networks
CBS	committed buffer space
CC	control channel continuity check
CCM	continuity check message
CE	customer edge circuit emulation
CEM	circuit emulation
CES	circuit emulation services
CESoPSN	circuit emulation services over packet switched network
CFM	connectivity fault management
CIDR	classless inter-domain routing
CIR	committed information rate
CLI	command line interface
CLP	cell loss priority
CoS	class of service
CPE	customer premises equipment
Cpipe	circuit emulation (or TDM) VLL
CPM	Control and Processing Module (CPM is used instead of CSM when referring to CSM filtering to align with CLI syntax used with other SR products). CSM management ports are referred to as CPM management ports in the CLI.
CPU	central processing unit
CRC	cyclic redundancy check
CRON	a time-based scheduling service (from chronos = time)

Acronym	Expansion
CSM	Control and Switching Module
CSNP	complete sequence number PDU
CSPF	constrained shortest path first
C-TAG	customer VLAN tag
CV	connection verification customer VLAN (tag)
CW	control word
DC	direct current
DC-C	DC return - common
DCE	data communications equipment
DC-I	DC return - isolated
DCO	digitally controlled oscillator
DDoS	distributed DoS
DES	data encryption standard
DF	do not fragment
DHB	decimal, hexadecimal, or binary
DHCP	dynamic host configuration protocol
DHCPv6	dynamic host configuration protocol for IPv6
DIS	designated intermediate system
DM	delay measurement
DNS	domain name server
DoS	denial of service
dot1p	IEEE 802.1p bits, found in Ethernet or VLAN ingress packet headers and used to map traffic to up to eight forwarding classes
dot1q	IEEE 802.1q encapsulation for Ethernet interfaces
DPI	deep packet inspection

Acronym	Expansion
DPLL	digital phase locked loop
DSCP	differentiated services code point
DSL	digital subscriber line
DSLAM	digital subscriber line access multiplexer
DTE	data termination equipment
DU	downstream unsolicited
DUID	DHCP unique identifier
DV	delay variation
e911	enhanced 911 service
EAP	Extensible Authentication Protocol
EAPOL	EAP over LAN
E-bit	ending bit (last packet of a fragment)
ECMP	equal cost multi-path
EFM	Ethernet in the first mile
EGP	exterior gateway protocol
EIA/TIA-232	Electronic Industries Alliance/Telecommunications Industry Association Standard 232 (also known as RS-232)
ELER	egress label edge router
E&M	ear and mouth earth and magneto exchange and multiplexer
Epipe	Ethernet VLL
EPL	Ethernet private line
ERO	explicit route object
ESD	electrostatic discharge
ESMC	Ethernet synchronization message channel
ETE	end-to-end

Acronym	Expansion
ETH-CFM	Ethernet connectivity fault management (IEEE 802.1ag)
EVDO	evolution - data optimized
EVPL	Ethernet virtual private link
EXP bits	experimental bits (currently known as TC)
FC	forwarding class
FCS	frame check sequence
FDB	forwarding database
FDL	facilities data link
FEAC	far-end alarm and control
FEC	forwarding equivalence class
FF	fixed filter
FIB	forwarding information base
FIFO	first in, first out
FNG	fault notification generator
FOM	figure of merit
FRR	fast reroute
FTN	FEC-to-NHLFE
FTP	file transfer protocol
GFP	generic framing procedure
GigE	Gigabit Ethernet
GRE	generic routing encapsulation
GSM	Global System for Mobile Communications (2G)
HCM	high capacity multiplexing
HDB3	high density bipolar of order 3
HEC	header error control
HMAC	hash message authentication code

Acronym	Expansion
HSDPA	high-speed downlink packet access
HSPA	high-speed packet access
HVPLS	hierarchical virtual private line service
IANA	internet assigned numbers authority
IBN	isolated bonding networks
ICMP	Internet control message protocol
ICMPv6	Internet control message protocol for IPv6
ICP	IMA control protocol cells
IEEE	Institute of Electrical and Electronics Engineers
IEEE 1588v2	Institute of Electrical and Electronics Engineers standard 1588-2008
IES	Internet Enhanced Service
IETF	Internet Engineering Task Force
IGP	interior gateway protocol
ILER	ingress label edge router
ILM	incoming label map
IMA	inverse multiplexing over ATM
IOM	input/output module
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPIP	IP in IP
Ipipe	IP interworking VLL
IPoATM	IP over ATM
IS-IS	Intermediate System-to-Intermediate System
IS-IS-TE	IS-IS-traffic engineering (extensions)
ISO	International Organization for Standardization

Acronym	Expansion
LB	loopback
lbf-in	pound force inch
LBM	loopback message
LBO	line buildout
LBR	loopback reply
LCP	link control protocol
LDP	label distribution protocol
LER	label edge router
LFIB	label forwarding information base
LIB	label information base
LLDP	link layer discovery protocol
LLDPDU	link layer discovery protocol data unit
LLF	link loss forwarding
LLID	loopback location ID
LM	loss measurement
LSA	link-state advertisement
LSDB	link-state database
LSP	label switched path link-state PDU (for IS-IS)
LSR	label switch router link-state request
LSU	link-state update
LT	linktrace
LTE	line termination equipment
LTM	linktrace message
LTN	LSP ID to NHLFE

Acronym	Expansion
LTR	linktrace reply
MA	maintenance association
MAC	media access control
MA-ID	maintenance association identifier
MBB	make-before-break
MBS	maximum buffer space maximum burst size media buffer space
MBSP	mobile backhaul service provider
MC-MLPPP	multi-class multilink point-to-point protocol
MD	maintenance domain
MD5	message digest version 5 (algorithm)
MDA	media dependent adapter
MDDDB	multidrop data bridge
MDL	maintenance data link
ME	maintenance entity
MED	multi-exit discriminator
MEF	Metro Ethernet Forum
MEG	maintenance entity group
MEG-ID	maintenance entity group identifier
MEN	Metro Ethernet network
MEP	maintenance association end point
MFC	multi-field classification
MHF	MIP half function
MIB	management information base
MIP	maintenance association intermediate point

Acronym	Expansion
MIR	minimum information rate
MLPPP	multilink point-to-point protocol
MP	merge point multilink protocol
MP-BGP	multiprotocol border gateway protocol
MPLS	multiprotocol label switching
MPR	see 9500 MPR
MRRU	maximum received reconstructed unit
MRU	maximum receive unit
MSDU	MAC Service Data Unit
MS-PW	multi-segment pseudowire
MTIE	maximum time interval error
MTSO	mobile trunk switching office
MTU	maximum transmission unit multi-tenant unit
M-VPLS	management virtual private line service
MW	microwave
N·m	newton meter
NBMA	non-broadcast multiple access (network)
NE	network element
NET	network entity title
NHLFE	next hop label forwarding entry
NHOP	next-hop
NLRI	network layer reachability information
NNHOP	next next-hop
NNI	network-to-network interface

Acronym	Expansion
Node B	similar to BTS but used in 3G networks — term is used in UMTS (3G systems) while BTS is used in GSM (2G systems)
NSAP	network service access point
NSSA	not-so-stubby area
NTP	network time protocol
OAM	operations, administration, and maintenance
OAMPDU	OAM protocol data units
OC3	optical carrier, level 3
ORF	outbound route filtering
OS	operating system
OSI	Open Systems Interconnection (reference model)
OSINLCP	OSI Network Layer Control Protocol
OSPF	Open Shortest Path First
OSPF-TE	OSPF-traffic engineering (extensions)
OSS	operations support system
OSSP	Organization Specific Slow Protocol
OTP	one time password
PADI	PPPoE active discovery initiation
PADR	PPPoE active discovery request
PAE	port authentication entities
PCP	priority point code
PDU	protocol data units
PDV	packet delay variation
PDVT	packet delay variation tolerance
PE	provider edge router
PHB	per-hop behavior

Acronym	Expansion
PHY	physical layer
PID	protocol ID
PIR	peak information rate
PLCP	Physical Layer Convergence Protocol
PLR	point of local repair
POP	point of presence
POS	packet over SONET
PPP	point-to-point protocol
PPPoE	point-to-point protocol over Ethernet
PRC	primary reference clock
PSN	packet switched network
PSNP	partial sequence number PDU
PTP	precision time protocol performance transparency protocol
PVC	permanent virtual circuit
PVCC	permanent virtual channel connection
PW	pseudowire
PWE	pseudowire emulation
PWE3	pseudowire emulation edge-to-edge
QL	quality level
QoS	quality of service
RADIUS	Remote Authentication Dial In User Service
RAN	Radio Access Network
RBS	robbed bit signaling
RD	route distinguisher
RDI	remote defect indication

Acronym	Expansion
RED	random early discard
RESV	reservation
RIB	routing information base
RJ-45	registered jack 45
RNC	Radio Network Controller
RRO	record route object
RS-232	Recommended Standard 232 (also known as EIA/TIA-232)
RSHG	residential split horizon group
RSTP	Rapid Spanning Tree Protocol
RSVP-TE	resource reservation protocol - traffic engineering
RT	receive/transmit
RTM	routing table manager
RTN	battery return
RTP	real-time protocol
R&TTE	Radio and Telecommunications Terminal Equipment
RTU	remote terminal unit
RU	rack unit
SAA	service assurance agent
SAP	service access point
SAR-8	7705 Service Aggregation Router - 8-slot chassis
SAR-18	7705 Service Aggregation Router - 18-slot chassis
SAR-F	7705 Service Aggregation Router - fixed form-factor chassis
SAToP	structure-agnostic TDM over packet
SCADA	surveillance, control and data acquisition
SCP	secure copy
SD	signal degrade

Acronym	Expansion
SDH	synchronous digital hierarchy
SDI	serial data interface
SDP	service destination point
SE	shared explicit
SF	signal fail
SFP	small form-factor pluggable (transceiver)
SGT	self-generated traffic
SHA-1	secure hash algorithm
SHG	split horizon group
SIR	sustained information rate
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNPA	subnetwork point of attachment
SNTP	simple network time protocol
SONET	synchronous optical networking
S-PE	switching provider edge router
SPF	shortest path first
SPT	shortest path tree
SR	service router (includes 7710 SR, 7750 SR)
SRLG	shared risk link group
SSH	secure shell
SSM	synchronization status messaging
SSU	system synchronization unit
S-TAG	service VLAN tag
STM1	synchronous transport module, level 1
SVC	switched virtual circuit

Acronym	Expansion
SYN	synchronize
TACACS+	Terminal Access Controller Access-Control System Plus
TC	traffic class (formerly known as EXP bits)
TCP	transmission control protocol
TDEV	time deviation
TDM	time division multiplexing
TE	traffic engineering
TFTP	trivial file transfer protocol
TLDP	targeted LDP
TLV	type length value
ToS	type of service
T-PE	terminating provider edge router
TPID	tag protocol identifier
TPMR	two-port MAC relay
TTL	time to live
TTM	tunnel table manager
U-APS	unidirectional automatic protection switching
UBR	unspecified bit rate
UDP	user datagram protocol
UMTS	Universal Mobile Telecommunications System (3G)
UNI	user-to-network interface
V.35	V-series Recommendation 35
VC	virtual circuit
VCC	virtual channel connection
VCCV	virtual circuit connectivity verification
VCI	virtual circuit identifier

Acronym	Expansion
VID	VLAN ID
VLAN	virtual LAN
VLL	virtual leased line
VoIP	voice over IP
Vp	peak voltage
VP	virtual path
VPC	virtual path connection
VPI	virtual path identifier
VPLS	virtual private LAN service
VPN	virtual private network
VPRN	virtual private routed network
VRF	virtual routing and forwarding table
VSE	vendor-specific extension
VSO	vendor-specific option
WCDMA	wideband code division multiple access (transmission protocol used in UMTS networks)
WRED	weighted random early discard
WTR	wait to restore

Preface

About This Guide

This guide describes the Quality of Service (QoS) functionality provided by the Alcatel-Lucent 7705 Service Aggregation Router (7705 SAR), and presents configuration and implementation examples.

The guide 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 guide is intended for network administrators who are responsible for configuring the 7705 SAR routers. It is assumed that the network administrators have an understanding of networking principles and configurations. Concepts, policies, and profiles described in this guide include the following:

- CLI concepts
- QoS policies and profiles

List of Technical Publications

The 7705 SAR OS documentation set is composed of the following guides:

- 7705 SAR OS Basic System Configuration Guide
This guide describes basic system configurations and operations.
- 7705 SAR OS System Management Guide
This guide describes system security and access configurations as well as event logging and accounting logs.
- 7705 SAR OS Interface Configuration Guide
This guide describes card and port provisioning.

- **7705 SAR OS Router Configuration Guide**
This guide describes logical IP routing interfaces, IP-based filtering, and routing policies.
- **7705 SAR OS MPLS Guide**
This guide describes how to configure Multiprotocol Label Switching (MPLS), Resource Reservation Protocol for Traffic Engineering (RSVP-TE), and Label Distribution Protocol (LDP).
- **7705 SAR OS Services Guide**
This guide describes how to configure service parameters such as service access points (SAPs), service destination points (SDPs), customer information, and user services.
- **7705 SAR OS Quality of Service Guide**
This guide describes how to configure Quality of Service (QoS) policy management.
- **7705 SAR OS Routing Protocols Guide**
This guide provides an overview of dynamic routing concepts and describes how to configure them.
- **7705 SAR OS OAM and Diagnostics Guide**
This guide provides information on Operations, Administration and Maintenance (OAM) tools.

Multiple PDF File Search

You can use Adobe Reader, Release 6.0 or later, to search multiple PDF files for a term. Adobe Reader displays the results in a display panel. The results are grouped by PDF file. You can expand the entry for each file.



Note: The PDF files in which you search must be in the same folder.

To search multiple PDF files for a term:

Step 1. Open Adobe Reader.

Step 2. Choose Edit – Search from the Adobe Reader main menu. The Search panel appears.

Step 3. Enter the term to search for.

Step 4. Select the All PDF Documents in radio button.

Step 5. Choose the folder in which to search using the drop-down menu.

Step 6. Select the following criteria if required:

- Whole words only
- Case-Sensitive
- Include Bookmarks
- Include Comments

Step 7. Click on the Search button.

Adobe Reader displays the search results. You can expand the entries for each file by clicking on the + symbol.

Step 8. Click on a search result to go directly to that location in the selected file.

Technical Support

If you purchased a service agreement for your 7705 SAR 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, check this link for instructions to contact Support personnel:

Web: <http://support.alcatel-lucent.com>

Getting Started

In This Chapter

This chapter provides process flow information to configure Quality of Service (QoS) policies on the 7705 SAR.

Alcatel-Lucent 7705 SAR QoS Configuration Process

[Table 1](#) lists the tasks necessary to configure and apply QoS policies.

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
Service configuration	Configure QoS policies:	
	• Network	Network QoS Policies
	• Network queue	Network Queue QoS Policies
	• Service egress/service ingress	Service Egress and Ingress QoS Policies
	• Slope	Slope QoS Policies
	• ATM traffic descriptor	ATM QoS Traffic Descriptor Profiles
	• Fabric profile	QoS Fabric Profiles

Notes on 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F

The 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F run the same operating system software. The main difference between the products is their hardware platforms.

The 7705 SAR-8 is an 8-slot chassis that supports 2 CSMs, a Fan module, and 6 adapter cards. The 7705 SAR-18 chassis has 18 slots; in Release 4.0, it supports 2 CSMs, a Fan module, an Alarm module, and 12 adapter cards.

The 7705 SAR-F chassis has a fixed hardware configuration. The 7705 SAR-F replaces the CSM, Fan module, and the 16-port T1/E1 ASAP Adapter card and 8-port Ethernet Adapter card with an all-in-one unit that provides comparable functional blocks, as detailed in [Table 2](#).

The fixed configuration of the 7705 SAR-F means that provisioning the router at the “card slot” and “type” levels is preset and is not user-configurable. Operators begin configurations at the port level.



Note: Unless stated otherwise, references to the terms “Adapter card” and “CSM” throughout the 7705 SAR OS documentation set include the equivalent functional blocks on the 7705 SAR-F.

Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison

7705 SAR-8, 7705 SAR-18	7705 SAR-F	Notes
CSM	Control and switching functions	The control and switching functions include the console and management interfaces, the alarm and fan functions, the synchronization interfaces, system LEDs, and so on.
Fan module	Integrated with the control and switching functions	

Table 2: 7705 SAR-8, 7705 SAR-18, and 7705 SAR-F Comparison (Continued)

7705 SAR-8, 7705 SAR-18	7705 SAR-F	Notes
16-port T1/E1 ASAP Adapter card	16 individual T1/E1 ports on the faceplate	<p>The T1/E1 ports on the 7705 SAR-F are equivalent to the T1/E1 ports on the 16-port T1/E1 ASAP Adapter card, version 1, except that the 16 T1/E1 ports on the 7705 SAR-F support multiple synchronization sources to support two timing references. The 16-port T1/E1 ASAP Adapter card, version 2, also supports two timing references.</p> <p>On the 7705 SAR-8 and 7705 SAR-18, the CLI indicates the MDA type for the 16-port T1/E1 ASAP Adapter card as <code>a16-chds1</code> for version 1 and <code>a16-chds1v2</code> for version 2.</p> <p>On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F ports as <code>i16-chds1</code>.</p>
8-port Ethernet Adapter card	8 individual Ethernet ports on the faceplate	<p>The –48 VDC versions of the 7705 SAR-8 support two versions of the 8-port Ethernet Adapter card, with version 2 having additional support for Synchronous Ethernet. The +24 VDC version of the 7705 SAR-8 supports only version 2 of the 8-port Ethernet Adapter card.</p> <p>The 7705 SAR-18 supports only version 2 of the card.</p> <p>The Ethernet ports on the 7705 SAR-F are functionally equivalent to the Ethernet ports on version 2 of the 8-port Ethernet Adapter card and support multiple synchronization sources to support two timing references.</p> <p>On the 7705 SAR-8, the CLI indicates the MDA type for the 8-port Ethernet Adapter card as <code>a8-eth</code> or <code>a8-ethv2</code>. On the 7705 SAR-18, the CLI indicates the MDA type as <code>a8-ethv2</code>. On the 7705 SAR-F, the CLI indicates the MDA type for the 7705 SAR-F Ethernet ports as <code>i8-eth</code>.</p>
Requires user configuration at card (IOM) and MDA (adapter card) levels	Configuration at card (IOM) and MDA (adapter card) levels is preset and users cannot change these types	

In This Chapter

This chapter provides an overview of the 7705 SAR Quality of Service (QoS) and information about QoS policy management. Topics in this chapter include:

- [QoS Overview on page 37](#)
 - [Egress and Ingress Traffic Direction on page 39](#)
 - [Forwarding Classes on page 40](#)
 - [Traffic Classification at the Access Ingress on page 41](#)
 - [Access Ingress Queues on page 44](#)
 - [Ingress Queuing and Scheduling on page 45](#)
 - [Ingress Shaping to Fabric \(Access and Network\) on page 49](#)
 - [Configurable Ingress Shaping to Fabric \(Access and Network\) on page 51](#)
 - [Traffic Flow Across the Fabric on page 54](#)
 - [Network Egress Queuing Aggregation on page 56](#)
 - [Network Egress Scheduling on page 56](#)
 - [Network Egress Shaping on page 58](#)
 - [Network Egress Marking and Re-Marking on page 59](#)
 - [Network Ingress Classification on page 59](#)
 - [Network Ingress Queuing on page 60](#)
 - [Network Ingress Queuing for BMU Traffic on page 61](#)
 - [Network Ingress Scheduling on page 62](#)
 - [Access Egress Queuing and Scheduling on page 64](#)

- [QoS Policies Overview on page 69](#)
 - [Service Ingress QoS Policies on page 72](#)
 - [Service Egress QoS Policies on page 74](#)
 - [MC-MLPPP SAP Egress QoS Policies on page 76](#)
 - [Network and Service QoS Policies on page 77](#)
 - [WRED and RED Slope Policies on page 91](#)
 - [ATM Traffic Descriptor Profiles on page 93](#)
 - [Fabric Profiles on page 93](#)
 - [QoS Policy Entities on page 93](#)
- [Configuration Notes on page 95](#)
 - [Reference Sources on page 95](#)

QoS Overview

In order to provide what network engineers call Quality of Service (QoS), the flow of data in the form of packets must be predetermined and resources must be somehow assured for that predetermined flow. Simple routing does not provide a predetermined path for the traffic, and priorities that are described by Class of Service (CoS) coding simply increase the odds of successful transit for one packet over another. There is still no guarantee of service quality. The guarantee of service quality is what distinguishes QoS from CoS. CoS is an element of overall QoS.

By utilizing the traffic management features of the 7705 SAR, network engineers can achieve a QoS for their customers. Multiprotocol Label Switching (MPLS) provides a predetermined path, while policing, shaping, scheduling, and marking features ensure that traffic flows in a predetermined and predictable manner.

There is a need to distinguish between high-priority (that is, mission-critical traffic like signaling) and best-effort traffic priority levels when managing traffic flow. Within these priority levels, it is important to have a second level of prioritization, that is, between a certain volume of traffic that is contracted/needed to be transported, and the amount of traffic that is transported if the system resources allow. Throughout this guide, contracted traffic is referred to as in-profile traffic. Traffic that exceeds the user-configured traffic limits is either serviced using a lower priority or discarded in an appropriate manner to ensure that an overall quality of service is achieved.

The 7705 SAR must be properly configured to provide QoS. To ensure end-to-end QoS, each and every intermediate node together with the egress node must be coherently configured. Proper QoS configuration requires careful end-to-end planning, allocation of appropriate resources and coherent configuration among all the nodes along the path of a given service. Once properly configured, each service provided by the 7705 SAR will be contained within QoS boundaries associated with that service and the general QoS parameters assigned to network links.

The 7705 SAR is designed with QoS mechanisms at both egress and ingress to support different customers and different services per physical interface or card, concurrently and harmoniously (refer to [Egress and Ingress Traffic Direction](#) for a definition of egress and ingress traffic). The 7705 SAR has extensive and flexible capabilities to classify, police, shape and mark traffic to make this happen.



Note: The characteristics and nature of traffic flows in an ingress and egress direction are usually totally different. As an example, traffic is usually shaped at egress for pacing purposes and jitter tolerance imposed by the network transport rules, whereas at ingress, traffic is usually policed to ensure it fits into the traffic volumes defined in the Service Level Agreement. Thus, segregation between ingress and egress offers not only the seamless flexibility to address different requirements but as well allows fine-tuning of appropriate parameters in each direction.

The 7705 SAR supports multiple forwarding classes (FCs) and associated class-based queuing. Ingress traffic can be classified to multiple FCs, and the FCs can be flexibly associated with queues. This provides the ability to control the priority and drop priority of a packet while allowing the fine-tuning of bandwidth allocation to individual flows.

Each forwarding class is important only in relation to the other forwarding classes. A forwarding class allows network elements to weigh the relative importance of one packet over another. With such flexible queuing, packets belonging to a specific flow within a service can be preferentially forwarded based on the CoS of a queue. The forwarding decision is based on the forwarding class of the packet, as assigned by the ingress QoS policy defined for the service access point (SAP).

7705 SAR routers use QoS policies to control how QoS is handled at distinct points in the service delivery model within the device. QoS policies act like a template. Once a policy is created, it can be applied to many other similar services and ports. As an example, if there is a group of Node Bs connected to a 7705 SAR node, one QoS policy can be applied to all services of the same type, such as High-Speed Downlink Packet Access (HSDPA) offload services.

There are different types of QoS policies that cater to the different QoS needs at each point in the service delivery model. QoS policies are defined in a global context in the 7705 SAR and only take effect when the policy is applied to a relevant entity.

QoS policies are uniquely identified with a policy ID number or name. Policy ID 1 or policy ID default is reserved for the default policy, which is used if no policy is explicitly applied.

The different QoS policies within the 7705 SAR can be divided into two main types.

- QoS policies are used for classification, queue attributes, and marking.
- Slope policies define default buffer allocations and Random Early Discard (RED) and Weighted Random Early Discard (WRED) slope definitions.

The sections that follow provide an overview of the QoS traffic management performed on the 7705 SAR.

Egress and Ingress Traffic Direction

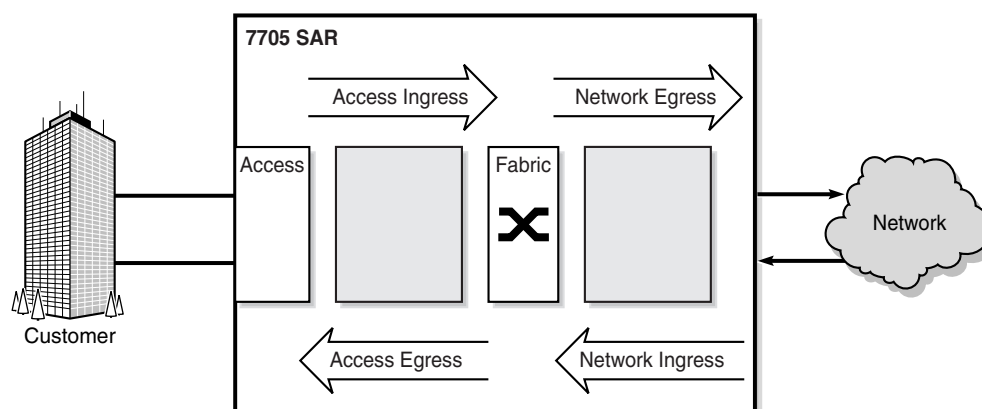
Throughout this document, the terms ingress and egress, when describing traffic direction, are always defined relative to the fabric. For example:

- egress direction describes packets moving from the switch fabric and into a port (on an adapter card)
- ingress direction describes packets moving into the switch fabric away from a port (on an adapter card)
- access egress direction describes packets switched from the switch fabric toward customer equipment
- access ingress direction describes packets coming in from customer equipment and switched toward the switch fabric
- network egress direction describes packets switched from the switch fabric into the network
- network ingress direction describes packets switched in from the network and moving toward the switch fabric



Note: Throughout this guide, the terms access ingress/egress and service ingress/egress are interchangeable. This section ([QoS Overview](#)) uses the term access, and the following sections (beginning with [QoS Policies Overview](#)) use the term service.

Figure 1: Egress and Ingress Traffic Direction



19763

Forwarding Classes

Queues can be created for each forwarding class to determine the manner in which the queue output is scheduled and the type of parameters the queue accepts.

The 7705 SAR supports eight forwarding classes per SAP. [Table 3](#) shows the default mapping of these forwarding classes in order of priority. Network Control, High-1, Expedited, and High-2 forwarding classes have higher priority than Low-1, Assured, Low-2, and Best Effort forwarding classes.

Table 3: Default Forwarding Classes

FC Name	FC Designation	Queue Type	Typical use
Network Control	NC	Expedited	For network control and traffic synchronization
High-1	H1		For delay/jitter sensitive traffic
Expedited	EF		For delay/jitter sensitive traffic
High-2	H2		For delay/jitter sensitive traffic
Low-1	L1	Best Effort	For best-effort traffic
Assured	AF		For best-effort traffic
Low-2	L2		For best-effort traffic
Best Effort	BE		For best-effort traffic

The traffic flows of different forwarding classes are mapped to the queues. This mapping is user-configurable. Each queue has a unique priority. Packets from high-priority queues are scheduled separately, before packets from low-priority queues. More than one forwarding class can be mapped to a single queue. In such a case, the queue type defaults to the priority of the lowest forwarding class. By default, the following logical order is followed:

- FC-8 - NC
- FC-7 - H1
- FC-6 - EF
- FC-5 - H2
- FC-4 - L1
- FC-3 - AF
- FC-2 - L2
- FC-1 - BE

At access ingress, traffic can be classified as unicast traffic or one of the multipoint traffic types (broadcast, multicast, or unknown (BMU)). After classification, traffic can be assigned to a queue that is configured to support one of the four traffic types, namely:

- unicast (or implicit)
- broadcast
- multicast
- unknown

Traffic Classification at the Access Ingress

Traffic classification identifies a traffic flow and maps the packets belonging to that flow to a preset forwarding class, so that the flow can receive the required special treatment. Up to eight forwarding classes are supported for traffic classification. Refer to [Table 3](#) for a list of these forwarding classes.

For TDM channel groups, all of the traffic is mapped to a single forwarding class. Similarly, for ATM VCs, each VC is linked to one forwarding class. On Ethernet ports and VLANs, up to eight forwarding classes can be configured based on 802.1p (dot1p) bits or Differentiated Services Code Point (DSCP) bits classification. On PPP/MLPPP SAPs, up to eight forwarding classes can be configured based on DSCP bits classification.



Note: If an Ethernet port is set to null encapsulation, the dot1p value has no meaning and cannot be used for classification purposes.

Once the classification takes place, forwarding classes are mapped to queues as described in the sections that follow.

Traffic Classification Types

The various traffic classification methods used on the 7705 SAR are described in [Table 4](#).

Table 4: Traffic Classification Types

Traffic Classification Based on...	Description
a channel group ($n \times \text{DS0}$)	<p>Applies to 16-port T1/E1 ASAP Adapter card and 32-port T1/E1 ASAP Adapter card ports, 2-port OC3/STM1 Channelized Adapter card ports, 12-port Serial Data Interface card ports, and 6-port E&M Adapter card ports in structured or unstructured circuit emulation mode. In this mode, a number of DS0s are transported within the payload of the same Circuit Emulation over Packet Switched Networks (CESoPSN) packet or Structure-Agnostic TDM over Packet (SAToP) packet. Thus the timeslots transporting the same type of traffic are classified all at once.</p> <p>Note: The 6-port E&M Adapter card and 12-port Serial Data Interface card are not supported on the 7705 SAR-18 for Release 4.0.</p>
an ATM VCI	<p>On ATM-configured ports, any virtual connection regardless of service category is mapped to the configured forwarding class. One-to-one mapping is the only supported option.</p> <p>VP- or VC-based classifications are both supported. A VC with a specified VPI and VCI is mapped to the configured forwarding class. A VP connection with a specified VPI is mapped to the configured forwarding class.</p>
an ATM service category	<p>Similar ATM service categories can be mapped against the same forwarding class. Traffic from a given VC with a specified service category is mapped to the configured forwarding class. VC selection is based on the ATM VC identifier.</p>
an Ethernet port	<p>All the traffic from an access ingress Ethernet port is mapped to the selected forwarding class. More granular classification can be performed based on dot1p or DSCP bits of the incoming packets. Classification rules applied to traffic flows on Ethernet ports behave similarly to access/filter lists. There can be multiple tiers of classification rules associated with an Ethernet port. In this case, classification is performed based on priority of classifier. The order of the priorities is described in Hierarchy of Classification Rules.</p>
an Ethernet VLAN (dot1q)	<p>Traffic from an access Ethernet VLAN (dot1q) interface can be mapped to a forwarding class. Each VLAN can be mapped to one forwarding class.</p>
IEEE 802.1p bits (dot1p)	<p>The dot1p bits in the Ethernet/VLAN ingress packet headers are used to map the traffic to up to eight forwarding classes.</p>

Table 4: Traffic Classification Types (Continued)

Traffic Classification Based on...	Description
PPP/MLPPP SAPs	Traffic from an access ingress PPP/MLPPP SAP is mapped to the selected forwarding class. More granular classification can be performed based on DSCP bits of the incoming packets.
DSCP bits	When the Ethernet payload is IP, ingress traffic can be mapped to a maximum of eight forwarding classes based on DSCP bit values. DSCP-based classification supports untagged, single-tagged and double-tagged Ethernet frames. If an ingress frame has more than two VLAN tags, then dot1q-based or dot1p-based classification must be used.

Hierarchy of Classification Rules

If more than one classification rule is created and assigned to the same port, this order is followed:

- TDM ports:
 - port-based classification, 1 FC only
 - channel group-based classification, 1 FC only
- ATM ports:
 - ATM connection identifiers-based classification, 1 FC only
- Ethernet ports:
 - port-based classification, 1 FC only
 - dot1q-based classification, 1 FC only
 - dot1p-based classification, up to 8 FCs
 - DSCP-based classification, up to 8 FCs
- PPP/MLPPP SAPs
 - default classification, 1 FC only
 - DSCP-based classification, up to 8 FCs

Discard Probability of Classified Traffic

Once the traffic is mapped against a forwarding class, the discard probability for the traffic can be configured as high or low priority at ingress. Once the traffic is further classified as high or low priority, different congestion management schemes could be applied based on this priority. For example WRED curves can then be run against the high- and low-priority traffic separately, as described in [WRED and RED Slope Policies](#).

This ability to specify the discard probability is very significant because it controls the amount of traffic that is discarded under congestion or high utilization. If you know the characteristics of your traffic, particularly the burst characteristics, the ability to change the discard probability can be used to great advantage. The objective is to customize the properties of the random discard functionality such that the minimal amount of data is discarded.

Access Ingress Queues

Once the traffic is classified to different forwarding classes, the next step is to create the ingress queues and bind forwarding classes to these queues.

There is no restriction of a one-to-one association between a forwarding class and a queue. That is, more than one forwarding class can be mapped to the same queue. This capability is beneficial in that it allows a bulk-sum amount of resources to be allocated to traffic flows of a similar nature. For example, in the case of 3G UMTS services, HSDPA and OAM traffic are both considered BE in nature. However, HSDPA traffic can be mapped to a better forwarding class (such as L2) while OAM traffic can remain mapped to a BE forwarding class. But they both can be mapped to a single queue to control the total amount of resources for the aggregate of the two flows.

A large but finite amount of memory is available for the queues. Within this memory space, many queues can be created. The queues are defined by user-configurable parameters. This flexibility and complexity is necessary in order to create services that offer optimal quality of service and is much better than a restrictive and fixed buffer implementation alternative.

Buffer space is allocated to queues based on the committed queue depth, the maximum queue depth and availability of the resources, and the total amount of buffer space. The Committed Buffer Space (CBS) and the Maximum Buffer Space (MBS) are used to define the queue depth for a particular queue. The MBS is the maximum number of bytes that can be allocated to a particular queue. Whether that much space actually can be allocated or not depends on buffer usage (that is, the number of other queues and their depth).

If no CBS or MBS is configured, then the maximum queue depth (that is, the shared buffer pool size) can grow up to the whole buffer pool size but it is not guaranteed.

Memory allocation is optimized to guarantee the CBS for each queue. The allocated queue space beyond the CBS that is bounded by the MBS depends on the utilization of buffer space and existing guarantees to queues (that is, the CBS). The CBS is defaulted to 6 kbytes for all access ingress queues on the 7705 SAR. With a preset guaranteed small queue depth, it is ensured that some queuing resources are available for all traffic flows. The default value would need to be altered to meet the requirements of a specific traffic flow or flows.

Ingress Queuing and Scheduling

Traffic management on the 7705 SAR uses a packet-based implementation of the dual leaky bucket model. Each queue has a guaranteed space limited with CBS and a maximum depth limited with MBS. New packets are queued as they arrive. Any packet that causes the MBS to be exceeded is discarded.

The packets in the queue are serviced by two different schedulers, the In-Profile and Out-of-Profile schedulers. These two schedulers empty the queue continuously.

Profiled Scheduling

Each queue is serviced based on the user-configured CIR and PIR values. If the packets that are collected by a scheduler from a queue are flowing at a rate that is less than or equal to the CIR value, then the packets are scheduled as in-profile. Packets with a flow rate that exceeds the CIR value but is less than the PIR value are scheduled as out-of-profile. [Figure 2](#) depicts this behavior.

This behavior is comparable to the dual leaky bucket implementation in ATM networks. With in-profile and out-of-profile scheduling, traffic that flows at rates up to the traffic contract (that is, CIR) from all the queues is serviced prior to traffic that flows at rates exceeding the traffic contract. This mode of operation ensures that Service Level Agreements are honored and traffic that is committed to be transported is switched prior to traffic that exceeds the contract agreement.



Note: A profile is an arithmetical analysis of the rates that are permitted for a particular packet flow; therefore, profiled scheduling may also be called rate-based scheduling.

Queue-Type-Based Scheduling

As well as profiled scheduling described above, queue-type-based scheduling is supported at access ingress. Queues are divided into two categories, those that are serviced by the Expedited scheduler and those that are serviced by the Best Effort scheduler.

The Expedited scheduler has precedence over the Best Effort scheduler. Thus, at access ingress, CoS queues that are marked with an Expedited priority are serviced first. Then, the Best Effort marked queues are serviced. In a default configuration, the Expedited scheduler services the following CoS queues before the Best Effort scheduler services the rest:

- Expedited scheduler: NC, H1, EF, H2
- Best-Effort scheduler: L1, AF, L2, BE

If a packet with an Expedited forwarding class arrives while a Best Effort marked queue is being serviced, then the Expedited Scheduler will take over and service the Expedited marked CoS queue, as soon as the packet from the Best Effort scheduler is serviced.

The schedulers at access ingress in the 7705 SAR service the group of all Expedited queues exhaustively ahead of the group of all Best Effort queues. This means that all expedited queues have to be empty before any packet from a Best Effort queue is serviced.



Note: There is no user configuration for the schedulers. The operation of the schedulers is described for informational purposes. A user can control the mapping of traffic flows based on classification controls, that is, by mapping forwarding classes to up eight CoS queues.

The following basic rules apply to the queue-type-based scheduling of CoS queues.

1. Queues marked for Expedited scheduling are serviced in a round-robin fashion before any queues marked as Best Effort (in a default configuration, these would be queues CoS-8 through CoS-5).
2. These Expedited queues are serviced exhaustively within the round robin. For example, if in a default configuration there are two packets scheduled for service in both CoS-8 and CoS-5, one packet from CoS-8 is serviced, then one packet from CoS-5 is serviced, and then the scheduler returns back to CoS-8, until all the packets are serviced.
3. Once the Expedited scheduler has serviced all the packets in the queues marked for Expedited scheduling, the Best Effort scheduler starts serving the queues marked as Best Effort. The same principle described in step 2 is followed, until all the packets in the Best Effort queues are serviced.

4. If a packet arrives at any of the queues marked for Expedited scheduling while the scheduler is servicing a packet from a Best Effort queue, the Best Effort scheduler finishes servicing the current packet and then the Expedited scheduler immediately activates to service the packet in the Expedited queue. If there are no other packets to be serviced in any of the Expedited queues, the Best Effort scheduler resumes servicing the packets in the Best Effort queues. If the queues are configured according to the tables and defaults described in this guide, CoS-4 will be scheduled prior to CoS-1 among queues marked as Best Effort.
5. After one cycle is completed across all the queues marked as Best Effort, the next pass is started until all the packets in all the queues marked as Best Effort are serviced, or a packet arrives to a queue marked as Expedited and is serviced as described in step 2.

Profiled Scheduling and Queue-Type-Based Scheduling Combined

The 7705 SAR combines and applies profiled scheduling and queue-type-based scheduling to all of the access ingress queues. The schedulers used for these two types of scheduling are combined and applied to all the queues to provide maximum flexibility and scalability that meet the stringent QoS requirements of modern network applications.

Packets with a flow rate that is less than or equal to the CIR value of a queue are scheduled as in-profile. Packets with a flow rate that exceeds the CIR value but is less than the PIR value of a queue are scheduled as out-of-profile.

The scheduling cycle for the combined profiled and queue-type-based scheduling of CoS queues is shown in [Figure 2](#). The following basic steps apply:

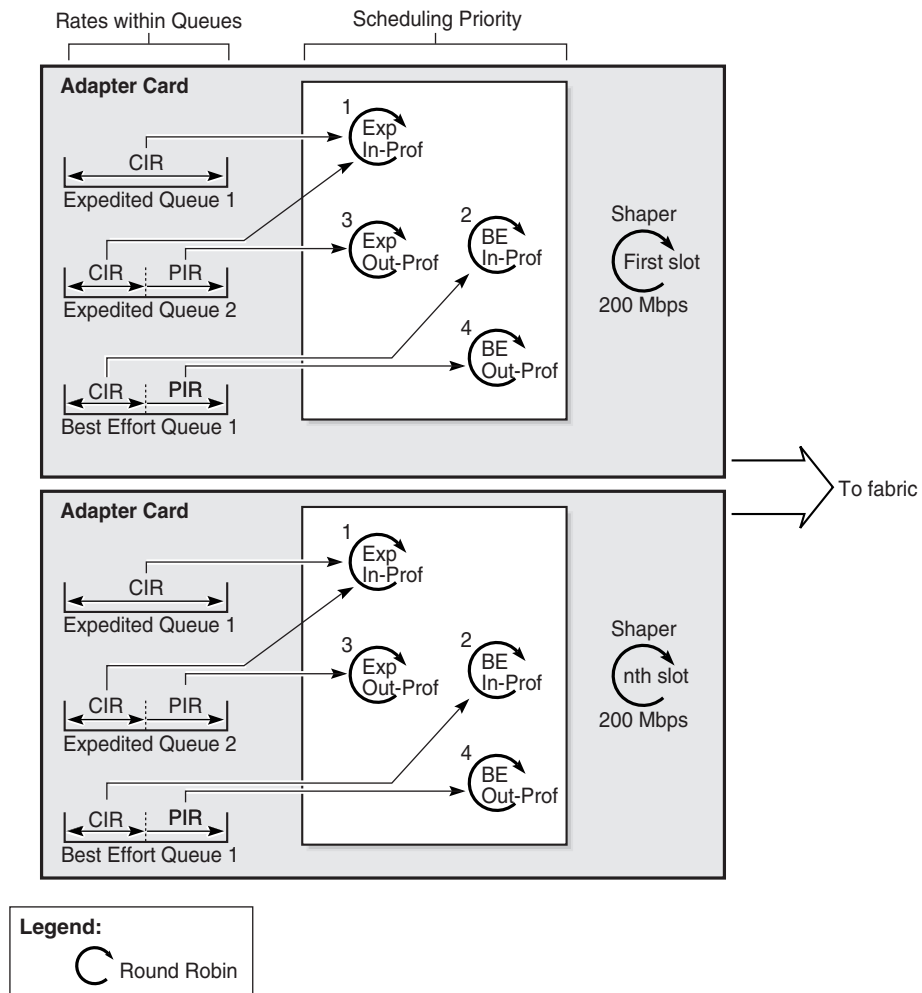
1. In-profile traffic from Expedited queues is serviced in round-robin fashion up to the CIR value. When a queue exceeds its configured CIR value, its state is changed to out-of-profile.
2. Once all of the in-profile packets from the Expedited queues are serviced, in-profile packets from Best Effort queues are serviced in a round-robin fashion until the configured CIR value is exceeded. When a queue exceeds its configured CIR value, its state is changed to out-of-profile.
3. Once all of the in-profile packets from the Best Effort queues are serviced, out-of-profile packets from Expedited queues are serviced in a round-robin fashion.

4. Once all of the out-of-profile packets from the Expedited queues are serviced, the out-of-profile packets from the Best Effort queues are serviced in a round-robin fashion.



Note: If a packet arrives at any of the queues marked for Expedited scheduling while the scheduler is servicing a packet from a Best Effort queue or is servicing an out-of-profile packet, the scheduler finishes servicing the current packet and then returns to the Expedited queues immediately.

Figure 2: Profiled and Queue-Type-Based Scheduling Combined



19761

Ingress Queuing and Scheduling for BMU Traffic

The 7705 SAR OS treats broadcast, multicast, and unknown traffic in the same way as unicast traffic. After being classified, the BMU traffic can be mapped to individual queues in order to be forwarded to the fabric. Classification of unicast and BMU traffic does not differ, which means that BMU traffic that has been classified to a BMU-designated queue can be shaped at its own rate, offering better control and fairer utilization of fabric resources. For more information, see [BMU Support](#).

Ingress Shaping to Fabric (Access and Network)

After the traffic is scheduled, it must be sent to the fabric interface. In order to avoid congestion in the fabric and ease the effects of possible bursts, a shaper is implemented on each adapter card.

The shapers smooth out any packet bursts and ease the flow of traffic onto the fabric. This utilizes buffer space on the adapter cards and eliminates the need for large ingress buffers in the fabric.

The ingress to-fabric shapers are user-configurable, and can operate at a maximum rate of 1 Gb/s per destination card. See [Configurable Ingress Shaping to Fabric \(Access and Network\)](#) for details.

After the shaping function, all of the traffic is forwarded to the fabric interface in round-robin fashion, one packet at a time, from every access ingress adapter card.

BMU Support

Fabric shapers support both unicast and multipoint traffic. Multipoint traffic can be any combination of broadcast, multicast, and unknown (BMU) frames. From access ingress to the fabric, BMU traffic is treated as unicast traffic. A single copy of BMU traffic is handed off to the fabric, where it is replicated and sent to all potential destination adapter cards.

Aggregate Mode BMU Support

An aggregate mode shaper provides a single aggregate shaping rate. The rate defines the maximum bandwidth that an adapter card can switch through its fabric interface at any given time. The rate is a bulk value and is independent of the destination or the type of traffic. For example, in aggregate mode, an ingress adapter card might use the full rate to communicate with a single destination adapter card, or it might use the same rate to communicate with multiple egress adapter cards.

Aggregate mode and the aggregate rate apply to fabric shapers that handle combined unicast/BMU traffic, unicast-only traffic, or BMU-only traffic. One aggregate rate sets the rate on all adapter cards. The proportional distribution between unicast and BMU traffic can be fine-tuned via queue-level schedulers, while the to-fabric shaper imposes a maximum rate that ensures fairness on the fabric for traffic from all adapter cards.

When services (IES, VPRN, and VPLS) are enabled, the fabric profile mode for access ingress should be set to aggregate mode.

Destination Mode BMU Support

Destination mode offers granular to-fabric shaping rates on a per-destination adapter card basis. While destination mode offers more flexibility and gives more control than aggregate mode, it also requires a greater understanding of network topology and flow characteristics under conditions such as node failures and link, adapter card, or port failures.

In a destination mode fabric profile, the unicast traffic and BMU traffic are always shaped separately.

For unicast traffic, individual destination rates can be configured on each adapter card. For BMU traffic, one multipoint rate sets the rate on all adapter cards. Fairness among different BMU flows is ensured by tuning the QoS queues associated with the port.

Configurable Ingress Shaping to Fabric (Access and Network)

The use of fabric profiles allows the ingress (to the fabric) shapers to be user-configurable at rates up to 1 Gb/s switching throughput. These configurable fabric shapers apply to access ingress and network ingress traffic.

By allowing a rate of up to 1 Gb/s to be configured from any adapter card to the fabric, the fabric may become congested. Therefore, the collection and display of fabric statistics are provided. These statistics report about the fabric traffic flow and potential discards. Refer to the 7705 SAR OS Interface Configuration Guide, “Configuring Adapter Card Fabric Statistics” and “Card, Adapter Card, and Port Command Reference” for information on how to configure, show, and monitor fabric statistics on an adapter card.

The ingress buffers for a card are much larger than the ingress buffers for the fabric; therefore, it is advantageous to utilize the larger card buffers for ingress shaping. In order to utilize the ingress card buffers and have much more granular control over traffic, two fabric profile modes are supported, per-destination mode and aggregate mode. Both modes offer shaping towards the fabric from an adapter card, but per-destination shapers offer the maximum flexibility by precisely controlling the amount of traffic to each destination card at a user-defined rate. Aggregate mode is used for simpler deployments, where the amount of traffic flowing to a destination adapter card is not controlled.

The default mode of operation for the 7705 SAR is set to aggregate, and the fixed aggregate rate of 200 Mb/s is set for both access ingress and network ingress traffic. Therefore, in a default configuration, each adapter card can switch up to 200 Mb/s of access ingress and network ingress traffic towards the fabric.

All the switched traffic can be destined for a single adapter card or it can be spread among multiple adapter cards. For higher-bandwidth applications, a network traffic analysis is recommended to determine which shaper rates would best suit the application and traffic patterns of a particular environment.

The to-fabric shapers are provided on the 7705 SAR to ensure adequate use of ingress buffers in case of congestion. With the ingress shapers, the large ingress card buffers can be configured to absorb bursty traffic and pace the traffic for better use of resources.

For example, if the average access ingress traffic bandwidth for an adapter card is 400 Mb/s and the peak bandwidth is 800 Mb/s, the rate of the to-fabric shapers can be configured to be 400 Mb/s. This allows the bursty ingress traffic to be paced by absorbing the bursty traffic after being shaped at 400 Mb/s. The initial burst is absorbed at the adapter card where the bursty traffic ingresses the 7705 SAR. The ingress buffers are used to absorb the burst and the fabric buffers are not exhausted by any single adapter card. The same example applies to network ingress traffic.

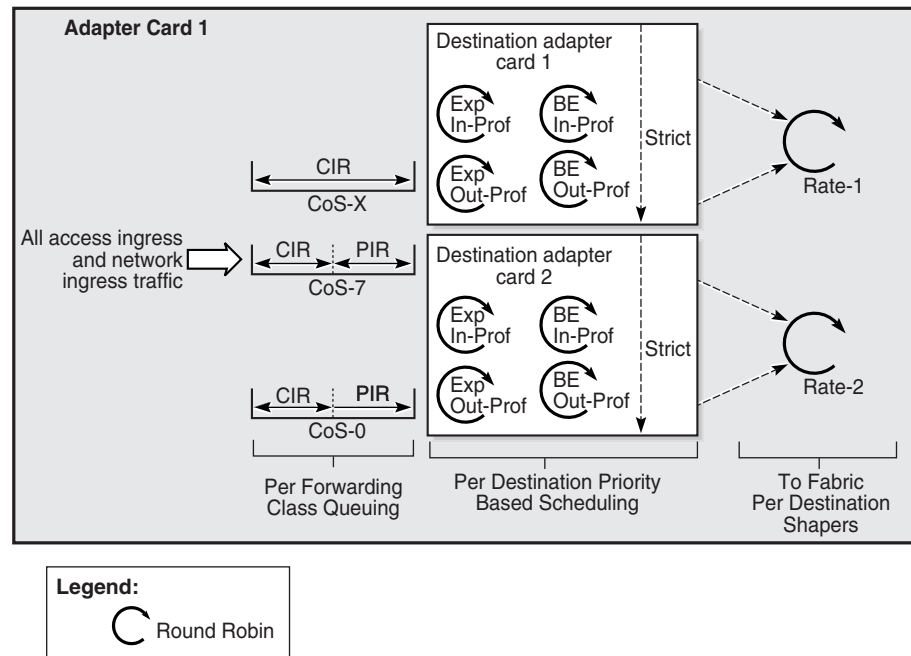
Table 5 summarizes the different capabilities offered by the two modes.

Table 5: Fabric Profile Modes Options and Capabilities

Capability	Per Destination Mode	Aggregate Mode
Access ingress to-fabric shapers	✓	✓
Network ingress to-fabric shapers	✓	✓
Individual shaping from an ingress card towards each destination card based on a user-defined rate	✓	—
Aggregate/bulk sum shaping regardless of destination from an ingress card	—	✓

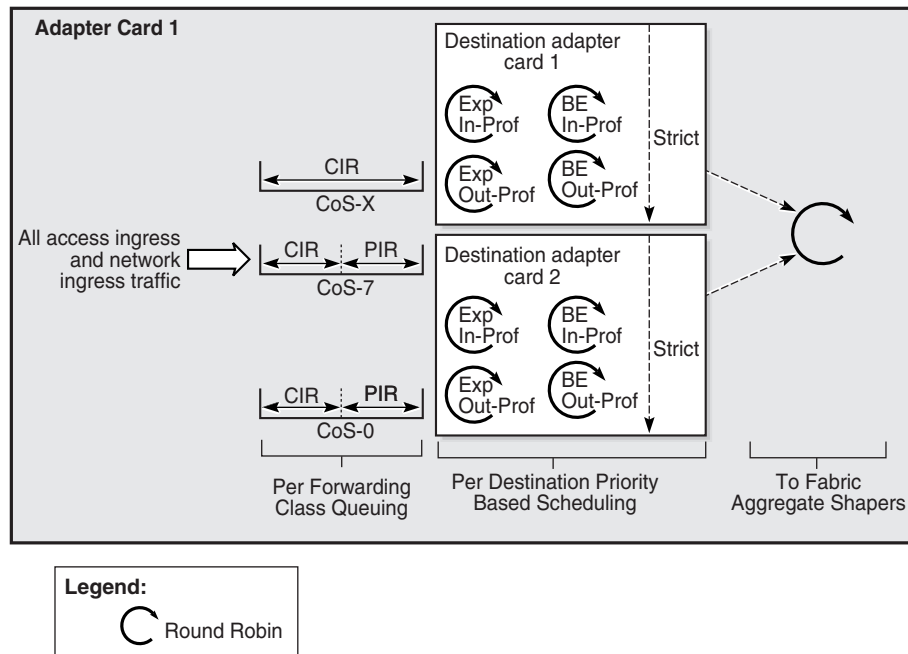
Figure 3 and Figure 4 illustrate the functionality of fabric shapers in per-destination mode and aggregate mode, respectively.

Referring to Figure 3, once the per-destination prioritization and scheduling takes place, as described in previous sections in this chapter, the per-destination adapter card shapers take effect. With per destination shapers, the maximum amount of bandwidth that each destination adapter card can receive from the fabric can be controlled. For example, the maximum amount of bandwidth that adapter card 1 can switch to the remaining adapter cards, as well as the amount of bandwidth switched back to adapter card 1, can be configured at a set rate.

Figure 3: Fabric Shapers in Per Destination Mode

20174

Figure 4 illustrates the functionality of fabric shapers in aggregate mode. Once the policing, classification, queuing and per-destination based priority queuing takes place, as described in previous sections in this chapter, the aggregate mode adapter card shapers take effect. In aggregate mode, the aggregate of all the access ingress and network ingress traffic is shaped at a user-configured rate regardless of the destination adapter card.

Figure 4: Fabric Shapers in Aggregate Mode

20175

Traffic Flow Across the Fabric

The 7705 SAR utilizes an Ethernet-based fabric. Each packet that is sent to the fabric is equipped with a fabric header that contains its specific CoS requirement. Since all of the packets switched across the fabric are already classified, queued, scheduled and marked according to the desired QoS parameters, each of these packets has been passed through the Traffic Management (TM) block on an adapter card, or the Control and Switching Module (CSM) in the case of control packets. Therefore, each packet arrives at the fabric having been already scheduled for optimal flow. The function of the fabric is to switch each packet through to the appropriate destination adapter card, or CSM in the case of control packets, in an efficient manner.

Since the traffic is shaped at a certain rate by the ingress adapter card (that is, bursts are smoothed by the TM function), minimal buffering should be needed on the switch fabric. However, the buffer space allocation and usage is in accordance with the priorities at the ingress adapter card. As is the case with schedulers at the adapter cards, there are four priorities supported on the switch fabric. The switch fabric serves the traffic in the following priority order:

1. Expedited, in-profile
2. Best Effort, in-profile
3. Expedited, out-of-profile
4. Best Effort, out-of-profile



Note: Since the fabric has a limited buffer space, it is possible for tail drop to occur. Tail drop discards any packet that exceeds the maximum buffer space allocation. The shaping that is performed on the adapter cards helps to prevent or minimize congestion.

BMU Traffic at Network Egress

BMU traffic at network egress is handled in the same way as unicast traffic in terms of scheduling, queuing, or port-level shaping. Both unicast and BMU traffic are mapped to queues as per the FC markings. Traffic from these queues, whether unicast or BMU, is scheduled according to user-configured rates. Port-level shapers treat all the queues identically, regardless of traffic type.

Network Egress Queuing Aggregation

After traffic is switched through the fabric from one or several access ingress adapter cards to a network egress adapter card, queuing level aggregation on a per-forwarding-class basis is performed on all of the received packets.

An adapter card that is used for network egress can receive—and will likely receive—packets from multiple adapter cards that are configured for access ingress operations, and from the CSM. Adapter cards that are configured for network access permit user configuration of queues and the association of forwarding classes to the queues. These are the same configuration principles that are used for adapter cards that are configured for access ingress connectivity. Like access ingress, more than one forwarding class can share the same queue.

Aggregation of different forwarding classes under queues takes place for each bundle or port. If a port is a member of a bundle, such as a Multilink Point-to-Point Protocol (MLPPP) bundle, then the aggregation and queuing is implemented for the entire bundle. If a port is a standalone port, that is, not a member of bundle, then the queuing takes place for the port.

Network Egress Scheduling

Network egress scheduling is supported on:

- 16-port T1/E1 ASAP Adapter cards
- 32-port T1/E1 ASAP Adapter cards
- 2-port OC3/STM1 Channelized Adapter cards
- 4-port OC3/STM1 Clear Channel Adapter cards
- 4-port DS3/E3 Adapter cards
- 8-port Ethernet Adapter cards, versions 1 and 2 on the 7705 SAR-8 and version 2 on the 7705 SAR-18

Network Egress Scheduling on the T1/E1 ASAP Adapter Cards, 2-port OC3/STM1 Channelized Adapter Card, 4-port OC3/STM1 Clear Channel Adapter Card, and 4-port DS3/E3 Adapter Card

Profiled scheduling (rate-based scheduling) is supported on network egress ports of the above cards. Packets less than or up to the CIR are scheduled as in-profile. Packets that arrive at rates greater than the CIR, but less than the PIR, are scheduled as out-of-profile.

In-profile traffic is exhaustively transmitted from the queues before out-of-profile traffic is transmitted. That is, all of the in-profile packets must be transmitted before any out-of-profile packets are transmitted.

Queue-type-based scheduling (Expedited vs. Best-effort scheduling) combined with profiled scheduling is also available for network egress ports on the above cards. This combination is known as 4-priority scheduling.



Note: The encapsulation type for the 16-port T1/E1 ASAP Adapter card, 32-port T1/E1 ASAP Adapter card, 4-port DS3/E3 Adapter card, and 2-port OC3/STM1 Channelized Adapter card must be ppp-auto for PPP/MLPPP bundles. The encapsulation type for the 4-port OC3/STM1 Clear Channel Adapter card must be ppp-auto (the card must be configured for POS).

The implementation of network egress scheduling on these cards is very similar to the scheduling mechanisms used for adapter cards that are configured for access ingress traffic. The default configuration of scheduling CoS queues provides a logical and consistent means to manage the traffic priorities. The default configuration is as follows:

- CoS-8 to CoS-5 Expedited in-profile
- CoS-4 to CoS-1 Best Effort in-profile
- CoS-8 to CoS-5 Expedited out-of-profile
- CoS-4 to CoS-1 Best Effort out-of-profile

Expedited queues are always scheduled prior to Best Effort queues, and in-profile queues are scheduled prior to out-of-profile queues.



Note: Default configuration means that the queues are configured according to the tables and defaults described in this guide. Customers can configure the queues differently.

The order shown below is maintained when scheduling the traffic on the adapter card's network ports. A strict priority is applied between the four schedulers, and all four schedulers are exhaustive:

- Expedited in-profile traffic
- Best Effort in-profile traffic
- Expedited out-of-profile traffic
- Best Effort out-of-profile traffic

Network Egress Scheduling on 8-port Ethernet Adapter Cards

Profiled scheduling (rate-based scheduling) is supported on 8-port Ethernet Adapter card egress ports. Packets less than or up to the CIR are scheduled as in-profile. Packets that arrive at rates greater than the CIR, but less than the PIR, are scheduled as out-of-profile.

In-profile traffic is exhaustively transmitted from the queues before out-of-profile traffic is transmitted. That is, all of the in-profile packets must be transmitted before any out-of-profile packets are transmitted.

Queue-type-based scheduling (Expedited vs. Best-effort scheduling) combined with profiled scheduling (4-priority scheduling) is also available for network egress ports on the 8-port Ethernet Adapter card.

Users can configure either profiled scheduling or 4-priority scheduling on a per-port basis. The default is profiled scheduling. If the port is configured for 4-priority scheduling, the traffic on the port is scheduled in the same way as for the 16-port T1/E1 ASAP Adapter card, 32-port T1/E1 ASAP Adapter card, 2-port OC3/STM1 Channelized Adapter card, 4-port OC3/STM1 Clear Channel Adapter card, and 4-port DS3/E3 Adapter card. The following order is followed in strict priority fashion:

- Expedited in-profile traffic
- Best-Effort in-profile traffic
- Expedited out-of-profile traffic
- Best-effort out-of-profile traffic

The scheduler mode is set at the interface level in the `config>port>ethernet>network` context. The encapsulation type for an 8-port Ethernet Adapter card in profiled scheduling mode or 4-priority scheduling mode can be either null or dot1q.

Network Egress Shaping

All the network egress traffic is shaped at the bundle or interface rate. An interface may not necessarily correspond directly to a port, and an interface could be a sub-channel of a port. As an example, Fast Ethernet could be the choice of network egress, but the leased bandwidth could still be a fraction of the port speed. In this case, it is possible to shape at the interface rate of 15 Mb/s, for example.

The same also applies to MLPPP bundles. The shaping takes place per MLPPP bundle, and the traffic is shaped at the aggregate rate of the MLPPP bundle.

Network Egress Marking and Re-Marking

The EXP bit settings can be marked at network egress. The EXP bit markings of the forwarding class are used for this purpose. The tunnel and pseudowire EXP bits are marked to the forwarding class value.

The default network egress QoS marking settings are given in [Table 16](#).

Network Egress Marking and Re-Marking on Ethernet ports

For MPLS tunnels, if network egress Ethernet ports are used, dot1p bit marking can be enabled in conjunction with EXP bit marking. In this case, the tunnel and pseudowire EXP bits do not have to be the same as the dot1p bits.

For GRE and IP tunnels, dot1p marking and pseudowire EXP marking can be enabled, and DSCP marking can also be enabled.

Network egress dot1p is supported for Ethernet frames, which can carry IPv4, IPv6, or MPLS packets. EXP re-marking is supported for MPLS packets.

Network Ingress Classification

Network ingress traffic originates from a network egress port located on another interworking device, such as a 7710 or 7750 Service Router or another 7705 SAR, and flows from the network toward the fabric in the 7705 SAR.

The ingress MPLS packets can be mapped to forwarding classes based on EXP bits that are part of the headers in the MPLS packets. These EXP bits are used across the network to ensure an end-to-end network-wide QoS offering. With pseudowire services, there are two labels, one for the MPLS tunnel and one for the pseudowire. Mapping is performed using the EXP values from the outer tunnel MPLS label. This ensures that the EXP bit settings, which may have been altered along the path by the tandem label switch routers (LSRs), are used to identify the forwarding class of the encapsulated traffic.

Ingress GRE and IP packets are mapped to forwarding classes based on DSCP bit settings of the IP header. GRE tunnels are not supported for IPv6; therefore, DSCP bit classification of GRE packets is only supported for IPv4. DSCP bit classification of IP packets is supported for both IPv4 and IPv6.

Network Ingress Queuing

Network ingress traffic can be classified in up to eight different forwarding classes, which are served by 16 queues (eight queues for unicast traffic and eight queues for multicast (BMU) traffic). Each queue serves at least one of the eight forwarding classes that are identified by the incoming EXP bits. These queues are automatically created by the 7705 SAR. [Table 6](#) shows the default network QoS policy for the 16 CoS queues.

For the 16-port T1/E1 ASAP Adapter card and 32-port T1/E1 ASAP Adapter card, the total buffer pool for CBS is limited to 36.1 Mbytes (16 520 packets) and 57.23 Mbytes (24 840 packets), respectively. For the 8-port Ethernet Adapter card, the 2-port OC3/STM1 Channelized Adapter card, the 4-port OC3/STM1 Clear Channel Adapter card, and the 4-port DS3/E3 Adapter card, the total buffer pool for CBS is limited to 151 Mbytes, which corresponds to 65 535 packets.

The maximum configurable MBS on the 16-port T1/E1 ASAP Adapter card and 32-port T1/E1 ASAP Adapter card is 36.9 Mbytes (16 000 packets). The maximum configurable MBS on the 8-port Ethernet Adapter card, the 2-port OC3/STM1 Channelized Adapter card, the 4-port OC3/STM1 Clear Channel Adapter card, and the 4-port DS3/E3 Adapter card is 131 Mbytes (56 800 packets).

The value for CBS and MBS is a percentage of the size of the buffer pool for the adapter card. CBS cannot be shared across queues. MBS can be shared across queues, which allows overbooking to occur.

Table 6: Default Network Ingress QoS Policy

Queue /FC	CIR (%)	PIR (%)	CBS (%)	MBS (%)
Queue-1/BE	0	100	0.1	5
Queue-2/L2	25	100	0.25	5
Queue-3/AF	25	100	0.75	5
Queue-4/L1	25	100	0.25	2.5
Queue-5/H2	100	100	0.75	5
Queue-6/EF	100	100	0.75	5
Queue-7/H1	10	100	0.25	2.5
Queue-8/NC	10	100	0.25	2.5
Queue-9/BE	0	100	0.1	5
Queue-10/L2	5	100	0.1	5
Queue-11/AF	5	100	0.1	5

Table 6: Default Network Ingress QoS Policy (Continued)

Queue /FC	CIR (%)	PIR (%)	CBS (%)	MBS (%)
Queue-12/L1	5	100	0.1	2.5
Queue-13/H2	100	100	0.1	5
Queue-14/EF	100	100	0.1	5
Queue-15/H1	10	100	0.1	2.5
Queue-16/NC	10	100	0.1	2.5

Network Ingress Queuing for BMU Traffic

At network ingress, broadcast, multicast, and unknown (BMU) traffic identified via DSCP and/or EXP (also known as LSP TC) is mapped to a forwarding class (FC). Since BMU traffic is considered to be multipoint traffic, the queue hosting BMU traffic must be configured with the `multipoint` keyword. Queues 9 through 16 support multipoint traffic (see [Table 6](#)). For any adapter card hosting any number of network ports, up to 16 queues can be configured to host 8 unicast and 8 multicast queues.

Similar to unicast queues, BMU queues require configuration of:

- queue depth (committed and maximum)
- scheduled rate (committed and peak)

In addition, as is the case for unicast queues, all other queue-based congestion management techniques apply to multipoint queues.

The benefits of using multipoint queues occur when the to-fabric shapers begin scheduling traffic towards the destination line card. To-fabric shapers can be configured for `aggregate` or `per-destination` mode. For more information, see [BMU Support](#).

Network Ingress Scheduling

Network ingress scheduling is supported on:

- 16-port T1/E1 ASAP Adapter cards
- 32-port T1/E1 ASAP Adapter cards
- 2-port OC3/STM1 Channelized Adapter cards
- 4-port OC3/STM1 Clear Channel Adapter cards
- 4-port DS3/E3 Adapter cards
- 8-port Ethernet Adapter cards, versions 1 and 2 on the 7705 SAR-8 and version 2 on the 7705 SAR-18

Network Ingress Scheduling on the T1/E1 ASAP Adapter Cards, 2-port OC3/STM1 Channelized Adapter Card, 4-port OC3/STM1 Clear Channel Adapter Card, and 4-port DS3/E3 Adapter Card

The above adapter cards can receive network ingress traffic. For the 16-port T1/E1 ASAP Adapter card, 32-port T1/E1 ASAP Adapter card, 4-port DS3/E3 Adapter card, and 2-port OC3/STM1 Channelized Adapter card, one or more ports on the card is configured for PPP/MLPPP for this purpose.



Note: The encapsulation type for the 16-port T1/E1 ASAP Adapter card, 32-port T1/E1 ASAP Adapter card, 4-port DS3/E3 Adapter card, and 2-port OC3/STM1 Channelized Adapter card must be ppp-auto for PPP/MLPPP bundles. The encapsulation type for the 4-port OC3/STM1 Clear Channel Adapter card must be ppp-auto (the card must be configured for POS).

The adapter cards provide sets of eight queues for incoming traffic: seven sets of queues for the 7705 SAR-8 and 13 sets of queues for the 7705 SAR-18. Each set of queues is specific to a destination adapter card. For example, for the 7705 SAR-8 and 7705 SAR-18 (respectively), 6 and 12 sets of queues are automatically created for each possible access egress adapter card, plus 1 set of queues for multicast traffic.

There is one additional set of queues for slow-path (control) traffic that is destined for the CSM(s).

The individual queues within each set of queues provide buffer space for traffic isolation based on the CoS values being applied (from the received EXP bits).

All of the network ingress ports of the adapter card share the same sets of queues, which are created automatically.

Once the packets received from the network are mapped to queues, four access ingress-like queue-type-based and profile (rate-based) schedulers per destination card service the queues in strict priority. This scheduling is done in the same manner for access ingress traffic described earlier in this guide in [Profiled Scheduling](#). The following queue-type-based and profiled schedulers service the queues in the order listed.

1. Expedited in-profile scheduler
2. Best Effort in-profile scheduler
3. Expedited out-of-profile scheduler
4. Best Effort out-of-profile scheduler

To complete the operation, user-configurable shapers operating at a maximum throughput rate of 1 Gb/s per destination card send the traffic into the fabric. See [Configurable Ingress Shaping to Fabric \(Access and Network\)](#) for details. Throughout this operation, each packet retains its individual CoS value.

Network Ingress Scheduling on 8-port Ethernet Adapter Cards

The 8-port Ethernet Adapter card provides sets of eight queues for incoming traffic. Each set of queues is specific to a destination adapter card. For example, for the 7705 SAR-8, 6 sets of queues are automatically created for each possible access egress adapter card, plus 1 set of queues for multicast traffic. For the 7705 SAR-8, 13 sets of queues are automatically created, plus 1 set of queues for multicast traffic. For both the 7705 SAR-8 and the 7705 SAR-18, there is 1 additional set of queues for slow-path (control) traffic that is destined for the CSM(s).

Each queue within each set provides buffer space for traffic isolation based on the classification carried out on EXP bits of the MPLS packet header (that is, the CoS setting).

All of the network ingress ports on the 8-port Ethernet Adapter card share the same sets of queues, which are created automatically.

Once the packets received from the network are mapped to queues, two profiled (rate-based) schedulers per destination card service the queues in strict priority. This scheduling is done in the same manner as for access ingress traffic described in [Profiled Scheduling](#). The following profiled schedulers service the queues in the order shown.

- in-profile scheduler
- out-of-profile scheduler

To complete the operation, user-configurable shapers operating at a maximum throughput rate of 1 Gb/s per destination card send the traffic into the fabric.

See [Configurable Ingress Shaping to Fabric \(Access and Network\)](#) for details. Throughout this operation, each packet retains its individual CoS value.

Access Egress Queuing and Scheduling

The sections that follow discuss the queuing and scheduling of access egress traffic, which is traffic that egresses the fabric on the access side.

Access egress scheduling takes place at the native traffic layer. As an example, once the ATM pseudowire payload is delivered from the network ingress to the access egress, the playback of the ATM cells to the appropriate ATM SAP is done according to ATM traffic management specifications.

Access Egress Scheduling and Queuing for BMU Traffic

At access egress, the 7705 SAR OS handles traffic management for unicast and BMU traffic in the same way. Unicast and/or BMU traffic is mapped to a queue and the mapping is based on the FC classification. Individual queues are then scheduled based on the available traffic.

ATM Access Egress Queuing and Scheduling

After the ATM pseudowire is terminated at the access egress, all the ATM cells are mapped to the default queue, which is queue 1, and queuing is performed per SAP. ATM access egress queuing and scheduling applies to the 16-port T1/E1 ASAP Adapter card, 32-port T1/E1 ASAP Adapter card, and 2-port OC3/STM1 Channelized Adapter card with atm/ima encapsulation. ATM access egress queuing and scheduling applies to the 4-port OC3/STM1 Clear Channel Adapter card and 4-port DS3/E3 Adapter card with atm encapsulation.

Once the per-SAP queuing takes place, the ATM Scheduler services these queues in the fashion and order defined below, based on the service categories assigned to each of these SAPs.

At access egress, CBR and rt-VBR VCs are always shaped, since there is no option to the user to turn shaping off. Shaping for nrt-VBR is optional.

Strict priority scheduling in an exhaustive fashion takes place for the shaped VCs in the order listed below:

1. CBR (always shaped)
2. rt-VBR (always shaped)

3. nrt-VBR (when shaped, user-configurable for shaped or unshaped)

UBR traffic is not shaped. To offer maximum flexibility to the user, nrt-VBR unshaped (also known as scheduled) is implemented.

ATM traffic is serviced in priority order. CBR traffic has the highest priority and is serviced ahead of all other traffic. After all of the CBR traffic has been serviced, rt-VBR traffic is serviced. Then, nrt-VBR traffic is serviced.

After scheduling all the other traffic from the CBR and VBR service categories, UBR is serviced. If there is no other traffic, UBR can burst up to the line rate. Scheduled nrt-VBR is treated the same way as UBR. Both UBR and unshaped nrt-VBR are scheduled using the weighted round-robin scheduler.

The scheduler weight assigned to queues hosting scheduled nrt-VBR and UBR traffic is determined by the configured traffic rate. The weight used by the scheduler for UBR+ VCs is dependent on the Minimum Information Rate (MIR) defined by the user. UBR with no MIR traffic has an MIR of 0.

Similarly, the scheduler weight is dependent on the Sustained Information Rate (SIR) for scheduled nrt-VBR. Weight used by the scheduler is programmed automatically based on the user-configured MIR/SIR value and is not user-configurable.

For UBR+, [Table 7](#) and [Table 8](#) are used to determine the weight of a UBR+ VC. These tables are also applicable to scheduled nrt-VBR weight determination. Instead of the MIR, the SIR is used to determine the scheduler weight.

Table 7: Scheduler Weight Values (WRR) based on MIR for the 16-port T1/E1 ASAP Adapter Card, 32-port T1/E1 ASAP Adapter Card, and 2-port OC3/STM1 Channelized Adapter Card

Minimum Information Rate	Scheduler Weight
<64 kb/s	1
<128 kb/s	2
<256 kb/s	3
<512 kb/s	4
<1024 kb/s	5
<1536 kb/s	6
<1920 kb/s	7
≥1920 kb/s	8

Table 8: Scheduler Weight Values (WRR) based on MIR for the 4-port OC3/STM1 Clear Channel Adapter Card

Range OC3 ATM	Range DS3 ATM	Weight
0 to 1 Mb/s	0 to 512 kb/s	1
>1 Mb/s to 4 Mb/s	>512 kb/s to 1 Mb/s	2
>4 Mb/s to 8 Mb/s	>1 Mb/s to 2 Mb/s	3
>8 Mb/s to 16 Mb/s	>2 Mb/s to 4 Mb/s	4
>16 Mb/s to 32 Mb/s	>4 Mb/s to 8 Mb/s	5
>32 Mb/s to 50 Mb/s	>8 Mb/s to 16 Mb/s	6
>50 Mb/s to 100 Mb/s	>16 Mb/s to 32 Mb/s	7
>100 Mb/s	>32 Mb/s	8

The access egress ATM scheduling behavior is shown in [Table 9](#). For UBR traffic, the scheduler weight of the lowest possible value is always used, which is the value of 1. Only cell-based operations are carried out.

Table 9: ATM Scheduling and Relative Priorities

Flow type	Transmission Rate	Priority
Shaped CBR	Limited to configured PIR	Strict priority over all other traffic
Shaped rt-VBR	Limited to configured SIR, but with bursts up to PIR within MBS	Strict priority over all but shaped CBR
Shaped nrt-VBR	Limited to configured SIR, but with bursts up to PIR within MBS	Strict priority over all scheduled traffic
Scheduled nrt-VBR	Weighted share (according to SIR) of port bandwidth remaining after shaped traffic has been exhausted	In the same WRR scheduler as UBR+ and UBR

Table 9: ATM Scheduling and Relative Priorities (Continued)

Flow type	Transmission Rate	Priority
Scheduled UBR+	Weighted share (according to MIR) of port bandwidth remaining after shaped traffic has been exhausted	In the same WRR scheduler as nrt-VBR and UBR
Scheduled UBR	Weighted share (with weight of 1) of port bandwidth remaining after shaped traffic has been exhausted	In the same WRR scheduler as nrt-VBR and UBR+

Ethernet Access Egress Queuing and Scheduling

Ethernet access egress queuing and scheduling is very similar to the Ethernet access ingress behavior. Once the Ethernet pseudowire is terminated, traffic is mapped to up to eight different forwarding classes per SAP. Mapping traffic to different forwarding classes is performed based on the EXP bit settings of the received Ethernet pseudowire by network ingress classification.

Queue-type-based and profile-based scheduling are both supported for Ethernet access egress ports. If the queues are configured according to the tables and defaults described in this guide (implying a default mode of operation), the configuration is as follows:

- CoS-8 to CoS-5 Expedited in-profile
- CoS-4 to CoS-1 Best Effort in-profile
- CoS-8 to CoS-5 Expedited out-of-profile
- CoS-4 to CoS-1 Best Effort out-of-profile

In this default configuration, for queue-type-based scheduling, CoS-8 to CoS-5 are serviced by the Expedited scheduler, and CoS-4 to CoS-1 are serviced by the Best Effort scheduler. This default mode of operation can be altered to better fit the operating characteristics of certain SAPs.

With profile-based scheduling, the Ethernet frames can be either in-profile or out-of-profile, and scheduling takes into account the state of the Ethernet frames in conjunction with the configured CIR and PIR rates.

After the queuing, an aggregate queue-type-based and profile-based scheduling takes place in the following order:

1. Expedited in-profile traffic
2. Best Effort in-profile traffic
3. Expedited out-of-profile traffic
4. Best Effort out-of-profile traffic

Once the traffic is scheduled using the aggregate queue-type-based and profile-based schedulers, the per-port shapers shape the traffic at a sub-rate (that is, at the configured/shaped port rate). Per-port shapers ensure that a sub-rate is met and attainable at all times.

Access Egress Marking/Re-Marking

At access egress, where the network-wide QoS boundary is reached, there may be a requirement to mark or re-mark the CoS indicators to match customer requirements. Dot1p and DSCP marking and re-marking is supported at Ethernet access egress.

Similar to access ingress for Ethernet, DSCP marking or re-marking is supported for untagged, single, or double-tagged Ethernet frames.

On Ipipe SAPs over an Ethernet VLAN, both dot1p and DSCP marking and re-marking is supported at access egress. On Ipipe SAPs over PPP/MLPPP, DSCP marking and re-marking is supported at access egress.

QoS Policies Overview

7705 SAR QoS policies are applied on service ingress, service egress, and network interfaces. The service ingress and service egress points may be considered as the network QoS boundaries for the service being provided.

The QoS policies define:

- classification rules for how traffic is mapped to forwarding classes
- how forwarding classes are aggregated under queues
- the queue parameters used for policing, shaping, and buffer allocation
- QoS marking/interpretation

There are several types of QoS policies (see [Table 10](#) for summaries and references to details):

- service ingress (also known as access ingress)
- service egress (also known as access egress)
- MC-MLPPP SAP egress
- network (for ingress and egress)
- network queue (for ingress and egress)
- slope
- ATM traffic descriptor profile
- fabric profile



Note: The terms access ingress/egress and service ingress/egress are interchangeable. The previous sections used the term access, and the sections that follow use the term service.

Service ingress QoS policies are applied to the customer-facing Service Access Points (SAPs) and map traffic to forwarding class queues on ingress. The mapping of traffic to queues can be based on combinations of customer QoS marking (dot1p bits and DSCP values). The number of forwarding class queues for ingress traffic and the queue characteristics are defined within the policy. There can be up to eight ingress forwarding class queues in the policy, one for each forwarding class.

Within a service ingress QoS policy, up to three queues per forwarding class can be used for multipoint traffic for multipoint services. Multipoint traffic consists of broadcast, multicast, and unknown (BMU) traffic types. For VPLS, four types of forwarding are supported (which are not to be confused with forwarding classes): unicast, broadcast, multicast, and unknown. The BMU types are flooded to all destinations within the service, while the unicast forwarding type is handled in a point-to-point fashion within the service.

Service ingress QoS policies on the 7705 SAR permits flexible arrangement of these queues. For example, more than one FC can be mapped to a single queue, both unicast and multipoint (BMU) traffic can be mapped to a single queue, or unicast and BMU traffic can be mapped to separate queues. Therefore, customers are not limited to the default configurations that are described in this guide.

Service egress QoS policies are applied to egress SAPs and provide the configurations needed to map forwarding classes to service egress queues. Each service can have up to eight queues configured, since a service may require multiple forwarding classes. A service egress QoS policy also defines how to re-mark dot1p bits and DSCP values of the customer traffic in native format based on the forwarding class of the customer traffic.

Network ingress and egress QoS policies are applied to network interfaces. On ingress for traffic received from the network, the policy maps incoming EXP values to forwarding classes and profile states. On egress, the policy maps forwarding classes and profile states to EXP values for traffic to be transmitted into the network.

On the network side, there are two types of queue policies: network and network queue (see [Table 10](#)). The network type is applied to the network interface under the `config>router>interface` command and contains the EXP marking rules for both ingress and egress. The network queue type defines all of the internal settings; that is, how the queues, or sets of queues (for ingress), are set up and used per physical port on egress and per adapter card for ingress.

If GRE or IP tunneling is enabled, policy mapping can be set up to use DSCP bits.

Network queue policies are applied on egress to network ports and channels and on ingress to adapter cards. The policies define the forwarding class queue characteristics for these entities.

Service ingress, service egress, and network QoS policies are defined with a **scope** of either *template* or *exclusive*. Template policies can be applied to multiple SAPs or interfaces, whereas exclusive policies can only be applied to a single entity.

One service ingress QoS policy and one service egress QoS policy can be applied to a specific SAP. One network QoS policy can be applied to a specific interface. A network QoS policy defines both ingress and egress behavior. If no QoS policy is explicitly applied to a SAP or network interface, a default QoS policy is applied.

[Table 10](#) provides a summary of the major functions performed by the QoS policies.

Table 10: QoS Policy Types and Descriptions

Policy Type	Applied at...	Description	Page
Service Ingress	SAP ingress	<ul style="list-style-type: none"> Defines up to eight forwarding class queues and queue parameters for traffic classification Defines match criteria to map flows to the queues based on combinations of customer QoS (dot1p bits and DSCP values) 	72
Service Egress	SAP egress	<ul style="list-style-type: none"> Defines up to eight forwarding class queues and queue parameters for traffic classification Maps one or more forwarding classes to the queues 	74
MC-MLPPP	SAP egress	<ul style="list-style-type: none"> Defines up to eight forwarding class queues and queue parameters for traffic classification Maps one or more forwarding classes to the queues 	76
Network	Network interface	<ul style="list-style-type: none"> Packets are marked using QoS policies on edge devices, such as the 7705 SAR at access ingress. Invoking a QoS policy on a network port allows for the packets that match the policy criteria to be re-marked at network egress for appropriate CoS handling across the network. 	78
Network Queue	Adapter card network ingress and egress	<ul style="list-style-type: none"> Defines forwarding class mappings to network queues 	83
Slope	Adapter card ports	<ul style="list-style-type: none"> Enables or disables the high-slope and low-slope parameters within the egress or ingress queue 	91
ATM Traffic Descriptor Profile	SAP ingress	<ul style="list-style-type: none"> Defines the expected rates and characteristics of traffic. Specified traffic parameters are used for policing ATM cells and for selecting the service category for the per-VC queue. 	93
ATM Traffic Descriptor Profile	SAP egress	<ul style="list-style-type: none"> Defines the expected rates and characteristics of traffic. Specified traffic parameters are used for scheduling and shaping ATM cells and for selecting the service category for the per-VC queue. 	93
Fabric Profile	Adapter card access and network ingress	<ul style="list-style-type: none"> Defines access and network ingress to-fabric shapers at user-configurable rates of up to 1 Gb/s 	93

Service Ingress QoS Policies

Service ingress QoS policies define ingress service forwarding class queues and map flows to those queues. When a service ingress QoS policy is created, it always has a default ingress traffic queue defined that cannot be deleted. These queues exist within the definition of the policy. The queues only get created when the policy is applied to a SAP.

In the simplest service ingress QoS policy, all traffic is treated as a single flow and mapped to a single queue. The required elements to define a service ingress QoS policy are:

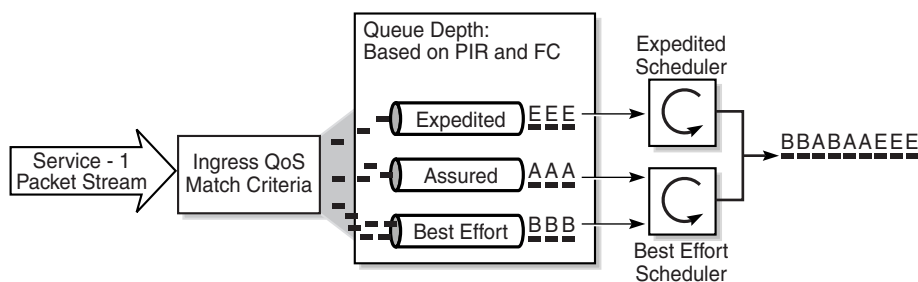
- a unique service ingress QoS policy ID
- a QoS policy scope of template or exclusive
- at least one default ingress forwarding class queue. The parameters that can be configured for a queue are discussed in [Network and Service QoS Queue Parameters](#).

Optional service ingress QoS policy elements include:

- additional ingress queues up to a total of eight
- QoS policy match criteria to map packets to a forwarding class

Each queue can have unique queue parameters to allow individual policing and rate shaping of the flow mapped to the forwarding class. [Figure 5](#) depicts service traffic being classified into three different forwarding class queues.

Figure 5: Traffic Queuing Model for Three Queues and Three Classes



19695

Mapping flows to forwarding classes is controlled by comparing each packet to the match criteria in the QoS policy. The ingress packet classification to forwarding class and enqueueing priority is subject to a classification hierarchy. Each type of classification rule is interpreted with a specific priority in the hierarchy.

Table 11 is given as an example for an Ethernet SAP (that is, a SAP defined over a whole Ethernet port or over a single VLAN). It lists the classification rules in the order in which they are evaluated.

Table 11: Forwarding Class and Enqueuing Priority Classification Hierarchy Based on Rule Type

Rule	Forwarding Class	Enqueuing Priority	Comments
default-fc	<ul style="list-style-type: none"> Set to the policy's default FC 	<ul style="list-style-type: none"> Set to the policy default 	All packets match the default rule
dot1p <i>dot1p-value</i>	<ul style="list-style-type: none"> Set when an <i>fc-name</i> exists in the policy Otherwise, preserve from the previous match 	<ul style="list-style-type: none"> Set when the <i>priority</i> parameter is high or low Otherwise, preserve from the previous match 	Each <i>dot1p-value</i> must be explicitly defined. Each packet can only match a single dot1p rule.
dscp <i>dscp-name</i>	<ul style="list-style-type: none"> Set when an <i>fc-name</i> exists in the policy Otherwise, preserve from the previous match 	<ul style="list-style-type: none"> Set when the <i>priority</i> parameter is high or low in the entry Otherwise, preserve from the previous match 	Each <i>dscp-name</i> that defines the DSCP value must be explicitly defined. Each packet can only match a single DSCP rule.

The enqueuing priority is specified as part of the classification rule and is set to high or low. The enqueuing priority relates to the forwarding class queue's high-priority-only allocation, where only packets with a high enqueuing priority are accepted into the queue once the queue's depth reaches the defined threshold. See [High-Priority-Only Buffers](#).

The mapping of ingress traffic to a forwarding class based on 802.1p or DSCP bits is optional. The default service ingress policy is implicitly applied to all SAPs that do not explicitly have another service ingress policy assigned. The characteristics of the default policy are listed in [Table 12](#).

Table 12: Default Service Ingress Policy ID 1 Definition

Characteristic	Item	Definition
Queues	Queue 1	One queue for all ingress traffic: <ul style="list-style-type: none"> Forwarding Class: Best Effort (BE) CIR = 0 PIR = max (line rate) MBS, CBS and HP Only = default (value for MBS = max, for CBS = 6 kbytes, and for HP Only = 10%)
Flows	Default FC	One flow defined for all traffic: <ul style="list-style-type: none"> all traffic mapped to Best Effort (BE) with a low priority

Service Egress QoS Policies

Service egress queues are implemented at the transition from the service network to the service access network. The advantages of per-service queuing before transmission into the access network are:

- per-service egress shaping, soft-policing capabilities
- more granular, more fair scheduling per service into the access network
- per-service statistics for forwarded and discarded service packets

The substrate capabilities and per-service scheduling control are required to make multiple services per physical port possible. Without egress shaping, it is impossible to support more than one service per port. There is no way to prevent service traffic from bursting to the available port bandwidth and starving other services.

For accounting purposes, per-service statistics can be logged. When statistics from service ingress queues are compared with service egress queues, the ability to conform to per-service QoS requirements within the service network can be measured. The service network statistics are a major asset to network provisioning tools.

Service egress QoS policies define egress service queues and map forwarding class flows to queues. In the simplest service egress QoS policy, all forwarding classes are treated as a single flow and mapped to a single queue.

To define a basic service egress QoS policy, the following are required:

- a unique service egress QoS policy ID
- a QoS policy scope of template or exclusive
- at least one defined default queue. The parameters that can be configured for a queue are discussed in [Network and Service QoS Queue Parameters](#).

Optional service egress QoS policy elements include:

- additional queues, up to a total of eight separate queues
- dot1p priority and DSCP value re-marking based on forwarding class

Each queue in a policy is associated with one or more of the supported forwarding classes. Each queue can have its individual queue parameters, allowing individual rate shaping of the forwarding class(es) mapped to the queue. More complex service queuing models are supported in the 7705 SAR where each forwarding class is associated with a dedicated queue.

The forwarding class determination per service egress packet is determined at ingress. If the packet ingressed the service on the same 7705 SAR router, the service ingress classification rules determine the forwarding class of the packet. If the packet was received over a service transport tunnel, the forwarding class is marked in the tunnel transport encapsulation.

Service egress QoS policy ID 1 is reserved as the default service egress policy. The default policy cannot be deleted or changed.

The default service egress policy is applied to all SAPs that do not have another service egress policy explicitly assigned. The characteristics of the default policy are listed in [Table 13](#).

Table 13: Default Service Egress Policy ID 1 Definition

Characteristic	Item	Definition
Queues	Queue 1	One queue defined for all traffic classes: <ul style="list-style-type: none"> • CIR = 0 • PIR = max (line rate) • MBS, CBS and HP Only = default (value for MBS = max, for CBS = 6 kbytes, for HP Only = 10%)
Flows	Default action	One flow defined for all traffic classes: <ul style="list-style-type: none"> • all traffic mapped to queue 1 with no marking of IEEE 802.1p or DSCP values

MC-MLPPP SAP Egress QoS Policies

SAPs running MC-MLPPP have their own SAP egress QoS policies that differ from standard policies. Unlike standard SAP policies, MC-MLPPP SAP egress policies do not contain queue types, CIR, CIR adaptation rules, or dot1p re-marking.

Standard and MC-MLPPP SAP egress policies can never have the same policy ID except when the policy ID is 1 (default). Standard SAP egress QoS policies cannot be applied to SAPs running MC-MLPPP. Similarly, MC-MLPPP SAP egress QoS policies cannot be applied to standard SAPs. The default policy can be applied to both MC-MLPPP and other SAPs. It will remain the default policy regardless of SAP type.

MC-MLPPP on the 7705 SAR supports scheduling based on multi-class implementation. Instead of the standard profiled queue-type-based scheduling, an MC-MLPPP encapsulated access port performs class-based traffic servicing.

The four MC-MLPPP classes are scheduled in a strict priority fashion, as shown in [Table 14](#).

Table 14: MC-MLPPP Class Priorities

MC-MLPPP Class	Priority
0	Priority over all other classes
1	Priority over classes 2 and 3
2	Priority over class 3
3	No priority

For example, if a packet is sent to an MC-MLPPP class 3 queue and all other queues are empty, the 7705 SAR fragments the packet according to the configured fragment size and begins sending the fragments. If a new packet is sent to an MC-MLPPP class 2 queue, the 7705 SAR finishes sending any fragments of the class 3 packet that are on the wire, then holds back the remaining fragments in order to service the higher-priority packet. The fragments of the first packet remain at the top of the class 3 queue. For packets of the same class, MC-MLPPP class queues operate on a first-in, first-out basis.

The user configures the required number of MLPPP classes to use on a bundle. The forwarding class of the packet, as determined by the ingress QoS classification, is used to determine the MLPPP class for the packet. The mapping of forwarding class to MLPPP class is a function of the user-configurable number of MLPPP classes. The default mapping for a 4-class, 3-class, and 2-class MLPPP bundle is shown in [Table 15](#).

Table 15: Packet Forwarding Class to MLPPP Class Mapping

FC ID	FC Name	MLPPP Class 4-class bundle	MLPPP Class 3-class bundle	MLPPP Class 2-class bundle
7	NC	0	0	0
6	H1	0	0	0
5	EF	1	1	1
4	H2	1	1	1
3	L1	2	2	1
2	AF	2	2	1
1	L2	3	2	1
0	BE	3	2	1

If one or more forwarding classes are mapped to a queue, the scheduling priority of the queue is based on the lowest forwarding class mapped to it. For example, if forwarding classes 0 and 7 are mapped to a queue, the queue is serviced by MC-MLPPP class 3 in a 4-class bundle model.

Network and Service QoS Policies

The QoS mechanisms within the 7705 SAR are specialized for the type of traffic on the interface. For customer interfaces, there is service ingress and service egress traffic, and for network interfaces, there is network ingress and network egress traffic.

The 7705 SAR uses QoS policies applied to a SAP for a service or to a network port to define the queuing, queue attributes, and QoS marking/interpretation.

The 7705 SAR supports the following types of network and service QoS policies:

- [Network QoS Policies](#)
- [Network Queue QoS Policies](#)
- [Service Ingress QoS Policies](#) (described previously)
- [Service Egress QoS Policies](#) (described previously)



Note: Queuing parameters are the same for both network and service QoS policies. See [Network and Service QoS Queue Parameters](#).

Network QoS Policies

Network QoS policies define egress QoS marking and ingress QoS classification for traffic on network interfaces. The 7705 SAR automatically creates egress queues for each of the forwarding classes on network interfaces.

A network QoS policy defines both the ingress and egress handling of QoS on the network interface. The following functions are defined:

- ingress
 - defines label switched path Experimental bit (LSP EXP) value mappings to forwarding classes
 - defines DSCP name mappings to forwarding classes
- egress
 - defines forwarding class to LSP EXP and dot1p value markings
 - defines forwarding class to DSCP value markings

The required elements to be defined in a network QoS policy are:

- a unique network QoS policy ID
- egress forwarding class to LSP EXP value mappings for each forwarding class used
- egress forwarding class to DSCP value mappings for each forwarding class used
- a default ingress forwarding class and in-profile/out-of-profile state

Optional network QoS policy elements include the LSP EXP value or DSCP name to forwarding class and profile state mappings for all EXP values or DSCP values received. Network policy ID 1 is reserved as the default network QoS policy. The default policy cannot be deleted or changed. The default network QoS policy is applied to all network interfaces that do not have another network QoS policy explicitly assigned.

[Table 16](#) lists the default mapping of forwarding class to LSP EXP values and DSCP names for network egress.

Table 16: Default Network QoS Policy Egress Marking

FC-ID	FC Name	FC Label	DiffServ Name	Egress LSP EXP Marking		Egress DSCP Marking	
				In-Profile	Out-of-Profile	In-Profile Name	Out-of-Profile Name
7	Network Control	nc	NC2	111 - 7	111 - 7	nc2 111000 - 56	nc2 111000 - 56
6	High-1	h1	NC1	110 - 6	110 - 6	nc1 110000 - 48	nc1 110000 - 48
5	Expedited	ef	EF	101 - 5	101 - 5	ef 101110 - 46	ef 101110 - 46
4	High-2	h2	AF4	100 - 4	100 - 4	af41 100010 - 34	af42 100100 - 36
3	Low-1	l1	AF2	011 - 3	010 - 2	af21 010010 - 18	af22 010100 - 20
2	Assured	af	AF1	011 - 3	010 - 2	af11 001010 - 10	af12 001100 - 12
1	Low-2	l2	CS1	001 - 1	001 - 1	cs1 001000 - 8	cs1 001000 - 8
0	Best Effort	be	BE	000 - 0	000 - 0	be 000000 - 0	be 000000 - 0

For network ingress, [Table 17](#) lists the default mapping of DSCP name to forwarding class and profile state for the default network QoS policy.

Table 17: Default Network QoS Policy DSCP to Forwarding Class Mappings

Ingress DSCP			Forwarding Class		
DSCP Name	DSCP Value	FC ID	Name	Label	Profile State
Default ⁽¹⁾		0	Best-Effort	be	Out
ef	101110 - 46	5	Expedited	ef	In
cs1	001000 - 8	1	Low-2	l2	In
nc-1	110000 - 48	6	High-1	h1	In
nc-2	111000 - 56	7	Network Control	nc	In
af11	001010 - 10	2	Assured	af	In
af12	001100 - 12	2	Assured	af	Out
af13	001110 - 14	2	Assured	af	Out
af21	010010 - 18	3	Low-1	l1	In
af22	010100 - 20	3	Low-1	l1	Out
af23	010110 - 22	3	Low-1	l1	Out
af31	011010 - 26	3	Low-1	l1	In
af32	011100 - 28	3	Low-1	l1	Out
af33	011110 - 30	3	Low-1	l1	Out
af41	100010 - 34	4	High-2	h2	In
af42	100100 - 36	4	High-2	h2	Out
af43	100110 - 38	4	High-2	h2	Out

Note: (1) The default forwarding class mapping is used for all DSCP name values for which there is no explicit forwarding class mapping.

Table 18 lists the default mapping of LSP EXP values to forwarding class and profile state for the default network QoS policy.

Table 18: Default Network QoS Policy LSP EXP to Forwarding Class Mappings

Ingress LSP EXP			Forwarding Class		
LSP EXP ID	LSP EXP Value	FC ID	Name	Label	Profile State
Default ⁽¹⁾		0	Best-Effort	be	Out
1	001 - 1	1	Low-2	l2	In
2	010 - 2	2	Assured	af	Out
3	011 - 3	2	Assured	af	In
4	100 - 4	4	High-2	h2	In
5	101 - 5	5	Expedited	ef	In
6	110 - 6	6	High-1	h1	In
7	111 - 7	7	Network Control	nc	In

Note: (1) The default forwarding class mapping is used for all LSP EXP values for which there is no explicit forwarding class mapping.

CoS Marking for Self-generated Traffic

The 7705 SAR is the source of some types of traffic; for example, a link state PDU for sending IS-IS topology updates or an SNMP trap sent to indicate that an event has happened. This type of traffic that is created by the 7705 SAR is considered to be self-generated traffic (SGT). Another example of self-generated traffic is Telnet, but in that application, user commands initiate the sending of the Telnet traffic.

In earlier releases, the DSCP bits of IP self-generated traffic were always marked with H1 (with the exception of SNMP, whose DSCP bits were configurable).

Network operators often have different QoS models throughout their networks and apply different QoS schemes to portions of the networks in order to better accommodate delay, jitter, and loss requirements of different applications. The class of service (DSCP or dot1p) bits of self-generated traffic can be marked on a per-application basis to match the network operator's QoS scheme. This marking option enhances the ability of the 7705 SAR to match the various requirements of these applications.

The 7705 SAR supports marking self-generated traffic for the router and VPRN service. Refer to "QoS Policies" in the 7705 SAR OS Services Guide for information on sgt-qos as applied to VPRN service.

The forwarding class of the self-generated IP traffic is determined by a user-configurable mapping of the DSCP value to one of the eight FCs. The self-generated traffic is queued with other traffic belonging to the same forwarding class.



Note: IS-IS and ARP traffic are not IP-generated traffic types and are not DSCP-configurable; however, the dot1p bits can be configured in the same way as the DSCP bits. The default setting for the dot1p bits for both types of traffic is 111. For all other applications, the dot1p bits are marked based on the mapped network egress forwarding class.

Table 19 lists various applications and indicates whether they have configurable DSCP or dot1p markings.

Table 19: Applications and Support for Configurable DSCP or dot1p Markings

Application	Supported Marking	Default DSCP/dot1p
IS-IS	dot1p	7
ARP	dot1p	7
BGP	DSCP	NC1
DHCP	DSCP	NC1
1588 PTP	DSCP	NC1
LDP (T-LDP)	DSCP	NC1
RSVP	DSCP	NC1
OSPF	DSCP	NC1
Telnet	DSCP	AF41
TFTP	DSCP	AF41
FTP	DSCP	AF41
SSH (SCP)	DSCP	AF41
SNMP (get, set, etc.)	DSCP	AF41
SNMP trap/log	DSCP	AF41
syslog	DSCP	AF41
ICMP (ping)	DSCP	BE
Traceroute	DSCP	BE
TACACS+	DSCP	AF41

Table 19: Applications and Support for Configurable DSCP or dot1p Markings (Continued)

Application	Supported Marking	Default DSCP/dot1p
DNS	DSCP	AF41
NTP	DSCP	NC1
SNTP	DSCP	AF41
RADIUS	DSCP	AF41

**Notes:**

- PTP in the context of SGT QoS is defined as Precision Timing Protocol and is an application in the 7705 SAR. The PTP application name is also used in areas such as event-control and logging. Precision Timing Protocol is defined in IEEE 1588-2008.
- PTP in the context of IP filters is defined as Performance Transparency Protocol. IP protocols can be used as IP filter match criteria; the match is made on the 8-bit protocol field in the IP header.

Network Queue QoS Policies

Network queue policies define the queue characteristics that are used in determining the scheduling and queuing behavior for a given forwarding class or forwarding classes. Network queue policies are applied on ingress and egress network ports.

Network queue policies are identified with a unique policy name that conforms to the standard 7705 SAR alphanumeric naming conventions. The policy name is user-configured when the policy is created.

Network queue policies can be configured to use up to 16 queues (8 unicast and 8 multicast). This means that the number of queues can vary. Not all user-created policies will require and use 16 queues; however, the default network queue policy does define 16 queues.

The queue characteristics that can be configured on a per-forwarding class basis are:

- Committed Buffer Size (CBS) as a percentage of the buffer pool
- Maximum Buffer Size (MBS) as a percentage of the buffer pool
- High-Priority-Only Buffers as a percentage of MBS
- Peak Information Rate (PIR) as a percentage of egress port bandwidth
- Committed Information Rate (CIR) as a percentage of egress port bandwidth

The system default network queue policy is named “**default**” and cannot be modified or deleted. [Table 20](#) describes the default network queue policy definition.



Note: In the table, the value for Rate in the Definition column is the PIR value.

Table 20: Default Network Queue Policy Definition

Forwarding Class	Queue	Definition	Queue	Definition
Network-Control (nc)	8	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%	16	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.1% High-Prio-Only = 10%
High-1 (h1)	7	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%	15	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.1% High-Prio-Only = 10%
Expedited (ef)	6	Rate = 100% CIR = 100% MBS = 5% CBS = 0.75% High-Prio-Only = 10%	14	Rate = 100% CIR = 100% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
High-2 (h2)	5	Rate = 100% CIR = 100% MBS = 5% CBS = 0.75% High-Prio-Only = 10%	13	Rate = 100% CIR = 100% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
Low-1 (l1)	4	Rate = 100% CIR = 25% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%	12	Rate = 100% CIR = 5% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%

Table 20: Default Network Queue Policy Definition (Continued)

Forwarding Class	Queue	Definition	Queue	Definition
Assured (af)	3	Rate = 100% CIR = 25% MBS = 5% CBS = 0.75% High-Prio-Only = 10%	11	Rate = 100% CIR = 5% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
Low-2 (l2)	2	Rate = 100% CIR = 25% MBS = 5% CBS = 0.25% High-Prio-Only = 10%	10	Rate = 100% CIR = 5% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
Best Effort (be)	1	Rate = 100% CIR = 0% MBS = 5% CBS = 0.1% High-Prio-Only = 10%	9	Rate = 100% CIR = 0% MBS = 5% CBS = 0.1% High-Prio-Only = 10%

Network and Service QoS Queue Parameters

The following queue parameters are provisioned on network and service queues:

- [Queue ID](#)
- [Committed Information Rate](#)
- [Peak Information Rate](#)
- [Adaptation Rule](#)
- [Committed Burst Size](#)
- [Maximum Burst Size](#)
- [High-Priority-Only Buffers](#)
- [High and Low Enqueuing Thresholds](#)
- [Queue Counters](#)
- [Queue Types](#)
- [Rate Limiting](#)

Queue ID

The queue ID is used to uniquely identify the queue. The queue ID is only unique within the context of the QoS policy within which the queue is defined.

Committed Information Rate

The CIR for a queue defines a limit for scheduling. Packets queued at service ingress queues are serviced by in-profile or out-of-profile schedulers based on the queue's CIR and the rate at which the packets are flowing. For each packet in a service ingress queue, the CIR is checked with the current transmission rate of the queue. If the current rate is at or below the CIR threshold, the transmitted packet is internally marked in-profile. If the flow rate is above the threshold, the transmitted packet is internally marked out-of-profile.

All 7705 SAR queues support the concept of in-profile and out-of-profile. The network QoS policy applied at network egress determines how or if the profile state is marked in packets transmitted into the network core. This is done by enabling or disabling the appropriate priority marking of network egress packets within a particular forwarding class. If the profile state is marked in the packets that are sent toward the network core, then out-of-profile packets are preferentially dropped over in-profile packets at congestion points in the network.

When defining the CIR for a queue, the value specified is the administrative CIR for the queue. The 7705 SAR maps a user-configured value to a hardware supported rate that it uses to determine the operational CIR for the queue. The user has control over how the administrative CIR is converted to an operational CIR if a slight adjustment is required. The interpretation of the administrative CIR is discussed in [Adaptation Rule](#).

The CIR value for a service queue is assigned to ingress and egress service queues based on service ingress QoS policies and service egress QoS policies, respectively.

The CIR value for a network queue is defined within a network queue policy specifically for the forwarding class. The *queue-id* parameter links the CIR values to the forwarding classes. The CIR values for the forwarding class queues are defined as a percentage of the network interface bandwidth.

Peak Information Rate

The PIR value defines the maximum rate at which packets are allowed to exit the queue. It does not specify the maximum rate at which packets may enter the queue; this is governed by the queue's ability to absorb bursts and is user-configurable using its maximum burst size (MBS) value.

The PIR value is provisioned on ingress and egress service queues within service ingress QoS policies and service egress QoS policies, respectively.

The PIR values for network queues are defined within network queue policies and are specific for each forwarding class. The PIR value for each queue for the forwarding class is defined as a percentage of the network interface bandwidth.

When defining the PIR for a queue, the value specified is the administrative PIR for the queue. The 7705 SAR maps a user-configured value to a hardware supported rate that it uses to determine the operational PIR for the queue. The user has control over how the administrative PIR is converted to an operational CIR if a slight adjustment is required. The interpretation of the administrative PIR is discussed in [Adaptation Rule](#).

Adaptation Rule

The schedulers on the network processor can only operate with a finite set of rates. These rates are called the operational rates. The configured rates for PIR and CIR do not necessarily correspond to the operational rates. In order to offer maximum flexibility to the user, the `adaptation-rule` command can be used to choose how an operational rate is selected based on the configured PIR or CIR rate.

The *max* parameter causes the network processor to be programmed at an operational rate that is less than the configured PIR or CIR rate by up to 0.5%. The *min* parameter causes the network processor to be programmed at an operational rate that is greater than the configured PIR or CIR rate by up to 0.5%. The *closest* parameter causes the network processor to be programmed at an operational rate that is closest to the configured PIR or CIR rate.

Committed Burst Size

The CBS parameter specifies the committed buffer space allocated for a given queue.

The CBS is provisioned on ingress and egress service queues within service ingress QoS policies and service egress QoS policies, respectively. The CBS for a queue is specified in kilobytes.

The CBS values for network queues are defined within network queue policies based on the forwarding class. The CBS values for the queues for the forwarding class are defined as a percentage of buffer space for the pool.

Maximum Burst Size

Once the reserved buffers for a given queue have been used, the queue contends with other queues for additional buffer resources up to the maximum burst size. The MBS parameter specifies the maximum queue depth to which a queue can grow. This parameter ensures that a traffic flow (that is, a customer or a traffic type within a customer port) that is massively or continuously over-subscribing the PIR of a queue will not consume all the available buffer resources. For high-priority forwarding class service queues, the MBS can be small because the high-priority service packets are scheduled with priority over other service forwarding classes. In other words, very small queues would be needed for high-priority traffic since the contents of the queues should have been scheduled by the best available scheduler.

The MBS value is provisioned on ingress and egress service queues within service ingress QoS policies and service egress QoS policies, respectively. The MBS value for a queue is specified in kilobytes.

The MBS values for network queues are defined within network queue policies based on the forwarding class. The MBS values for the queues for the forwarding class are defined as a percentage of buffer space for the pool.

High-Priority-Only Buffers

High-priority-only buffers are defined on a queue and allow buffers to be reserved for traffic classified as high priority. When the queue depth reaches a specified level, only high-priority traffic can be enqueued. The high-priority-only reservation for a queue is defined as a percentage of the MBS value.

On service ingress, the high-priority-only reservation for a queue is defined in the service ingress QoS policy. High-priority traffic is specified in the match criteria for the policy.

On service egress, the high-priority-only reservation for a queue is defined in the service egress QoS policy. Service egress queues are specified by forwarding class. High-priority traffic for a given traffic class is traffic that has been marked as in-profile either on ingress classification or based on interpretation of the QoS markings.

The high-priority-only buffers for network queues are defined within network queue policies based on the forwarding class. High-priority-only traffic for a specific traffic class is marked as in-profile either on ingress classification or based on interpretation of the QoS markings.

High and Low Enqueuing Thresholds

The high/low priority feature allows a provider to offer a customer the ability to have some packets treated with a higher priority when buffered to the ingress queue. If the queue is configured with a *hi-prio-only* setting (setting the high-priority MBS threshold higher than the queue's low-priority MBS threshold) a portion of the ingress queue's allowed buffers are reserved for high-priority traffic. An access ingress packet must hit an ingress QoS action in order for the ingress forwarding plane to treat the packet as high priority (the default is low priority).

If the packet's ingress queue is above the low-priority MBS, the packet will be discarded unless it has been classified as high priority. The priority of the packet is not retained after the packet is placed into the ingress queue. Once the packet is scheduled out of the ingress queue, the packet will be considered in-profile or out-of-profile based on the dynamic rate of the queue relative to the queue's CIR parameter.

If an ingress queue is not configured with a *hi-prio-only* parameter, the low-priority and high-priority MBS thresholds will be the same. There will be no difference in high-priority and low-priority packet handling. At access ingress, the priority of a packet has no effect on which packets are scheduled first. Only the first buffering decision is affected. At ingress and egress, the current dynamic rate of the queue relative to the queue's CIR does affect the scheduling priority between queues going to the same destination (egress port). From highest to lowest, the strict operating priority for queues is:

- expedited queues within the CIR (conform)
- best effort queues within the CIR (conform)
- expedited queues above the CIR (exceed)
- best effort queues above the CIR (exceed)

For access ingress, the CIR controls both dynamic scheduling priority and the marking threshold. At network ingress, the queue's CIR affects the scheduling priority but does not provide a profile marking function (as the network ingress policy trusts the received marking of the packet based on the network QoS policy).

At egress, the profile of a packet is only important for egress queue buffering decisions and egress marking decisions, not for scheduling priority. The egress queue's CIR will determine the dynamic scheduling priority, but will not affect the packet's ingress determined profile.

Queue Counters

The 7705 SAR maintains extensive counters for queues within the system to allow granular or extensive debugging and planning; that is, the utilization of queues and the scheduler used for servicing a queue or packet is extremely useful in network planning activities. The following separate billing and accounting counters are maintained for each queue:

- counters for packets and octets accepted into the queue
- counters for packets and octets rejected at the queue
- counters for packets and octets transmitted in-profile
- counters for packets and octets transmitted out-of-profile

Queue Types

The 7705 SAR allows the user to specify two different ways to configure the queue types. The queue types can be configured as “expedite” or “best-effort” with specific commands, or the queue types can be configured automatically by using the auto-expedite type.

With auto-expedite, the queue type is automatically determined by the forwarding classes that are assigned to the queue. The queues that are set as auto-expedite still must be (and work as) either expedited or best-effort queues, but that is determined by the forwarding classes. Therefore, in a default configuration, four of the eight forwarding classes result in an expedited queue, whereas the assignment of any one of the other four forwarding classes results in a best-effort type assignment, even if other expedited forwarding classes are also assigned.

The expedite, best-effort, and auto-expedite queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective.

Rate Limiting

The 7705 SAR supports egress rate limiting on Ethernet network ports. Rate limiting sets a limit on the amount of traffic that can leave the port, thus controlling the total bandwidth on the interface. If the rate limit is reached, the port applies backpressure on the queues, which stops the flow of traffic until the queue buffers are emptied.

This feature is useful in scenarios where there is a fixed amount of bandwidth; for example, a mobile operator who has leased a fixed amount of bandwidth from the service provider.

The egress rate is set at the interface level in the `config>port>ethernet` context.

WRED and RED Slope Policies

As part of 7705 SAR queue management, WRED and/or RED queue management (also known as congestion management) policies can be enabled at both access and network ports and associated with both ingress and egress queues, to manage the queue depths.

Without WRED and RED, once a queue reaches its maximum fill size, the queue discards any new packets arriving at the queue.

WRED and RED policies prevent a queue from reaching its maximum size by starting random discards once the queue hits a certain threshold value. This way, the brick impact where all the new incoming packets are discarded can be avoided. By starting random discards after user-configurable thresholds, the customer devices at an end-system may be adjusted to the available bandwidth.

As an example, TCP has built-in mechanisms to adjust for packet drops. TCP-based flows lower the transmission rate when some of the packets fail to reach the far end. This mode of operation provides a much better way of dealing with congestion than dropping all the packets after the whole queue space is depleted.

The WRED and RED curve algorithms are based on two user-configurable thresholds, `minThreshold` and `maxThreshold`. The `MinThreshold` indicates the level when the discards should start. The `MaxThreshold` is the level where the discard probability reaches its maximum. Beyond this level, all newly arriving packets are discarded. The steepness of the slope is derived from the `MaxDProbability`. The `MaxDProbability` indicates the random discard probability at `maxThreshold`.

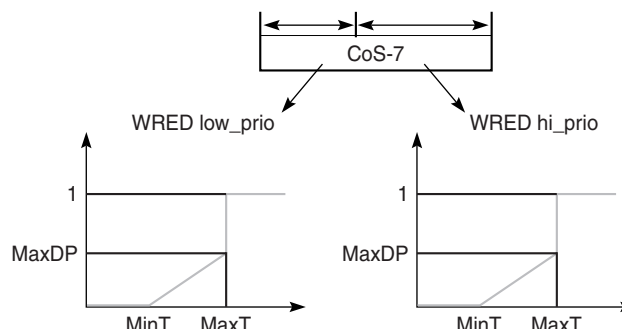
The main difference between WRED and RED is that with WRED, there can be more than one curve managing the fill rate of the same queue.

WRED slope curves can run against high-priority and low-priority traffic separately for ingress and egress queues. This allows the flexibility to treat low-priority and high-priority traffic differently. Instead of configuring the `minThreshold`, `maxThreshold` and `maxDProbability` values against every queue, WRED slope policies are used to configure these threshold, and are then applied to individual queues. WRED slope policies thus affect how and when the high-priority and low-priority traffic is discarded within the same queue.

Referring to [Figure 6](#), one WRED slope curve can manage discards on high-priority traffic and another WRED slope curve can manage discards on low-priority traffic. The `minThreshold`, `maxThreshold` and `MaxDProbability` values configured for high-priority and low-priority traffic can be different and can start discarding traffic at different thresholds.



Note: The figure shows a step function at `MaxT`. The `MaxDP` value is the target for the configuration entered and it partly determines the slope of the weighting curve. At `MaxT`, if the arrival of a new packet will overflow the buffer, the discard probability becomes 1, which is not the `MaxDP` value. Therefore, a step function exists in this graph.

Figure 6: WRED for High-Priority and Low-Priority Traffic on the Same Queue

19696

The formula to calculate the average queue size is:

- average queue size = (previous average $\times (1 - 1/2^{\text{TAF}})$) + (current queue size $\times 1/2^{\text{TAF}}$)

The Time Average Factor (TAF) is the exponential weight factor used in calculating the average queue size. The *time_average_factor* parameter is non-user-configurable, and is set to a system-wide default value of 3. By locking TAF to a static value of 3, the average queue size closely tracks the current queue size so that WRED can respond quickly to long queues.

WRED MinThreshold and MaxThreshold Computation

CBS and MBS are both configured as kilobytes through the CLI. These configured values are converted to number of packets. This converted value is a non-user-configurable fixed default value that is equal to the maximum frame size to ensure that even the largest frames can be hosted in the allocated buffer pools.

A user-defined MaxThreshold and MinThreshold value, defined as a percentage, are also converted. The MaxThreshold is converted to the system-MaxThreshold and the MinThreshold is converted to the system-MinThreshold, as packet values.

The system-MinThreshold must be the absolute closest value to the MinThreshold, which satisfies the formula below:

- $\text{system-maxThreshold} - \text{system-minThreshold} = 2^x$

ATM Traffic Descriptor Profiles

Traffic descriptor profiles capture the cell arrival pattern for resource allocation. Source traffic descriptors for an ATM connection include at least one of the following:

- Sustained Information Rate (SIR)
- Peak Information Rate (PIR)
- Minimum Information Rate (MIR)
- Maximum Burst Size (MBS)

QoS traffic descriptor profiles are applied on ATM VLL (Apipe) SAPs.

Fabric Profiles

Fabric profiles allow access and network ingress to-fabric shapers to be user-configurable at rates that provide up to 1 Gb/s switching throughput from an adapter card towards the fabric.

Two fabric profile modes are supported, per-destination mode and aggregate mode. Both modes offer shaping towards the fabric from an adapter card, but per-destination shapers offer the maximum flexibility by precisely controlling the amount of traffic to each destination card at a user-defined rate.

QoS Policy Entities

Services are configured with default QoS policies. Additional policies must be explicitly created and associated. There is one default service ingress QoS policy, one default service egress QoS policy, and one default network QoS policy. Only one ingress QoS policy and one egress QoS policy can be applied to a SAP or network port.

When you create a new QoS policy, default values are provided for most parameters with the exception of the policy ID and queue ID values, descriptions, and the default action queue assignment. Each policy has a scope, default action, a description, and at least one queue. The queue is associated with a forwarding class.

All QoS policy parameters can be configured in the CLI. QoS policies can be applied to the following service types:

- Epipe — both ingress and egress policies are supported on an Epipe SAP
- Apipe — both ingress and egress policies are supported on an Apipe SAP
- Cpipe — only ingress policies are supported on a Cpipe SAP
- Ipipe — both ingress and egress policies are supported on an Ipipe SAP

QoS policies can be applied to the following network entities:

- network ingress interface
- network egress interface

Default QoS policies treat all traffic with equal priority and allow an equal chance of transmission (Best Effort forwarding class) and an equal chance of being dropped during periods of congestion. QoS prioritizes traffic according to the forwarding class and uses congestion management to control access ingress, access egress, and network traffic with queuing according to priority.

Configuration Notes

The following caveats apply to the implementation of QoS policies.

- Creating additional QoS policies is optional.
- Default policies are created for service ingress, service egress, network, network-queue, and slope policies.
- Associating a service with a QoS policy other than the default policy is optional.
- A network queue, service egress, and service ingress QoS policy must consist of at least one queue. Queues define the forwarding class, CIR, and PIR associated with the queue.

Reference Sources

For information on supported IETF drafts and standards, as well as standard and proprietary MIBs, refer to [Standards and Protocol Support](#).

Network QoS Policies

In This Chapter

This chapter provides information to configure network QoS policies using the command line interface (CLI).

Topics in this chapter include:

- [Overview on page 98](#)
- [Basic Configuration on page 99](#)
- [Service Management Tasks on page 107](#)
- [Network QoS Policy Command Reference on page 109](#)

Overview

The network QoS policy consists of an ingress and egress component.

The ingress component of the QoS policy defines how DSCP bits (for GRE and IP) and multiprotocol label switching (MPLS) Experimental (EXP) bits are mapped to internal forwarding class and profile state. The forwarding class and profile state define the per-hop behavior (PHB) or the QoS treatment through the 7705 SAR.

The egress component of the QoS policy defines the DSCP bit, MPLS EXP bit, and the dot1p marking based on the forwarding class and the profile state.

The mapping on each network interface defaults to the mappings defined in the default network QoS policy until an explicit policy is defined for the network interface. Network policy-id 1 exists as the default policy that is applied to all network interfaces by default. The network policy-id 1 cannot be modified or deleted. For the ingress, it defines the default DSCP-to-FC and MPLS EXP-to-FC mapping. For the egress, it defines eight forwarding classes that represent the packet marking criteria.

New (non-default) network policy parameters can be modified. The **no** form of the command reverts the object to the default values.

Changes made to a policy are applied immediately to all network interfaces where the policy is applied. For this reason, when a policy requires several changes, it is recommended that you copy the policy to a work area policy-id. The work-in-progress copy can be modified until all the changes are made, and then the original policy-id can be overwritten with the `config qos copy` command.

For information about the tasks and commands necessary to access the command line interface and to configure and maintain your 7705 SAR devices, refer to the 7705 SAR OS Basic System Configuration Guide, “CLI Usage”.

Basic Configuration

A basic network QoS policy must conform to the following rule.

- Each network QoS policy must have a unique policy ID.

Creating a Network QoS Policy

Configuring and applying QoS policies other than the default policy is optional.

Define the following to create a network QoS policy:

- a network policy ID value — the system does not dynamically assign a value
- a description — a text string description of policy features
- scope — the policy scope as exclusive or template
- egress criteria — you can modify egress criteria to customize the forwarding class to be instantiated. Otherwise, the default values are applied.
 - dot1p — the dot1p-in-profile and dot1p-out-profile mapping for the forwarding class
 - DSCP — the DSCP value is used for all GRE and IP packets (in or out of profile) requiring marking that egress on this forwarding class
 - LSP EXP — the EXP value is used for all MPLS labeled packets (in or out of profile) requiring marking that egress on this forwarding class
- ingress criteria — the DSCP to forwarding class mapping for all GRE and IP packets and the MPLS EXP bits to forwarding class mapping for all labeled packets
 - default-action — the default action to be taken for packets that have undefined DSCP or MPLS EXP bits set. The default-action specifies the forwarding class to which such packets are assigned. The default-action is automatically created when the policy is created.
 - DSCP — a mapping between the DSCP bits of the network ingress traffic and the forwarding class. Ingress traffic that matches the specified DSCP bits will be assigned to the corresponding forwarding class.
 - LSP EXP — a mapping between the LSP EXP bits of the network ingress traffic and the forwarding class. Ingress traffic that matches the specified LSP EXP bits will be assigned to the corresponding forwarding class.

Use the following CLI syntax to create a network QoS policy:

CLI Syntax:

```
config>qos#
network network-policy-id
  description description-string
  scope {exclusive|template}
  egress
    fc {be|l2|af|l1|h2|ef|h1|nc}
    dot1p dot1p-priority
    dot1p-in-profile dot1p-priority
    dot1p-out-profile dot1p-priority
    dscp-in-profile dscp-name
    dscp-out-profile dscp-name
    lsp-exp-in-profile lsp-exp-value
    lsp-exp-out-profile lsp-exp-value
  ingress
    default-action fc {be|l2|af|l1|h2|ef|h1|nc}
    profile {in|out}
    dscp dscp-name fc {be|l2|af|l1|h2|ef|h1|nc}
    profile {in|out}
    lsp-exp lsp-exp-value fc fc-name profile {in|out}
```

Example:

```
configure qos network 700 create
config>qos>network$ description "Net Policy"
config>qos>network$ scope template
config>qos>network$ egress fc be
config>qos>network>egress>fc$ dot1p 1
config>qos>network>egress>fc$ lsp-exp-in-profile 2
config>qos>network>egress>fc$ lsp-exp-out-profile 3
config>qos>network>egress>fc$ exit
config>qos>network$ ingress
config>qos>network>ingress$ default-action fc be profile
in
config>qos>network>ingress$ exit
config>qos>network$ exit
```

The following sample output displays the configuration for network policy 700:

```
*A:ALU-1>config>qos# info
-----
echo "QoS Policy Configuration"
#-----
network 700 create
    description "Net Policy"
    ingress
        default-action fc be profile in
    exit
    egress
        fc be
            lsp-exp-in-profile 2
            lsp-exp-out-profile 3
            dot1p-in-profile 1
            dot1p-out-profile 1
        exit
    exit
exit
-----
```

Applying Network Policies

Use the following CLI syntax to apply network policies to router interfaces:

CLI Syntax: config>router
 interface *interface-name*
 qos *network-policy-id*

Example: config>router# interface ALU-1
 config>router>if\$ qos 700
 config>router>if\$ exit

The following sample output displays the configuration for router interface ALU-1 with network policy 700 applied to the interface.

```
A:ALU-1>config>router# info
-----
echo "IP Configuration"
#-----
    interface "ALU-1"
        qos 700
    exit
    interface "ip-100.0.0.2"
        address 100.10.0.2/10
    exit
-----
```

Default Network Policy Values

The default network policy is identified as policy-id 1. Default policies cannot be modified or deleted. [Table 21](#) lists the default network policy parameters.

Table 21: Network Policy Defaults

Field	Default	
description	"Default network QoS policy"	
scope	template	
ingress		
default-action	fc be profile out	
dscp:		
be	fc be	profile out
ef	fc ef	profile in
cs1	fc l2	profile in
nc1	fc h1	profile in
nc2	fc nc	profile in
af11	fc af	profile in
af12	fc af	profile out
af13	fc af	profile out
af21	fc l1	profile in
af22	fc l1	profile out
af23	fc l1	profile out
af31	fc l1	profile in
af32	fc l1	profile out
af33	fc l1	profile out
af41	fc h2	profile in
af42	fc h2	profile out
af43	fc h2	profile out
lsp-exp:		
0	fc be	profile out
1	fc l2	profile in
2	fc af	profile out
3	fc af	profile in
4	fc h2	profile in
5	fc ef	profile in
6	fc h1	profile in
7	fc nc	profile in

Table 21: Network Policy Defaults (Continued)

Field	Default	
egress		
fc af:		
dscp-in-profile	af11	
dscp-out-profile	af12	
lsp-exp-in-profile	3	
lsp-exp-out-profile	2	
dot1p-in-profile	2	
dot1p-out-profile	2	
fc be:		
dscp-in-profile	be	
dscp-out-profile	be	
lsp-exp-in-profile	0	
lsp-exp-out-profile	0	
dot1p-in-profile	0	
dot1p-out-profile	0	
fc ef:		
dscp-in-profile	ef	
dscp-out-profile	ef	
lsp-exp-in-profile	5	
lsp-exp-out-profile	5	
dot1p-in-profile	5	
dot1p-out-profile	5	
fc h1:		
dscp-in-profile	nc1	
dscp-out-profile	nc1	
lsp-exp-in-profile	6	
lsp-exp-out-profile	6	
dot1p-in-profile	6	
dot1p-out-profile	6	
fc h2:		
dscp-in-profile	af41	
dscp-out-profile	af42	
lsp-exp-in-profile	4	
lsp-exp-out-profile	4	
dot1p-in-profile	4	
dot1p-out-profile	4	

Table 21: Network Policy Defaults (Continued)

Field	Default	
fc 11:		
dscp-in-profile	af21	
dscp-out-profile	af22	
lsp-exp-in-profile	3	
lsp-exp-out-profile	2	
dot1p-in-profile	3	
dot1p-out-profile	3	
fc 12:		
dscp-in-profile	cs1	
dscp-out-profile	cs1	
lsp-exp-in-profile	1	
lsp-exp-out-profile	1	
dot1p-in-profile	1	
dot1p-out-profile	1	
fc nc:		
dscp-in-profile	nc2	
dscp-out-profile	nc2	
lsp-exp-in-profile	7	
lsp-exp-out-profile	7	
dot1p-in-profile	7	
dot1p-out-profile	7	

The following sample output displays a default network policy configuration:

```
A:ALU-1>config>qos>network# info detail
-----
description "Default network QoS policy."
scope template
ingress
  default-action fc be profile out
  dscp be fc be profile out
  dscp ef fc ef profile in
  dscp cs1 fc l2 profile in
  dscp ncl fc h1 profile in
  dscp nc2 fc nc profile in
  dscp af11 fc af profile in
  dscp af12 fc af profile out
  dscp af13 fc af profile out
  dscp af21 fc l1 profile in
  dscp af22 fc l1 profile out
  dscp af23 fc l1 profile out
  dscp af31 fc l1 profile in
  dscp af32 fc l1 profile out
  dscp af33 fc l1 profile out
  dscp af41 fc h2 profile in
  dscp af42 fc h2 profile out
  dscp af43 fc h2 profile out
  lsp-exp 0 fc be profile out
  lsp-exp 1 fc l2 profile in
  lsp-exp 2 fc af profile out
  lsp-exp 3 fc af profile in
  lsp-exp 4 fc h2 profile in
  lsp-exp 5 fc ef profile in
  lsp-exp 6 fc h1 profile in
  lsp-exp 7 fc nc profile in
exit
egress
  fc af
    dscp-in-profile af11
    dscp-out-profile af12
    lsp-exp-in-profile 3
    lsp-exp-out-profile 2
    dot1p-in-profile 2
    dot1p-out-profile 2
  exit
  fc be
    dscp-in-profile be
    dscp-out-profile be
    lsp-exp-in-profile 0
    lsp-exp-out-profile 0
    dot1p-in-profile 0
    dot1p-out-profile 0
  exit
  fc ef
    dscp-in-profile ef
    dscp-out-profile ef
    lsp-exp-in-profile 5
    lsp-exp-out-profile 5
    dot1p-in-profile 5
    dot1p-out-profile 5
  exit
```

```
fc h1
    dscp-in-profile ncl
    dscp-out-profile ncl
    lsp-exp-in-profile 6
    lsp-exp-out-profile 6
    dotlp-in-profile 6
    dotlp-out-profile 6
exit
fc h2
    dscp-in-profile af41
    dscp-out-profile af42
    lsp-exp-in-profile 4
    lsp-exp-out-profile 4
    dotlp-in-profile 4
    dotlp-out-profile 4
exit
fc l1
    dscp-in-profile af21
    dscp-out-profile af22
    lsp-exp-in-profile 3
    lsp-exp-out-profile 2
    dotlp-in-profile 3
    dotlp-out-profile 3
exit
fc l2
Press any key to continue (Q to quit)
```

Service Management Tasks

This section describes the following service management tasks:

- [Deleting QoS Policies](#)
- [Copying and Overwriting Network Policies](#)
- [Editing QoS Policies](#)

Deleting QoS Policies

A network policy is associated by default with router interfaces. You can replace the default policy with a non-default policy, but you cannot entirely remove the policy from the configuration. When you remove a non-default policy, the policy association reverts to the default network policy-id 1.

Use the following syntax to delete a network policy.

CLI Syntax: `config>qos# no network network-policy-id`

Example: `config>qos# no network 700`

Copying and Overwriting Network Policies

You can copy an existing network policy to a new policy ID value or overwrite an existing policy ID. The `overwrite` option must be specified or an error occurs if the destination policy ID exists.

Use the following syntax to overwrite an existing policy ID.

CLI Syntax: `config>qos# copy network source-policy-id dest-policy-id [overwrite]`

Example:

```
config>qos# copy network 1 600
config>qos# copy slope-policy 600 700
MINOR: CLI Destination "700" exists use {overwrite}.
config>qos# copy slope-policy 600 700 overwrite
config>qos#
```

The following sample output displays copied policies:

```
ALU-12>config>qos# info detail
-----
...
    network 1 create
      description "Default network QoS policy."
      scope template
      ingress
      default-action fc be profile out
...
    network 600 create
      description "Default network QoS policy."
      scope template
      ingress
      default-action fc be profile out
...
    network 700 create
      description "Default network QoS policy."
      scope template
      ingress
      default-action fc be profile out
...
-----
ALU-12>config>qos#
```

Editing QoS Policies

You can change existing policies, except the default policies, and entries in the CLI. The changes are applied immediately to all interfaces where the policy is applied. To prevent configuration errors, use the copy command to make a duplicate of the original policy in a work area, make the edits, and then overwrite the original policy.

Network QoS Policy Command Reference

Command Hierarchies

- [Configuration Commands](#)
- [Operational Commands](#)
- [Show Commands](#)

Configuration Commands

```

config
  — qos
    — [no] network network-policy-id [create]
      — description description-string
      — no description
      — scope {exclusive | template}
      — no scope
      — egress
        — [no] fc fc-name
          — dot1p dot1p-priority
          — no dot1p
          — dot1p-in-profile dot1p-priority
          — no dot1p-in-profile
          — dot1p-out-profile dot1p-priority
          — no dot1p-out-profile
          — dscp-in-profile dscp-name
          — no dscp-in-profile
          — dscp-out-profile dscp-name
          — no dscp-out-profile
          — lsp-exp-in-profile lsp-exp-value
          — no lsp-exp-in-profile
          — lsp-exp-out-profile lsp-exp-value
          — no lsp-exp-out-profile
        — ingress
          — default-action fc fc-name profile {in | out}
          — dscp dscp-name fc fc-name profile {in | out}
          — no dscp
          — lsp-exp lsp-exp-value fc fc-name profile {in | out}
          — no lsp-exp lsp-exp-value

```

Self-generated Traffic Configuration Commands

```
config
  — router
    — sgt-qos
      — application dscp-app-name dscp {dscp-value | dscp-name}
      — application dot1p-app-name dot1p dot1p-priority
      — no application {dscp-app-name | dot1p-app-name}
      — dscp dscp-name fc fc-name
      — no dscp dscp-name
```

Operational Commands

```
config
  — qos
    — copy network src-pol dst-pol [overwrite]
```

Show Commands

```
show
  — qos
    — dscp-table [value dscp-value]
    — network policy-id [detail]

show
  — router
    — sgt-qos
      — application [app-name] [dscp | dot1p]
      — dscp-map [dscp-name]
```

Command Descriptions

- [Configuration Commands on page 112](#)
- [Operational Commands on page 128](#)
- [Show Commands on page 129](#)

Configuration Commands

- [Generic Commands on page 113](#)
- [Network QoS Policy Commands on page 114](#)
- [Network Egress QoS Policy Commands on page 116](#)
- [Network Ingress QoS Policy Commands on page 118](#)
- [Network Egress QoS Policy Forwarding Class Commands on page 121](#)
- [Self-generated Traffic Commands on page 125](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>qos>network config>qos>mc-mlppp>sap-egress
Description	<p>This command associates a text string with a configuration context to help identify the context in the configuration file.</p> <p>The no form of this command removes any description string from the context.</p>
Default	none
Parameters	<i>description-string</i> — a text string describing the entity. 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.

Network QoS Policy Commands

network

Syntax	[no] network <i>network-policy-id</i> [create]				
Context	config>qos				
Description	<p>This command creates or edits a QoS network policy. The network policy defines the treatment that GRE, IP, or MPLS packets receive as they ingress and egress the network port.</p> <p>Network <i>policy-id</i> 1 exists as the default policy that is applied to all network interfaces by default. Network <i>policy-id</i> 1 cannot be modified or deleted.</p> <p>If a new network policy is created (for instance, <i>policy-id</i> 2), only the default action and egress forwarding class parameters are identical to the default <i>policy-id</i> 1. A new network policy does not contain the default DSCP-to-FC or MPLS EXP-to-FC mapping. To create a new network policy that includes the default ingress DSCP-to-FC or MPLS EXP-to-FC mapping, the default network <i>policy-id</i> 1 can be copied (using the copy command). You can modify parameters or use the no modifier to remove an object from the configuration.</p> <p>Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network interfaces where this policy is applied. For this reason, when many changes are required on a policy, it is highly recommended that the policy be copied to a work area <i>policy-id</i>. That work-in-progress policy can be modified until complete and then written over the original <i>policy-id</i>. Use the config qos copy command to maintain policies in this manner.</p> <p>The no form of this command deletes the network policy. A policy cannot be deleted until it is removed from all services where it is applied. The default network policy <i>policy-id</i> 1 cannot be deleted.</p>				
Default	System Default Network Policy 1 defined				
Parameters	<p><i>network-policy-id</i> — uniquely identifies the policy on the 7705 SAR</p> <table> <tr> <td>Values</td><td>2 to 65535</td></tr> <tr> <td>Default</td><td>n/a</td></tr> </table> <p>create — keyword used to create a network QoS policy</p>	Values	2 to 65535	Default	n/a
Values	2 to 65535				
Default	n/a				

scope

Syntax	scope {exclusive template} no scope
Context	config>qos>network
Description	<p>This command configures the network policy scope as exclusive or template. The policy's scope cannot be changed if the policy is applied to an interface.</p> <p>The no form of this command sets the scope of the policy to the default of template.</p>
Default	template
Parameters	<p>exclusive — when the scope of a policy is defined as exclusive, the policy can only be applied to one network. If a policy with an exclusive scope is assigned to a second network, an error message is generated. If the policy is removed from the exclusive network, it will become available for assignment to another exclusive network.</p> <p>The system default policies cannot be defined as exclusive scope. An error will be generated if scope exclusive is executed in any policies with a <i>policy-id</i> equal to 1.</p> <p>template — when the scope of a policy is defined as template, the policy can be applied to multiple networks on the router.</p> <p>Default QoS policies are configured with template scopes. An error is generated if you try to modify the template scope parameter to exclusive scope on default policies.</p>

Network Egress QoS Policy Commands

egress

Syntax	egress
Context	config>qos>network
Description	<p>This command is used to enter the CLI mode that creates or edits egress policy entries that specify the forwarding class to be instantiated when this policy is applied to the network port.</p> <p>The forwarding class and profile state mapping to in-profile and out-of-profile DSCP and MPLS EXP bits mapping for all labeled packets are also defined under this node.</p> <p>For MPLS tunnels, if network egress Ethernet ports are used, dot1p bit marking can be enabled in conjunction with EXP bit marking. In this case, the tunnel and pseudowire EXP bits do not have to be the same as the dot1p bits.</p> <p>For GRE and IP tunnels, dot1p marking and pseudowire EXP marking can be enabled, and DSCP marking can also be enabled.</p> <p>The service packets are transported over an MPLS LSP, GRE tunnel, or IP tunnel.</p> <p>All out-of-profile service packets are marked with the corresponding DSCP (for GRE or IP packets) or EXP (for MPLS packets) bit value at network egress. All in-profile service packets are marked with the corresponding in-profile DSCP or EXP bit value based on the forwarding class they belong to.</p>

fc

Syntax	[no] fc <i>fc-name</i>
Context	config>qos>network>egress
Description	<p>This command specifies the forwarding class name. The fc <i>fc-name</i> represents a CLI parent node that contains sub-commands or parameters describing the marking criteria for that forwarding class. The fc command overrides the default parameters for that forwarding class defined in the network default <i>policy-id</i> 1.</p> <p>The no form of this command reverts to the defined parameters in the default network policy <i>policy-id</i> 1. If the <i>fc-name</i> is removed from the default network policy <i>policy-id</i> 1, that forwarding class reverts to the factory defaults.</p>
Default	Undefined forwarding classes default to the configured parameters in the default network policy <i>policy-id</i> 1.

Parameters	<i>fc-name</i> — the case-sensitive, system-defined forwarding class name for which policy entries will be created
Values	be, l2, af, ll, h2, ef, h1, nc
Default	none

Network Ingress QoS Policy Commands

ingress

Syntax	ingress
Context	config>qos>network
Description	<p>This command is used to enter the CLI mode that creates or edits policy entries that specify the DSCP to forwarding class mapping for all GRE or IP packets and define the MPLS EXP bits to forwarding class mapping for all labeled packets.</p> <p>When pre-marked GRE, IP, or MPLS packets ingress on a network port, they get a per-hop behavior (that is, the QoS treatment through the 7705 SAR based on the mapping defined under the current node).</p>

default-action

Syntax	default-action fc <i>fc-name</i> profile {in out}
Context	config>qos>network>ingress
Description	<p>This command defines or edits the default action to be taken for packets that have undefined DSCP or MPLS EXP bits set. The default-action command specifies the forwarding class to which such packets are assigned.</p> <p>Multiple default-action commands will overwrite each previous default-action command.</p>
Default	none
Parameters	<p><i>fc-name</i> — specifies the forwarding class name. All packets with DSCP or MPLS EXP bits not defined will be placed in this forwarding class.</p> <p>Default be</p> <p>Values be, l2, af, l1, h2, ef, h1, nc</p> <p>profile {in out} — all packets that are assigned to this forwarding class will be considered in or out of profile based on this command. In case of congestion, the in-profile packets are preferentially queued over the out-of-profile packets.</p> <p>Values in, out</p> <p>Default out</p>

dscp

Syntax	dscp dscp-name fc fc-name profile {in out} no dscp
Context	config>qos>network>ingress
Description	<p>This command creates a mapping between the DSCP of the network ingress traffic and the forwarding class for GRE or IP packets.</p> <p>Ingress traffic that matches the specified DSCP is assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all 64 DSCP values with the forwarding class. For undefined code points, packets are assigned to the forwarding class specified under the default-action command.</p> <p>The no form of this command removes the DSCP-to-FC association. The default-action then applies to that code point value.</p>
Default	none
Parameters	<p><i>dscp-name</i> — specifies the DSCP to be associated with the forwarding class. The DSCP value is derived from the most significant six bits in the IP header ToS byte field (DSCP bits). The six DSCP bits define 64 DSCP values used to map packets to per-hop QoS behavior.</p> <p>A maximum of 64 DSCP rules are allowed on a single policy. The specified name must exist as a <i>dscp-name</i>. Table 22 lists all the valid DSCP names.</p>

Table 22: Valid DSCP Names

dscp-name
be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, cp35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

fc-name — specifies the forwarding class name with which the DSCP will be associated

Default be

Values be, l2, af, l1, h2, ef, h1, nc

profile {in | out} — all packets that are assigned to this forwarding class will be considered in or out of profile based on this command. In case of congestion, the in-profile packets are preferentially queued over the out-of-profile packets.

Values in, out


Default out

lsp-exp

Syntax	lsp-exp <i>lsp-exp-value</i> fc <i>fc-name</i> profile { in out } no lsp-exp <i>lsp-exp-value</i>
Context	config>qos>network>ingress
Description	<p>This command creates a mapping between the LSP EXP bits of the network ingress traffic and the forwarding class.</p> <p>Ingress traffic that matches the specified LSP EXP bits will be assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all of the eight LSP EXP bit values with the forwarding class. For undefined values, packets are assigned to the forwarding class specified under the default-action command.</p> <p>The no form of this command removes the association of the LSP EXP bit value with the forwarding class. The default-action then applies to that LSP EXP bit pattern.</p>
Default	none
Parameters	<p><i>lsp-exp-value</i> — specifies the LSP EXP values to be associated with the forwarding class</p> <p>Default none</p> <p>Values 0 to 7 (decimal representation of 3-bit EXP field)</p> <p><i>fc-name</i> — specifies the FC name that the EXP bit pattern will be associated with</p> <p>Default none</p> <p>Values be, l2, af, l1, h2, ef, h1, nc</p> <p>profile {in out} — indicates whether the LSP EXP value is the in-profile or out-of-profile value</p> <p>Values in, out</p> <p>Default none</p>

Network Egress QoS Policy Forwarding Class Commands

dot1p

Syntax	dot1p <i>dot1p-priority</i> no dot1p
Context	config>qos>network>egress>fc
Description	This command explicitly defines the egress dot1p priority bits values for the forwarding class.
	Note: When a single <i>dot1p-priority</i> is specified, it is applied to both in-profile and out-of-profile packets. The other forms of the command described below (dot1p-in-profile and dot1p-out-profile) allow different dot1p values for in-profile or out-of-profile packets to be specified.
	The no form of the command sets the dot1p priority bits value to 0.
Default	0
Parameters	<i>dot1p-priority</i> — the explicit dot1p value for the specified forwarding class. Setting the value to 0 is equivalent to removing the marking value.
	Values 0 to 7
	Default n/a

dot1p-in-profile

Syntax	dot1p-in-profile <i>dot1p-priority</i> no dot1p-in-profile
Context	config>qos>network>egress>fc
Description	This command specifies dot1p in-profile mappings.
	The no form of the command reverts to the factory default in-profile <i>dot1p-priority</i> setting for <i>policy-id</i> 1.
Parameters	<i>dot1p-priority</i> — defines the dot1p marking for the forwarding class
	A maximum of eight dot1p rules are allowed on a single policy.
	Values 0 to 7

dot1p-out-profile

Syntax	dot1p-out-profile <i>dot1p-priority</i> no dot1p-out-profile
Context	config>qos>network>egress>fc
Description	This command specifies dot1p out-profile mappings. The no form of the command reverts to the factory default out-profile <i>dot1p-priority</i> setting for <i>policy-id</i> 1.
Parameters	<i>dot1p-priority</i> — defines the dot1p marking for the forwarding class A maximum of eight dot1p rules are allowed on a single policy. Values 0 to 7

dscp-in-profile

Syntax	dscp-in-profile <i>dscp-name</i> no dscp-in-profile
Context	config>qos>network>egress>fc
Description	This command specifies the in-profile DSCP name for the forwarding class. The corresponding DSCP value is used for all in-profile GRE or IP packets that require marking at egress on this forwarding class. When multiple DSCP names are associated with the forwarding class at network egress, the last name entered overwrites the previous value. The no form of this command reverts to the factory default <i>in-profile dscp-name</i> setting for <i>policy-id</i> 1.
Default	policy-id 1: factory setting policy-id 2 to 65535: <i>policy-id</i> 1 setting
Parameters	<i>dscp-name</i> — specifies the DSCP to be associated with the forwarding class. The DSCP value is derived from the most significant six bits in the IP header ToS byte field (DSCP bits). The six DSCP bits define 64 DSCP values used to map packets to per-hop QoS behavior. A maximum of 64 DSCP rules are allowed on a single policy. The specified name must exist as a <i>dscp-name</i> . Table 22 lists all the valid DSCP names.

dscp-out-profile

Syntax	dscp-out-profile <i>dscp-name</i> no dscp-out-profile
Context	config>qos>network>egress>fc
Description	<p>This command specifies the out-of-profile DSCP name for the forwarding class. The corresponding DSCP value is for all out-of-profile GRE or IP packets that require marking at egress on this forwarding class.</p> <p>When multiple DSCP names are associated with the forwarding class at network egress, the last name entered overwrites the previous value.</p> <p>The no form of this command reverts to the factory default <i>out-profile dscp-name</i> setting for <i>policy-id</i> 1.</p>
Default	<p>policy-id 1: factory setting</p> <p>policy-id 2 to 65535: <i>policy-id</i> 1 setting</p>
Parameters	<p><i>dscp-name</i> — specifies the DSCP to be associated with the forwarding class. The DSCP value is derived from the most significant six bits in the IP header ToS byte field (DSCP bits). The six DSCP bits define 64 DSCP values used to map packets to per-hop QoS behavior.</p> <p>A maximum of 64 DSCP rules are allowed on a single policy. The specified name must exist as a <i>dscp-name</i>. Table 22 lists all the valid DSCP names.</p>

lsp-exp-in-profile

Syntax	lsp-exp-in-profile <i>lsp-exp-value</i> no lsp-exp-in-profile				
Context	config>qos>network>egress>fc				
Description	<p>This command specifies the in-profile LSP EXP value for the forwarding class. The EXP value will be used for all in-profile LSP labeled packets requiring marking at egress on this forwarding class.</p> <p>When multiple EXP values are associated with the forwarding class at network egress, the last name entered overwrites the previous value.</p> <p>The no form of this command reverts to the factory default in-profile EXP setting for policy-id 1.</p>				
Default	<p>policy-id 1: factory setting</p> <p>policy-id 2 to 65535: <i>policy-id</i> 1 setting</p>				
Parameters	<p><i>lsp-exp-value</i> — the 3-bit LSP EXP bit value, expressed as a decimal integer</p> <table> <tr> <td>Values</td><td>0 to 7</td></tr> <tr> <td>Default</td><td>none</td></tr> </table>	Values	0 to 7	Default	none
Values	0 to 7				
Default	none				

lsp-exp-out-profile

Syntax	lsp-exp-out-profile <i>lsp-exp-value</i> no lsp-exp-out-profile				
Context	config>qos>network>egress>fc				
Description	<p>This command specifies the out-of-profile LSP EXP value for the forwarding class. The EXP value will be used for all out-of-profile LSP labeled packets requiring marking at egress on this forwarding class queue.</p> <p>When multiple EXP values are associated with the forwarding class at network egress, the last name entered overwrites the previous value.</p> <p>The no form of this command reverts to the factory default out-of-profile EXP setting for <i>policy-id 1</i>.</p>				
Default	<p>policy-id 1: factory setting</p> <p>policy-id 2 to 65535: <i>policy-id 1</i> setting</p>				
Parameters	<p><i>lsp-exp-value</i> — the 3-bit LSP EXP bit value, expressed as a decimal integer</p> <table> <tr> <td>Values</td><td>0 to 7</td></tr> <tr> <td>Default</td><td>none</td></tr> </table>	Values	0 to 7	Default	none
Values	0 to 7				
Default	none				

Self-generated Traffic Commands

sgt-qos

Syntax	sgt-qos
Context	config>router <i>router-name</i>
Description	This command enables the context to configure DSCP or dot1p re-marking for self-generated traffic.
Parameters	<i>router-name</i> — the router instance
Values	keyword: Base or management
Default	Base

application

Syntax	application <i>dscp-app-name</i> dscp { <i>dscp-value</i> <i>dscp-name</i> } application <i>dot1p-app-name</i> dot1p <i>dot1p-priority</i> no application { <i>dscp-app-name</i> <i>dot1p-app-name</i> }
Context	config>router <i>router-name</i> >sgt-qos
Description	<p>This command configures DSCP or dot1p re-marking for self-generated application traffic. When an application is configured using this command, the specified DSCP name or value is used for all packets generated by this application.</p> <p>The value set in this command:</p> <ul style="list-style-type: none"> • sets the DSCP bits in the IP packet • maps to the FC; this value will be signaled from the CSM to the egress forwarding complex • based on this signaled FC, the egress forwarding complex QoS policy sets the IEEE 802.1 dot1p bits • the dot1p and the LSP EXP bits are set by the egress complex for all packets based on the signaled FC. This includes ARP and IS-IS packets that, due to their nature, do not carry DSCP bits. • the DSCP value in the egress IP header will be as configured in this command, and the egress QoS policy will not overwrite this value <p>Only one DSCP name or value can be configured per application. If multiple entries are configured, the subsequent entry overrides the previously configured entry.</p> <p>The no form of this command reverts the DSCP value for the application back to its default value.</p>
Default	none (that is, sgt-qos does not enforce a DSCP value and the application uses its default value, as shown in Table 19)

Parameters *dscp-app-name* — the DSCP application name

Values bgp, dhcp, dns, ftp, icmp, ldp, ntp, ospf, ptp, radius, rsvp, snmp, snmp-notification, ssh, syslog, tacplus, telnet, tftp, traceroute



Notes:

- PTP in the context of SGT QoS is defined as Precision Timing Protocol and is an application in the 7705 SAR. The PTP application name is also used in areas such as event-control and logging. Precision Timing Protocol is defined in IEEE 1588-2008.
- PTP in the context of IP filters is defined as Performance Transparency Protocol. IP protocols can be used as IP filter match criteria; the match is made on the 8-bit protocol field in the IP header.

dscp-value — the value that maps to the DSCP name

Values 0 to 63

dscp-name — the DSCP to be associated with the forwarding class. [Table 22](#) lists the valid DSCP names.

dot1p-app-name — the dot1p application name

Values arp, isis

dot1p-priority — the dot1p priority

Values none | 0 to 7

dscp

Syntax **dscp** *dscp-name* **fc** *fc-name*
no dscp *dscp-name*

Context config>router *router-name*>sgt-qos

Description This command creates a mapping between the DSCP of the self-generated traffic and the forwarding class.

Self-generated traffic that matches the specified DSCP is assigned to the corresponding forwarding class. Multiple commands can be entered to associate some or all of the 64 DSCP values with the forwarding class.

All DSCP names that define a DSCP value must be explicitly defined.

The **no** form of the command removes the DSCP-to-FC association.

Default none

Parameters *dscp-name* — the DSCP to be associated with the forwarding class. [Table 22](#) lists the valid DSCP names.

fc-name — the forwarding class name with which the DSCP will be associated

Values be, l2, af, l1, h2, ef, h1, nc

Default be

Operational Commands

copy

Syntax	copy network <i>src-pol dst-pol</i> [overwrite]
Context	config>qos
Description	<p>This command copies existing QoS policy entries for a QoS policy ID to another QoS policy ID.</p> <p>The copy command is used to create new policies using existing policies and also allows bulk modifications to an existing policy with the use of the overwrite keyword.</p>
Parameters	<p><i>src-pol dst-pol</i> — indicates that the source and destination policies are network policy IDs. Specify the source policy that the copy command will copy and specify the destination policy to which the command will duplicate the policy to a new or different policy ID.</p> <p>Values 1 to 65535</p> <p>overwrite — specifies that the existing destination policy is to be replaced. Everything in the existing destination policy will be overwritten with the contents of the source policy. If overwrite is not specified, an error will occur if the destination policy ID exists.</p> <pre> ALU>config>qos# copy network 1 427 MINOR: CLI Destination "427" exists use {overwrite}. ALU>config>qos# copy network 1 427 overwrite </pre>

Show Commands

dscp-table

Syntax	dscp-table [value <i>dscp-value</i>]
Context	show>qos
Description	This command displays DSCP name to DSCP value mappings.
Parameters	value <i>dscp-value</i> — the specific DSCP value for which to display information Values 0 to 63 Default show all values
Output	The following output is an example of DSCP name to DSCP value mappings information, and Table 23 describes the fields.

Sample Output

```
*A:ALU-1# show qos dscp-table
```

```
=====
DSCP Mapping
=====
```

DSCP Name	DSCP Value	TOS (bin)	TOS (hex)
be	0	0000 0000	00
cp1	1	0000 0100	04
cp2	2	0000 1000	08
cp3	3	0000 1100	0C
cp4	4	0001 0000	10
cp5	5	0001 0100	14
cp6	6	0001 1000	18
cp7	7	0001 1100	1C
cs1	8	0010 0000	20
cp9	9	0010 0100	24
af11	10	0010 1000	28
cp11	11	0010 1100	2C
af12	12	0011 0000	30
cp13	13	0011 0100	34
af13	14	0011 1000	38
cp15	15	0011 1100	3C
cs2	16	0100 0000	40
cp17	17	0100 0100	44
af21	18	0100 1000	48
cp19	19	0100 1100	4C
af22	20	0101 0000	50
cp21	21	0101 0100	54
af23	22	0101 1000	58
cp23	23	0101 1100	5C
cs3	24	0110 0000	60
cp25	25	0110 0100	64

af31	26	0110 1000	68
cp27	27	0110 1100	6C
af32	28	0111 0000	70
cp29	29	0111 0100	74
af33	30	0111 1000	78
cp31	31	0111 1100	7C
cs4	32	1000 0000	80
cp33	33	1000 0100	84
af41	34	1000 1000	88
cp35	35	1000 1100	8C
af42	36	1001 0000	90
cp37	37	1001 0100	94
af43	38	1001 1000	98
cp39	39	1001 1100	9C
cs5	40	1010 0000	A0
cp41	41	1010 0100	A4
cp42	42	1010 1000	A8
cp43	43	1010 1100	AC
cp44	44	1011 0000	B0
cp45	45	1011 0100	B4
ef	46	1011 1000	B8
cp47	47	1011 1100	BC
nc1	48	1100 0000	C0
cp49	49	1100 0100	C4
cp50	50	1100 1000	C8
cp51	51	1100 1100	CC
cp52	52	1101 0000	D0
cp53	53	1101 0100	D4
cp54	54	1101 1000	D8
cp55	55	1101 1100	DC
nc2	56	1110 0000	E0
cp57	57	1110 0100	E4
cp58	58	1110 1000	E8
cp59	59	1110 1100	EC
cp60	60	1111 0000	F0
cp61	61	1111 0100	F4
cp62	62	1111 1000	F8
cp63	63	1111 1100	FC
=====			
*A:ALU-1#			

Table 23: DSCP Name to Value Mappings Command Output Fields

Label	Description
DSCP Name	The name of the DSCP to be associated with the forwarding class
DSCP Value	The DSCP value ranges (from 0 to 63)
TOS (bin)	The type of service in binary format
TOS (hex)	The type of service in hexadecimal format

network

Syntax	network [<i>policy-id</i>] [detail]
Context	show>qos
Description	This command displays network policy information.
Parameters	<p><i>policy-id</i> — displays information for the specific policy ID</p> <p>Values 1 to 65535</p> <p>Default all network policies</p> <p>detail — displays detailed information for the specific policy ID</p>
Output	The following output is an example of network policy information, and Table 24 describes the fields.

Sample Output

```
*A:ALU-1# show qos network
```

```
=====
Network Policies
=====
Policy-Id      Description
-----
1              Default network QoS policy.
100           Network QoS policy 100.
=====
```

```
*A:ALU-1# show qos network detail
```

```
=====
QoS Network Policy
=====
-----
Network Policy (1)
-----
Policy-id      : 1
Forward Class  : be                      Profile      : Out
Description    : Default network QoS policy.

-----
DSCP           Forwarding Class      Profile
-----
be             be                      Out
ef             ef                      In
cs1            l2                      In
nc1            h1                      In
nc2            nc                      In
af11           af                      In
af12           af                      Out
af13           af                      Out
af21           l1                      In
af22           l1                      Out
af23           l1                      Out
af31           l1                      In
```

af32	l1	Out
af33	l1	Out
af41	h2	In
af42	h2	Out
af43	h2	Out

LSP EXP Bit Map	Forwarding Class	Profile
0	be	Out
1	l2	In
2	af	Out
3	af	In
4	h2	In
5	ef	In
6	h1	In
7	nc	In

Egress Forwarding Class Queuing

FC Value : 0	FC Name : be
- DSCP Mapping	
Out-of-Profile : be	In-Profile : be
- Dot1p Mapping	
Out-of-Profile : 0	In-Profile : 0
- LSP EXP Bit Mapping	
Out-of-Profile : 0	In-Profile : 0
FC Value : 1	FC Name : l2
- DSCP Mapping	
Out-of-Profile : cs1	In-Profile : cs1
- Dot1p Mapping	
Out-of-Profile : 1	In-Profile : 1
- LSP EXP Bit Mapping	
Out-of-Profile : 1	In-Profile : 1
FC Value : 2	FC Name : af
- DSCP Mapping	
Out-of-Profile : af12	In-Profile : af11
- Dot1p Mapping	
Out-of-Profile : 2	In-Profile : 2
- LSP EXP Bit Mapping	
Out-of-Profile : 2	In-Profile : 3
FC Value : 3	FC Name : l1
- DSCP Mapping	
Out-of-Profile : af22	In-Profile : af21
- Dot1p Mapping	
Out-of-Profile : 3	In-Profile : 3

- LSP EXP Bit Mapping		
Out-of-Profile : 2	In-Profile	: 3
FC Value : 4	FC Name	: h2
- DSCP Mapping		
Out-of-Profile : af42	In-Profile	: af41
- Dot1p Mapping		
Out-of-Profile : 4	In-Profile	: 4
- LSP EXP Bit Mapping		
Out-of-Profile : 4	In-Profile	: 4
FC Value : 5	FC Name	: ef
- DSCP Mapping		
Out-of-Profile : ef	In-Profile	: ef
- Dot1p Mapping		
Out-of-Profile : 5	In-Profile	: 5
- LSP EXP Bit Mapping		
Out-of-Profile : 5	In-Profile	: 5
FC Value : 6	FC Name	: h1
- DSCP Mapping		
Out-of-Profile : nc1	In-Profile	: nc1
- Dot1p Mapping		
Out-of-Profile : 6	In-Profile	: 6
- LSP EXP Bit Mapping		
Out-of-Profile : 6	In-Profile	: 6
FC Value : 7	FC Name	: nc
- DSCP Mapping		
Out-of-Profile : nc2	In-Profile	: nc2
- Dot1p Mapping		
Out-of-Profile : 7	In-Profile	: 7
- LSP EXP Bit Mapping		
Out-of-Profile : 7	In-Profile	: 7

Interface Association

Interface : system		
IP Addr. : n/a	Port Id	: system
Interface : address		
IP Addr. : n/a	Port Id	: n/a
Interface : back		
IP Addr. : n/a	Port Id	: n/a
Interface : dhcp_interface		
IP Addr. : n/a	Port Id	: n/a
Interface : int_formpls		
IP Addr. : n/a	Port Id	: 1/3/11.1
Interface : interface_1		
IP Addr. : n/a	Port Id	: n/a
Interface : router_interface_1		

```

IP Addr.      : 20.20.20.20/32          Port Id      : n/a
Interface     : vprn_interface
IP Addr.      : n/a                    Port Id      : n/a
Interface     : ipv6_interface
IP Addr.      : n/a                    Port Id      : n/a
Interface     : management
IP Addr.      : 138.120.210.88/24      Port Id      : A/1

```

```

=====
*A:ALU-1#

```

Table 24: Network Policy Command Output Fields

Label	Description
Policy-Id	The ID that uniquely identifies the policy
Forward Class	The forwarding class name
Description	A text string that helps identify the policy's context in the configuration file
DSCP	The DSCP name associated with the forwarding class
Forwarding Class	The forwarding class associated with the DSCP
Profile	Whether the DSCP mapping pertains to in-profile or out-of-profile traffic
LSP EXP Bit Map	The LSP EXP mapping value used for in-profile or out-of-profile traffic
Forwarding Class	The default-action forwarding class name. All packets with MPLS EXP bits not defined will be placed in this forwarding class.
Profile	Whether the LSP EXP bit mapping pertains to in-profile or out-of-profile traffic
Egress/Ingress Forwarding Class Queuing	
FC Value	The forwarding class value
FC Name	The forwarding class name
DSCP Mapping	Out-of-Profile - the out-of-profile DSCP mapping for the forwarding class
	In-Profile - the in-profile DSCP mapping for the forwarding class

Table 24: Network Policy Command Output Fields (Continued)

Label	Description
Dot1p Mapping	Out-of-Profile - the out-of-profile dot1p bit mapping for the forwarding class
	In-Profile - the in-profile dot1p bit mapping for the forwarding class
LSP EXP Bit Mapping	Out-of-Profile - the out-of-profile LSP EXP bit mapping for the forwarding class
	In-Profile - the in-profile LSP EXP bit mapping for the forwarding class
Interface Association	
Interface	The name of the interface
IP Addr.	The IP address of the interface
Port Id	The physical port identifier that associates the interface

sgt-qos

Syntax	sgt-qos
Context	show>router
Description	This command displays QoS information about self-generated traffic.

application

Syntax	application [<i>app-name</i>] [dscp dot1p]
Context	show>router>sgt-qos
Description	This command displays application QoS settings.

Parameters *app-name* — the specified application

Values arp, bgp, dhcp, dns, ftp, icmp, isis, ldp, ntp, ospf, ptp, radius, rsvp, snmp, snmp-notification, ssh, syslog, tacplus, telnet, tftp, traceroute



Notes:

- PTP in the context of SGT QoS is defined as Precision Timing Protocol and is an application in the 7705 SAR. The PTP application name is also used in areas such as event-control and logging. Precision Timing Protocol is defined in IEEE 1588-2008.
- PTP in the context of IP filters is defined as Performance Transparency Protocol. IP protocols can be used as IP filter match criteria; the match is made on the 8-bit protocol field in the IP header.

dscp — specifies to show all DSCP applications

dot1p — specifies to show all dot1p applications

Output The following output is an example of application QoS information, and [Table 25](#) describes the fields.

Sample Output

```
A:ALU-1# show router sgt-qos application
```

DSCP Application Values		
Application	DSCP Value	Default DSCP Value
bgp	none	none
dhcp	none	none
dns	nc2	none
ftp	none	none
icmp	none	none
ldp	none	none
ntp	none	none
ospf	none	none
radius	none	none
rsvp	none	none
snmp	none	none
snmp-notification	none	none
ssh	none	none
syslog	none	none
tacplus	none	none
telnet	be	none
tftp	none	none
traceroute	none	none


```

=====
Dot1p Application Values
=====
Application          Dot1p Value          Default Dot1p Value
-----
arp                   5                    7
isis                  none                 7
=====
A:ALU-1#

```

Table 25: Application QoS Output Fields

Label	Description
Application	The DSCP or dot1p application
DSCP Value	The DSCP name or value assigned to the application; if you assign a value to the application (0 to 63), the DSCP name that maps to the value is displayed
Default DSCP Value	The default DSCP value
Dot1p Value	The dot1p priority assigned to the application (applies only to ARP and IS-IS)
Default Dot1p Value	The default dot1p value

dscp-map

- Syntax** **dscp-map** [*dscp-name*]
- Context** show>router>sgt-qos
- Description** This command displays the DSCP-to-FC mappings.
- Parameters** *dscp-name* — the specified DSCP name. [Table 22](#) lists the valid DSCP names.
- Output** The following output is an example of DSCP-to-FC mapping information, and [Table 26](#) describes the fields.

Sample Output

```
A:ALU-1# show router sgt-qos dscp-map
```

```
=====
```

```
DSCP to FC Mappings
```

```
=====
```

DSCP Value	FC Value	Default FC Value
be	nc	nc
cp1	be	be
cp2	be	be
cp3	be	be
cp4	be	be
cp5	be	be
cp6	be	be
cp7	be	be
cs1	be	be
cp9	be	be
af11	af	af
cp11	be	be
af12	af	af
cp13	be	be
af13	af	af
cp15	be	be
cs2	be	be
cp17	be	be
af21	l1	l1
cp19	be	be
af22	l1	l1
cp21	be	be
af23	l1	l1
cp23	be	be
cs3	be	be
cp25	be	be
af31	l1	l1
cp27	be	be
af32	l1	l1
cp29	be	be
af33	l1	l1
cp31	be	be
cs4	be	be
cp33	be	be
af41	nc	nc
cp35	be	be
af42	af	h2
cp37	be	be
af43	h2	h2
cp39	be	be
cs5	be	be
cp41	be	be
cp42	be	be
cp43	be	be
cp44	be	be
cp45	be	be
ef	ef	ef
cp47	be	be
nc1	nc	nc
cp49	be	be
cp50	h2	h2

```

cp51          be          be
cp52          be          be
cp53          be          be
cp54          be          be
cp55          be          be
nc2           nc          nc
cp57          be          be
cp58          be          be
cp59          be          be
cp60          be          be
cp61          be          be
cp62          be          be
cp63          be          be
=====
A:ALU-1#

```

Table 26: DSCP-to-FC Mapping Output Fields

Label	Description
DSCP Value	The DSCP values (displayed as names) of the self-generated traffic
FC Value	The FC value mapped to each DSCP value
Default FC Value	The default FC value

Network Queue QoS Policies

In This Chapter

This chapter provides information to configure network queue QoS policies using the command line interface.

Topics in this chapter include:

- [Overview on page 142](#)
- [Basic Configuration on page 143](#)
 - [Creating a Network Queue QoS Policy on page 143](#)
 - [Applying Network Queue Policies on page 145](#)
- [Service Management Tasks on page 152](#)
 - [Deleting QoS Policies on page 152](#)
 - [Copying and Overwriting QoS Policies on page 152](#)
 - [Editing QoS Policies on page 154](#)
- [Network Queue QoS Policy Command Reference on page 155](#)

Overview

Network queue policies define the network queuing characteristics on the network adapter cards.

There is one default network queue policy. Each policy can have up to 16 ingress queues (8 unicast and 8 multipoint). The default policies cannot be deleted but can be copied and the copy can be modified. The default policies are identified as `network-queue "default"`.

Default network queue policies are applied to adapter card network ingress ports. You must explicitly create and then associate other network queue QoS policies.

For information about the tasks and commands necessary to access the command line interface and to configure and maintain the 7705 SAR, refer to the 7705 SAR OS Basic System Configuration Guide, “CLI Usage”.

Basic Configuration

A basic network queue QoS policy must conform to the following rules.

- Each network queue QoS policy must have a unique policy name.
- Queue parameters can be modified, but not deleted.

Creating a Network Queue QoS Policy

Configuring and applying QoS policies other than the default policy is optional. A default network queue policy is applied to network ingress and network egress ports.

Perform the following when creating a network queue policy.

- Enter a network queue policy name. The system does not dynamically assign a name.
- Include a description. The description provides a brief overview of policy features.
- Assign a forwarding class. You can assign a forwarding class to a specific queue after the queue has been created.

By default, all network queue policies are created with queue 1 and (multipoint) queue 9 applied to the policy. Similarly, when an FC is created within a network queue policy, the default unicast queue 1 and multicast queue 9 are assigned to the FC. The `multipoint` keyword applies to queues 9 to 16.

Use the following CLI syntax to create a network queue QoS policy.

CLI Syntax:

```
config>qos
    network-queue policy-name
        description description-string
        fc fc-name
            multicast-queue queue-id
            queue queue-id
        queue queue-id [multipoint] [queue-type]
            adaptation-rule [pir adaptation-rule] [cir
                adaptation-rule]
            cbs percent
            high-prio-only percent
            mbs percent
            rate percent[cir percent]
            slope-policy name
```

The following example creates a unicast and a multipoint network queue policy.

Example:

```
ALU-1# config>qos# network-queue NQ1 create
config>qos>network-queue$ description "NetQueue1"
config>qos>network-queue$ fc be create
config>qos>network-queue>fc$ exit
config>qos>network-queue# queue 10 multipoint create
config>qos>network-queue>queue# exit
config>qos>network-queue$ fc h1 create
config>qos>network-queue>fc$ multicast-queue 10
config>qos>network-queue>fc$ exit
config>qos>network-queue# exit
config>qos# exit
ALU-1#
```

The following sample output displays the configuration for NQ1.

```
ALU-1>config>qos# network-queue NQ1
ALU-1>config>qos>network-queue# info detail
-----
description "NetQueue1"
queue 1 auto-expedite create
    no avg-frame-overhead
    rate 100 cir 0
    adaptation-rule pir closest cir closest
    mbs 5
    cbs 0.10
    high-prio-only 10
    slope-policy "default"
exit
queue 9 multipoint auto-expedite create
    no avg-frame-overhead
    rate 100 cir 0
    adaptation-rule pir closest cir closest
    mbs 5
    cbs 0.10
    high-prio-only 10
    slope-policy "default"
exit
queue 10 multipoint auto-expedite create
    no avg-frame-overhead
    rate 100 cir 0
    adaptation-rule pir closest cir closest
    mbs 5
    cbs 0.10
    high-prio-only 10
    slope-policy "default"
exit
fc be create
    multicast-queue 9
    queue 1
exit
fc h1 create
    multicast-queue 10
    queue 1
exit
-----
ALU-1>config>qos>network-queue#
```


Applying Network Queue Policies

Apply network queue policies to the following entities:

- [Adapter Cards](#)
- [Network Ports](#)

Adapter Cards

Use the following CLI syntax to apply a network queue policy to an adapter card network ingress port.

CLI Syntax:

```
config>card
      mda mda-slot
      network
      ingress
      queue-policy name
```

Example:

```
ALU-1# configure card 1
config>card# mda 1
config>card>mda# network
config>card>mda>network# ingress
config>card>mda>network>ingress# queue-policy NQ1
config>card>mda>network>ingress# exit
config>card>mda>network# exit
config>card>mda# exit
config>card# exit
ALU-1#
```

The following sample output displays network ingress queue policy NQ1 applied to the adapter cards.

```
A:ALU-1# configure card 1
*A:ALU-1>config>card# info
-----
card-type iom-sar
mda 1
  mda-type a16-chds1
  network
    ingress
      queue-policy "NQ1"
    exit
  exit
exit
mda 2
  mda-type a8-eth
  network
    ingress
      queue-policy "NQ1"
```

```
        exit
    exit
exit
mda 3
    mda-type a8-eth
    network
        ingress
            queue-policy "NQ1"
        exit
    exit
exit
mda 4
    mda-type a16-chds1
    network
        ingress
            queue-policy "NQ1"
        exit
    exit
exit
exit
-----
*A:ALU-1>config>card#
```

Network Ports

Use the following CLI syntax to apply network queue policy NQ1 to a network port.

CLI Syntax:

```
config>port#
    ethernet
        network
            queue-policy name
```

Example:

```
ALU-1# config# port 1/1/1
config>port# ethernet
config>port>ethernet# network
config>port>ethernet>network# queue-policy NQ1
config>port>ethernet>network# exit
ALU-1#
```

The following sample output displays a network port configuration.

```
*A:ALU-1>config>port# info
-----
    ethernet
        network
            queue-policy "NQ1"
        exit
    exit
    no shutdown
-----
*A:ALU-1>config>port#
```

Default Network Queue Policy Values

The default network queue policies are identified as `policy-id default`. The default policies cannot be modified or deleted. [Table 27](#) displays default policy parameters.

Table 27: Default Network Queue Policy Definition

Forwarding Class	Queue	Definition	Queue	Definition
Network-Control (nc)	8	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%	16	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.1% High-Prio-Only = 10%
High-1 (h1)	7	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%	15	Rate = 100% CIR = 10% MBS = 2.5% CBS = 0.1% High-Prio-Only = 10%
Expedited (ef)	6	Rate = 100% CIR = 100% MBS = 5% CBS = 0.75% High-Prio-Only = 10%	14	Rate = 100% CIR = 100% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
High-2 (h2)	5	Rate = 100% CIR = 100% MBS = 5% CBS = 0.75% High-Prio-Only = 10%	13	Rate = 100% CIR = 100% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
Low-1 (l1)	4	Rate = 100% CIR = 25% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%	12	Rate = 100% CIR = 5% MBS = 2.5% CBS = 0.25% High-Prio-Only = 10%

Table 27: Default Network Queue Policy Definition (Continued)

Forwarding Class	Queue	Definition	Queue	Definition
Assured (af)	3	Rate = 100% CIR = 25% MBS = 5% CBS = 0.75% High-Prio-Only = 10%	11	Rate = 100% CIR = 5% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
Low-2 (l2)	2	Rate = 100% CIR = 25% MBS = 5% CBS = 0.25% High-Prio-Only = 10%	10	Rate = 100% CIR = 5% MBS = 5% CBS = 0.1% High-Prio-Only = 10%
Best Effort (be)	1	Rate = 100% CIR = 0% MBS = 5% CBS = 0.1% High-Prio-Only = 10%	9	Rate = 100% CIR = 0% MBS = 5% CBS = 0.1% High-Prio-Only = 10%

The following sample output displays the network queue policy default configuration.

```

ALU-1>config>qos>network-queue# info detail
-----
description "Default network queue QoS policy."
queue 1 auto-expedite create
  no avg-frame-overhead
  rate 100 cir 0
  adaptation-rule pir closest cir closest
  mbs 5
  cbs 0.10
  high-prio-only 10
  slope-policy "default"
exit
queue 2 auto-expedite create
  no avg-frame-overhead
  rate 100 cir 25
  adaptation-rule pir closest cir closest
  mbs 5
  cbs 0.25
  high-prio-only 10
  slope-policy "default"
exit
queue 3 auto-expedite create
  no avg-frame-overhead
  rate 100 cir 25
  adaptation-rule pir closest cir closest
  mbs 5

```

```

        cbs 0.75
        high-prio-only 10
        slope-policy "default"
    exit
queue 4 auto-expedite create
    no avg-frame-overhead
    rate 100 cir 25
    adaptation-rule pir closest cir closest
    mbs 2.5
    cbs 0.25
    high-prio-only 10
    slope-policy "default"
exit
queue 5 auto-expedite create
    no avg-frame-overhead
    rate 100 cir 100
    adaptation-rule pir closest cir closest
    mbs 5
    cbs 0.75
    high-prio-only 10
    slope-policy "default"
exit
queue 6 auto-expedite create
    no avg-frame-overhead
    rate 100 cir 100
    adaptation-rule pir closest cir closest
    mbs 5
    cbs 0.75
    high-prio-only 10
    slope-policy "default"
exit
queue 7 auto-expedite create
    no avg-frame-overhead
    rate 100 cir 10
    adaptation-rule pir closest cir closest
    mbs 2.5
    cbs 0.25
    high-prio-only 10
    slope-policy "default"
exit
queue 8 auto-expedite create
    no avg-frame-overhead
    rate 100 cir 10
    adaptation-rule pir closest cir closest
    mbs 2.5
    cbs 0.25
    high-prio-only 10
    slope-policy "default"
exit
queue 9 multipoint auto-expedite create
    no avg-frame-overhead
    rate 100 cir 0
    adaptation-rule pir closest cir closest
    mbs 5
    cbs 0.10
    high-prio-only 10
    slope-policy "default"
exit
queue 10 multipoint auto-expedite create

```

```
no avg-frame-overhead
rate 100 cir 5
adaptation-rule pir closest cir closest
mbs 5
cbs 0.10
high-prio-only 10
slope-policy "default"
exit
queue 11 multipoint auto-expedite create
no avg-frame-overhead
rate 100 cir 5
adaptation-rule pir closest cir closest
mbs 5
cbs 0.10
high-prio-only 10
slope-policy "default"
exit
queue 12 multipoint auto-expedite create
no avg-frame-overhead
rate 100 cir 5
adaptation-rule pir closest cir closest
mbs 2.5
cbs 0.25
high-prio-only 10
slope-policy "default"
exit
queue 13 multipoint auto-expedite create
no avg-frame-overhead
rate 100 cir 100
adaptation-rule pir closest cir closest
mbs 5
cbs 0.10
high-prio-only 10
slope-policy "default"
exit
queue 14 multipoint auto-expedite create
no avg-frame-overhead
rate 100 cir 100
adaptation-rule pir closest cir closest
mbs 5
cbs 0.10
high-prio-only 10
slope-policy "default"
exit
queue 15 multipoint auto-expedite create
no avg-frame-overhead
rate 100 cir 10
adaptation-rule pir closest cir closest
mbs 2.5
cbs 0.10
high-prio-only 10
slope-policy "default"
exit
queue 16 multipoint auto-expedite create
no avg-frame-overhead
rate 100 cir 10
adaptation-rule pir closest cir closest
mbs 2.5
cbs 0.10
```

```
        high-prio-only 10
        slope-policy "default"
exit
fc af create
    multicast-queue 11
    queue 3
exit
fc be create
    multicast-queue 9
    queue 1
exit
fc ef create
    multicast-queue 14
    queue 6
exit
fc h1 create
    multicast-queue 15
    queue 7
exit
fc h2 create
    multicast-queue 13
    queue 5
exit
fc l1 create
    multicast-queue 12
    queue 4
exit
fc l2 create
    multicast-queue 10
    queue 2
exit
fc nc create
    multicast-queue 16
    queue 8
```

Service Management Tasks

This section describes the following service management tasks:

- [Deleting QoS Policies](#)
- [Copying and Overwriting QoS Policies](#)
- [Editing QoS Policies](#)

Deleting QoS Policies

A network queue policy is associated by default with adapter card network ingress ports. You can replace the default policy with a customer-configured policy, but you cannot entirely remove a QoS policy. When you remove a QoS policy, the policy association reverts to the default network-queue policy **default**.

Use the following CLI syntax to delete a network queue policy.

CLI Syntax: `config>qos# no network-queue policy-name`

Example: `config>qos# no network-queue NQ1`

Copying and Overwriting QoS Policies

You can copy an existing network queue policy, rename it with a new policy ID name, or overwrite an existing network queue policy. The `overwrite` option must be specified or an error occurs if the destination policy ID exists.

Use the following CLI syntax to overwrite an existing network queue policy.

CLI Syntax: `config>qos# copy network-queue source-policy-id
dest-policy-id [overwrite]`

Example: `A:ALU-1>config>qos# copy network-queue NQ1 NQ2 overwrite
config>qos# exit
*A:ALU-1#`

The following sample output displays the copied policies:

```
*A:ALU-1>config>qos# info
-----
#-----
echo "QoS Policy Configuration"
#-----

    network-queue "NQ1" create
        description "NetQueue1"
        queue 1 create
            rate 10
            mbs 5
            cbs 0.10
            high-prio-only 10
        exit
        queue 9 multipoint create
            rate 10
            mbs 5
            cbs 0.10
            high-prio-only 10
        exit
        fc be create
            multicast-queue 9
            queue 1
        exit
    exit
network-queue "NQ2" create
    description "NetQueue1"
    queue 1 create
        rate 10
        mbs 5
        cbs 0.10
        high-prio-only 10
    exit
    queue 9 multipoint create
        rate 10
        mbs 5
        cbs 0.10
        high-prio-only 10
    exit
    fc be create
        multicast-queue 9
        queue 1
    exit
exit
network-queue "nq1" create
    description "NetQ1"
    queue 1 create
        rate 10
        mbs 5
        cbs 0.10
        high-prio-only 10
    exit
    queue 9 multipoint create
        rate 10
        mbs 5
        cbs 0.10
        high-prio-only 10
    exit
exit
```

```
        fc be create
          multicast-queue 9
          queue 1
        exit
    exit
network-queue "nq3" create
  description "NetQ3"
  queue 1 create
    mbs 5
    cbs 0.10
    high-prio-only 10
  exit
  queue 9 multipoint create
    rate 10
    mbs 5
    cbs 0.10
    high-prio-only 10
  exit
  fc be create
    multicast-queue 9
    queue 1
  exit
exit
network-queue "netq2" create
Press any key to continue (Q to quit)
```

Editing QoS Policies

You can change existing policies, except the default policies, and entries in the CLI. The changes are applied immediately to all interfaces where the policy is applied. To prevent configuration errors, use the **copy** command to make a duplicate of the original policy to a work area, make the edits, and then overwrite the original policy.

Network Queue QoS Policy Command Reference

Command Hierarchies

- [Configuration Commands](#)
- [Operational Commands](#)
- [Show Commands](#)

Configuration Commands

```

config
  — qos
      — [no] network-queue policy-name [create]
          — description description-string
          — no description
          — [no] fc fc-name [create]
              — multicast-queue queue-id
              — no multicast-queue
              — queue queue-id
              — no queue
          — queue queue-id [multipoint] [queue-type] [create]
          — no queue queue-id
              — avg-frame-overhead percent
              — no avg-frame-overhead
              — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
              — no adaptation-rule
              — cbs percent
              — no cbs
              — high-prio-only percent
              — no high-prio-only
              — mbs percent
              — no mbs
              — rate percent [cir percent]
              — no rate
              — slope-policy name
              — no slope-policy

config
  — [no] port port-id
      — ethernet
          — egress-rate sub-rate
          — no egress-rate
          — network
              — scheduler-mode {profile | 4-priority}

```

Operational Commands

```
config
  — qos
    — copy network-queue src-name dst-name [overwrite]
```

Show Commands

```
show
  — qos
    — network-queue [network-queue-policy-name] [detail]
```

Command Descriptions

- [Configuration Commands on page 158](#)
- [Operational Commands on page 173](#)
- [Show Commands on page 174](#)

Configuration Commands

- [Generic Commands on page 159](#)
- [Network Queue QoS Policy Commands on page 160](#)
- [Network Queue QoS Policy Forwarding Class Commands on page 171](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>qos>network-queue config>qos>network config>qos>sap-egress config>qos>sap-ingress
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes any description string from the context.
Default	none
Parameters	<i>description-string</i> — a text string describing the entity. 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.

Network Queue QoS Policy Commands

network-queue

Syntax	[no] network-queue <i>policy-name</i> [create]
Context	config>qos
Description	<p>This command creates a context to configure a network queue policy. Network queue policies define the ingress and egress network queuing at the adapter card network node level.</p> <p>Network queue policies define ingress and egress network queues similar to a service ingress QoS policy.</p> <p>The no form of this command removes the network-queue policy from use. However, the network queue with <i>policy-name</i> default cannot be modified or deleted.</p>
Default	default
Parameters	<p><i>policy-name</i> — the name of the network queue policy</p> <p>Values Valid names consist of 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.</p> <p>create — keyword used to create a network queue policy</p>

queue

Syntax	queue <i>queue-id</i> multipoint [<i>queue-type</i>] [create] no queue <i>queue-id</i>
Context	config>qos>network-queue
Description	<p>This command creates the context to configure a QoS network-queue policy queue. Network queues are created with default queue 1 (non-multipoint) and queue 9 (multipoint) automatically assigned.</p> <p>The queue command with the multipoint keyword allows the creation of multipoint queues. Only multipoint queues can receive ingress packets that need flooding to multiple destinations. By separating the unicast traffic from multipoint traffic at network ingress and handling the traffic on separate multipoint queues, special handling of the multipoint traffic is possible. Each queue acts as an accounting and (optionally) shaping device, offering precise control over potentially expensive broadcast, multicast, and unknown unicast traffic. Only the back-end support of multipoint traffic (between the forwarding class and the queue based on forwarding type) needs to be defined. The individual classification rules used to place traffic into forwarding classes are not affected. Queues must be defined as multipoint at the time of creation within the policy.</p>

The multipoint queues are for multipoint-destined service traffic. Within non-multipoint services, such as Epipe services, all traffic is considered unicast due to the nature of the service type. Multicast and broadcast-destined traffic in an Epipe service will not be mapped to a multipoint service queue.

The **no** form of this command removes the forwarding class-to-queue mapping, causing the forwarding class to use the default queue instead. When a queue is removed, any pending accounting information for each network queue created due to the definition of the queue in the policy is discarded.

Parameters

queue-id — the queue identifier for the queue, expressed as an integer. The *queue-id* uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.

Values 1 to 8 (unicast)
 9 to 16 (multipoint)

Default 1 (unicast)
 9 (multipoint)

multipoint — specifies that this *queue-id* is for multipoint forwarded traffic only. This *queue-id* can only be explicitly mapped to the forwarding class broadcast, multicast, or unknown unicast (BMU) ingress traffic. If you attempt to map forwarding class unicast traffic to a queue designated as multipoint, an error is generated and no changes are made to the current unicast traffic queue mapping.

A queue that will be used for multipoint traffic must be created as multipoint. The multipoint designator cannot be defined after the queue is created. If an attempt is made to modify the command to include the multipoint keyword, an error is generated and the command will not execute.

The **multipoint** keyword can be entered in the command line on a pre-existing multipoint queue to edit *queue-id* parameters.

Values multipoint or not present

Default not present (the queue is created as a unicast queue)

queue-type — the **expedite**, **best-effort** and **auto-expedite** queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective. A keyword must be specified at the time the queue is created in the network-queue policy. If an attempt is made to change the keyword after the queue is initially defined, an error is generated.

expedite — the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue

best-effort — the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue

auto-expedite — the system auto-defines the way the queue is serviced by the hardware. When **auto-expedite** is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types *nc*, *ef*, *h1*, or *h2*. When a single non-expedited forwarding class is mapped to the queue (*be*, *af*, *11*, or *12*), the queue automatically falls back to non-expedited status.

Values expedite, best-effort, auto-expedite

Default auto-expedite

create — keyword used to create a network QoS policy

avg-frame-overhead

Syntax	avg-frame-overhead <i>percent</i> no avg-frame-overhead
Context	config>qos>network-queue>queue
Description	This command configures the average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire.

When calculating the frame encapsulation overhead for port scheduling purposes, the system determines the following values:

- offered-load — the offered-load of a queue is calculated by starting with the queue depth in octets, adding the received octets at the queue and subtracting queue discard octets. The result is the number of octets the queue has available to transmit. This is the packet-based offered-load.
- frame-encapsulation-overhead — using the **avg-frame-overhead** *percent* parameter, the frame-encapsulation-overhead is the queue's current offered-load (how much has been received by the queue) multiplied by the avg-frame-overhead. If a queue has an offered load of 10 000 octets and the **avg-frame-overhead** equals 10%, the frame-encapsulation-overhead would be $10\,000 \times 0.1$ or 1000 octets.
- frame-based offered-load — the frame-based offered-load is calculated by adding the offered-load to the frame-encapsulation-overhead. If the offered-load is 10 000 octets and the encapsulation-overhead is 1000 octets, the frame-based offered-load would equal 11 000 octets.
- packet-to-frame factor — the packet-to-frame factor is calculated by dividing the frame-encapsulation-overhead by the queue's offered-load (packet-based). If the frame-encapsulation-overhead is 1000 octets and the offered-load is 10 000 octets then the packet-to-frame factor would be $1000 / 10\,000$ or 0.1. When in use, the **avg-frame-overhead** will be the same as the packet-to-frame factor, making this calculation unnecessary.
- frame-based CIR — the frame-based CIR is calculated by multiplying the packet-to-frame factor with the queue's configured CIR and then adding that result to that CIR. If the queue CIR is set at 500 octets and the packet to frame factor equals 0.1, the frame-based CIR would be 500×1.1 or 550 octets.

- frame-based within-cir offered-load — the frame-based within-cir offered-load is the portion of the frame-based offered-load considered to be within the frame-based CIR. The frame-based within-cir offered-load is the lesser of the frame-based offered-load and the frame-based CIR. If the frame-based offered-load equaled 11 000 octets and the frame-based CIR equaled 550 octets, the frame-based within-cir offered-load would be limited to 550 octets. If the frame-based offered-load equaled 450 octets and the frame-based CIR equaled 550 octets, the frame-based within-cir offered-load would equal 450 octets (or the entire frame-based offered-load).

The **no** form of this command restores the average frame overhead parameter for the queue to the default value of 0%.

Default 0

Parameters *percent* — this parameter sets the average amount of packet-to-frame encapsulation overhead expected for the queue. This value is not used by the system for egress network queues.

Values 0.00 to 100.00

adaptation-rule

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

Context config>qos>network-queue>queue

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the queue 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 **adaptation-rule pir closest cir closest**

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

cir — defines the constraints enforced when adapting the CIR rate defined within the **queue** *queue-id* **rate** 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 adaptation rule to be used while computing the operational CIR or PIR value

Values

max — the **max** (maximum) option is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR or CIR for the queue will be equal to or less than the administrative rate specified using the **rate** command.

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

closest — the **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR or CIR for the queue will be the rate closest to the rate specified using the **rate** command.

cbs

Syntax	cbs percentage no cbs
Context	config>qos>network-queue>queue
Description	<p>This command specifies the relative amount of reserved buffers for a specific ingress network adapter card forwarding class queue or egress network port forwarding class queue. The value is entered as a percentage.</p> <p>The resultant CBS size can be larger than the MBS. This will result in a portion of the CBS for the queue to be unused and therefore should be avoided.</p> <p>The no form of this command returns the CBS size for the queue to the default for the forwarding class.</p>
Special Cases	<p>Forwarding Class Queue on Egress Network Ports or Bundles — the total reserved buffers based on the total percentages can exceed 100%. This might not be desirable and should be avoided as a rule of thumb. If the total percentage equals or exceeds 100% of the queue size, no buffers will be available in the shared portion of the pool. Any queue exceeding its CBS size will experience a hard drop on all packets until it drains below this threshold.</p> <p>Forwarding Class Queue on Ingress Adapter Cards — the total reserved buffers based on the total percentages can exceed 100%. This might not be desirable and should be avoided as a rule of thumb. If the total percentage equals or exceeds 100% of the queue size, no buffers will be available in the shared portion of the pool. Any queue exceeding its CBS size will experience a hard drop on all packets until it drains below this threshold.</p>
Default	Table 28 lists the cbs forwarding class defaults.

Table 28: CBS Forwarding Class Defaults

Forwarding Class	Forwarding Class Label	Unicast Queues		Multicast Queues	
		Queue ID	Default CBS (%)	Queue ID	Default CBS (%)
Network-Control	nc	8	0.25	16	0.1
High-1	h1	7	0.25	15	0.1
Expedited	ef	6	0.75	14	0.1
High-2	h2	5	0.75	13	0.1
Low-1	l1	4	0.25	12	0.1
Assured	af	3	0.75	11	0.1
Low-2	l2	2	0.25	10	0.1
Best-Effort	be	1	0.1	9	0.1

Parameters

percent — the percent of buffers reserved from the total queue space, expressed as a decimal integer.

If 10 Mbytes is the total buffer value in the queue, a value of 0.1 would reserve 1 Mbyte (10%) of buffer space for the forwarding class queue. The value 0 specifies that no reserved buffers are required by the queue (a minimal reserved size can be applied for scheduling purposes).

Values 0.00 to 100.00

high-prio-only

Syntax **high-prio-only** *percent*
no high-prio-only

Context config>qos>network-queue>queue

Description The **high-prio-only** command allows the reservation of queue buffers for use exclusively by in-profile packets as a default condition for access buffer queues for this network queue policy. For network queues, in-profile packets are high priority, and out-of-profile packets are low priority.



Note: When a low-priority (W)RED slope is enabled on a queue, the high-prio-only setting is not used. When that slope is disabled, then the high-prio-setting is used.

Modifying the current MBS for the queue through the **mbs** command will cause the default **high-prio-only** function to be recalculated and applied to the queue.

The **no** form of this command restores the default value.

Default Table 29 lists the **high-prio-only** forwarding class defaults.

Table 29: High-prio-only Forwarding Class Defaults

Forwarding Class	Forwarding Class Label	Unicast Queues		Multicast Queues	
		Queue ID	Default high-prio-only	Queue ID	Default high-prio-only
Network-Control	nc	8	10	16	10
High-1	h1	7	10	15	10
Expedited	ef	6	10	14	10
High-2	h2	5	10	13	10
Low-1	l1	4	10	12	10
Assured	af	3	10	11	10
Low-2	l2	2	10	10	10
Best-Effort	be	1	10	9	10

Parameters *percent* — the amount of queue buffer space reserved for in-profile packets, expressed as a decimal percentage

Values 0 to 100 | default

mbs

Syntax **mbs** *percent*
no mbs

Context config>qos>network-queue>queue

Description This command specifies the relative amount of the queue space for the maximum buffers for a specific ingress network adapter card forwarding class queue or egress network port forwarding class queue. The value is entered as a percentage.

The Maximum Burst Size (MBS) value is used by a queue to determine whether it has exhausted its total allowed buffers while enqueueing packets. Once the queue has exceeded its maximum amount of buffers, all packets are discarded until the queue transmits a packet. A queue that has not exceeded its MBS size is not guaranteed that a buffer will be available when needed or that the packet's RED/WRED slope will not force the discard of the packet. Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED/WRED slope parameters for the needs of the network queues.

The MBS size can sometimes be smaller than the CBS. This will result in a portion of the CBS for the queue to be unused and should be avoided.

The **no** form of this command returns the MBS size for the queue to the default for the forwarding class.

Special Cases **Forwarding Class Queue on Egress Network Ports or Bundles** — the total MBS settings for all network egress queues on the port or channel based on the total percentages can exceed 100%. Some oversubscription can be desirable to allow exceptionally busy forwarding classes more access to buffer space. The proper use of CBS settings will ensure that oversubscribing MBS settings will not starve other queues of buffers when needed.

Forwarding Class Queue on Ingress Adapter Cards — the **mbs** value is used to calculate the queue's MBS size based on the total amount of buffer space allocated to the network ingress queue on the adapter card.

The total MBS settings for all network egress queues on the port or channel based on the total percentages can exceed 100%. Some oversubscription can be desirable to allow exceptionally busy forwarding classes more access to buffer space. The proper use of CBS settings will ensure that oversubscribing MBS settings will not starve other queues of buffers when needed.

Default [Table 30](#) lists the **mbs** forwarding class defaults.

Table 30: MBS Forwarding Class Defaults

Forwarding Class	Forwarding Class Label	Unicast Queue		Multicast Queue	
		Queue ID	Default MBS	Queue ID	Default MBS
Network-Control	nc	8	2.5	16	2.5
High-1	h1	7	2.5	15	2.5
Expedited	ef	6	5	14	5
High-2	h2	5	5	13	5
Low-1	l1	4	2.5	12	2.5
Assured	af	3	5	11	5
Low-2	l2	2	5	10	5
Best-Effort	be	1	5	9	5

Parameters *percent* — the percent of buffers from the total queue space allowed for the maximum amount of buffers, expressed as a decimal percentage

Values 0 to 100

rate

Syntax	rate [<i>percent</i>] [<i>cir percent</i>] no rate
Context	config>qos>network-queue>queue
Description	<p>This command defines the administrative Peak Information Rate (PIR) and the administrative Committed Information Rate (CIR) parameters for the queue. Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.</p> <p>The CIR defines the percentage at which the system prioritizes the queue over other queues competing for the same bandwidth.</p> <p>The rate command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the SAP ingress or SAP egress QoS policy with the <i>queue-id</i>.</p> <p>The no form of the command returns all queues created with the <i>queue-id</i> by association with the QoS policy to the default PIR and CIR parameters (100, 0).</p>
Parameters	<p><i>percent</i> — defines the percentage of the maximum rate allowed 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 100 is assumed. Fractional values are not allowed and must be given as a positive integer.</p> <p>The actual PIR rate is dependent on the queue's adaptation-rule parameters and the actual hardware where the queue is provisioned.</p> <p>Values 1 to 100</p> <p>Default 100</p> <p><i>cir percent</i> — defines the percentage of the maximum rate allowed for 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.</p> <p>Values 0 to 100</p> <p>Default 0</p>

slope-policy

Syntax	slope-policy <i>name</i> no slope-policy
Context	config>qos>network-queue>queue
Description	This command specifies the name of slope policy associated with the network queue.
Parameters	<i>name</i> — specifies the name for the slope policy
Values	Valid names consist of 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.
Default	default

egress-rate

Syntax	egress-rate <i>sub-rate</i> no egress-rate
Context	config>port>ethernet
Description	This command configures the rate of traffic leaving the network. The no form of this command returns the value to the default.
Default	no egress-rate
Parameters	<i>sub-rate</i> — the egress rate in kb/s
Values	1 to 10000000

scheduler-mode

Syntax	scheduler-mode { profile 4-priority }
Context	config>port>ethernet>network
Description	This command selects the network side scheduling option for the 8-port Ethernet Adapter card. With profiled (or rate-based) scheduling, both in-profile and out-of-profile scheduling are supported. Packets with a flow rate that is less than or equal to the CIR value of a queue are scheduled as in-profile. Packets with a flow rate that exceeds the CIR value, but is less than the PIR value, of a queue are scheduled as out-of-profile. In-profile traffic has strict priority over out-of-profile traffic.

Profiled scheduling does not take queue type into consideration. With queue type-based scheduling, queues are divided into two categories – those that are serviced by the Expedited scheduler and those that are serviced by the Best-Effort scheduler. The Expedited scheduler has precedence over the Best-Effort scheduler.

Four-priority scheduling combines both profiled and queue type-based scheduling. The combination provides four scheduling priorities. Packets are scheduled in the following order, in strict priority fashion:

- Expedited in-profile packets
- Best-effort in-profile packets
- Expedited out-of-profile packets
- Best-effort out-of-profile packets

Default **profile**

Network Queue QoS Policy Forwarding Class Commands

fc

Syntax	[no] fc <i>fc-name</i> [create]
Context	config>qos>network-queue
Description	<p>The fc is created with default unicast <i>queue-id</i> 1 and default multicast <i>queue-id</i> 9 automatically configured. The specified queues contain the PIR, CIR, CBS, and MBS configurations.</p> <p>Use the multicast-queue and queue commands to change the fc to <i>queue-id</i> assignments from their default queue assignments.</p> <p>The no form of this command restores the default queue.</p>
Parameters	<p><i>fc-name</i> — the forwarding class name for which the contained PIR, CIR, CBS, and MBS queue attributes apply. An instance of fc is allowed for each <i>fc-name</i>.</p> <p>Values be, l2, af, l1, h2, ef, h1, nc</p> <p>create — keyword used to create a forwarding class policy</p>

multicast-queue

Syntax	multicast-queue <i>queue-id</i> no multicast-queue
Context	config>qos>network-queue>fc
Description	<p>This command overrides the default multicast forwarding type queue mapping for fc <i>fc-name</i>. The specified <i>queue-id</i> must exist within the policy as a multipoint queue before the mapping can be made. Once the forwarding class mapping is executed, all multicast traffic at network ingress using this policy is forwarded using the <i>queue-id</i>. Use the queue <i>queue-id</i> multipoint command to create the specified <i>queue-id</i>.</p> <p>The multicast forwarding type includes the unknown forwarding type and the broadcast forwarding type unless each is explicitly assigned to a different multipoint queue. When the unknown and broadcast forwarding types are left as default, they will track the defined queue for the multicast forwarding type.</p> <p>The no form of the command sets the multicast forwarding type <i>queue-id</i> back to the default queue (queue 9).</p>
Parameters	<p><i>queue-id</i> — an existing multipoint queue defined in the config>qos>network-queue context.</p> <p>Values 9 to 16</p> <p>Default 9</p>

queue

Syntax	queue <i>queue-id</i> no queue				
Context	config>qos>network-queue>fc				
Description	<p>This command creates the context to configure forwarding-class-to-queue mappings.</p> <p>The no form of this command removes the <i>queue-id</i> from the network-queue policy and from any existing network ingress or network egress ports using the policy, and sets the <i>queue-id</i> back to the default queue (queue 1).</p>				
Parameters	<p><i>queue-id</i> — the queue identifier for the queue, expressed as an integer. The <i>queue-id</i> uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.</p> <table><tr><td>Values</td><td>1 to 8</td></tr><tr><td>Default</td><td>1</td></tr></table>	Values	1 to 8	Default	1
Values	1 to 8				
Default	1				

Operational Commands

copy

Syntax	copy network-queue <i>src-name dst-name</i> [overwrite]
Context	config>qos
Description	<p>This command copies or overwrites existing network queue QoS policies to another network queue policy ID.</p> <p>The copy command is a configuration level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the overwrite keyword.</p>
Parameters	<p>network-queue <i>src-name dst-name</i> — indicates that the source policy ID and the destination policy ID are network-queue policy IDs. Specify the source policy ID that the copy command will attempt to copy from and specify the destination policy ID to which the command will copy a duplicate of the policy.</p> <p>overwrite — specifies that the existing destination policy is to be replaced. Everything in the existing destination policy will be overwritten with the contents of the source policy. If overwrite is not specified, a message is generated saying that the destination policy ID exists.</p> <pre>SAR12>config>qos# copy network-queue nq1 nq2 MINOR: CLI Destination "nq2" exists - use {overwrite}. SAR12>config>qos# copy network-queue nq1 nq2 overwrite</pre>

Show Commands

network-queue

Syntax	network-queue [<i>network-queue-policy-name</i>] [detail]
Description	This command displays network queue policy information. This includes queue parameters information, forwarding class-to-queue mappings, and network port/adapter card queue associations.
Context	show>qos
Parameters	<i>network-queue-policy-name</i> — the name of the network queue policy <div style="margin-left: 40px;"> Values Valid names consist of 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. detail — displays detailed network queue information </div>
Output	The following output is an example of network queue policy information, and Table 31 describes the fields.

Sample Output

```

ALU-1>show>qos# network-queue policy102

=====
QoS Network Queue Policy
=====
-----
Network Queue Policy (policy102)
-----
Policy           : policy102
Description      : (Not Specified)
-----
Associations
-----
No Matching Entries
=====

```

```
ALU-1>show>qos# network-queue policy102 detail
```

```
=====
QoS Network Queue Policy
=====
```

```
-----
Network Queue Policy (policy102)
-----
```

```
Policy      : policy102
Description  : (Not Specified)
```

```
-----
Queue CIR      PIR      CBS      MBS      HiPrio AvgOvrhd Slope-Policy
   CIR Rule    PIR Rule
-----
1      0      100      def      def      10      0.00      default
      closest closest
2      0      100      def      def      def      0.00      default
      closest closest
9      0      100      def      def      10      0.00      default
      closest closest
10     0      100      def      def      def      0.00      default
      closest closest
-----
```

```
-----
FC      UCastQ      MCastQ
-----
h2      1          9
h1      1          9
-----
```

```
-----
Associations
-----
```

```
No Matching Entries
```

```
=====
ALU-1>show>qos#
```

Table 31: Network Queue Policy Command Output

Label	Description
Policy	The policy name that uniquely identifies the policy
Description	A text string that helps identify the policy's context in the configuration file
Queue	The queue ID
CIR	The committed information rate

Table 31: Network Queue Policy Command Output (Continued)

Label	Description
CIR Rule	min - the operational CIR for the queue will be equal to or greater than the administrative rate specified using the rate command except where the derived operational CIR is greater than the operational PIR. If the derived operational CIR is greater than the derived operational PIR, the operational CIR will be made equal to the operational PIR.
	max - the operational CIR for the queue will be equal to or less than the administrative rate specified using the rate command
	closest - the operational CIR for the queue will be the rate closest to the rate specified using the rate command without exceeding the operational PIR
PIR	The peak information rate
PIR Rule	min - the operational PIR for the queue will be equal to or greater than the administrative rate specified using the rate command
	max - the operational PIR for the queue will be equal to or less than the administrative rate specified using the rate command
	closest - the operational PIR for the queue will be the rate closest to the rate specified using the rate command
CBS	The committed burst size
MBS	The maximum burst size
HiPrio	The high-priority value
AvgOvrhd	The average percentage that the offered load to a queue will expand during the frame encapsulation process before sending traffic on-the-wire
Slope-Policy	The slope policy for the queue
FC	The value of a predefined forwarding class
UCastQ	The specific unicast queue to be used for packets in the forwarding class
MCastQ	The specific multicast queue to be used for packets in the forwarding class
Associations	The unique service and customer identifiers

Service Egress and Ingress QoS Policies

In This Chapter

This chapter provides information to configure service egress and ingress QoS policies using the command line interface.

Topics in this chapter include:

- [Overview on page 178](#)
- [Basic Configuration on page 179](#)
 - [Creating Service Egress and Ingress QoS Policies on page 179](#)
 - [Default Service Egress and Ingress Policy Values on page 192](#)
- [Service Management Tasks on page 195](#)
 - [Deleting QoS Policies on page 195](#)
 - [Copying and Overwriting QoS Policies on page 197](#)
 - [Editing QoS Policies on page 198](#)
- [Service Egress and Ingress QoS Policy Command Reference on page 199](#)

Overview

There is one default policy for service ingress and one default policy for service egress and MC-MLPPP SAP egress. Each policy can have up to eight ingress queues and eight egress queues per service. The default policies can be copied and modified but they cannot be deleted. The default policies are identified as policy ID 1.



Note: Throughout this guide, the terms service ingress/egress and access ingress/egress are interchangeable. This section ([Service Egress and Ingress QoS Policies](#)) uses the term service ingress/egress.

The eight ingress queues can be designated as a unicast, broadcast, multicast, or unknown queue for the purposes of FC-to-queue mapping.

The default policies are applied to the appropriate interface, by default. For example, the default service ingress policy is applied to access ingress SAPs. The default service egress policy is applied to access egress SAPs and MC-MLPPP egress SAPs. You must explicitly associate other QoS policies.

For information about the tasks and commands necessary to access the command line interface and to configure and maintain the 7705 SAR, refer to the 7705 SAR OS Basic System Configuration Guide, “CLI Usage”.

Basic Configuration

A basic service egress QoS policy must conform to the following:

- have a unique service egress QoS policy ID
- have a QoS policy scope of template or exclusive
- have at least one defined default queue

A basic service ingress QoS policy must conform to the following:

- have a unique service ingress QoS policy ID
- have a QoS policy scope of template or exclusive
- have at least one default unicast forwarding class queue

Creating Service Egress and Ingress QoS Policies

Configuring and applying QoS policies is optional. If no QoS policy is explicitly applied to a SAP or IP interface, a default QoS policy is applied. Perform the following to configure a QoS policy:

- [Creating a Service Egress QoS Policy](#)
- [Creating a Service Ingress QoS Policy](#)
- [Creating an MC-MLPPP SAP Egress QoS Policy](#)
- [Applying Service Egress and Ingress Policies](#)

Creating a Service Egress QoS Policy

Define the following attributes to create a service egress policy:

- a unique policy ID value — the system does not dynamically assign a value
- a default queue for the service egress policy
- the scope — the service egress policy must be defined as having either an *exclusive* scope for one-time use or a *template* scope that enables its use with multiple SAPs

After the policy is created, the policy's behavior can be defined.

Use the following CLI syntax to create a service egress QoS policy:

CLI Syntax:

```
config>qos
      sap-egress policy-id
        description description-string
        queue queue-id [queue-type]
        scope {exclusive|template}
```

Example:

```
*A:ALU-1>configure qos sap-egress 600 create
config>qos>sap-egress$ fc be create
config>qos>sap-egress>fc$ exit
config>qos>sap-egress$ queue 2 expedite create
config>qos>sap-egress>queue$ exit
config>qos>sap-egress# scope exclusive
config>qos>sap-egress# exit
*A:ALU-1#
```

The following sample output displays the service egress policy 600 configuration:

```
*A:ALU-1 config>qos# info
-----
#-----
echo "QoS Policy Configuration"
#-----
...
      sap-egress 600 create
        scope exclusive
        queue 1 create
        exit
        queue 2 expedite create
        exit
        fc be create
        exit
      exit
-----
*A:ALU-1
```

Creating a Service Egress QoS Forwarding Class

Define the following attributes to create a service egress forwarding class:

- the egress dot1p priority bits value
- the DSCP name and DSCP priority bits mapping

Optionally, you can enter a *queue-id* value to override the default forwarding class-to-queue mapping for the egress policy.

Use the following CLI syntax to create a service egress forwarding class:

CLI Syntax:

```
config>qos
    sap-egress policy-id
        fc fc-name
            dscp dscp-name
            dscp in-profile dscp-name out-profile dscp-name
            dot1p dot1p-value
            dot1p in-profile dot1p-value out-profile
            dot1p-value
            queue queue-id
```

Example:

```
*A:ALU-1>config>qos# sap-egress 600 fc be create
config>qos>sap-egress>fc# dscp cp1
config>qos>sap-egress>fc# dot1p in-profile 2 out-profile 3
config>qos>sap-egress>fc# exit
config>qos# exit
*A:ALU-1#
```

The following sample output displays the forwarding class configuration for service egress policy 600:

```
*A:ALU-1>config>qos# info
-----
#-----
echo "QoS Policy Configuration"
#-----
....
    sap-egress 600 create
        scope exclusive
        queue 1 create
        exit
        queue 2 expedite create
        exit
        fc be create
            dot1p in-profile 2 out-profile 3
            dscp cp1
        exit
    exit
-----
*A: ALU-1
```

Creating a Service Egress QoS Queue

Define the following attributes to create a service egress queue:

- **adaptation-rule** —the method used by the system to derive the PIR and CIR for the queue
- **cbs** — overrides the reserved buffers default for the queue
- **high-prio-only** — the percentage of buffer space for the queue to be used exclusively by in-profile packets
- **mbs** — the maximum amount of buffers allowed for a specific queue
- **rate** — the PIR and CIR values for the queue
- **slope-policy** — the slope policy for the queue

Use the following CLI syntax to configure the service egress QoS queue parameters:

CLI Syntax:

```
config>qos
      sap-egress policy-id
        queue queue-id [queue-type]
          adaptation-rule [pir adaptation-rule]
            [cir adaptation-rule]
          cbs size-in-kbytes
          high-prio-only percent
          mbs size-in-kbytes
          rate pir-rate [cir cir-rate]
          slope-policy name
```

Example:

```
*A:ALU-1# configure qos sap-egress 500
config>qos>sap-egress# queue 7
config>qos>sap-egress>queue# adaptation-rule pir closest
cir closest
config>qos>sap-egress>queue# cbs 10
config>qos>sap-egress>queue# high-prio-only 10
config>qos>sap-egress>queue# mbs 10
config>qos>sap-egress>queue# rate max cir max
config>qos>sap-egress>queue# slope-policy "Slope Policy"
config>qos>sap-egress>queue# exit
config>qos>sap-egress# exit
*A:ALU-1#
```

The following sample output displays the queue configuration for service egress policy 500:

```
ALU-1>config>qos# info
-----
#-----
echo "QoS Policy Configuration"
#-----
....
    sap-egress 500 create
        description "Egress Policy 500"
        queue 1 create
        exit
        queue 7 best-effort create
            rate max cir max
            cbs 10
            mbs 10
            high-prio-only 10
        exit
        fc be create
        exit
        fc ef create
            dscp in-profile cp2 out-profile cp3
        exit
```

Creating a Service Ingress QoS Policy

To create an service ingress policy, define the following:

- a policy ID value — the system does not dynamically assign a value
- a description — provides a brief overview of policy features
- a default forwarding class for the policy — all packets received on an ingress SAP using this ingress QoS policy will be classified to the default forwarding class
- a default priority for all packets received on an ingress SAP using this policy
- the dot1p parameters — this configuration creates a mapping between the dot1p bits of the ingress traffic and the forwarding class
- the DSCP parameters — this configuration creates a mapping between the DSCP of the ingress traffic and the forwarding class
- the forwarding class parameters — overrides the default forwarding class for the policy by assigning the forwarding class to one or more of the following queue designations: broadcast-queue, multicast-queue, unknown-queue, or (unicast) queue (see [Defining a Service Ingress Forwarding Class](#))

A service ingress policy is created with a template scope. The scope can be modified to exclusive for a special one-time use policy. Otherwise, the template scope enables the policy to be applied to multiple SAPs.

Use the following CLI syntax to create a service ingress QoS policy:

CLI Syntax:

```
config>qos
    sap-ingress policy-id
        description description-string
        default-fc fc-name
        default-priority {low|high}
        dot1p dot1p-priority fc fc-name priority
            {high|low}
        dscp dscp-name fc fc-name priority {high|low}
```

Example:

```
*A:ALU-1>config>qos#
config>qos# sap-ingress 100 create
config>qos>sap-ingress$ description "Used on VPN SAP"
config>qos>sap-ingress$ default-fc be
config>qos>sap-ingress$ default-priority low
config>qos>sap-ingress$ dot1p 1 fc be priority low
config>qos>sap-ingress$ dscp be fc be priority low
config>qos>sap-ingress$ exit
config>qos# exit
*A:ALU-1#
```

The following sample output displays the configuration for service ingress policy 100:

```
ALU-1>config>qos# info
#-----
echo "QoS Policy Configuration"
#-----
....
    sap-ingress 100 create
        description "Used on VPN SAP"
        queue 1 priority-mode create
        exit
        dot1p 1 fc "be" priority low
        dscp be fc "be" priority low
    exit
...
-----
```


Creating a Service Ingress QoS Queue

To create service ingress queue parameters, define the following:

- a new queue ID value — the system does not dynamically assign a value
- the queue parameters — ingress queues support explicit and auto-expedite hardware queue scheduling

Use the following CLI syntax to configure SAP ingress QoS queue parameters:

CLI Syntax:

```
config>qos# sap-ingress policy-id
      queue queue-id [queue-type] [queue-mode]
      adaptation-rule [pir adaptation-rule]
      [cir adaptation-rule]
      cbs {size-in-kbytes}
      high-prio-only percent
      mbs size-in-kbytes
      rate pir-rate [cir cir-rate]
      slope-policy name
```

Example:

```
*A:ALU-1# configure qos sap-ingress 100 queue 2 create
config>qos>sap-ingress>queue$ adaptation-rule pir closest
cir closest
config>qos>sap-ingress>queue$ cbs 1500
config>qos>sap-ingress>queue$ high-prio-only 10
config>qos>sap-ingress>queue$ mbs 10
config>qos>sap-ingress>queue$ rate 2500 cir 2500
config>qos>sap-ingress>queue$ slope-policy
"SlopePolicyIngress"
config>qos>sap-ingress>queue$ exit
*A:ALU-1#
```

The following sample output displays the queue configuration for service ingress policy 100:

```
ALU-1>config>qos# info
#-----
echo "QoS Policy Configuration"
#-----
...
    sap-ingress 100 create
    description "Used on VPN SAP"
    queue 1 priority-mode create
    exit
    queue 2 priority-mode create
    rate 2500 cir 2500
    mbs 10
    cbs 1500
    high-prio-only 10
    exit
...
```

Defining a Service Ingress Forwarding Class

Use the following syntax to define a service ingress forwarding class that overrides the default forwarding type that is defined by the **default-fc** command.

CLI Syntax: `config>qos>sap-ingress policy-id`
 `fc fc-name`
 `broadcast-queue queue-id`
 `queue queue-id`
 `multicast-queue queue-id`
 `unknown-queue queue-id`

Example: `*A:ALU-1# config>qos# sap-ingress 100 fc af create`
`config>qos>sap-ingress>fc# queue 2`
`config>qos>sap-ingress>fc# broadcast-queue 3`
`config>qos>sap-ingress>fc# multicast-queue 3`
`config>qos>sap-ingress>fc# unknown-queue 3`
`config>qos>sap-ingress>fc# exit`
`config>qos# exit`
`*A:ALU-1#`

The following sample output displays the forwarding class override value configuration for service ingress policy 100:

```
ALU-1>config>qos# info
#-----
#-----
echo "QoS Policy Configuration"
#-----
      sap-ingress 100 create
...
      fc "af" create
        queue 2
        broadcast-queue 3
        multicast-queue 3
        unknown-queue 3
      exit
      fc "ef" create
        queue 4
        broadcast-queue 5
        multicast-queue 5
        unknown-queue 5
      exit
    exit
...
```

Creating an MC-MLPPP SAP Egress QoS Policy

Define the following attributes to create an MC-MLPPP SAP egress policy:

- a unique policy ID value — the system does not dynamically assign a value
- a default queue for the MC-MLPPP SAP egress policy

Use the following CLI syntax to create an MC-MLPPP SAP egress QoS policy:

CLI Syntax: `config>qos>mc-mlppp`
 `sap-egress policy-id`
 `description description-string`
 `fc fc-name`
 `queue queue-id`

Example: *A:ALU-1>configure qos>mc-mlppp# sap-egress 300 create
 config>qos>mc-mlppp>sap-egress\$ fc be create
 config>qos>mc-mlppp>sap-egress>fc\$ exit
 config>qos>mc-mlppp>sap-egress\$ queue 2 create
 config>qos>mc-mlppp>sap-egress>queue\$ exit
 config>qos>mc-mlppp>sap-egress# exit
 *A:ALU-1#

The following sample output displays the MC-MLPPP SAP egress policy 300 configuration:

```
*A:ALU-1 config>qos# info
-----
#-----
echo "QoS Policy Configuration"
#-----
...
    sap-egress 300 create
        queue 1 create
        exit
        queue 2 create
        exit
        fc be create
        exit
    exit
-----
*A:ALU-1
```

Creating an MC-MLPPP SAP Egress QoS Forwarding Class

Define the following attributes to create an MC-MLPPP SAP egress forwarding class:

- the DSCP name and DSCP priority bits mapping

Optionally, you can enter a *queue-id* value to override the default forwarding class-to-queue mapping for the egress policy.

Use the following CLI syntax to create an MC-MLPPP SAP egress forwarding class:

CLI Syntax:

```
config>qos>mc-mlppp
      sap-egress policy-id
      fc fc-name
      dscp dscp-name
      queue queue-id
```

Example:

```
*A:ALU-1>config>qos>mc-mlppp# sap-egress 300 fc be create
config>qos>mc-mlppp>sap-egress>fc# dscp af13
config>qos>mc-mlppp>sap-egress>fc# exit
config>mc-mlppp>qos# exit
*A:ALU-1#
```

The following sample output displays the forwarding class configuration for MC-MLPPP SAP egress policy 300:

```
*A:ALU-1>config>qos# info
-----
#-----
echo "QoS Policy Configuration"
#-----
....
      sap-egress 300 create
      queue 1 create
      exit
      queue 2 create
      exit
      fc be create
      dscp af13
      exit
      exit
-----
*A: ALU-1
```

Creating an MC-MLPPP SAP Egress QoS Queue

Define the following attributes to create an MC-MLPPP SAP egress queue:

- adaptation-rule — the method used by the system to derive the PIR for the queue
- cbs — overrides the reserved buffers default for the queue
- high-prio-only — the percentage of buffer space for the queue to be used exclusively by in-profile packets
- mbs — the maximum amount of buffer space allowed for a specific queue
- rate — the PIR value for the queue
- slope-policy — the slope policy for the queue

Use the following CLI syntax to configure the MC-MLPPP SAP egress QoS queue parameters:

CLI Syntax:

```
config>qos>mc-mlppp
      sap-egress policy-id
      queue queue-id
          adaptation-rule [pir adaptation-rule]
          cbs size-in-kbytes
          high-prio-only percent
          mbs size-in-kbytes
          rate pir-rate
          slope-policy name
```

Example:

```
*A:ALU-1# configure qos mc-mlppp sap-egress 300
config>qos>mc-mlppp>sap-egress# queue 7
config>qos>mc-mlppp>sap-egress>queue# adaptation-rule pir
closest
config>qos>mc-mlppp>sap-egress>queue# cbs 10
config>qos>mc-mlppp>sap-egress>queue# high-prio-only 10
config>qos>mc-mlppp>sap-egress>queue# mbs 10
config>qos>mc-mlppp>sap-egress>queue# rate max
config>qos>mc-mlppp>sap-egress>queue# slope-policy "Slope
Policy"
config>qos>mc-mlppp>sap-egress>queue# exit
config>qos>mc-mlppp>sap-egress# exit
*A:ALU-1#
```

The following sample output displays the queue configuration for MC-MLPPP SAP egress policy 300:

```
ALU-1>config>qos# info
-----
#-----
echo "QoS Policy Configuration"
#-----
....
    sap-egress 300 create
        description "Egress Policy 300"
        queue 1 create
        exit
        queue 7 best-effort create
            rate max
            cbs 10
            mbs 10
            high-prio-only 10
        exit
        fc be create
        exit
        fc ef create
            dscp af13
        exit
    exit
...
-----
ALU-1#
```

Applying Service Egress and Ingress Policies

Apply service egress and ingress policies to the following service SAPs:

- Epipe
- Cpipe
- Apipe
- Ipipe
- IES
- VPRN

Refer to the 7705 SAR OS Services Guide, “Service Overview”, for information about configuring service parameters.

The section that follows pertains to Epipe configuration.

Epipe

Use the following CLI syntax to apply QoS policies to service ingress and/or service egress Epipe SAPs:

CLI Syntax: config>service> epipe *service-id* customer *customer-id*
 sap *sap-id*
 egress
 qos *sap-egress-policy-id*
 ingress
 qos *sap-ingress-policy-id*

The following sample output displays an Epipe service configuration with service ingress policy 100 and service egress policy 105 applied to the SAP.

```
ALU-1>config>service# info
#-----
echo "QoS Policy Configuration"
#-----
#-----
...
    epipe 6 customer 6 vpn 6 create
        description "Distributed Epipe service to west coast"
        sap 1/1/10:0 create
            ingress
                qos 100
            exit
            egress
                qos 105
            exit
        exit
    spoke-sdp 2:6 create
        ingress
            vc-label 6298
        exit
        egress
            vc-label 6300
        exit
    exit
    no shutdown
    exit
...
#-----
ALU-1>config>service#
```

Default Service Egress and Ingress Policy Values

The default service egress and ingress policies are identified as policy-id **1**. The default policies cannot be edited or deleted. The following sections display default policy parameters:

- [Service Egress Policy Defaults](#)
- [Service Ingress Policy Defaults](#)

Service Egress Policy Defaults

The following sample output shows the service egress policy defaults.

```
ALU-1>config>qos>info detail
#-----
#-----
echo "QoS Policy Configuration"
#-----
...
    sap-egress 1 create
        description "Default SAP egress QoS policy."
        scope template
        queue 1 auto-expedite create
            adaptation-rule pir closest cir closest
            rate max cir 0
            cbs default
            mbs default
            high-prio-only default
            slope-policy "default"
        exit
    exit
...
```

[Table 32](#) lists the service egress policy defaults.

Table 32: Service Egress Policy Defaults

Field	Default
description	Default SAP egress QoS policy
scope	template
queue	id = 1, type = auto-expedite
adaptation-rule	pir = closest, cir = closest
rate	pir = max, cir = 0
cbs	default
mbs	default
high-prio-only	default
slope-policy	default

Service Ingress Policy Defaults

The following sample output shows the service ingress policy defaults.

```

ALU-1>config>qos>info detail
#-----
#-----
echo "QoS Policy Configuration"
#-----
...
    sap-ingress 1 create
        description "Default SAP ingress QoS policy."
        scope template
        queue 1 priority-mode auto-expedite create
            adaptation-rule pir closest cir closest
            rate max cir 0
            mbs default
            cbs default
            high-prio-only default
            slope-policy "default"
        exit
        default-fc "be"
        default-priority low
    exit
...

```

Table 33 lists the service ingress policy defaults.

Table 33: Service Ingress Policy Defaults

Field	Default
description	Default SAP ingress QoS policy
scope	template
queue	id = 1, mode = priority-mode, type = auto-expedite
adaptation-rule	pir = closest, cir = closest
rate	pir = max, cir = 0
cbs	default
mbs	default
high-prio-only	default
slope-policy	default
default-fc	be
default-priority	low

Service Management Tasks

This section describes the following service management tasks:

- [Deleting QoS Policies](#)
- [Copying and Overwriting QoS Policies](#)
- [Editing QoS Policies](#)

Deleting QoS Policies

Every service SAP is associated, by default, with the appropriate service egress or ingress policy (policy-id 1). You can replace the default policy with a customer-configured policy, but you cannot entirely remove the policy from the SAP configuration. When you remove a non-default service egress or ingress policy, the association reverts to the default policy-id 1.

A QoS policy cannot be deleted until it is removed from all SAPs where it is applied.

Removing a QoS Policy from a Service SAP

Use the following syntax to remove a QoS policy from an Epipe service SAP. The syntax for Apipe, Cpipe, and Ipipe service SAPs is similar.

CLI Syntax: `config>service> {epipe} service-id customer customer-id
sap sap-id
egress
no qos policy-id
ingress
no qos policy-id`

Example: `config>service>epipe# sap 1/1/10:0
config>service>epipe>sap# ingress
config>service>epipe>sap>ingress# no qos
config>service>epipe>sap>ingress# exit
config>service>epipe>sap# egress
config>service>epipe>sap>egress# no qos
config>service>epipe>sap>egress# exit`

The following Epipe service sample output shows that the SAP service egress and ingress reverted to policy-id “1” when the non-default policies were removed from the configuration.

```
ALU-1>config>service>epipe# info detail
-----
description "Distributed Epipe service to west coast"
service-mtu 1514
sap 1/1/10:0 create
  no description
  no multi-service-site
  ingress
    qos 1
    exit
  egress
    qos 1
    exit
  no collect-stats
  no accounting-policy
  no shutdown
exit
spoke-sdp 2:6 vc-type ether create
  no shutdown
exit
no shutdown
-----
ALU-1>config>service>epipe#
```

Removing a Policy from the QoS Configuration

Use the following syntax to remove a QoS policy:

CLI Syntax: config>qos# no sap-ingress *policy-id*

Copying and Overwriting QoS Policies

You can copy an existing service egress or ingress policy, rename it with a new policy ID value, or overwrite an existing policy ID. The `overwrite` option must be specified or an error occurs if the destination policy ID exists.

Use the following syntax to overwrite an existing QoS policy ID:

CLI Syntax: `config>qos> copy sap-ingress source-policy-id dest-policy-id overwrite`

Example:

```
config>qos# copy sap-ingress 100 200
config>qos# copy sap-ingress 200 101
MINOR: CLI Destination "101" exists use {overwrite}
config>qos# copy sap-ingress 200 101 overwrite
config>qos#
```

The following sample output displays the copied policies:

```
ALU-1>config>qos# info
-----
...
exit
      sap-ingress 100 create
      description "Used on VPN sap"
      queue 1 create
      exit
      rate 11000
      exit
...
      sap-ingress 101 create
      description "Used on VPN sap"
      queue 1 create
      exit
      rate 11000
      exit
      sap-ingress 200 create
      description "Used on VPN sap"
      queue 1 create
      exit
      rate 11000
      exit
...
-----
ALU-1>config>qos#
```

Editing QoS Policies

You can change existing QoS policies and entries in the CLI. The changes are applied immediately to all services where this policy is applied. To prevent configuration errors, copy the policy to a work area, make the edits, and then write over the original policy.

Service Egress and Ingress QoS Policy Command Reference

Command Hierarchies

- [Service Egress QoS Policy Configuration Commands](#)
- [Service Ingress QoS Policy Configuration Commands](#)
- [MC-MLPPP SAP Egress QoS Policies](#)
- [Operational Commands](#)
- [Show Commands](#)

Service Egress QoS Policy Configuration Commands

```

config
  — qos
    — [no] sap-egress policy-id [create]
      — description description-string
      — no description
      — [no] fc fc-name [create]
        — dot1p {dot1p-value | in-profile dot1p-value out-profile dot1p-value}
        — no dot1p
        — dscp dscp-name
        — dscp in-profile dscp-name out-profile dscp-name
        — no dscp
        — queue queue-id
        — no queue
      — queue queue-id [queue-type] [create]
      — no queue queue-id
        — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
        — no adaptation-rule
        — cbs {size-in-kbytes | default}
        — no cbs
        — high-prio-only percent
        — no high-prio-only
        — mbs {size-in-kbytes | default}
        — no mbs
        — rate pir-rate [cir cir-rate]
        — no rate
        — slope-policy name
        — no slope-policy
      — scope {exclusive | template}
      — no scope

```


Service Ingress QoS Policy Configuration Commands

```

config
  — qos
    — [no] sap-ingress policy-id [create]
      — default-fc fc-name
      — no default-fc
      — default-priority {low | high}
      — no default-priority
      — description description-string
      — no description
      — dot1p dot1p-priority [fc fc-name] [priority {low | high}]
      — no dot1p dot1p-priority
      — dscp dscp-name [fc fc-name] [priority {low | high}]
      — no dscp dscp-name
      — [no] fc fc-name [create]
        — broadcast-queue queue-id
        — no broadcast-queue
        — multicast-queue queue-id
        — no multicast-queue
        — queue queue-id
        — no queue
        — unknown-queue queue-id
        — no unknown-queue
      — queue queue-id [queue-type] [queue-mode] [create]
      — no queue queue-id
        — adaptation-rule [pir adaptation-rule] [cir adaptation-rule]
        — no adaptation-rule
        — cbs {size-in-kbytes | default}
        — no cbs
        — high-prio-only percent
        — no high-prio-only
        — mbs {size-in-kbytes | default}
        — no mbs
        — rate pir-rate [cir cir-rate]
        — no rate
        — slope-policy name
        — no slope-policy
      — scope {exclusive | template}
      — no scope

```

MC-MLPPP SAP Egress QoS Policies

```

config
  — qos
    — mc-mlppp
      — [no] sap-egress policy-id [create]
        — description description-string
        — no description
        — [no] fc fc-name [create]
          — dscp dscp-name
          — no dscp
          — queue queue-id
          — no queue
        — [no] queue queue-id [create]
          — adaptation-rule pir adaptation-rule
          — no adaptation-rule
          — cbs {size-in-kbytes | default}
          — no cbs
          — high-prio-only percent
          — no high-prio-only
          — mbs size-in-kbytes
          — no mbs
          — rate pir-rate
          — no rate
          — slope-policy name
          — no slope-policy
        — scope {exclusive | template}
        — no scope

```

Operational Commands

```
config
  — qos
    — copy sap-egress src-pol dst-pol [overwrite]
    — copy sap-ingress src-pol dst-pol [overwrite]
```

Show Commands

```
show
  — qos
    — sap-ingress policy-id [detail]
    — sap-egress [policy-id] [standard | mc-mlppp] [detail]
  — pools mda-id [detail]
```

Command Descriptions

- [Configuration Commands on page 205](#)
- [Operational Commands on page 237](#)
- [Show Commands on page 238](#)

Configuration Commands

- [Generic Commands on page 206](#)
- [Service Egress QoS Policy Commands on page 207](#)
- [Service Egress QoS Policy Forwarding Class Commands on page 211](#)
- [MC-MLPPP SAP Egress QoS Policy Commands on page 214](#)
- [MC-MLPPP Forwarding Class Commands on page 217](#)
- [MC-MLPPP Queue Commands on page 218](#)
- [Service Ingress QoS Policy Commands on page 222](#)
- [Service Ingress QoS Policy Forwarding Class Commands on page 229](#)
- [Service Queue QoS Policy Commands on page 231](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>qos>sap-egress config>qos>sap-ingress config>qos>mc-mlppp>sap-egress
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes any description string from the context.
Default	n/a
Parameters	<i>description-string</i> — a text string describing the entity. 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.

Service Egress QoS Policy Commands

sap-egress

Syntax	[no] sap-egress <i>policy-id</i> [create]
Context	config>qos
Description	<p>This command is used to create or edit a service egress QoS policy. The egress policy defines the Service Level Agreement (SLA) for service packets as they egress on the SAP.</p> <p>Policies in effect are templates that can be applied to multiple services as long as the scope of the policy is template. The queues defined in the policy are not instantiated until a policy is applied to a service.</p> <p>A sap-egress policy differs from sap-ingress policies in the complexity of the QoS parameters that can be defined. At ingress, policies determine queue mappings based on ingress DSCP and dot1p criteria. Multiple queues can be created per forwarding class and each queue can have different CIR or PIR parameters.</p> <p>At egress, the policies are much simpler, since the forwarding class and in- or out-of-profile determination is done at the original service ingress SAP. Egress SAP QoS policies allow the definition of queues and the mapping of forwarding classes to those queues. Each queue needs to have a relative CIR for determining its allocation of QoS resources during periods of congestion. A PIR can also be defined that forces a hard limit on the packets transmitted through the queue. When the forwarding class is mapped to the queue, a dot1p value can optionally be specified. If specified, and the SAP has a dot1q encapsulation type, the dot1p value will be used for all packets that egress on that forwarding class. If the dot1p value is not specified, a dot1p value of 0 will be used. If the SAP is null encapsulated, the dot1p value has no meaning.</p> <p>The sap-egress policy with <i>policy-id</i> 1 is the default sap-egress QoS policy and is applied to service egress SAPs when an explicit policy is not specified or removed.</p> <p>The factory default settings for sap-egress <i>policy-id</i> 1 define a single queue with PIR set to the maximum value and a CIR set to 0. The single queue is the default queue and all forwarding classes will map to it. Packets being tagged according to the defined SAP encapsulation will have the dot1p bits set to 0.</p> <p>Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all egress SAPs where this policy is applied. For this reason, when many changes are required on a policy, it is highly recommended that the policy be copied to a work area <i>policy-id</i>. That work-in-progress policy can be modified until complete and then written over the original <i>policy-id</i>. Use the config qos copy command to maintain policies in this manner.</p> <p>The no form of this command deletes the sap-egress policy. A policy cannot be deleted until it is removed from all service SAPs where it is applied. When a sap-egress policy is removed from a SAP, the SAP will revert to the default sap-egress <i>policy-id</i> 1.</p>

Parameters *policy-id* — uniquely identifies the policy on the 7705 SAR

Values	1 to 65535
Default	n/a

create — keyword used to create a service egress QoS policy

fc

Syntax **[no] fc** *fc-name* [**create**]

Context config>qos>sap-egress

Description The **fc** *fc-name* mode within the SAP egress QoS policy is used to contain the explicitly defined queue mapping and dot1p marking commands for *fc-name*. When the mapping for *fc-name* points to the default queue and the dot1p marking is not defined, the mode for *fc-name* is not displayed in the **show configuration** or **save configuration** output unless the **detail** option is specified.

The **no** form of the command removes the explicit queue mapping and dot1p marking commands for *fc-name*. The queue mapping reverts to the default queue for *fc-name*, and the dot1p marking (if appropriate) uses the default of 0.

Default n/a

Parameters *fc-name* — specifies the forwarding class queue mapping or dot1p marking is to be edited. The value given for *fc-name* must be one of the predefined forwarding classes in the system.

Values	be, l2, af, l1, h2, ef, h1, nc
---------------	--------------------------------

create — keyword used to create a SAP egress forwarding class policy

queue

Syntax **queue** *queue-id* [*queue-type*] [**create**]
no queue *queue-id*

Context config>qos>sap-egress

Description This command creates the context to configure a service egress policy queue. Explicit definition of an egress queue's hardware scheduler status is supported. A single egress queue allows support for multiple forwarding classes.

The default behavior automatically chooses the expedited or non-expedited nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1, or h2), the queue is treated as an expedited queue by the hardware schedulers. When any non-expedited forwarding classes are mapped to the queue (be, af, l1, or l2), the queue is treated as best effort (be) by the hardware schedulers. The expedited hardware schedulers are used to enforce expedited access to egress ports. The hardware status of the queue must be defined at the time of queue creation within the policy.

The **no** form of the command removes the *queue-id* from the service egress policy. Removing the *queue-id* also removes it from any existing SAPs using the policy. If any forwarding classes are mapped to the queue, they revert to the default queue.

When a queue is removed, pending accounting information for each service egress queue created due to the definition of the queue in the policy is discarded.

Default	n/a
Parameters	<p><i>queue-id</i> — the <i>queue-id</i> for the service egress queue, expressed as a decimal integer. The <i>queue-id</i> uniquely identifies the queue within the policy.</p> <p>Values 1 to 8</p> <p>Default none</p> <p><i>queue-type</i> — the expedite, best-effort and auto-expedite queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective. A keyword must be specified at the time the queue is created in the service egress policy. If an attempt is made to change the keyword after the queue is initially defined, an error is generated.</p> <p>expedite — the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue</p> <p>best-effort — the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue</p> <p>auto-expedite — the system auto-defines the way the queue is serviced by the hardware. When auto-expedite is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types <i>nc</i>, <i>ef</i>, <i>h1</i> or <i>h2</i>. When a single non-expedited forwarding class is mapped to the queue (<i>be</i>, <i>af</i>, <i>l1</i> and <i>l2</i>) the queue automatically falls back to non-expedited status.</p> <p>Values expedite, best-effort, auto-expedite</p> <p>Default auto-expedite</p> <p>create — keyword used to create a service egress queue policy</p>

scope

Syntax	scope {exclusive template} no scope
Context	config>qos>sap-egress
Description	<p>This command is used to enter the scope of the policy. The scope of the policy cannot be changed if the policy is applied to one or more services.</p> <p>The no form of this command sets the scope of the policy to the default of template.</p>
Default	template

- Parameters**
- exclusive** — when the scope of a policy is defined as **exclusive**, the policy can only be applied to a single SAP. Attempting to assign the policy to a second SAP will result in an error message. If the policy is removed from the exclusive SAP, it will become available for assignment to another exclusive SAP.
 - template** — when the scope of a policy is defined as **template**, the policy can be applied to multiple SAPs on the router

Service Egress QoS Policy Forwarding Class Commands

dot1p

Syntax	dot1p { <i>dot1p-value</i> in-profile <i>dot1p-value</i> out-profile <i>dot1p-value</i> } no dot1p
Context	config>qos>sap-egress>fc
Description	This command explicitly defines the egress dot1p priority bits values for the forwarding class.



Note: When the **dot1p** *dot1p-value* command is used, the value is applied to both in-profile and out-of-profile packets. When the **dot1p in-profile** *dot1p-value* **out-profile** *dot1p-value* form is used, different dot1p values for in-profile or out-of-profile packets can be specified.

The **no** form of the command sets the dot1p priority bits value to 0.

Default	0												
Parameters	<i>dot1p-value</i> — the explicit dot1p value for the specified forwarding class. Setting the value to 0 is equivalent to removing the marking value. <table><tr><td>Values</td><td>0 to 7</td></tr><tr><td>Default</td><td>none</td></tr></table> <i>in-profile dot1p-value</i> — the dot1p in-profile mapping for the specified forwarding class. Setting the value to 0 is equivalent to removing the mapping value. <table><tr><td>Values</td><td>0 to 7</td></tr><tr><td>Default</td><td>none</td></tr></table> <i>out-profile dot1p-value</i> — the dot1p out-profile mapping for the specified forwarding class. Setting the value to 0 is equivalent to removing the mapping value. <table><tr><td>Values</td><td>0 to 7</td></tr><tr><td>Default</td><td>none</td></tr></table>	Values	0 to 7	Default	none	Values	0 to 7	Default	none	Values	0 to 7	Default	none
Values	0 to 7												
Default	none												
Values	0 to 7												
Default	none												
Values	0 to 7												
Default	none												


dscp

Syntax	dscp <i>dscp-name</i>
Context	config>qos>sap-egress>fc
Description	This command defines the DSCP name for the forwarding class.
Default	none
Parameters	<i>dscp-name</i> — a system-defined, case-sensitive name
Values	A maximum of 64 DSCP rules are allowed on a single policy. The specified name must exist as a <i>dscp-name</i> . Table 34 lists all the valid DSCP names.

Table 34: Valid DSCP Names

dscp-name
be, cp1, cp2, cp3, cp4, cp5, cp6, cp7, cs1, cp9, af11, cp11, af12, cp13, af13, cp15, cs2, cp17, af21, cp19, af22, cp21, af23, cp23, cs3, cp25, af31, cp27, af32, cp29, af33, cp31, cs4, cp33, af41, c p35, af42, cp37, af43, cp39, cs5, cp41, cp42, cp43, cp44, cp45, ef, cp47, nc1, cp49, cp50, cp51, cp52, cp53, cp54, cp55, nc2, cp57, cp58, cp59, cp60, cp61, cp62, cp63

dscp

Syntax	dscp <i>dscp-name</i> dscp in-profile <i>dscp-name</i> out-profile <i>dscp-name</i> no dscp
Context	config>qos>sap-egress>fc
Description	This command defines the DSCP priority bits mapping for the forwarding class.
	Note: When the dscp <i>dscp-name</i> command is used, the <i>dscp-name</i> is applied to all packets regardless of the profile state. The in-profile and out-profile form of the command allows differentiated values to be applied to packets based on the profile state.
	The no form of the command removes the DSCP mapping associated with the forwarding class.
Default	none
Parameters	in-profile <i>dscp-name</i> — the DSCP in-profile mapping for the specified forwarding class
Values	any name listed in Table 34
	out-profile <i>dscp-name</i> — the DSCP out-profile mapping for the specified forwarding class
Values	any name listed in Table 34

queue

Syntax	queue <i>queue-id</i> no queue				
Context	config>qos>sap-egress>fc				
Description	<p>This command specifies the egress queue to which the traffic associated with the forwarding class is to be forwarded. The command overrides the default queue mapping for fc <i>fc-name</i>. The specified <i>queue-id</i> must exist within the policy before the mapping can be made. Once the forwarding class mapping is executed, all traffic classified to the <i>fc-name</i> on a SAP using this policy will use the indicated queue.</p> <p>The no form of the command sets the <i>queue-id</i> back to the default queue for the forwarding class (queue 1).</p>				
Default	no queue				
Parameters	<p><i>queue-id</i> — the service egress <i>queue-id</i> to be associated with the forwarding class. The <i>queue-id</i> must be an existing queue defined in sap-egress <i>policy-id</i>.</p> <table><tr><td>Values</td><td>1 to 8</td></tr><tr><td>Default</td><td>1</td></tr></table>	Values	1 to 8	Default	1
Values	1 to 8				
Default	1				

MC-MLPPP SAP Egress QoS Policy Commands

mc-mlppp

Syntax	mc-mlppp
Context	config>qos
Description	This command creates the context to configure MC-MLPPP SAP egress QoS commands.

sap-egress

Syntax	[no] sap-egress <i>policy-id</i> [create]
Context	config>qos>mc-mlppp
Description	This command is used to create or edit an MC-MLPPP SAP egress QoS policy. The egress policy defines the Service Level Agreement (SLA) for service packets as they egress on the SAP.

Policies are templates that can be applied to multiple services as long as the scope of the policy is **template**. The queues defined in the policy are not instantiated until a policy is applied to a service.

At egress, the forwarding class and in- or out-of-profile determination is done at the original service ingress SAP. MC-MLPPP egress SAP QoS policies allow the definition of queues and the mapping of forwarding classes to those queues. Each queue must have a PIR defined that forces a hard limit on the packets transmitted through the queue.

The sap-egress policy with *policy-id* 1 is the default sap-egress QoS policy and is applied to MC-MLPPP egress SAPs when an explicit policy is not specified or is removed.

The default settings for **sap-egress *policy-id* 1** define a single queue with PIR set to the maximum value. The single queue is the default queue and all forwarding classes will map to it.

Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all egress SAPs where this policy is applied. For this reason, when many changes are required on a policy, it is highly recommended that the policy be copied to a work area *policy-id*. That work-in-progress policy can be modified until complete and then written over the original *policy-id*. Use the **config qos copy** command to maintain policies in this manner.

The **no** form of this command deletes the sap-egress policy. A policy cannot be deleted until it is removed from all service SAPs where it is applied. When a sap-egress policy is removed from a SAP, the SAP will revert to the default **sap-egress *policy-id* 1**, which cannot be deleted.

Parameters	<i>policy-id</i> — uniquely identifies the policy on the 7705 SAR
Values	1 to 65535
Default	n/a
create	— keyword used to create an MC-MLPPP SAP egress QoS policy

fc

Syntax	[no] fc <i>fc-name</i> [create]
Context	config>qos>mc-mlppp>sap-egress
Description	<p>The fc <i>fc-name</i> mode within the MC-MLPPP SAP egress QoS policy is used to contain the explicitly defined queue mapping for <i>fc-name</i>.</p> <p>The no form of the command removes the explicit queue mapping for <i>fc-name</i>. The queue mapping reverts to the default queue for <i>fc-name</i>.</p>
Default	n/a
Parameters	<p><i>fc-name</i> — specifies that the forwarding class queue mapping is to be edited. The value given for <i>fc-name</i> must be one of the predefined forwarding classes in the system.</p> <p>Values be, l2, af, l1, h2, ef, h1, nc</p> <p>create — keyword used to create the context to configure an MC-MLPPP SAP egress forwarding class mapping queue</p>

queue

Syntax	[no] queue <i>queue-id</i> [create]
Context	config>qos>mc-mlppp>sap-egress
Description	<p>This command creates the context to configure an MC-MLPPP SAP egress policy queue. Explicit definition of an egress queue's hardware scheduler status is supported. A single egress queue allows support for multiple forwarding classes.</p> <p>The no form of the command removes the <i>queue-id</i> from the MC-MLPPP SAP egress policy. Removing the <i>queue-id</i> also removes it from any existing SAPs using the policy. If any forwarding classes are mapped to the queue, they revert to the default queue.</p> <p>When a queue is removed, pending accounting information for each SAP egress queue created due to the definition of the queue in the policy is discarded.</p>
Default	n/a

Parameters *queue-id* — the *queue-id* for the MC-MLPPP SAP egress queue, expressed as a decimal integer. The *queue-id* uniquely identifies the queue within the policy.

Values 1 to 8

create — keyword used to create the context to configure an MC-MLPPP SAP egress policy queue

scope

Syntax **scope {exclusive | template}**
no scope

Context config>qos>mc-mlppp>sap-egress

Description This command is used to enter the scope of the policy. The scope of the policy cannot be changed if the policy is applied to one or more services.

The **no** form of this command sets the scope of the policy to the default of template.

Default **template**

Parameters **exclusive** — when the scope of a policy is defined as **exclusive**, the policy can only be applied to a single SAP. Attempting to assign the policy to a second SAP will result in an error message. If the policy is removed from the exclusive SAP, it will become available for assignment to another exclusive SAP.

template — when the scope of a policy is defined as **template**, the policy can be applied to multiple SAPs on the router

MC-MLPPP Forwarding Class Commands

dscp

Syntax	dscp <i>dscp-name</i> no dscp
Context	config>qos>mc-mlppp>sap-egress>fc
Description	This command defines the DSCP name for the forwarding class.
Default	none
Parameters	<i>dscp-name</i> — a system-defined, case-sensitive name Values any name listed in Table 34

queue

Syntax	queue <i>queue-id</i> no queue
Context	config>qos>mc-mlppp>sap-egress>fc
Description	<p>This command specifies the MC-MLPPP egress queue to which the traffic associated with the forwarding class is to be forwarded. The command overrides the default queue mapping for fc <i>fc-name</i>. The specified <i>queue-id</i> must exist within the policy before the mapping can be made. Once the forwarding class mapping is executed, all traffic classified to the <i>fc-name</i> on a SAP using this policy will use the indicated queue.</p> <p>The no form of the command sets the <i>queue-id</i> back to the default queue for the forwarding class (queue 1).</p>
Default	queue 1
Parameters	<i>queue-id</i> — the MC-MLPPP SAP egress <i>queue-id</i> to be associated with the forwarding class. The <i>queue-id</i> must be an existing queue defined in sap-egress <i>policy-id</i> . Values 1 to 8 Default 1

MC-MLPPP Queue Commands

adaptation-rule

Syntax	adaptation-rule pir <i>adaptation-rule</i> no adaptation-rule
Context	config>qos>mc-mlppp>sap-egress>queue
Description	<p>This command is used to define how an operational rate is selected based on the configured PIR rate. Operational rates are the finite set of rates at which the schedulers on the network processor can operate.</p> <p>The no form of the command removes any adaptation-rule constraints used to derive the operational rates for the policy. When a specific adaptation-rule is removed, the default constraints for rate apply.</p>
Default	closest
Parameters	<p><i>adaptation-rule</i> — specifies the constraints to be used while computing the operational PIR rate</p> <p>Values</p> <p><i>max</i> — the <i>max</i> (maximum) parameter is mutually exclusive with <i>min</i> and <i>closest</i>. The <i>max</i> parameter causes the network processor to be programmed at an operational rate that is less than the configured PIR rate by up to 0.5%.</p> <p><i>min</i> — the <i>min</i> (minimum) parameter is mutually exclusive with <i>max</i> and <i>closest</i>. The <i>min</i> parameter causes the network processor to be programmed at an operational rate that is greater than the configured PIR rate by up to 0.5%.</p> <p><i>closest</i> — the <i>closest</i> parameter is mutually exclusive with <i>max</i> and <i>min</i>. The <i>closest</i> parameter causes the network processor to be programmed at an operational rate that is closest to the configured PIR rate.</p>

cbs

Syntax	cbs { <i>size-in-kbytes</i> default } no cbs
Context	config>qos>mc-mlppp>sap-egress>queue
Description	<p>This command overrides the default Committed Buffer Space (CBS) reserved buffers for the queue.</p> <p>The no form of this command returns the CBS size to the default value.</p>
Default	6 (kilobytes)

Parameters *size-in-kbytes* — this parameter is an integer expression of the number of kilobytes reserved for the queue. 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 0 to 131072

default — returns the CBS size to the default value

high-prio-only

Syntax **high-prio-only** *percent*
no high-prio-only

Context config>qos>mc-mlppp>sap-egress>queue

Description The **high-prio-only** command configures the percentage of buffer space for the queue, used exclusively by high-priority packets. The specified value overrides the default value for the context.

The priority of a packet can only be set in the service ingress policy and is only applicable on the ingress queues for a SAP. The profile state is used for enqueueing priority at sap-egress.

The **no** form of this command restores the default high-priority reserved size.

Default 10 (percent)

Parameters *percent* — the percentage reserved for high priority traffic on the queue

Values 0 to 100 | default 1

mbs

Syntax **mbs** *size-in-kbytes*
no mbs

Context config>qos>mc-mlppp>sap-egress>queue

Description This command provides the explicit definition of the Maximum Burst Size (MBS) value of buffers allowed for a specific queue. The value is given in kilobytes and overrides the default value for the context.

The value in kilobytes is converted automatically to packets. The conversion algorithm uses a non-user-configurable value of 2304 bytes. The algorithm is:

$$\text{Number of packets} = \text{Configured MBS value in kilobytes} / 2.304$$

The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueueing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.

The sum of the MBS for all queues on an adapter card can exceed the total amount of buffering available. Therefore, a packet arriving at a queue that has not exceeded its MBS size is not guaranteed that a buffer will be available. If a buffer is not available, the packet will be discarded. RED/WRED slope parameters can be configured to control congestion in the case where the buffer capacity of the card is becoming exhausted.

Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED/WRED slope parameters for the needs of services on this port or channel.

The **no** form of this command returns the MBS size assigned to the queue to the default value.

Default	180 (kilobytes) (converted to: 78 packets)
Parameters	<i>size-in-kbytes</i> — the size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. A value of 4 or less causes the queue to discard all packets.
Values	0 to 131072 default

rate

Syntax	rate <i>pir-rate</i> no rate
Context	config>qos>mc-mlppp>sap-egress>queue
Description	<p>This command defines the administrative PIR parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets out an egress interface. Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.</p> <p>The rate command can be executed at any time, altering the PIR rates for all queues created through the association of the MC-MLPPP SAP egress policy with the <i>queue-id</i>.</p> <p>The no form of the command returns all queues created with the <i>queue-id</i> by association with the QoS policy to the default PIR parameters (max).</p>
Default	max — The max default specifies the amount of bandwidth in kilobits per second. The max value is mutually exclusive to the pir-rate value.
Parameters	<p><i>pir-rate</i> — 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.</p> <p>The actual PIR rate is dependent on the queue's adaptation-rule parameters and the actual hardware where the queue is provisioned.</p> <p>Values 1 to 100000000 max</p>

slope-policy

Syntax	slope-policy <i>name</i> no slope-policy
Context	config>qos>mc-mlppp>sap-egress queue
Description	<p>This command specifies the slope parameters controlling the queue.</p> <p>The no form of this command reverts to the default value.</p>
Default	default
Parameters	<i>name</i> — the name of the slope policy
Values	Valid names consist of 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.

Service Ingress QoS Policy Commands

sap-ingress

Syntax	[no] sap-ingress <i>policy-id</i> [create]
Context	config>qos
Description	<p>This command is used to create or edit the ingress policy. The ingress policy defines the Service Level Agreement (SLA) enforcement that service packets receive as they ingress a SAP. SLA enforcement is accomplished through the definition of queues that have Forwarding Class (FC), Committed Information Rate (CIR), Peak Information Rate (PIR) and Maximum Burst Size (MBS) characteristics. The simplest policy defines a single queue that all ingress traffic flows through. Complex policies have multiple queues that indicate which queue a packet will flow through.</p> <p>Policies in effect are templates that can be applied to multiple services as long as the scope of the policy is template. Queues defined in the policy are not instantiated until a policy is applied to a service SAP.</p> <p>It is possible that a service ingress policy will include the dscp map command and the dot1p map command. When multiple matches occur for the traffic, the order of precedence will be used to arrive at the final action. The order of precedence is as follows:</p> <ol style="list-style-type: none"> 1. 802.1p bits 2. DSCP <p>The service ingress policy with <i>policy-id</i> 1 is a system-defined policy applied to services when no other policy is explicitly specified. The system service ingress policy cannot be modified or deleted. The no sap-ingress command restores the factory default settings when used on <i>policy-id</i> 1. The default service ingress policy defines one queue associated with the best effort (be) forwarding class, with CIR of 0 and PIR of line rate.</p> <p>Any changes made to the existing policy, using any of the sub-commands, are applied immediately to all services where this policy is applied. For this reason, when many changes are required on a policy, it is recommended that the policy be copied to a work area policy ID. That work-in-progress policy can be modified until complete and then written over the original <i>policy-id</i>. Use the config qos copy command to maintain policies in this manner.</p> <p>The no sap-ingress <i>policy-id</i> command deletes the service ingress policy. A policy cannot be deleted until it is removed from all services where it is applied. The system default sap-ingress policy is a special case; the no command restores the factory defaults to <i>policy-id</i> 1.</p>
Parameters	<i>policy-id</i> — uniquely identifies the policy
Values	1 to 65535
	create — keyword used to create a sap-ingress policy

scope

Syntax	scope {exclusive template} no scope
Context	config>qos>sap-ingress
Description	<p>This command configures the Service Ingress QoS policy scope as exclusive or template.</p> <p>The policy's scope cannot be changed if the policy is applied to a service.</p> <p>The no form of this command sets the scope of the policy to the default of template.</p>
Default	template
Parameters	<p>exclusive — when the scope of a policy is defined as exclusive, the policy can only be applied to one SAP. If a policy with an exclusive scope is assigned to a second SAP, an error message is generated. If the policy is removed from the exclusive SAP, it will become available for assignment to another exclusive SAP.</p> <p>template — when the scope of a policy is defined as template, the policy can be applied to multiple SAPs on the router</p>

default-fc

Syntax	default-fc <i>fc-name</i> no default-fc
Context	config>qos>sap-ingress
Description	<p>This command configures the default forwarding class for the policy. In the event that an ingress packet does not match a higher priority (more explicit) classification command, the default forwarding class will be associated with the packet. Unless overridden by an explicit forwarding class classification rule, all packets received on an ingress SAP using this ingress QoS policy will be classified to the default forwarding class. Optionally, the default ingress enqueueing priority for the traffic can be overridden as well.</p> <p>The default forwarding class for default-fc is best effort (be). The default-fc settings are displayed in the show configuration and save output regardless of inclusion of the detail keyword.</p> <p>The no form of this command reverts to the default value.</p>
Default	be
Parameters	<p><i>fc-name</i> — specifies the forwarding class name for the queue. The value given for <i>fc-name</i> must be one of the predefined forwarding classes in the system.</p> <p>Values be, l2, af, l1, h2, ef, h1, nc</p>

default-priority

Syntax	default-priority {low high} no default-priority
Context	config>qos>sap-ingress
Description	<p>This command configures the default enqueueing priority for all packets received on an ingress SAP using this policy.</p> <p>The no form of this command reverts to the default value.</p>
Default	low
Parameters	<p>high — setting the enqueueing parameter to high for a packet increases the likelihood of enqueueing the packet when the ingress queue is congested. Ingress enqueueing priority only affects ingress SAP queuing; once the packet is placed in a buffer on the ingress queue, the significance of the enqueueing priority is lost.</p> <p>low — setting the enqueueing parameter to low for a packet decreases the likelihood of enqueueing the packet when the ingress queue is congested. Ingress enqueueing priority only affects ingress SAP queuing; once the packet is placed in a buffer on the ingress queue, the significance of the enqueueing priority is lost.</p>

fc

Syntax	[no] fc <i>fc-name</i> [create]				
Context	config>qos>sap-ingress				
Description	<p>This command is used to create a class of the forwarding class <i>fc-name</i>.</p> <p>The no form of the command removes all the explicit queue mappings for <i>fc-name</i> forwarding types. The queue mappings revert to the default queues for <i>fc-name</i>.</p>				
Parameters	<p><i>fc-name</i> — specifies the forwarding class name for the queue. The value given for <i>fc-name</i> must be one of the predefined forwarding classes in the system.</p> <table> <tr> <td>Values</td><td>class: be, l2, af, l1, h2, ef, h1, nc</td></tr> <tr> <td>Default</td><td>n/a</td></tr> </table> <p>create — keyword used to create a forwarding class</p>	Values	class: be, l2, af, l1, h2, ef, h1, nc	Default	n/a
Values	class: be, l2, af, l1, h2, ef, h1, nc				
Default	n/a				

dot1p

Syntax	dot1p <i>dot1p-priority</i> [fc <i>fc-name</i>] [priority { low high }] no dot1p <i>dot1p-priority</i>
Context	config>qos>sap-ingress
Description	<p>This command explicitly sets the forwarding class and/or enqueueing priority when a packet is marked with a <i>dot1p-priority</i> specified. Adding a dot1p rule on the policy forces packets that match the <i>dot1p-priority</i> specified to override the forwarding class and enqueueing priority based on the parameters included in the dot1p rule. When the forwarding class is not specified in the rule, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy. When the enqueueing priority is not specified in the rule, a matching packet preserves (or inherits) the existing enqueueing priority derived from earlier matches in the classification hierarchy.</p> <p>The <i>dot1p-priority</i> is derived from the most significant three bits in the IEEE 802.1Q or IEEE 802.1P header. The three dot1p bits define eight Class-of-Service (CoS) values commonly used to map packets to per-hop Quality-of-Service (QoS) behavior.</p> <p>The no form of this command removes the explicit dot1p classification rule from the service ingress policy. Removing the rule on the policy immediately removes the rule on all ingress SAPs using the policy.</p>
Parameters	<p><i>dot1p-priority</i> — this value is a required parameter that specifies the unique IEEE 802.1P value that will match the dot1p rule. If the command is executed multiple times with the same <i>dot1p-value</i>, the previous forwarding class and enqueueing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueueing priority parameter is missing.</p> <p>A maximum of eight dot1p rules are allowed on a single policy.</p> <p>Values 0 to 7</p> <p><i>fc-name</i> — the value given for the <i>fc-name</i> parameter must be one of the predefined forwarding classes in the system. Specifying the <i>fc-name</i> is optional. When a packet matches the rule, the forwarding class is only overridden when the <i>fc-name</i> parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.</p> <p>Values be, l2, af, l1, h2, ef, h1, nc</p> <p>Default none</p> <p>priority — the priority keyword is used to override the default enqueueing priority for all packets received on an ingress SAP using this policy that match this rule. Specifying the priority is optional. When a packet matches the rule, the enqueueing priority is only overridden when the priority parameter is defined on the rule. If the packet matches and the priority is not explicitly defined in the rule, the enqueueing priority is inherited based on previous rule matches.</p> <p>high — the high keyword is used in conjunction with the priority keyword. Setting the enqueueing parameter to high for a packet increases the likelihood of enqueueing the packet when the ingress queue is congested. Ingress enqueueing priority only affects ingress SAP queuing; once the packet is placed in a buffer on the ingress queue, the significance of the enqueueing priority is lost.</p>

low — the **low** keyword is used in conjunction with the **priority** keyword. Setting the enqueueing parameter to low for a packet decreases the likelihood of enqueueing the packet when the ingress queue is congested. Ingress enqueueing priority only affects ingress SAP queuing; once the packet is placed in a buffer on the ingress queue, the significance of the enqueueing priority is lost.

Default none

dscp

Syntax **dscp** *dscp-name* [**fc** *fc-name*] [**priority** {**high** | **low**}]
no dscp *dscp-name*

Context config>qos>sap-ingress

Description This command explicitly sets the forwarding class and/or enqueueing priority when a packet is marked with the DiffServ Code Point (DSCP) value contained in *dscp-name*. Adding a DSCP rule on the policy forces packets that match the specified DSCP value to override the forwarding class and enqueueing priority based on the parameters included in the DSCP rule.

When the forwarding class is not specified in the rule, a matching packet preserves (or inherits) the existing forwarding class derived from earlier matches in the classification hierarchy. When the enqueueing priority is not specified in the rule, a matching packet preserves (or inherits) the existing enqueueing priority derived from earlier matches in the classification hierarchy.

The DSCP value (referred to by *dscp-name*) is derived from the most significant six bits in the IP header ToS byte field (DSCP bits). The six DSCP bits define 64 DSCP values used to map packets to per-hop QoS behavior.

The **no** form of this command removes the DiffServ code point to forwarding class association. The **default-action** then applies to that code point value.

Parameters *dscp-name* — the *dscp-name* is a required parameter that specifies the unique IP header ToS byte DSCP bits value that will match the DSCP rule.

A maximum of 64 DSCP rules are allowed on a single policy. The specified name must exist as a *dscp-name*. [Table 34](#) lists all the valid DSCP names.

fc-name — the value given for *fc-name* must be one of the predefined forwarding classes in the system. Specifying the *fc-name* is optional. When a packet matches the rule, the forwarding class is only overridden when the *fc-name* parameter is defined on the rule. If the packet matches and the forwarding class is not explicitly defined in the rule, the forwarding class is inherited based on previous rule matches.

Values be, l2, af, l1, h2, ef, h1, nc

Default inherit (when *fc-name* is not defined, the rule preserves the previous forwarding class of the packet)

priority — this keyword overrides the default enqueueing priority for all packets received on an ingress SAP using this policy that match this rule. Specifying the priority is optional. When a packet matches the rule, the enqueueing priority is only overridden when the **priority** keyword is defined on the rule. If the packet matches and **priority** is not explicitly defined in the rule, the enqueueing priority is inherited based on previous rule matches.

Default inherit

high — this keyword is used in conjunction with the **priority** keyword. Setting the enqueueing parameter to **high** for a packet increases the likelihood of enqueueing the packet when the ingress queue is congested. Ingress enqueueing priority only affects ingress SAP queuing; once the packet is placed in a buffer on the ingress queue, the significance of the enqueueing priority is lost.

Default high

low — this keyword is used in conjunction with the **priority** keyword. Setting the enqueueing parameter to **low** for a packet decreases the likelihood of enqueueing the packet when the ingress queue is congested. Ingress enqueueing priority only affects ingress SAP queuing; once the packet is placed in a buffer on the ingress queue, the significance of the enqueueing priority is lost.

Default low

queue

Syntax	queue <i>queue-id</i> [<i>queue-type</i>] [<i>queue-mode</i>] [create] no queue <i>queue-id</i>
Context	config>qos>sap-ingress
Description	This command creates the context to configure a service ingress policy queue.

Explicit definition of an ingress queue's hardware scheduler status is supported. A single ingress queue allows support for multiple forwarding classes.

The default behavior automatically chooses the expedited or non-expedited nature of the queue based on the forwarding classes mapped to it. As long as all forwarding classes mapped to the queue are expedited (nc, ef, h1, or h2), the queue is treated as an expedited queue by the hardware schedulers. When any non-expedited forwarding classes are mapped to the queue (be, af, l1, or l2), the queue is treated as best effort (be) by the hardware schedulers.

The expedited hardware schedulers are used to enforce expedited access to internal switch fabric destinations. The hardware status of the queue must be defined at the time of queue creation within the policy.

The **no** form of this command removes the *queue-id* from the service ingress policy and from any existing SAPs using the policy. If any forwarding class forwarding types are mapped to the queue, they revert to their default queues. When a queue is removed, any pending accounting information for each service queue created due to the definition of the queue in the policy is discarded.

Parameters *queue-id* — the queue identifier for the queue, expressed as an integer. The *queue-id* uniquely identifies the queue within the policy. This is a required parameter each time the queue command is executed.

Values 1 to 8

queue-type — the **expedite**, **best-effort**, and **auto-expedite** queue types are mutually exclusive. Each defines the method that the system uses to service the queue from a hardware perspective. A keyword must be specified at the time the queue is created in the service ingress policy. If an attempt is made to change the keyword after the queue is initially defined, an error is generated.

expedite — the queue is treated in an expedited manner independent of the forwarding classes mapped to the queue

best-effort — the queue is treated in a non-expedited manner independent of the forwarding classes mapped to the queue

auto-expedite — the system auto-defines the way the queue is serviced by the hardware. When **auto-expedite** is defined on the queue, the queue is treated in an expedited manner when all forwarding classes mapped to the queue are configured as expedited types *nc*, *ef*, *h1*, or *h2*. When a single non-expedited forwarding class is mapped to the queue (*be*, *af*, *l1*, and *l2*) the queue automatically falls back to non-expedited status.

Values expedite, best-effort, auto-expedite

Default auto-expedite

queue-mode — this optional parameter specifies the queue mode. The only valid value is **priority-mode**, which means that the queue is capable of handling traffic with two distinct priorities in different ways. These priorities are assigned by the stages preceding the queueing framework in the system. In priority mode, the queue does not have the functionality to support the profiled traffic. However, the converse is not valid and a queue in profile mode should be capable of supporting the different priorities of traffic.

create — keyword used to create a sap-ingress queue context

Service Ingress QoS Policy Forwarding Class Commands

broadcast-queue

Syntax	broadcast-queue <i>queue-id</i> no broadcast-queue
Context	config>qos>sap-ingress>fc
Description	<p>This command maps the broadcast forwarding type queue to the fc <i>fc-name</i>. The specified <i>queue-id</i> must already have been created within the policy before the mapping can be made. Once the forwarding class mapping is executed, all broadcast traffic on a SAP using this policy will be forwarded using the <i>queue-id</i>.</p> <p>The no form of the command sets the broadcast forwarding type <i>queue-id</i> back to the default of no mapping to an FC.</p>
Default	no broadcast-queue
Parameters	<i>queue-id</i> — an existing queue defined in the config>qos>sap-ingress context. Values 1 to 8

multicast-queue

Syntax	multicast-queue <i>queue-id</i> no multicast-queue
Context	config>qos>sap-ingress>fc
Description	<p>This command maps the multicast forwarding type queue to the fc <i>fc-name</i>. The specified <i>queue-id</i> must already have been created within the policy before the mapping can be made. Once the forwarding class mapping is executed, all multicast traffic on a SAP using this policy will be forwarded using the <i>queue-id</i>.</p> <p>The no form of the command sets the multicast forwarding type <i>queue-id</i> back to the default of no mapping to an FC.</p>
Default	no multicast-queue
Parameters	<i>queue-id</i> — an existing queue defined in the config>qos>sap-ingress context. Values 1 to 8

queue

Syntax	queue <i>queue-id</i> no queue
Context	config>qos>sap-ingress>fc
Description	<p>This command overrides the default forwarding type queue mapping for fc <i>fc-name</i>.</p> <p>The no form of this command sets the <i>queue-id</i> back to the default queue for the forwarding class (queue 1).</p>
Parameters	<i>queue-id</i> — an existing queue defined in the config>qos>sap-ingress context
Values	1 to 8
Default	1

unknown-queue

Syntax	unknown-queue <i>queue-id</i> no unknown-queue
Context	config>qos>sap-ingress>fc
Description	<p>This command maps the unknown forwarding type queue to the fc <i>fc-name</i>. The specified <i>queue-id</i> must already have been created within the policy before the mapping can be made. Once the forwarding class mapping is executed, all unknown forwarding type traffic on a SAP using this policy will be forwarded using the <i>queue-id</i>.</p> <p>The no form of the command sets the unknown forwarding type <i>queue-id</i> back to the default of no mapping to an FC.</p>
Default	no unknown-queue
Parameters	<i>queue-id</i> — an existing queue defined in the config>qos>sap-ingress context.
Values	1 to 8

Service Queue QoS Policy Commands

adaptation-rule

Syntax	adaptation-rule [pir <i>adaptation-rule</i>] [cir <i>adaptation-rule</i>] no adaptation-rule
Context	config>qos>sap-ingress>queue config>qos>sap-egress>queue
Description	<p>This command can be used to define how an operational rate is selected based on the configured PIR or CIR rate. Operational rates are the finite set of rates at which the schedulers on the network processor can operate.</p> <p>The no form of the command removes any adaptation-rule constraints used to derive the operational rates for the policy. When a specific adaptation-rule is removed, the default constraints for rate and cir apply.</p>
Default	pir closest cir closest
Parameters	<p><i>adaptation-rule</i> — specifies the constraints to be used while computing the operational CIR or PIR rate</p> <p>Values</p> <p>pir — defines the constraints enforced when adapting the PIR rate defined within the queue <i>queue-id</i> rate command. The pir keyword requires a qualifier that defines the constraint used when deriving the operational PIR rate for the queue. When the rate command is not specified, the default applies.</p> <p>cir — defines the constraints enforced when adapting the CIR rate defined within the queue <i>queue-id</i> rate command. The cir keyword requires a qualifier that defines the constraint used when deriving the operational CIR rate for the queue. When the cir keyword is not specified, the default constraint applies.</p> <p><i>max</i> — the <i>max</i> (maximum) parameter is mutually exclusive with <i>min</i> and <i>closest</i>. The <i>max</i> parameter causes the network processor to be programmed at an operational rate which is less than the configured PIR or CIR rate by up to 0.5%.</p> <p><i>min</i> — the <i>min</i> (minimum) parameter is mutually exclusive with <i>max</i> and <i>closest</i>. The <i>min</i> parameter causes the network processor to be programmed at an operational rate which is greater than the configured PIR or CIR rate by up to 0.5%.</p> <p><i>closest</i> — the <i>closest</i> parameter is mutually exclusive with <i>max</i> and <i>min</i>. The <i>closest</i> parameter causes the network processor to be programmed at an operational rate which is closest to the configured PIR or CIR rate.</p>

cbs

Syntax	cbs { <i>size-in-kbytes</i> default } no cbs
Context	config>qos>sap-ingress>queue config>qos>sap-egress>queue
Description	This command overrides the default Committed Buffer Space (CBS) reserved buffers for the queue. The no form of this command returns the CBS size to the default value.
Default	6 (kilobytes)
Parameters	<i>size-in-kbytes</i> — this parameter is an integer expression of the number of kilobytes reserved for the queue. 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 0 to 131072 default

high-prio-only

Syntax	high-prio-only <i>percent</i> no high-prio-only
Context	config>qos>sap-ingress>queue config>qos>sap-egress>queue
Description	The high-prio-only command configures the percentage of buffer space for the queue, used exclusively by high-priority packets. The specified value overrides the default value for the context. The priority of a packet can only be set in the service ingress policy and is only applicable on the ingress queues for a SAP. The profile state is used for enqueueing priority at sap-egress. The no form of this command restores the default high-priority reserved size.
Parameters	<i>percent</i> — the percentage reserved for high priority traffic on the queue Values 0 to 100 default 1 Default 10

mbs

Syntax	mbs { <i>size-in-kbytes</i> default } no mbs
Context	config>qos>sap-ingress>queue config>qos>sap-egress>queue
Description	<p>This command provides the explicit definition of the Maximum Burst Size (MBS) value of buffers allowed for a specific queue. The value is given in kilobytes and overrides the default value for the context.</p> <p>The value in kilobytes is converted automatically to packets. The conversion algorithm uses a non-user-configurable value of 2304 bytes. The algorithm is:</p> $\text{Number of packets} = \text{Configured MBS value in kilobytes} / 2.304$ <p>The MBS value is used by a queue to determine whether it has exhausted all of its buffers while enqueueing packets. Once the queue has exceeded the amount of buffers allowed by MBS, all packets are discarded until packets have been drained from the queue.</p> <p>The sum of the MBS for all queues on an adapter card can exceed the total amount of buffering available. Therefore, a packet arriving at a queue that has not exceeded its MBS size is not guaranteed that a buffer will be available. If a buffer is not available, the packet will be discarded. RED/WRED slope parameters can be configured to control congestion in the case where the buffer capacity of the card is becoming exhausted.</p> <p>Setting proper CBS parameters and controlling CBS oversubscription is one major safeguard to queue starvation (when a queue does not receive its fair share of buffers). Another is properly setting the RED/WRED slope parameters for the needs of services on this port or channel.</p> <p>The no form of this command returns the MBS size assigned to the queue to the default value.</p>
Default	180 (kilobytes) (converted to: 78 packets)
Parameters	<p><i>size-in-kbytes</i> — the size parameter is an integer expression of the maximum number of kilobytes of buffering allowed for the queue. A value of 4 or less causes the queue to discard all packets.</p> <p>Values 0 to 131072 default</p>

rate

Syntax	rate <i>pir-rate</i> [cir <i>cir-rate</i>] no rate
Context	config>qos>sap-ingress>queue
Description	<p>This command defines the administrative PIR and the administrative CIR parameters for the queue. Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.</p> <p>The cir keyword defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth. For service ingress, the cir keyword also defines the rate that packets are considered in-profile by the system. In-profile packets are preferentially queued by the system at egress and at subsequent next hop nodes where the packet can traverse. To be properly handled as in- or out-of-profile throughout the network, the packets must be marked accordingly for profiling at each hop.</p> <p>The rate command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the service ingress or service egress QoS policy with the <i>queue-id</i>.</p> <p>The no form of the command returns all queues created with the <i>queue-id</i> by association with the QoS policy to the default PIR and CIR parameters (max, 0).</p>
Default	rate max cir 0 — the max default specifies the amount of bandwidth in kilobits per second. The max value is mutually exclusive to the pir-rate value.
Parameters	<p><i>pir-rate</i> — defines the administrative PIR rate, in kilobits per second, 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.</p> <p>The actual PIR rate is dependent on the queue's adaptation-rule parameters and the actual hardware where the queue is provisioned.</p> <p>Values 1 to 100000000 max</p> <p>Default max</p> <p><i>cir-rate</i> — overrides the default administrative CIR used by the queue. When the rate command is executed, a <i>cir-rate</i> setting is optional. When the rate command has not been executed or the cir keyword is not explicitly specified, the default CIR (0) is assumed. Fractional values are not allowed and must be given as a positive integer.</p> <p>Values 0 to 100000000 max</p> <p>Default 0</p>

rate

Syntax	rate <i>pir-rate</i> [cir <i>cir-rate</i>] no rate
Context	config>qos>sap-egress>queue
Description	<p>This command defines the administrative PIR and the administrative CIR parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets out an egress interface (for service egress queues). Defining a PIR does not necessarily guarantee that the queue can transmit at the intended rate. The actual rate sustained by the queue can be limited by oversubscription factors or available egress bandwidth.</p> <p>The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth.</p> <p>The rate command can be executed at any time, altering the PIR and CIR rates for all queues created through the association of the service egress policy with the <i>queue-id</i>.</p> <p>For egress queues, this command is only valid for Epipes.</p> <p>The no form of the command returns all queues created with the <i>queue-id</i> by association with the QoS policy to the default PIR and CIR parameters (max, 0).</p>
Default	rate max cir 0 — The max default specifies the amount of bandwidth in kilobits per second. The max value is mutually exclusive to the pir-rate value.
Parameters	<p><i>pir-rate</i> — 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.</p> <p>The actual PIR rate is dependent on the queue's adaptation-rule parameters and the actual hardware where the queue is provisioned.</p> <p>Values 1 to 100000000 max</p> <p>Default max</p> <p><i>cir-rate</i> — 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.</p> <p>Values 0 to 100000000 max</p> <p>Default 0</p>

slope-policy

Syntax	slope-policy <i>name</i> no slope-policy
Context	config>qos>sap-ingress queue config>qos>sap-egress queue
Description	This command specifies the slope parameters controlling the queue.
Default	slope-policy default
Parameters	<i>name</i> — the name of the slope policy
Values	Valid names consist of 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.

Operational Commands

copy

Syntax	copy sap-egress <i>src-pol dst-pol</i> [overwrite] copy sap-ingress <i>src-pol dst-pol</i> [overwrite]
Context	config>qos
Description	<p>This command copies existing QoS policy entries for a QoS policy ID to another QoS policy ID.</p> <p>This command is a configuration level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the overwrite keyword.</p>
Parameters	<p><i>src-pol dst-pol</i> — indicates that the source policy ID and the destination policy ID are sap-egress or sap-ingress policy IDs. Specify the source policy ID that the copy command will attempt to copy from and specify the destination policy ID to which the command will copy a duplicate of the policy.</p> <p>Values 1 to 65535</p> <p>overwrite — specifies that the existing destination policy is to be replaced. Everything in the existing destination policy will be overwritten with the contents of the source policy. If overwrite is not specified, an error will occur if the destination policy ID exists.</p>

Show Commands

sap-ingress

Syntax	sap-ingress [<i>policy-id</i>] [<i>detail</i>]
Context	show>qos
Description	This command displays service ingress QoS policy information.
Parameters	<p><i>policy-id</i> — displays information about the specific policy</p> <p>Default all service ingress policies</p> <p>Values 1 to 65535</p> <p>detail — displays detailed policy information including policy associations</p>
Output	The following output is an example of service ingress QoS policy information, and Table 35 describes the fields.

Sample Output

```
A:ALU-1# show qos sap-ingress
=====
Sap Ingress Policies
=====
Policy-Id          Scope      Description
-----
1                  Template  Default SAP ingress QoS policy.
100                Template  Used on VPN SAP
=====
*A:ALU-1#
=====

A:ALU-1# show qos sap-ingress 100 detail
-----
Sap Ingress Policy (100)
-----
Policy-id          : 100                      Scope      : Template
Default FC         : be                      Priority    : Low
Description        : Used on VPN SAP
-----

Queue Mode      CIR Admin PIR Admin CBS   HiPrio Slope-Policy
                CIR Rule  PIR Rule  MBS
-----
1    Profile    0          max    def    def    default
                closest  closest def
2    Profile    2500       2500   1500   10     default
                closest  closest 10
-----
```

```

FC                UCastQ        MCastQ        BCastQ        UnknownQ
-----
h2                def            def            def            def
ef                6              def            7              def
h1                6              def            def            def
-----

Dot1p             FC                Priority
-----
1                 be                Low
-----

DSCP              FC                Priority
-----
be                be                Low
-----

Associations
-----
No Associations Found.

=====
*A:ALU-1#

```

Table 35: SAP Ingress Command Output

Label	Description
Policy-Id	The ID that uniquely identifies the policy
Scope	Exclusive - this policy can only be applied to a single SAP
	Template - this policy can be applied to multiple SAPs on the router
Description	A text string that helps identify the policy's context in the configuration file
Default FC	The default forwarding class for the policy
Priority	The default enqueueing priority
Queue	The queue number
Mode	The priority mode for the queue
CIR Admin	The CIR parameters for the queue. The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth.

Table 35: SAP Ingress Command Output (Continued)

Label	Description
CIR Rule	min - the operational CIR for the queue will be equal to or greater than the administrative rate specified using the rate command except where the derived operational CIR is greater than the operational PIR. If the derived operational CIR is greater than the derived operational PIR, the operational CIR will be made equal to the operational PIR.
	max - the operational CIR for the queue will be equal to or less than the administrative rate specified using the rate command
	closest - the operational CIR for the queue will be the rate closest to the rate specified using the rate command without exceeding the operational PIR
PIR Admin	The administrative PIR parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets through the switch fabric.
PIR Rule	min - the operational PIR for the queue will be equal to or greater than the administrative rate specified using the rate command
	max - the operational PIR for the queue will be equal to or less than the administrative rate specified using the rate command
	closest - the operational PIR for the queue will be the rate closest to the rate specified using the rate command
CBS	def - the CBS value reserved for the queue
	value - the value to override the default reserved buffers for the queue
MBS	def - the MBS value reserved for the queue
	value - the value to override the default maximum size for the queue
HiPrio	The percentage of buffer space for the queue, used exclusively by high-priority packets
Slope-Policy	The slope policy for the queue
UCastQ	The unicast forwarding type queue mapping (default or queue number)
MCastQ	The multicast forwarding type queue mapping (default or queue number)
BCastQ	The broadcast forwarding type queue mapping (default or queue number)
UnknownQ	The unknown unicast forwarding type queue mapping (default or queue number)

Table 35: SAP Ingress Command Output (Continued)

Label	Description
Dot1p	The forwarding class and/or enqueueing priority when a packet is marked with a <i>dot1p-value</i> specified
FC	The override for the forwarding class
Priority	The optional priority setting overrides the default enqueueing priority for the packets received on an ingress SAP that uses the policy that matches this rule
	High - the high enqueueing parameter for a packet increases the likelihood of enqueueing the packet when the ingress queue is congested
	Low - the low enqueueing parameter for a packet decreases the likelihood of enqueueing the packet when the ingress queue is congested
DSCP	The forwarding class and/or enqueueing priority when a packet is marked with the DiffServ Code Point (DSCP) value
FC	One of the predefined forwarding classes in the system. When a packet matches the rule, the forwarding class is only overridden when the fc <i>fc-name</i> parameter is defined on the rule.
Priority	The default enqueueing priority overrides for all packets received on an ingress SAP using this policy that match this rule
	High - the high enqueueing parameter for a packet increases the likelihood of enqueueing the packet when the ingress queue is congested
	Low - the low enqueueing parameter for a packet decreases the likelihood of enqueueing the packet when the ingress queue is congested
FC	The override for the forwarding class value
Associations	Service-Id - The unique service ID number that identifies the service in the service domain
	Customer-Id - The customer ID that identifies the customer to the service
	SAP - The SAP within the service where the service ingress policy is applied

sap-egress

Syntax	sap-egress [<i>policy-id</i>] [standard mc-mlppp] [detail]
Context	show>qos
Description	This command displays service egress and MC-MLPPP SAP egress QoS policy information.
Parameters	<p><i>policy-id</i> — displays information about the specific policy ID</p> <p>Default all service egress policies</p> <p>Values 1 to 65535</p> <p>standard — displays all standard SAP egress QoS policies</p> <p>mc-mlppp — displays only MC-MLPPP SAP egress policy information</p> <p>detail — displays detailed policy information including policy associations</p>
Output	The following output is an example of service egress and MC-MLPPP SAP egress QoS policy information, and Table 36 describes the fields.

Sample Output

```
*A:ALU-1# show qos sap-egress
=====
Sap Egress Policies
=====
Policy-Id   Type           Scope           Description
-----
1           Default        Template        Default SAP egress QoS policy.
200          Standard       Template        SAP Egress Policy 200
300          MC-MLPPP       Template        SAP Egress Policy 300
400          Standard       Exclusive       Egress Policy 400
500          Standard       Template        Egress Policy 500
550          MC-MLPPP       Template        New Multi-class type policy
600          Standard       Exclusive
=====
*A:ALU-1#
```

*A:ALU-1# show qos **sap-egress 500 detail**

=====

QoS Sap Egress

=====

Sap Egress Policy (500)

Policy-id	: 500	Scope	: Template
Description	: Egress Policy 500		

Queue	CIR	Admin	PIR	Admin	CBS	HiPrio	Slope-Policy
	CIR	Rule	PIR	Rule	MBS		
1	0		max		def	def	default
		closest		closest	def		
7		max		max	10	10	default
		closest		closest	10		

FC Name	Queue-id	Dot1p	Explicit/Default	DSCP Marking
be	def		Default	default
ef	def		Default	DSCP In:cp2 Out:cp3

Associations

No Associations Found.

=====

*A:ALU-1#

*A:ALU-1# show qos mc-mlppp **sap-egress 300 detail**

=====

QoS Sap Egress

=====

MC-MLPPP Sap Egress Policy (300)

Policy-id	: 300	Scope	: Template
Description	: MC-MLPPP Policy 300		

Queue	PIR	Admin	CBS	HiPrio	Slope-Policy
	PIR	Rule	MBS		
1	max		def	def	default
		closest		def	

FC Name	Queue-id	DSCP Marking
be	def	default

Associations

No Associations Found.

=====
*A:ALU-1#

Table 36: SAP Egress Command Output

Label	Description
Policy-Id	The ID that uniquely identifies the policy
Type	Indicates the type of SAP egress policy; Default, Standard, or MC-MLPPP
Scope	Exclusive - this policy can only be applied to a single SAP
	Template - this policy can be applied to multiple SAPs on the router
Description	A text string that helps identify the policy's context in the configuration file
Queue	
CIR Admin	The administrative Committed Information Rate (CIR) parameters for the queue. The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth.
CIR Rule	min - the operational CIR for the queue will be equal to or greater than the administrative rate specified using the rate command except where the derived operational CIR is greater than the operational PIR. If the derived operational CIR is greater than the derived operational PIR, the operational CIR will be made equal to the operational PIR.
	max - the operational CIR for the queue will be equal to or less than the administrative rate specified using the rate command
	closest - the operational CIR for the queue will be the rate closest to the rate specified using the rate command without exceeding the operational PIR
PIR Admin	The administrative Peak Information Rate (PIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets out an egress interface.
PIR Rule	min - the operational PIR for the queue will be equal to or greater than the administrative rate specified using the rate command
	max - the operational PIR for the queue will be equal to or less than the administrative rate specified using the rate command
	closest - the operational PIR for the queue will be the rate closest to the rate specified using the rate command

Table 36: SAP Egress Command Output (Continued)

Label	Description
CBS	def - the CBS value reserved for the queue
	value - the value to override the default reserved buffers for the queue
MBS	def - the MBS value reserved for the queue
	value - the value to override the default maximum size for the queue
HiPrio	The percentage of buffer space for the queue, used exclusively by high-priority packets
Slope-Policy	The slope policy for the queue
FC Name	The override for the forwarding class value
Queue-id	The <i>queue-id</i> that uniquely identifies the queue within the policy
Dot1p	The egress dot1p priority bits values for the forwarding class
Explicit/Default	Explicit - the egress IEEE 802.1P (dot1p) bits marking for <i>fc-name</i>
	Default - the default dot1p value (0) is used
DSCP	The DSCP name for the forwarding class
Marking	The DSCP priority bits mapping for the forwarding class
Associations	Service-Id - The unique service ID number that identifies the service in the service domain
	Customer-Id - The customer ID that identifies the customer to the service
	SAP - The Service Access Point within the service where the policy is applied

pools

Syntax	pools <i>mda-id</i> [detail]
Context	show
Description	<p>This command displays buffer pool information on the adapter card. This information pertains to the memory allocating used for queuing purposes.</p> <p>The information is displayed in packet size. There are 2304 bytes per packet allocation within the pool. This packet allocation is large enough for any supported MTU.</p>
Parameters	<p><i>mda-id</i> — the location of the adapter card (in the form <i>slot/card</i>)</p> <p>detail — displays detailed buffer pool information on the adapter card</p>
Output	The following output is an example of buffer pool information on an adapter card, and Table 37 describes the fields.

Sample Output

```
*A:ALU-1# show>pools# mda 1/2 detail
=====
Pool Information
=====
Pool Total          : 201044 pkts
Pool Shared         : 153458 pkts      Pool Resv          : 47586 pkts
Pool Total In Use   : 37 pkts
Pool Exhaustion Drop : 0

=====
Access Ingress Queues
=====
-----
Name                               FC-Maps   O.MBS (pkt) Depth (pkt)
                               O.CBS (pkt)
-----
1301->1/2/8:1->1
                               be 12 af 11 100      1
                               h2 ef h1 nc  3
1302->1/2/8:2->1
                               be 12 af 11 100      1
                               h2 ef h1 nc  3
1303->1/2/8:3->1
                               be 12 af 11 100      1
                               h2 ef h1 nc  3
1304->1/2/8:4->1
                               be 12 af 11 100      1
                               h2 ef h1 nc  3
1305->1/2/8:5->1
                               be 12 af 11 100      1
                               h2 ef h1 nc  3
1306->1/2/8:6->1
                               be 12 af 11 100      1
                               h2 ef h1 nc  3
```

1307->1/2/8:7->1	be l2 af l1 100 h2 ef h1 nc 3	1
1308->1/2/8:8->1	be l2 af l1 100 h2 ef h1 nc 3	1
1309->1/2/8:9->1	be l2 af l1 100 h2 ef h1 nc 3	1
1310->1/2/8:10->1	be l2 af l1 100 h2 ef h1 nc 3	1
1311->1/2/8:11->1	be l2 af l1 100 h2 ef h1 nc 3	1
1312->1/2/8:12->1	be l2 af l1 100 h2 ef h1 nc 3	1
1313->1/2/8:13->1	be l2 af l1 100 h2 ef h1 nc 3	1
1314->1/2/8:14->1	be l2 af l1 100 h2 ef h1 nc 3	1
1315->1/2/8:15->1	be l2 af l1 100 h2 ef h1 nc 3	1
1316->1/2/8:16->1	be l2 af l1 100 h2 ef h1 nc 3	1
=====		
Access Egress Queues		
=====		
Name	FC-Maps	O.MBS (pkt) O.CBS (pkt) Depth (pkt)

1301->1/2/8:1->1	be l2 af l1 100 h2 ef h1 nc 3	1
1302->1/2/8:2->1	be l2 af l1 100 h2 ef h1 nc 3	1
1303->1/2/8:3->1	be l2 af l1 100 h2 ef h1 nc 3	1
1304->1/2/8:4->1	be l2 af l1 100 h2 ef h1 nc 3	1
1305->1/2/8:5->1	be l2 af l1 100 h2 ef h1 nc 3	1
1306->1/2/8:6->1	be l2 af l1 100 h2 ef h1 nc 3	1
1307->1/2/8:7->1	be l2 af l1 100 h2 ef h1 nc 3	1

Service Egress and Ingress QoS Policy Command Reference

1308->1/2/8:8->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1309->1/2/8:9->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1310->1/2/8:10->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1311->1/2/8:11->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1312->1/2/8:12->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1313->1/2/8:13->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1314->1/2/8:14->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1315->1/2/8:15->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
1316->1/2/8:16->1	be l2 af l1	100	1
	h2 ef h1 nc	3	
=====			
Network Ingress Queues			
=====			
FC-Maps	Dest	O.MBS (pkt) O.CBS (pkt)	Depth (pkt)

be	1/1	10052 201	0
l2	1/1	10052 502	0
af	1/1	10052 1507	0
l1	1/1	5026 502	0
h2	1/1	10052 1507	0
ef	1/1	10052 1507	0
h1	1/1	5026 502	0
nc	1/1	5026 502	0
be	1/2	10052 201	0
l2	1/2	10052 502	0
af	1/2	10052 1507	0
l1	1/2	5026 502	0
h2	1/2	10052	0

Service Egress and Ingress QoS Policies

		1507	
ef	1/2	10052	0
		1507	
h1	1/2	5026	0
		502	
nc	1/2	5026	0
		502	
be	1/3	10052	0
		201	
l2	1/3	10052	0
		502	
af	1/3	10052	0
		1507	
l1	1/3	5026	0
		502	
h2	1/3	10052	0
		1507	
ef	1/3	10052	0
		1507	
h1	1/3	5026	0
		502	
nc	1/3	5026	0
		502	
be	1/4	10052	0
		201	
l2	1/4	10052	0
		502	
af	1/4	10052	0
		1507	
l1	1/4	5026	0
		502	
h2	1/4	10052	0
		1507	
ef	1/4	10052	0
		1507	
h1	1/4	5026	0
		502	
nc	1/4	5026	0
		502	
be	1/5	10052	0
		201	
l2	1/5	10052	0
		502	
af	1/5	10052	0
		1507	
l1	1/5	5026	0
		502	
h2	1/5	10052	0
		1507	
ef	1/5	10052	0
		1507	
h1	1/5	5026	0
		502	
nc	1/5	5026	0
		502	
be	1/6	10052	0
		201	
l2	1/6	10052	0
		502	

Service Egress and Ingress QoS Policy Command Reference

```

af                1/6      10052      0
                  1507
l1                1/6      5026       0
                  502
h2                1/6      10052      0
                  1507
ef                1/6      10052      0
                  1507
h1                1/6      5026       0
                  502
nc                1/6      5026       0
                  502
=====
Network Egress Queues
=====
-----
FC-Maps ID                O.MBS(pkt) Depth(pkt)
                        O.CBS(pkt)
-----
be          1/2/7                10052      0
                  201
l2          1/2/7                10052      0
                  502
af          1/2/7                10052      0
                  1507
l1          1/2/7                5026       0
                  502
h2          1/2/7                10052      0
                  1507
ef          1/2/7                10052      0
                  1507
h1          1/2/7                5026       0
                  502
nc          1/2/7                5026       0
                  502
=====
*A:ALU-1#

```

Table 37: Buffer Pool Command Output

Label	Description
Pool Total	The total number of available packets
Pool Shared	The number of packets which can be shared
Pool Total In Use	The total number of packets in use, in real-time
Pool Exhaustion Drop	The number of packets dropped due to pool exhaustion
Pool Resv	The number of packets reserved or committed
FC-Maps	The Forwarding Class-to-queue mappings
Depth	The queue occupancy (the number of packets in the queue), in real-time

Slope QoS Policies

In This Chapter

This chapter provides information to configure slope QoS policies using the command line interface.

Topics in this chapter include:

- [Overview on page 252](#)
- [Basic Configuration on page 253](#)
 - [Creating a Slope QoS Policy on page 253](#)
 - [Applying Slope Policies on page 254](#)
- [Service Management Tasks on page 256](#)
 - [Deleting QoS Policies on page 256](#)
 - [Copying and Overwriting QoS Policies on page 256](#)
 - [Editing QoS Policies on page 258](#)
- [Slope QoS Policy Command Reference on page 259](#)

Overview

Random Early Detection (RED) and Weighted Random Early Detection (WRED) queue management policies are associated with queues and can be created at both access and network ports and in both directions (that is, ingress and egress). The main difference is that with WRED, there can be more than one slope curve managing the fill rate of the same queue. One curve manages the discards on high-priority traffic, and another curve manages the discards on low-priority traffic. For more information, refer to [WRED and RED Slope Policies](#).

For information about the tasks and commands necessary to access the command line interface and to configure and maintain the 7705 SAR, refer to the 7705 SAR OS Basic System Configuration Guide, “CLI Usage”.

Basic Configuration

A basic slope QoS policy must conform to the following rules.

- Each slope policy must have a unique policy ID.
- High slope and low slope are shut down (default).
- Default values can be modified but parameters cannot be deleted.

Creating a Slope QoS Policy

Configuring and applying QoS policies is optional. If no QoS policy is explicitly defined, a default QoS policy is applied.

To create a new slope policy, you must define the following:

- a slope policy name — the system does not dynamically assign a name
- a description — a brief description of the of policy
- the high slope for the high-priority WRED/RED slope graph
- the low slope for the low-priority WRED/RED slope graph

Use the following CLI syntax to configure a slope policy:

CLI Syntax:

```
config>qos#
    slope-policy name
        description description-string
        high-slope
            max-avg percent
            max-prob percent
            start-avg percent
            no shutdown
        low-slope
            max-avg percent
            max-prob percent
            start-avg percent
            no shutdown
```

Example:

```
*A:ALU-1#
configure qos slope-policy "SlopePolicy1" create
config>qos>slope-policy$ description "Test1"
config>qos>slope-policy$ high-slope
config>qos>slope-policy>high-slope$ max-avg 90
config>qos>slope-policy>high-slope$ max-prob 60
config>qos>slope-policy>high-slope$ start-avg 90
config>qos>slope-policy>high-slope$ shutdown
```

```
config>qos>slope-policy>high-slope$ exit
config>qos>slope-policy$ low-slope
config>qos>slope-policy>low-slope$ max-avg 75
config>qos>slope-policy>low-slope$ max-prob 40
config>qos>slope-policy>low-slope$ start-avg 75
config>qos>slope-policy>low-slope$ exit
config>qos>slope-policy$ exit
*A:ALU-1#
```

The following sample output shows the configuration for SlopePolicy1:

```
*A:ALU-1>config>qos# info
#-----
echo "QoS Policy Configuration"
#-----
      slope-policy "SlopePolicy1" create
        description "Test1"
        high-slope
          shutdown
          start-avg 90
          max-prob 60
        exit
        low-slope
          shutdown
          start-avg 75
          max-prob 40
        exit
      exit
```

Applying Slope Policies

Slope policies are applied to network and access egress and ingress queues.

Use the following CLI syntax:

CLI Syntax: config>qos>network-queue>queue>slope-policy name
config>qos>sap-ingress>queue>slope-policy name
config>qos>sap-egress>queue>slope-policy name

Default Slope Policy Values

The default slope policies are identified as default. The default policies cannot be edited or deleted. [Table 38](#) displays the default slope policy parameters.

Table 38: Slope Policy Defaults

Field	Default
description	Default slope policy
high-slope	
shutdown	shutdown
start-avg	70
max-avg	90
max-prob	80
low-slope	
shutdown	shutdown
start-avg	50
max-avg	75
max-prob	80

The following sample output displays the default configuration:

```
A*A:ALU-1>config>qos# info detail
#-----
echo "QoS Policy Configuration"
#-----
...
    slope-policy "default" create
    description "Default slope policy."
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 80
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 80
    exit
...
```

Service Management Tasks

This section describes the following service management tasks:

- [Deleting QoS Policies](#)
- [Copying and Overwriting QoS Policies](#)
- [Editing QoS Policies](#)

Deleting QoS Policies

A QoS policy cannot be deleted until it is removed from a network or access egress/ingress queue. Use the following CLI syntax:

CLI Syntax: `config>qos>network-queue>queue>no slope-policy`
`config>qos>sap-ingress>queue>no slope-policy`
`config>qos>sap-egress>queue>no slope-policy`

Removing a Policy from the QoS Configuration

Use the following CLI syntax to delete a slope policy:

CLI Syntax: `config>qos# no slope-policy name`

Example: `config>qos# no slope-policy SlopePolicy1`

Copying and Overwriting QoS Policies

You can copy an existing slope policy, rename it with a new policy ID value, or overwrite an existing policy ID. The `overwrite` option must be specified or an error occurs if the destination policy ID exists.

Use the following syntax to overwrite an existing QoS slope policy.

CLI Syntax: `config>qos> copy slope-policy source-policy-name`
`dest-policy-name [overwrite]`

Example: `*A:ALU-1>config>qos# copy slope-policy SlopePolicy1`
`SlopePolicy2 overwrite`
`config>qos# exit`
`*A:ALU-2#`

The following sample output displays the copied policies:

```
*A:ALU-2>config>qos# info detail
#-----
echo "QoS Policy Configuration"
#-----
...
    slope-policy "default" create
        description "Default slope policy."
        high-slope
            shutdown
            start-avg 70
            max-avg 90
            max-prob 80
        exit
        low-slope
            shutdown
            start-avg 50
            max-avg 75
            max-prob 80
        exit
    exit
slope-policy "SlopePolicy2" create
    description "Test2"
    high-slope
        shutdown
        max-avg 100
        start-avg 100
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 75
        max-avg 75
        max-prob 40
    exit
exit
slope-policy "SlopePolicy1" create
    description "Test1"
    high-slope
        shutdown
        start-avg 90
        max-avg 60
        max-prob 90
    exit
    low-slope
        shutdown
        start-avg 75
        max-avg 75
        max-prob 40
    exit
exit
slope-policy "SlopePolicy2" create
    description "Test1"
    high-slope
        shutdown
        start-avg 90
        max-avg 60
        max-prob 90
```

```
exit
low-slope
    shutdown
    start-avg 75
    max-avg 75
    max-prob 40
exit
exit
...
```

Editing QoS Policies

You can change existing policies and entries in the CLI. The changes are applied immediately to all queues where this policy is applied. To prevent configuration errors, copy the policy to a work area, make the edits, and then write over the original policy.

Slope QoS Policy Command Reference

Command Hierarchies

- [Configuration Commands](#)
- [Operational Commands](#)
- [Show Commands](#)

Configuration Commands

```

config
  — qos
      — [no] slope-policy name [create]
          — description description-string
          — no description
          — [no] high-slope
              — max-avg percent
              — no max-avg
              — max-prob percent
              — no max-prob
              — start-avg percent
              — no start-avg
              — [no] shutdown
          — [no] low-slope
              — max-avg percent
              — no max-avg
              — max-prob percent
              — no max-prob
              — start-avg percent
              — no start-avg
              — [no] shutdown

```

Operational Commands

```

config
  — qos
      — copy slope-policy src-name dst-name [overwrite]

```

Show Commands

```
show
  — qos
    — slope-policy [slope-policy-name] [detail]
```

Command Descriptions

- [Configuration Commands on page 262](#)
- [Operational Commands on page 268](#)
- [Show Commands on page 269](#)

Configuration Commands

- [Generic Commands on page 263](#)
- [Slope Policy QoS Commands on page 264](#)
- [WRED/RED Slope Commands on page 266](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>qos>slope-policy
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes any description string from the context.
Default	none
Parameters	<i>description-string</i> — a text string describing the entity. 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.

Slope Policy QoS Commands

slope-policy

Syntax	[no] slope-policy <i>name</i> [create]
Context	config>qos
Description	This command enables the context to configure a QoS slope policy.
Default	slope-policy “default”
Parameters	<i>name</i> — the name of the slope policy <div style="margin-left: 40px;"> Values Valid names consist of 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. create — keyword used to create a slope policy </div>

high-slope

Syntax	[no] high-slope
Context	config>qos>slope-policy
Description	<p>The high-slope context contains the commands and parameters for defining the high-priority Weighted Random Early Detection (WRED) or Random Early Detection (RED) slope graph. Each queue supports a high-priority WRED/RED slope for managing access to the queue for low-priority or out-of-profile packets.</p> <p>The high-slope parameters can be changed at any time and the affected queue high-priority WRED/RED slopes will be adjusted appropriately.</p> <p>The no form of this command restores the high slope configuration commands to the default values. If the commands within high-slope are set to the default parameters, the high-slope mode will not appear in save config and show config output unless the detail parameter is present.</p>

low-slope

Syntax	[no] low-slope
Context	config>qos>slope-policy
Description	<p>The low-slope context contains the commands and parameters for defining the low-priority or high-priority WRED/RED slope graph. Each queue supports a low-priority WRED/RED slope for managing access to the queue for low-priority or out-of-profile packets.</p> <p>The low-slope parameters can be changed at any time and the queue low-priority WRED/RED slopes will be adjusted appropriately.</p> <p>The no form of this command restores the low slope configuration commands to the default values. If the leaf commands within low-slope are set to the default parameters, the low-slope mode will not appear in save config and show config output unless the detail parameter is present.</p>

WRED/RED Slope Commands

max-avg

Syntax	max-avg <i>percent</i> no max-avg
Context	config>qos>slope-policy>high-slope config>qos>slope-policy>low-slope
Description	<p>This command sets the low-priority or high-priority WRED or RED slope position for the queue average utilization value where the packet discard probability rises directly to one. The <i>percent</i> parameter is expressed as a percentage of the maximum queue depth.</p> <p>The no form of this command restores the max-avg value to the default setting. If the current start-avg setting is larger than the default, an error will occur and the max-avg setting will not be changed to the default.</p>
Default	max-avg 90 — high slope default is 90% queue utilization before discard probability is 1 max-avg 75 — low slope default is 75% queue utilization before discard probability is 1
Parameters	<p><i>percent</i> — the percentage of the maximum queue depth at which point the drop probability becomes 1. The value entered must be greater or equal to the current setting of start-avg. If the entered value is smaller than the current value of start-avg, an error will occur and no change will take place.</p> <p>Values 0 to 100</p>

max-prob

Syntax	max-prob <i>percent</i> no max-prob
Context	config>qos>slope-policy>high-slope config>qos>slope-policy>low-slope
Description	<p>This command sets the high-priority or low-priority WRED/RED maximum discard probability (at slope position max-avg). The <i>percent</i> parameter is expressed as a percentage of packet discard probability where always discard is a probability of 1. A max-prob value of 80 represents 80% of 1, or a packet discard probability of 0.8.</p> <p>The no form of this command restores the max-prob value to the default setting.</p>
Default	max-prob 80 — 80% maximum drop probability corresponding to the max-avg

Parameters	<i>percent</i> — the maximum drop probability percentage corresponding to the max-avg , expressed as a decimal integer
Values	0 to 100

shutdown

Syntax	[no] shutdown
Context	config>qos>slope-policy>high-slope config>qos>slope-policy>low-slope
Description	<p>This command enables or disables the administrative status of the WRED/RED slope.</p> <p>By default, all slopes are shut down and have to be explicitly enabled (no shutdown).</p> <p>The no form of this command administratively enables the WRED/RED slope.</p>
Default	shutdown — WRED/RED slope disabled, implying a zero (0) drop probability

start-avg

Syntax	start-avg percent no start-avg
Context	config>qos>slope-policy>high-slope config>qos>slope-policy>low-slope
Description	<p>This command sets the high-priority or low-priority WRED/RED slope position for the queue average utilization value where the packet discard probability starts to increase above zero. The <i>percent</i> parameter is expressed as a percentage of the maximum queue depth.</p> <p>The no form of this command restores the start-avg value to the default setting. If the max-avg setting is smaller than the default, an error will occur and the start-avg setting will not be changed to the default.</p>
Parameters	<p><i>percent</i> — the percentage of the maximum queue depth where the packet discard probability starts to increase above zero</p> <p>Values 0 to 100</p> <p>Default 50</p>

Operational Commands

copy

Syntax	copy slope-policy <i>src-name dst-name</i> [overwrite]
Context	config>qos
Description	<p>This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.</p> <p>The copy command is a configuration level maintenance tool used to create new policies using existing policies. It also allows bulk modifications to an existing policy with the use of the overwrite keyword.</p>
Parameters	<p>slope-policy <i>src-name dst-name</i> — indicates that the source policy ID and the destination policy ID are slope policy IDs. Specify the source policy ID that the copy command will attempt to copy from and specify the destination policy ID to which the command will copy a duplicate of the policy.</p> <p>overwrite — specifies that the existing destination policy is to be replaced. Everything in the existing destination policy will be overwritten with the contents of the source policy. If overwrite is not specified, an error will occur if the destination policy ID exists.</p>

Show Commands

slope-policy

Syntax	slope-policy [<i>slope-policy-name</i>] [detail]
Context	show>qos
Description	This command displays slope policy information.
Parameters	slope-policy <i>slope-policy-name</i> — the name of the slope policy detail — displays detailed information about the slope policy
Output	The following output is an example of slope policy information, and Table 39 describes the fields.

Sample Output

```
*A:ALU-1# show qos slope-policy SlopePolicy1 detail
```

```
=====
QoS Slope Policy
=====
```

```
Policy       : SlopePolicy1
Description  : Test1
Time Avg     : 3
```

```
-----
High Slope Parameters
-----
```

```
Start Avg      : 90                      Admin State : Disabled
Max Avg        : 90                      Max Prob.   : 60
```

```
-----
Low Slope Parameters
-----
```

```
Start Avg      : 75                      Admin State : Disabled
Max Avg        : 75                      Max Prob.   : 40
```

```
-----
Associations
-----
```

Object Type	Object Id	Queue
sap-ingress	1	1
sap-ingress	8	1
sap-ingress	8	2
sap-egress	1	1
network-queue	default	1
network-queue	default	2
network-queue	default	3
network-queue	default	4
network-queue	default	5
network-queue	default	6

```

network-queue default 7
network-queue default 8
network-queue default 9
network-queue default 10
network-queue default 11
network-queue default 12
network-queue default 13
network-queue default 14
network-queue default 15
network-queue default 16

```

```

=====
*A:ALU-1#

```

Table 39: Slope Policy Command Output Fields

Label	Description
Policy	The ID that uniquely identifies the policy
Description	A text string that helps identify the policy's context in the configuration file
Time Avg	The time average factor, which is the exponential weight factor used in calculating the average queue size. The <i>time_average_factor</i> parameter is non-user-configurable, and is set to a system-wide default value of 3.
High Slope Parameters	
Start Avg	The high-priority WRED/RED slope position for the queue average utilization value where the packet discard probability starts to increase above zero
Max Avg	The high-priority WRED or RED slope position for the queue average utilization value where the packet discard probability rises directly to one
Admin State	enabled - the administrative status of the WRED/RED slope is enabled
	disabled - the administrative status of the WRED/RED slope is disabled
Max Prob.	The high-priority WRED/RED maximum discard probability (at slope position max-avg)
Low Slope Parameters	
Start Avg	The low-priority WRED/RED slope position for the queue average utilization value where the packet discard probability starts to increase above zero
Max Avg	The low-priority WRED or RED slope position for the queue average utilization value where the packet discard probability rises directly to one

Table 39: Slope Policy Command Output Fields (Continued)

Label	Description
Admin State	enabled - the administrative status of the WRED/RED slope is enabled
	disabled - the administrative status of the WRED/RED slope is disabled
Max Prob.	The low-priority WRED/RED maximum discard probability (at slope position max-avg)
Associations	
Object Type	The type of object using the specified slope policy
Object Id	The identifier of the object using the specified slope policy
Queue	The number of the queue using the specified slope policy

ATM QoS Traffic Descriptor Profiles

In This Chapter

This chapter provides information to configure QoS Traffic Descriptor Profiles using the command line interface.

- [ATM Traffic Descriptor Profiles on page 274](#)
 - [ATM Traffic Management on page 274](#)
- [Basic Configuration on page 278](#)
 - [Creating an ATM Traffic Descriptor Profile QoS Policy on page 278](#)
 - [Applying ATM Traffic Descriptor Profile Policies on page 279](#)
- [Service Management Tasks on page 281](#)
 - [Removing an ATM Traffic Descriptor Profile from the QoS Configuration on page 281](#)
 - [Copying and Overwriting an ATM Traffic Descriptor Profile on page 281](#)
 - [Editing QoS Policies on page 281](#)
- [ATM QoS Policy Command Reference on page 283](#)

ATM Traffic Descriptor Profiles

This section provides a description of support for ATM QoS policy features. Each traffic descriptor defines the expected rates and characteristics of traffic.

ATM Traffic Management

The 7705 SAR supports the ATM Forum Traffic Management Specification Version 4.1. The following sections describe the QoS features for ATM Permanent Virtual Connections (PVCs).

ATM Service Categories

The 7705 SAR supports the following service categories:

- CBR – Constant Bit Rate
- rt-VBR – Real-Time Variable Bit Rate
- nrt-VBR –Non-Real-Time Variable Bit Rate
- UBR/UBR+MIR – Unspecified Bit Rate with Minimum Cell Rate (note that UBR is a special case of UBR+MIR where MIR=0)

ATM Traffic Descriptors and QoS Parameters

[Table 40](#) shows the ATM traffic descriptors supported on the 7705 SAR.

Table 40: ATM Traffic Descriptors

Service Category	Traffic Descriptors
CBR	P0_1
	PIR in kb/s (applies to CLP=0 and CLP=1 flows)
rt-VBR and nrt-VBR	P0_1 and S0_1
	PIR in kb/s (applies to CLP=0 and CLP=1 flows)
	SIR in kb/s (applies to CLP=0 and CLP=1 flows)
	MBS in cells (applies to CLP=0 and CLP=1 flows)

Table 40: ATM Traffic Descriptors (Continued)

Service Category	Traffic Descriptors
	P0_1 and S0
	PIR in kb/s (applies to CLP=0 and CLP=1 flows; non-conforming CLP=0 cells are discarded)
	SIR in kb/s (applies to CLP=0 flow only)
	MBS in cells (applies to CLP=0 flow only)
	P0_1 and S0_Tag
	PIR in kb/s (applies to CLP=0 and CLP=1 flows; non-conforming CLP=0 flows are tagged to CLP=1 flows)
UBR/UBR+MIR	P0_1
	PIR in kb/s (applies to CLP=0 and CLP=1 flows)
	MIR in kb/s (applies to CLP=0 and CLP=1 flows)

ATM Policing

The policing option, when enabled, applies only to ingress traffic. Similarly, the shaping option, if enabled, applies only to egress traffic. For example, if a traffic descriptor has both policing and shaping enabled, the policing option is enforced for the ingress traffic, while the shaping option is enforced for the egress traffic. The following ATM service category conformance definitions are supported:

- P0_1 – CBR
- P0_1 and S0_1 – VBR.1
- P0_1 and S0 – VBR.2
- P0_1 and S0_Tag – VBR.3

P represents the peak rate, S represents the sustained rate, 0 or 1 represents the CLP value to which policing is applied if the cell is non-conforming, and Tag indicates that the CLP value has changed from 0 to 1. For example:

- P0_1 — means that policing is applied to non-conforming peak rate cells with CLP values of 0 or 1
- P0_1 and S0_Tag — means that policing is applied to non-conforming peak rate cells with CLP values of 0 or 1 and policing is applied to non-conforming sustained rate cells with a CLP value of 0 with the action to change the CLP value to 1

Shaping

ATM layer egress shaping is supported for CBR, rt-VBR, and nrt-VBR VCs. A CBR VC is shaped to a single leaky bucket with the parameter PIR. An rt-VBR VC or an nrt-VBR VC is shaped to two leaky buckets with parameters PIR and {SIR, BT}, where BT is the Burst Tolerance and is a function of the MBS parameters configured by the user in the traffic descriptor.



Note: Shaping to the specified traffic descriptor in the ATM traffic descriptor profile is always enabled for CBR and rt-VBR VCs.

In order to enforce Service Level Agreement, ATM layer ingress policing is supported at ingress, so naturally no shaping is needed. At ingress, after optional policing is applied, packet level queue based soft-policing is supported per the service ingress QoS policy applied to the ATM SAP.

ATM Queuing and Scheduling

The 7705 SAR provides a per-VC queuing architecture on the 16-port T1/E1 ASAP Adapter card, 32-port T1/E1 ASAP Adapter card, and 2-port OC3/STM1 Channelized Adapter card with atm/ima encapsulation. The 7705 SAR provides a per-VC queuing architecture on the 4-port OC3/STM1 Clear Channel Adapter card and 4-port DS3/E3 Adapter card with atm encapsulation. In the egress direction toward the ATM port, the scheduling priority at the ATM layer is as follows.

- CBR VCs are always shaped and are scheduled with strict priority over all other service categories.
- rt-VBR VCs are always shaped and are scheduled next with strict priority over nrt-VBR and UBR VCs.
- nrt-VBR shaped VCs are scheduled next with strict priority over nrt-VBR unshaped VCs and UBR VCs.
- nrt-VBR unshaped VCs and UBR VCs are scheduled as a common class. Scheduling among these VCs is done using a Weighted Round Robin (WRR) scheduler, where the weight of each VC is determined by the configured SIR for nrt-VBR and by the MIR for UBR VCs. The scheduling is work-conserving, so each VC has access to excess bandwidth in proportion to its SIR/MIR. Under congestion, the performance of each VC degrades proportionally to the weight of the VC.

Congestion Avoidance

Congestion and potential discards are performed on a per-forwarding class basis in the SAP queues in the CSM.

Basic Configuration

A basic ATM QoS traffic descriptor profile must conform to the following rules.

- Each policy must have a unique policy ID.
- Default values can be modified but parameters cannot be deleted.

Creating an ATM Traffic Descriptor Profile QoS Policy

Configuring and applying QoS policies and profiles other than the default policy is optional. To create an ATM QoS traffic descriptor profile, perform the following:

- assign a policy ID (policy number) — the system does not dynamically assign an ID
- include a description — provides a brief overview of policy features
- configure traffic attributes of the ATM traffic profile
- determine whether egress shaping should occur

Use the following CLI syntax to configure an atm-td-profile policy.

CLI Syntax:

```
config>qos#
    atm-td-profile traffic-desc-profile-id
        description description-string
        descriptor-type
            {P0_1|P0_1andS0_Tag|P0_1andS0|P0_1andS0_1}
        [no] policing
        service-category service-category
        [no] shaping
        traffic [sir sir-val] [pir pir-val] [mir mir-val]
            [mbs mbs-val][cdvt cdvt-val]
```

The following sample output displays an example of the command syntax.

Example:

```
*A:ALU-1# configure qos
config>qos# atm-td-profile 3 create
config>qos>atm-td-profile$ description "ATM TD profile3"
config>qos>atm-td-profile$ service-category rt-vbr
config>qos>atm-td-profile$ descriptor-type P0_1andS0_1
config>qos>atm-td-profile$ policing
config>qos>atm-td-profile$ shaping
config>qos>atm-td-profile$ traffic sir 500 pir 500 mbs 500
cdvt 500
config>qos>atm-td-profile$ exit
config>qos# exit
*A:ALU-1#
```

The following sample output displays the profile configuration for ATM TD profile 3:

```
*A:ALU-1>config>qos# info
#-----
echo "QoS Policy Configuration"
#-----
...
    atm-td-profile 3 create
        description "ATM TD profile3"
        service-category rt-vbr
        traffic sir 500 pir 500 mbs 500 cdvt 500
        policing
    exit
...
*A:ALU-1
```

Applying ATM Traffic Descriptor Profile Policies

ATM QoS traffic descriptor profiles are applied to ATM VLL (Apipe) SAPs.

ATM VLL (Apipe) SAPs

Use the following CLI syntax to apply ATM QoS traffic descriptor profile policies to Apipe SAPs on ingress and egress.

```
CLI Syntax: config>service>apipe>sap# atm
                egress
                  traffic-desc traffic-desc-profile-id
                ingress
                  traffic-desc traffic-desc-profile-id
```

Default ATM Traffic Descriptor Profile Policy Values

The default ATM QoS traffic descriptor profile is 1. The default profile cannot be edited or deleted.

Table 41 below shows the ATM TD profile defaults.

Table 41: ATM-TD-Profile Defaults

Field	Default
atm-td-profile traffic-desc-profile-id	1
description	Default Traffic Descriptor
descriptor-type	Based on service category: CBR: P0_1 UBR: P0_1 UBR+MIR: P0_1 rt-VBR or nrt-VBR: P0_1 and S0_1
policing	No policing
service-category	UBR
traffic	No traffic
shaping	No shaping

The following sample output displays the default configuration:

```
A:ALU-1>config>qos# info detail
-----
Echo "QoS Policy Configuration"
-----
    atm-td-profile 1 create
      description "Default Traffic Descriptor"
      service-category ubr
      no traffic
      no policing
      descriptor-type P0_1
      no shaping
    exit
...
```


Service Management Tasks

This section describes the following ATM Traffic Descriptor Profile service management tasks:

- [Removing an ATM Traffic Descriptor Profile from the QoS Configuration](#)
- [Copying and Overwriting an ATM Traffic Descriptor Profile](#)
- [Editing QoS Policies](#)

Removing an ATM Traffic Descriptor Profile from the QoS Configuration

The default ATM traffic descriptor profile cannot be deleted.

To delete an ATM QoS traffic descriptor profile, enter the following command:

CLI Syntax: `config>qos# no atm-td-profile traffic-desc-profile-id`

Example: `config>qos# no atm-td-profile 3`

Copying and Overwriting an ATM Traffic Descriptor Profile

You can copy an existing profile, rename it with a new profile ID value, or overwrite an existing profile ID. The `overwrite` option must be specified or an error occurs if the destination profile ID exists.

CLI Syntax: `config>qos> copy atm-td-profile src-prof dst-prof [overwrite]`

Example: `*A:ALU-1#>config>qos# copy atm-td-profile 2 3`
`A:ALU-48>config>qos# copy atm-td-profile 2 3 overwrite`
`A:ALU-48>config>qos#`

Editing QoS Policies

You can change existing policies and entries in the CLI. The changes are applied immediately to all services where this policy is applied. To prevent configuration errors, copy the policy to a work area, make the edits, and then write over the original policy.

ATM QoS Policy Command Reference

Command Hierarchies

- [Configuration Commands](#)
- [Operational Commands](#)
- [Show Commands](#)

Configuration Commands

```

config
— qos
  [no] atm-td-profile traffic-desc-profile-id [create]
    — description description-string
    — no description
    — descriptor-type type
    — [no] policing
    — service-category service-category
    — [no] shaping
    — traffic [sir sir-val] [pir pir-val] [mir mir-val] [mbs mbs-val] [cdvt cdvt-val]
    — no traffic

```

Operational Commands

```

config
— qos
  — copy atm-td-profile src-prof dst-prof [overwrite]

```

Show Commands

```

show
— qos
  — atm-td-profile [traffic-desc-profile-id] [detail]
— service
  — sap-using [ingress | egress] atm-td-profile td-profile-id
  — sap-using [ingress | egress] qos-policy qos-policy-id

```

Command Descriptions

- [Configuration Commands on page 285](#)
- [Operational Commands on page 294](#)
- [Show Commands on page 295](#)

Configuration Commands

- [Generic Commands on page 286](#)
- [ATM QoS Policy Commands on page 287](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>qos>>atm-td-profile
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes any description string from the context.
Default	none
Parameters	<i>description-string</i> — a text string describing the entity. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

ATM QoS Policy Commands

atm-td-profile

Syntax	[no] atm-td-profile <i>traffic-desc-profile-id</i> [create]
Context	config>qos
Description	<p>This command is used to configure an ATM traffic descriptor profile as per ATM Forum Traffic Management Specification Version 4.1.</p> <p>Traffic descriptor profiles are used to:</p> <ul style="list-style-type: none"> • define traffic management capabilities for ATM PVCCs • calculate the total bandwidth consumed on a given port by all ATM PVCCs. The bandwidth taken by a PVCC is equal to: <ul style="list-style-type: none"> • PIR for CBR PVCCs • SIR for rt-vbr and nrt-vbr PVCCs • MIR for UBR PVCC • define ATM-level scheduling <p>The default traffic descriptor is preconfigured and non-modifiable. It cannot be deleted. All other traffic descriptor profiles must be explicitly created before use. The create keyword must follow each new profile configuration.</p> <p>Any changes made to the existing profile, using any of the sub-commands, are applied immediately to all objects where this profile is applied (a small traffic interruption in data traffic will occur during the data plane reprogramming with the newly modified profile).</p> <p>When many changes are required on a profile, it is recommended that the profile be copied to a work area profile ID. That work-in-progress profile can be modified until complete and then written over the original profile-id. Use the config>qos>copy command to maintain profiles in this manner.</p> <p>The weight assigned to each non-shaped PVCC in the Deficit Round Robin Scheduler depends on the service category and traffic rates (see the traffic command for more details).</p> <p>The no form of the command deletes a given traffic profile. Note that the profile to be deleted must not be associated with any object (for example a SAP). If this condition is not met, the command will return an error.</p>
Default	1 — the default traffic descriptor (UBR, no traffic, no shaping)
Parameters	<p><i>traffic-desc-profile-id</i> — the index identifier for a traffic descriptor profile</p> <p>Values 1 to 1000</p> <p>create — keyword used to create an ATM traffic descriptor profile</p>

descriptor-type

Syntax	descriptor-type <i>type</i>
Context	config>qos>atm-td-profile
Description	This command is used to specify the type of ATM traffic descriptor profile as per ATM Forum Traffic Management Specification Version 4.1.
Default	Table 42 defines descriptor-type default values based on service category.

Table 42: Service Category Descriptor Type Default Values

Service Category	Default Descriptor Type
CBR	P0_1
UBR	P0_1
UBR with MIR	P0_1
rt-VBR or nrt-VBR	P0_1and S0_1

Parameters *type* — the ATM traffic descriptor profile type

Values P0_1, P0_1andS0_Tag, P0_1andS0, P0_1andS0_1

The **descriptor-type** command defines interpretation of traffic parameters that are specified for this profile. [Table 43](#) details these rules.

Table 43: Traffic Descriptor Type Command Parameters

Descriptor-type Value	Rates Interpretation	Applicable Service Categories
P0_1	PIR in kb/s; applies to CLP=0 and CLP=1 cell flows MIR in kb/s; applies to CLP=0 and CLP=1 cell flows	CBR, UBR, UBR with MIR
P0_1and S0	PIR in kb/s; applies to CLP=0 and CLP=1 cell flows; non-conforming CLP=0 cell flows are discarded SIR in kb/s; applies to CLP=0 cell flows only	rt-VBR and nrt-VBR

Table 43: Traffic Descriptor Type Command Parameters (Continued)

Descriptor-type Value	Rates Interpretation	Applicable Service Categories
P0_1andS0_Tag	PIR in kb/s; applies to CLP=0 and CLP=1 cell flows; non-conforming CLP=0 cell flows are tagged to CLP=1 cell flows SIR in kb/s; applies to CLP=0 cell flows only	rt-VBR and nrt-VBR
P0_1and S0_1	PIR in kb/s; applies to CLP=0 and CLP=1 cell flows SIR in kb/s; applies to CLP=0 cell flows only	rt-VBR and nrt-VBR

Setting **descriptor-type** to a value not compatible with the service category (as defined in [Table 42](#)) results in an error message.

policing

Syntax	[no] policing
Context	config>qos>atm-td-profile
Description	This command determines whether ingress traffic is policed. Policing is valid for CBR, rt-VBR, nrt-VBR, and UBR. This policing is cell-based.
Default	disabled

service-category

Syntax	service-category <i>service-category</i>
Description	config>qos>atm-td-profile
Description	This command is used to configure an ATM service category attribute of an ATM traffic descriptor profile.
Default	ubr

Parameters [Table 44](#) describes the supported ATM service categories on the 16-port T1/E1 ASAP Adapter card, 32-port T1/E1 ASAP Adapter card, 4-port DS3/E3 Adapter card, 4-port OC3/STM1 Clear Channel Adapter card, and 2-port OC3/STM1 Channelized Adapter card.

Table 44: ATM Service Categories

Service Category	Description
CBR	Constant Bit Rate
rt-VBR	Real-time Variable Bit Rate
nrt-VBR	Non-real-time Variable Bit Rate
UBR	Unspecified Bit Rate without Minimum Desired Cell Rate (defined by specifying service category to be ubr, and MIR of 0)
UBR (with MIR)	Unspecified Bit Rate with non-zero Minimum Desired Cell Rate (defined by specifying service category to be ubr, and MIR > 0)

Changing the service category of a profile will reset all traffic attributes to their defaults (see the [traffic](#) command) and will cause reprogramming of the data path (with a small impact on user traffic) and a reset of VC statistics for all VCs using this traffic descriptor profile.

shaping

- Syntax** `[no] shaping`
- Context** `config>qos>atm-td-profile`
- Description** This command determines whether egress shaping should occur. Shaping is only applied in the egress direction.
- Default** The default is determined by the service category. [Table 45](#) describes default shaping values.

Table 45: Default Shaping Values

Applicable Service Category	Default Shaping Value	Comments
UBR	Disabled	Shaping cannot be enabled
CBR	Enabled	Shaping cannot be disabled
rt-VBR	Enabled	Shaping cannot be disabled
nrt-VBR	Enabled	Shaping cannot be disabled

traffic

Syntax	traffic [sir <i>sir-val</i>] [pir <i>pir-val</i>] [mir <i>mir-val</i>] [mbs <i>mbs-val</i>] [cdvt <i>cdvt-val</i>] no traffic
Context	config>qos>atm-td-profile
Description	This command is used to configure traffic attributes of an ATM traffic profile as per ATM Forum Traffic Management Specification Version 4.1.

The traffic parameters of a traffic descriptor that are configurable depend on the service category of this traffic descriptor profile. (See the [service-category](#) command.)

[Table 46](#) defines which traffic descriptor parameters are applicable for what service category and what the configuration rules are between the parameters. “Y” indicates that the parameter can be configured for a given service category and will be defaulted if not provided, and an “N/A” indicates that the parameter cannot be configured for a given service category (an error will be returned). If an applicable parameter is not specified, the current value will be preserved.

Table 46: Service Category Traffic Descriptor Parameters

Service Category	SIR	PIR	MBS	MIR	CDVT
CBR	N/A	Y	N/A	N/A	Y
rt-VBR	Y	Y (must be \geq SIR)	Y	N/A	Y
nrt-VBR	Y	Y (must be \geq SIR)	Y	N/A	Y
UBR	N/A	Y	N/A	N/A	Y
UBR with MIR	N/A	Y (must be \geq MIR)	N/A	Y (non-zero MIR specified)	Y

When a traffic descriptor profile is used to define egress scheduling, the following describes how traffic rates are used to derive scheduling weight:

The scheduling weight applies only to unshaped nrt-VBR and UBR. The scheduling weight is a value from 1 to 8. The scheduling weight is determined by the SIR value for nrt-VBR, and by the MIR value for UBR. The conversion from SIR/MIR to weight is as follows:

- Rate < 64K weight = 1
- Rate < 128K weight = 2
- Rate < 256K weight = 3
- Rate < 512K weight = 4
- Rate < 1024K weight = 5
- Rate < 1536K weight = 6
- Rate < 1920K weight = 7

Everything above 1920K will be assigned a weight of 8.

Since the 7705 SAR operates in cells/second with one cell granularity, PIR and SIR values programmed need to be converted to cells/second. When converting values to be used for the scheduler, the result is rounded up to the next cell when required by conversion.

When any of SIR, PIR, or MIR is greater than the physical maximum port/channel capacity for a given PVCC, then the maximum physical port/channel capacity is used in bandwidth accumulation and when configuring the hardware for that PVCC.

Hardware-enforceable MBS is in the inclusive range of 3 to 256 000 cells. Any value outside of that range will be accepted and rounded up or down to the minimum or maximum enforceable value.

The **no** form of the command restores traffic parameters to their defaults for a given service category.

Default [Table 47](#) shows the ATM traffic parameter defaults.

Table 47: ATM Traffic Parameter Defaults

Service Category	Traffic Parameter Defaults
CBR:	
PIR	0
CDVT	250
rt-VBR and nrt-VBR	
PIR	4294967295
SIR	0
MBS	32
CDVT	250
UBR (note by default UBR is without MIR)	
PIR	0
CDVT	250

Parameters	sir <i>value</i> — the Sustained Information Rate (including cell overhead) in kb/s
	Values 0 to 4294967295
	pir <i>value</i> — the Peak Information Rate (including cell overhead) in kb/s
	Values 0 to 4294967295
	mir <i>value</i> — the Minimum Desired Information Rate (including cell overhead) in kb/s
	Values 0 to 4294967295
	mbs <i>value</i> — the Maximum Burst Size in cells
	Values 0 to 4294967295
	cdvt <i>cdvt-val</i> — the Cell Delay Variation Tolerance (CDVT) in microseconds
	Default CBR/RT-VBR/NRT-VBR/UBR = 250
	Values 0 to 4294967295

Operational Commands

copy

Syntax	copy atm-td-profile <i>src-prof dst-prof</i> [overwrite]
Context	config>qos
Description	<p>This command copies the source ATM traffic descriptor profile into the destination ATM profile. If the destination profile was already defined, the keyword overwrite must be appended for the copy to complete.</p> <p>The copy command is a configuration level maintenance tool used to create new profiles using existing profiles. It also allows bulk modifications to an existing profile with the use of the overwrite keyword.</p>
Parameters	<p><i>src-prof dst-prof</i> — indicates that the source profile ID and the destination profile ID are atm-td-profile IDs. Specify the source ID that the copy command will copy and specify the destination ID to which the command will duplicate the profile.</p> <p>Values 1 to 1000</p> <p>overwrite — specifies that the existing destination profile is to be replaced. Everything in the existing destination profile will be overwritten with the contents of the source profile. If overwrite is not specified, an error will occur if the destination profile ID exists.</p> <p>ALU-48>config>qos# copy atm-td-profile 2 10 MINOR: CLI destination (10) exists use {overwrite}.</p> <p>ALU-48>config>qos# copy atm-td-profile 2 10 overwrite ALU-48>config>qos#</p>

Show Commands

atm-td-profile

Syntax	atm-td-profile [<i>traffic-desc-profile-id</i>] [detail]
Context	show>qos
Description	This command displays ATM traffic descriptor profile information.
Parameters	<p><i>traffic-desc-profile-id</i> — displays the ATM traffic descriptor profile</p> <p>Values 1 to 1000</p> <p>detail — displays detailed policy information including policy associations</p>
Output	The following output is an example of ATM traffic descriptor profile information, and Table 48 describes the fields.

Sample Output

```
*A:ALU-1>show>qos# atm-td-profile 3 detail

=====
Traffic Descriptor Profile (3)
=====
-----
TDP-id Description
      Service Cat SIR          PIR          MIR          MBS          CDVT
-----
3      ATM TD profile3
      RT-VBR      500          500          -          500          500
-----
TDP details
-----
Shaping          : enabled
Policing          : enabled
Descriptor-Type   : P0_1andS0_1
-----
Entities using TDP-3
=====
*A:ALU-1>show>qos#
```

Table 48: ATM Traffic Descriptor Profile Command Output

Label	Description
Maximum Supported Profiles	The maximum number of ATM traffic descriptor profiles that can be configured on this system
Currently Configured Profiles	The number of currently configured ATM traffic descriptor profiles on this system
TDP-Id	The ID that uniquely identifies the traffic descriptor policy
Description	A text string that helps identify the policy's context in the configuration file
Service Category	The ATM service category
SIR	The sustained cell rate in kb/s
PIR	The peak cell rate in kb/s
MIR	The Minimum Desired Cell Rate in kb/s
MBS	The maximum burst size in cells
CDVT	The Cell Delay Variation Tolerance, in microseconds
Shaping	Whether shaping is enabled or disabled for the traffic descriptor profile
Policing	Whether policing is enabled or disabled for the traffic descriptor profile
Descriptor Type	The descriptor type for the ATM TD profile
Entities using TDP-ID	The number of entities using the ATM traffic descriptor
-	The parameter is not applicable for the configured service category

sap-using

Syntax	sap-using [ingress egress] atm-td-profile <i>td-profile-id</i> sap-using [ingress egress] qos-policy <i>qos-policy-id</i>
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 egress — specifies matching an egress policy <i>qos-policy-id</i> — identifies the ingress or egress QoS policy for which to display matching SAPs Values 1 to 65535 <i>td-profile-id</i> — displays SAPs using the specified traffic description
Output	The following output is an example of SAP information, and Table 49 describes the fields.

Sample Output

```
*A:ALU-1>show>service# sap-using egress atm-td-profile 3

=====
Service Access Point Using ATM Traffic Profile 3
=====
PortId                SvcId      Ing.   Ing.   Egr.   Egr.   Adm  Opr
                   QoS      Fltr   QoS    Fltr
-----
No Matching Entries
```

Table 49: SAP Command Output

Label	Description
PortID	The ID of the access port where the SAP is defined
SvcID	The service identifier
Ing.QoS	The SAP ingress QoS policy number specified on the ingress SAP
Egr.QoS	The SAP egress QoS policy number specified on the egress SAP
Adm	The administrative state of the SAP
Opr	The operational state of the SAP

QoS Fabric Profiles

In This Chapter

This chapter provides information to configure QoS fabric profiles using the command line interface.

- [Basic Configuration on page 300](#)
 - [Creating a QoS Fabric Profile on page 300](#)
- [Service Management Tasks on page 303](#)
 - [Removing a Fabric Profile from the QoS Configuration on page 303](#)
 - [Copying and Overwriting a Fabric Profile on page 303](#)
 - [Editing QoS Policies on page 303](#)
- [QoS Fabric Profile Command Reference on page 305](#)

Basic Configuration

A QoS fabric profile must conform to the following rules.

- Each profile must be associated with a unique policy ID.
- Either aggregate mode or per-destination mode must be assigned.

Creating a QoS Fabric Profile

Creating a QoS fabric profile other than the default policy (“**default**”) is optional. To create a QoS fabric profile, perform the following:

- assign a policy ID (policy number) — the system does not dynamically assign an ID
- include an optional description of the policy
- assign the mode, either aggregate or per-destination. If no mode is assigned, the default aggregate mode is used.
- configure the to-fabric shaper rate

Use the following CLI syntax to configure a QoS fabric profile:

CLI Syntax: `config>qos#`

```

    fabric-profile policy-id aggregate-mode create
    description description-string
    aggregate-rate [1...1000000 | default]
    fabric-profile policy-id destination-mode create
    description description-string
    dest-mds <slot/mda | multipoint>
    rate [1...1000000 | default]
```

The following example shows the command syntax for creating and configuring a QoS fabric profile with a rate of 400 Mb/s.

Example:

```

*A:7705:Dut-C# configure qos
fabric-profile 4 destination-mode create
config>qos>fabric-profile$ description "Sample fabric
  profile QoS policy 4"
config>qos>fabric-profile$ dest-mds 1/1
config>qos>fabric-profile>dest-mds$ rate 400000
config>qos>fabric-profile>dest-mds$ exit
config>qos>fabric-profile$ dest-mds 1/2
config>qos>fabric-profile>dest-mds$ rate 400000
config>qos>fabric-profile>dest-mds$ exit
config>qos>fabric-profile$ dest-mds 1/3
config>qos>fabric-profile>dest-mds$ rate 400000
config>qos>fabric-profile>dest-mds$ exit
```

```

config>qos>fabric-profile$ dest-mda 1/4
config>qos>fabric-profile>dest-mda$ rate 400000
config>qos>fabric-profile>dest-mda$ exit
config>qos>fabric-profile$ dest-mda 1/5
config>qos>fabric-profile>dest-mda$ rate 400000
config>qos>fabric-profile>dest-mda$ exit
config>qos>fabric-profile$ dest-mda 1/6
config>qos>fabric-profile>dest-mda$ rate 400000
config>qos>fabric-profile>dest-mda$ exit
config>qos>fabric-profile$ dest-mda multipoint
config>qos>fabric-profile>dest-mda$ rate 400000
config>qos>fabric-profile>dest-mda$ exit
config>qos>fabric-profile$ exit
*A:7705:Dut-C#

```

The following sample output displays the profile configuration for fabric profile QoS policy 4.

```

*A:7705:Dut-C#>config>qos# info detail
#-----
echo "QoS Policy Configuration"
#-----
...
fabric-profile 4 destination-mode create
    description "Sample fabric profile QoS policy 4"
    dest-mda 1/1
        rate 40000
    exit
    dest-mda 1/2
        rate 400000
    exit
    dest-mda 1/3
        rate 400000
    exit
    dest-mda 1/4
        rate 400000
    exit
    dest-mda 1/5
        rate 400000
    exit
    dest-mda 1/6
        rate 400000
    exit
    dest-mda multipoint
        rate 400000
    exit
exit
...
*A:7705:Dut-C#

```

Default Fabric Profile Values

Table 50 shows the fabric profile default values.

Table 50: Fabric Profile Defaults

Field	Default
Policy-id	1
Mode	Aggregate
Rate	200000

The following sample output displays the default configuration:

```
A:ALU-1>config>qos# info detail
-----
Echo "QoS Policy Configuration"
-----
fabric-profile 1 aggregate-mode create
      description "Default Fabric Profile QoS policy."
      aggregate-rate 200000
exit
...
```

Service Management Tasks

This section describes the following fabric profile service management tasks:

- [Removing a Fabric Profile from the QoS Configuration](#)
- [Copying and Overwriting a Fabric Profile](#)
- [Editing QoS Policies](#)

Removing a Fabric Profile from the QoS Configuration

The default fabric profile cannot be deleted.

To delete a fabric profile, enter the following command:

CLI Syntax: `config>qos# no fabric-profile policy-id`

Example: `config>qos# no fabric-profile 3`

Copying and Overwriting a Fabric Profile

You can copy an existing profile, rename it with a new profile ID value, or overwrite an existing profile ID. The `overwrite` option must be specified or an error occurs if the destination profile ID exists.

CLI Syntax: `config>qos> copy fabric-profile src-prof dst-prof
[overwrite]`

Example: `*A:ALU-1#>config>qos# copy fabric-profile 2 3
config>qos# copy fabric-profile 2 3 overwrite
config>qos#`

Editing QoS Policies

You can change existing policies and entries in the CLI. The changes are applied immediately to the specified adapter card where the policy is applied. To prevent configuration errors, copy the policy to a work area, make the edits, and then write over the original policy.

QoS Fabric Profile Command Reference

Command Hierarchies

- [Configuration Commands](#)
- [Operational Commands](#)
- [Show Commands](#)

Configuration Commands

```

config
  — qos
    — fabric-profile policy-id [aggregate-mode | destination-mode] [create]
    — no fabric-profile policy-id
      — aggregate-rate value
      — description description-string
      — no description
      — dest-mds [slot/mda | multipoint]
        — rate value

```

Operational Commands

```

config
  — qos
    — copy fabric-profile src-prof dst-prof [overwrite]

```

Show Commands

```

show
  — qos
    — fabric-profile policy-id [association | detail]

```

Command Descriptions

- [Configuration Commands on page 307](#)
- [Operational Commands on page 311](#)
- [Show Commands on page 312](#)

Configuration Commands

- [Generic Commands on page 308](#)
- [QoS Fabric Policy Commands on page 309](#)

Generic Commands

description

Syntax	description <i>description-string</i> no description
Context	config>qos>fabric-profile
Description	This command creates a text description stored in the configuration file for a configuration context. The no form of this command removes any description string from the context.
Default	none
Parameters	<i>description-string</i> — a text string describing the entity. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters excluding double quotes. If the string contains special characters (#, \$, spaces, etc.), the entire string must be enclosed within double quotes.

QoS Fabric Policy Commands

fabric-profile

Syntax	fabric-profile <i>policy-id</i> [aggregate-mode destination-mode] [create] no fabric-profile <i>policy-id</i>
Context	config>qos
Description	<p>This command is used to configure a QoS fabric profile policy.</p> <p>The default mode is aggregate-mode, which means that the access-ingress and network-ingress fabric shapers on all adapter cards are set to the same rate, either by default or via the aggregate-rate command. Selecting destination-mode allows each adapter card to have its fabric shapers set to a different rate for unicast traffic and a common rate for BMU traffic, either by default or via the dest-mda rate command.</p> <p>The default fabric profile is preconfigured and non-modifiable. It cannot be deleted. All other fabric profiles must be explicitly created before use.</p> <p>The create keyword must follow each new profile configuration.</p>
Default	policy-id 1 aggregate-mode
Parameters	<p><i>policy-id</i> — the index identifier for a fabric profile policy</p> <p>Values 1 to 256</p> <p>aggregate-mode — assigns the aggregate fabric profile mode to the specified fabric profile</p> <p>destination-mode — assigns the per-destination fabric profile mode to the specified fabric profile</p> <p>create — keyword used to create a fabric profile policy</p>

aggregate-rate

Syntax	aggregate-rate <i>value</i>
Context	config>qos>fabric-profile
Description	<p>This command sets the rate of the fabric shapers in aggregate mode, in kilobits per second. The rate represents the maximum bandwidth that an adapter card can switch through its fabric interface. Each fabric shaper is set to the same aggregate rate. Using the default keyword sets the aggregate rate to 200000 kb/s.</p>
Default	200000 (“default”)

Parameters *value* — the rate of the fabric shapers in aggregate mode. Using the **default** keyword sets the aggregate rate to 200000 kb/s.

Values 1 to 1000000, or default

dest-md

Syntax **dest-md** [*slot/mda* | **multipoint**]

Context config>qos>fabric-profile

Description This command enables the context for setting the rate for per-destination mode shapers on a specific adapter card or all adapter cards. Using the *slot/mda* parameter specifies a particular destination adapter card. Using the **multipoint** keyword specifies that all adapter cards are destination cards and they will have their rate configured to the same value. The value of the rate is configured using the **rate** command.

Parameters *slot/mda* — the slot and mda identifier of the adapter card

Values slot: 1
mda: 1 to 6 on the 7705 SAR-8, 1 to 12 on the 7705 SAR-18

multipoint — specifies that all adapter cards are destination adapter cards

rate

Syntax **rate** *value*

Context config>qos>fabric-profile>dest-md

Description This command sets the rate of the fabric shapers in per-destination mode, in kilobits per second. When the **multipoint** keyword is used in the **dest-md** command, **rate** sets the bandwidth available to multipoint traffic through the fabric shapers; all adapter card shapers are set to the same value.

Using the **default** keyword sets the rate to 200000 kb/s.

Default 200000 (“default”)

Parameters *value* — the rate of the fabric shapers in destination mode

Values 1 to 1000000, or default

Operational Commands

copy

Syntax	copy fabric-profile <i>src-prof dst-prof</i> [overwrite]
Context	config>qos
Description	<p>This command copies a source QoS fabric profile into a destination QoS fabric profile. If the destination profile was already defined, the keyword overwrite must be appended for the copy to complete.</p> <p>The copy command is a configuration level maintenance tool used to create new profiles using existing profiles. It also allows bulk modifications to an existing profile with the use of the overwrite keyword.</p>
Parameters	<p><i>src-prof dst-prof</i> — specifies the source profile ID that will be copied and the destination profile ID that the source fabric profile will be copied to</p> <p>Values 1 to 256</p> <p>overwrite — specifies that the existing destination profile is to be replaced. Everything in the existing destination profile will be overwritten with the contents of the source profile. If overwrite is not specified, an error will occur if the destination profile ID exists.</p>

Show Commands

fabric-profile

Syntax	fabric-profile [<i>policy-id</i>] [association detail]
Context	show>qos
Description	This command displays QoS fabric profile information. If <i>policy-id</i> is not included in the command, the CLI shows a list of fabric policies.
Parameters	<p><i>policy-id</i> — specifies the QoS fabric profile</p> <p>Values 1 to 256</p> <p>association — displays all adapter cards to which the specified profile is assigned and in which direction; that is, network ingress to fabric or access ingress to fabric</p> <p>detail — displays detailed policy information including policy associations</p>
Output	The following output is an example of QoS fabric profile information, and Table 51 describes the fields.

Sample Output

```
*A:ALU-1>show>qos# fabric-profile

=====
Fabric Profile
=====
Policy-Id   Mode           Description
-----
1           aggregate     Default Fabric Profile QoS policy.
2           aggregate     Fast Shaping fabric profile policy.
100        destination
=====
*A:ALU-1>show>qos# fabric-profile

*A:ALU-1>show>qos# fabric-profile 4 detail

=====
QoS Fabric Profile
=====
-----
Fabric Profile Id (4)
-----
Policy-id      : 4
Mode           : destination
Description    : Sample fabric profile QoS policy 4
-----
```



```

Destination MDA      Rate (Kbps)
-----
1/1                  400000
1/2                  400000
1/3                  400000
1/4                  400000
1/5                  400000
1/6                  400000
multipoint           400000

-----
Associations
-----
MDA      : 1/1 (Network Ingress)
MDA      : 1/1 (Access Ingress)
MDA      : 1/2 (Network Ingress)
MDA      : 1/2 (Access Ingress)
MDA      : 1/3 (Network Ingress)
MDA      : 1/3 (Access Ingress)
MDA      : 1/4 (Network Ingress)
MDA      : 1/4 (Access Ingress)
MDA      : 1/5 (Network Ingress)
MDA      : 1/5 (Access Ingress)
MDA      : 1/6 (Network Ingress)
MDA      : 1/6 (Access Ingress)

=====
*A:ALU-1>show>qos#

*A:ALU-1>show>qos# fabric-profile 2 detail

=====
QoS Fabric Profile
=====
-----
Fabric Profile Id (2)
-----
Policy-id      : 2
Mode           : aggregate
Description    : Fast Shaping fabric profile policy
Aggregate-rate : 150 Kbps

-----
Associations
-----
MDA      : 1/1 (Network Ingress)
MDA      : 1/1 (Access Ingress)
MDA      : 1/2 (Network Ingress)
MDA      : 1/2 (Access Ingress)
MDA      : 1/3 (Network Ingress)
MDA      : 1/3 (Access Ingress)
MDA      : 1/4 (Network Ingress)
MDA      : 1/4 (Access Ingress)
MDA      : 1/5 (Network Ingress)
MDA      : 1/5 (Access Ingress)
MDA      : 1/6 (Network Ingress)
MDA      : 1/6 (Access Ingress)

=====

```

Table 51: QoS Fabric Profile Command Output

Label	Description
Policy-id	The fabric profile QoS policy number
Mode	The fabric profile mode, either aggregate or destination
Description	The description associated with the fabric profile
Aggregate-rate	The rate of the fabric shapers in aggregate mode, in kilobits per second
Destination MDA/Rate (Kbps)	The slot/mda number of the destination adapter card, and the rate of the fabric shapers in per-destination mode, in kilobits per second
Associations	The adapter cards to which the specified fabric profile is assigned and in which direction, that is, network ingress to fabric or access ingress to fabric

Standards and Protocol Support

Standards Compliance

IEEE 802.1ag	Service Layer OAM
IEEE 802.1p/q	VLAN Tagging
IEEE 802.3	10BaseT
IEEE 802.3ah	Ethernet OAM
IEEE 802.3u	100BaseTX
IEEE 802.3x	Flow Control
IEEE 802.3z	1000BaseSX/LX
IEEE 802.3-2008	Revised base standard
ITU-T Y.1731	OAM functions and mechanisms for Ethernet-based networks

Telecom Compliance

IC CS-03 Issue 9	Spectrum Management and Telecommunications
ACTA TIA-968-A	
AS/ACIF S016 (Australia/New Zealand)	Requirements for Customer Equipment for connection to hierarchical digital interfaces
ITU-T G.703	Physical/electrical characteristics of hierarchical digital interfaces
ITU-T G.707	Network node interface for the Synchronous Digital Hierarchy (SDH)
ITU-T G.712-2001	Transmission performance characteristics of pulse code modulation channels
ITU-T G.957	Optical interfaces for equipments and systems relating to the synchronous digital hierarchy
ITU-T V.24	List of definitions for interchange circuits between data terminal equipment (DTE) and data circuit- terminating equipment (DCE)
ITU-T V.36	Modems for synchronous data transmission using 60-108 kHz group band circuits
ITU-T X.21	Interface between Data Terminal Equipment and Data Circuit- Terminating Equipment for Synchronous Operation on Public Data Networks

Protocol Support

ATM

RFC 2514	Definitions of Textual Conventions and OBJECT_IDENTITIES for ATM Management, February 1999
RFC 2515	Definition of Managed Objects for ATM Management, February 1999
RFC 2684	Multiprotocol Encapsulation over ATM Adaptation Layer 5
af-tm-0121.000	Traffic Management Specification Version 4.1, March 1999
ITU-T Recommendation I.610	B-ISDN Operation and Maintenance Principles and Functions version 11/95
ITU-T Recommendation I.432.1	B-ISDN user- network interface - Physical layer specification: General characteristics
GR-1248-CORE	Generic Requirements for Operations of ATM Network Elements (NEs). Issue 3 June 1996
GR-1113-CORE	Bellcore, Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1, July 1994
AF-PHY-0086.001	Inverse Multiplexing for ATM (IMA)

BFD

draft-ietf-bfd-mib-00.txt	Bidirectional Forwarding Detection Management Information Base
draft-ietf-bfd-base-o5.txt	Bidirectional Forwarding Detection
draft-ietf-bfd-v4v6-1hop-06.txt	BFD IPv4 and IPv6 (Single Hop)
draft-ietf-bfd-multihop-06.txt	BFD for Multi-hop Paths

BGP

- RFC 1397 BGP Default Route Advertisement
- RFC 1997 BGP Communities Attribute
- RFC 2385 Protection of BGP Sessions via MDS
- RFC 2439 BGP Route Flap Dampening
- RFC 2547bis BGP/MPLS VPNs
- RFC 2918 Route Refresh Capability for BGP-4
- RFC 3107 Carrying Label Information in BGP-4
- RFC 3392 Capabilities Advertisement with BGP-4
- RFC 4271 BGP-4 (previously RFC 1771)
- RFC 4360 BGP Extended Communities Attribute
- RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs) (previously RFC 2574bis BGP/MPLS VPNs)
- RFC 4456 BGP Route Reflection: Alternative to Full-mesh IBGP (previously RFC 1966 and RFC 2796)
- RFC 4724 Graceful Restart Mechanism for BGP - GR Helper
- RFC 4760 Multi-protocol Extensions for BGP (previously RFC 2858)
- RFC 4893 BGP Support for Four-octet AS Number Space

DHCP/DHCPv6

- RFC 1534 Interoperation between DHCP and BOOTP
- RFC 2131 Dynamic Host Configuration Protocol (REV)
- RFC 3046 DHCP Relay Agent Information Option (Option 82)
- RFC 3315 Dynamic Host Configuration Protocol for IPv6

DIFFERENTIATED SERVICES

- RFC 2474 Definition of the DS Field in the IPv4 and IPv6 Headers
- RFC 2597 Assured Forwarding PHB Group
- RFC 2598 An Expedited Forwarding PHB
- RFC 3140 Per-Hop Behavior Identification Codes

DIGITAL DATA NETWORK MANAGEMENT

- V.35
- RS-232 (also known as EIA/TIA-232)

GRE

- RFC 2784 Generic Routing Encapsulation (GRE)

IPv6

- RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
- RFC 2462 IPv6 Stateless Address Autoconfiguration
- RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- RFC 3587 IPv6 Global Unicast Address Format
- RFC 3595 Textual Conventions for IPv6 Flow Label
- RFC 4007 IPv6 Scoped Address Architecture
- RFC 4193 Unique Local IPv6 Unicast Addresses
- RFC 4291 IPv6 Addressing Architecture
- RFC 4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
- RFC 4649 DHCPv6 Relay Agent Remote-ID Option
- RFC 4861 Neighbor Discovery for IP version 6 (IPv6)

LDP

- RFC 5036 LDP Specification

IS-IS

- RFC 1142 OSI IS-IS Intra-domain Routing Protocol (ISO 10589)
- RFC 1195 Use of OSI IS-IS for routing in TCP/IP & dual environments
- RFC 2763 Dynamic Hostname Exchange for IS-IS
- RFC 2966 Domain-wide Prefix Distribution with Two-Level IS-IS
- RFC 2973 IS-IS Mesh Groups
- RFC 3373 Three-Way Handshake for Intermediate System to Intermediate System (IS-IS) Point-to-Point Adjacencies
- RFC 3567 Intermediate System to Intermediate System (IS-IS) Cryptographic Authentication
- RFC 3719 Recommendations for Interoperable Networks using IS-IS
- RFC 3784 Intermediate System to Intermediate System (IS-IS) Extensions for Traffic Engineering (TE)
- RFC 3787 Recommendations for Interoperable IP Networks
- RFC 4205 for Shared Risk Link Group (SRLG) TLV draft-ietf-isis-igp-p2p-over-lan-05.txt
- RFC 5309 Point-to-Point Operation over LAN in Link State Routing Protocols

MPLS

- RFC 3031 MPLS Architecture
- RFC 3032 MPLS Label Stack Encoding
- RFC 3815 Definitions of Managed Objects for the Multiprotocol Label Switching (MPLS), Label Distribution Protocol (LDP)
- RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

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 1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis
- RFC 1850 OSPF-MIB
- RFC 1907 SNMPv2-MIB
- RFC 2011 IP-MIB
- RFC 2012 TCP-MIB
- RFC 2013 UDP-MIB
- RFC 2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 2096 IP-FORWARD-MIB
- RFC 2138 RADIUS
- RFC 2206 RSVP-MIB
- 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-BASED ACM-MIB
- RFC 2576 SNMP-COMMUNITY-MIB
- RFC 2588 SONET-MIB
- RFC 2665 EtherLike-MIB
- RFC 2819 RMON-MIB
- RFC 2863 IF-MIB
- RFC 2864 INVERTED-STACK-MIB
- RFC 3014 NOTIFICATION-LOG MIB
- RFC 3164 The BSD Syslog Protocol
- 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
- draft-ietf-mpls-ldp-mib-07.txt
- draft-ietf-ospf-mib-update-04.txt
- draft-ietf-mpls-lsr-mib-06.txt
- draft-ietf-mpls-te-mib-04.txt
- IANA-IFType-MIB

OSPF

- RFC 1765 OSPF Database Overflow
- RFC 2328 OSPF Version 2
- RFC 2370 Opaque LSA Support
- RFC 3101 OSPF NSSA Option
- RFC 3137 OSPF Stub Router Advertisement
- RFC 3630 Traffic Engineering (TE) Extensions to OSPF
- RFC 4203 Shared Risk Link Group (SRLG) sub-TLV

PPP

- RFC 1332 PPP Internet Protocol Control Protocol (IPCP)
- RFC 1570 PPP LCP Extensions
- RFC 1619 PPP over SONET/SDH
- RFC 1661 The Point-to-Point Protocol (PPP)
- RFC 1662 PPP in HDLC-like Framing
- RFC 1989 PPP Link Quality Monitoring
- RFC 1990 The PPP Multilink Protocol (MP)
- RFC 2686 The Multi-Class Extension to Multi-Link PPP

PSEUDOWIRES

- RFC 3550 RTP: A Transport Protocol for Real-Time Applications
- RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
- RFC 4385 Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN
- RFC 4446 IANA Allocation for PWE3
- RFC 4447 Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)

RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks
RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
RFC 4717 Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
RFC 5085 Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires
RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)
draft-ietf-pwe3-redundancy-02 Pseudowire (PW) Redundancy

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

RSVP-TE and FRR

RFC 2430 A Provider Architecture for DiffServ & TE
RFC 2961 RSVP Refresh Overhead Reduction Extensions
RFC 2702 Requirements for Traffic Engineering over MPLS
RFC 2747 RSVP Cryptographic Authentication
RFC 3097 RSVP Cryptographic Authentication - Updated Message Type Value
RFC 3209 Extensions to RSVP for LSP Tunnels
RFC 3210 Applicability Statement for Extensions to RSVP for LSP Tunnels
RFC 4090 Fast Reroute Extensions to RSVP-TE for LSP Tunnels

SONET/SDH

GR-253-CORE SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000
ITU-T Recommendation G.841 Telecommunication Standardization Section of ITU, Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum1 issued in July 2002

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

SYNCHRONIZATION

G.813 Timing characteristics of SDH equipment slave clocks (SEC)
G.8261 Timing and synchronization aspects in packet networks
G.8262 Timing characteristics of synchronous Ethernet equipment slave clock
GR 1244 CORE Clocks for the Synchronized Network: Common Generic Criteria
IEEE 1588v2 1588 PTP 2008

TACACS+

IETF draft-grant-tacacs-02.txt The TACACS+ Protocol

TCP/IP

RFC 768 User Datagram Protocol
RFC 791 Internet Protocol
RFC 792 Internet Control Message Protocol
RFC 793 Transmission Control Protocol
RFC 826 Ethernet Address Resolution Protocol
RFC 854 Telnet Protocol Specification
RFC 1350 The TFTP Protocol (Rev. 2)
RFC 1812 Requirements for IPv4 Routers

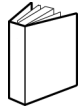
VPLS

RFC 4762 Virtual Private LAN Services Using LDP

Proprietary MIBs

TIMETRA-ATM-MIB.mib
TIMETRA-CAPABILITY-7705-V1.mib
TIMETRA-CFLOWD-MIB.mib
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-LDP-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MPLS-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-PPP-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-ROUTE-POLICY-MIB.mib
TIMETRA-RSVP-MIB.mib
TIMETRA-SAP-MIB.mib
TIMETRA-SDP-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib

Customer documentation and product support



Customer documentation

<http://www.alcatel-lucent.com/myaccess>

Product manuals and documentation updates are available at [alcatel-lucent.com](http://www.alcatel-lucent.com). If you are a new user and require access to this service, please contact your Alcatel-Lucent sales representative.



Technical Support

<http://support.alcatel-lucent.com>



Documentation feedback

documentation.feedback@alcatel-lucent.com

