Alcatel-Lucent

Service Access Switch| Release 6.0 Rev.06

7210 SAS-M and 7210 SAS-T OS
Quality of Service Guide

93-0489-01-06

Alcatel·Lucent

TABLE OF CONTENTS

Network QoS Policies

Network Queue QoS Policies

Service Ingress QoS Policies

Access Egress QoS Policies

QoS Port Scheduler Policies

Slope QoS Policies

LIST OF TABLES

Getting Started

QoS Policies

Port Level Egress Rate-Limiting

Frame Based Accounting

Network QoS Policies

Network Queue QoS Policies

Service Ingress QoS Policies

Access Egress QoS Policies

QoS Port Scheduler Policies

Slope QoS Policies

List of Figures

QoS Policies

Port Level Egress Rate-Limiting

Frame Based Accounting

Network QoS Policies

Network Queue QoS Policies

Service Ingress QoS Policies

Access Egress QoS Policies

QoS Port Scheduler Policies

Slope QoS Policies

Preface

About This Guide

This guide describes the Quality of Service (QoS) provided by the 7210-SAS-M and 7210 SAS-T OS and presents examples to configure and implement various protocols and services.

Notes:

- This user guide is applicable to all 7210 SAS-M platforms, unless specified otherwise.This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.
- On 7210 SAS devices, not all the CLI commands are supported on all the platforms and in all the modes. In many cases, it is mentioned explicitly in this document. In other cases, it is implied and easy to know the CLIs that are not supported on a particular platform.

Audience

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

- CLI concepts
- Quality of Service (QoS) policies and profiles

List of Technical Publications

The 7210 SAS-M, T, and X OS documentation set is composed of the following books:

- 7210 SAS-M, T, and X OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.
- 7210 SAS-M, T, and X OS System Management Guide

  This guide describes system security and access configurations as well as event logging and accounting logs.
- 7210 SAS-M, T, and X OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.
- 7210 SAS-M, T, and X OS Router Configuration Guide

  This guide describes logical IP routing interfaces and associated attributes such as an IP address, port, link aggregation group (LAG) as well as IP and MAC-based filtering.
- 7210 SAS-M, T, and X OS Services Guide

  This guide describes how to configure service parameters such as customer information, and user services.
- 7210 SAS-M, T, and X OS OAM and Diagnostic Guide

  This guide describes how to configure features such as service mirroring and Operations, Administration and Management (OAM) tools.
- 7210-SAS-M and 7210 SAS-T7210 SAS- X Quality of Service Guide

  This guide describes how to configure Quality of Service (QoS) policy management.
- 7210-SAS-M, T, and X OS MPLS Guide

  This guide describes how to configure Multiprotocol Label Switching (MPLS) and Label Distribution Protocol (LDP).
- 7210-SAS-M, T, and X OS Routing Protocols Guide

  This guide provides an overview of routing concepts and provides configuration examples for OSPF, IS-IS, and route policies.

Technical Support

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

Web: http://www1.alcatel-lucent.com/comps/pages/carrier_support.jhtml

Getting Started

In This Chapter

This chapter provides process flow information to configure Quality of Service (QoS) policies and provision services.

This guide provides information to configure QoS policies in both network mode and access-uplink mode. Unless otherwise noted, many of the qos policies are applicable to both network mode and access-uplink mode.

Alcatel-Lucent 7210 SAS-Series Services 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
Policy configuration	Configuring QoS Policies	
	• Egress Rate	Port Level Egress Rate-Limiting on page 85
	• Accounting Mode	Frame Based Accounting on page 95
	• Network	Network QoS Policies on page 105
	• Network queue	Network Queue QoS Policies on page 183
	• SAP ingress	Service Ingress QoS Policies on page 207
	• Access egress	Access Egress QoS Policies on page 315
	• Port scheduler	QoS Port Scheduler Policies on page 347
	• Slope	Slope QoS Policies on page 365
Reference	• List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support on page 401

QoS Policies

In This Chapter

This chapter provides information about Quality of Service (QoS) policy management.

Topics in this chapter include:

QoS Overview

The 7210 SAS M is designed with QoS mechanisms on both ingress and egress to support multiple services per physical port. The 7210 SAS M has extensive and flexible capabilities to classify, police, shape, and mark traffic.

In the Alcatel-Lucent service router’s service model, a service is provisioned on the provider-edge (PE) equipment. Service data is encapsulated and then sent in a service tunnel to the far-end Alcatel-Lucent service router where the service data is delivered.

The operational theory of a service tunnel is that the encapsulation of the data between the two Alcatel Lucent service routers appear like a Layer 2 path to the service data although it is really traversing an IP or IP/MPLS core. The tunnel from one edge device to the other edge device is provisioned with an encapsulation and the services are mapped to the tunnel that most appropriately supports the service needs.

The 7210 SAS supports eight forwarding classes internally named: Network-Control, High-1, Expedited, High-2, Low-1, Assured, Low-2 and Best-Effort. The forwarding classes are discussed in more detail in Forwarding Classes on page 80.

7210 SAS devices use QoS policies to control how QoS is handled at distinct points in the service delivery model within the device. 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 7210 SAS 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 QoS policies within the 7210 SAS can be divided into three main types:

- QoS policies are used for classification, defining metering and queuing attributes and marking .
- Slope policies define default buffer allocations and WRED slope definitions.
- Port Scheduler policies determine how queues are scheduled.

QoS Policies

7210 SAS M QoS policies are applied on service ingress, network port ingress and egress, access port egress, and network IP interfaceswhen configured to operate in network mode. When configured to operate in access-uplink mode, 7210 SAS M and 7210 SAS-T QoS policies are applied on service ingress, access port egress, and access-uplink port ingress and egress. These policies allow user to configure the following:

- Classification rules for how traffic is mapped to forwarding classes
- Forwarding class association with meters and meter parameters used for policing (rate-limiting).
- Queuing parameters for shaping and buffer allocation
- QoS marking/interpretation

There are several types of QoS policies:

- Service ingress
- Access egress
- Network (for ingress and egress)
- Network queue (for egress)
- Port scheduler
- Slope

Service ingress QoS policies are applied to the customer-facing Service Access Points (SAPs). Traffic that enters through the SAP is classified to map it to a Forwarding Class (FC). Forwarding class is associated with meters/policier on ingress. The mapping of traffic to meters can be based on combinations of customer QoS marking (IEEE 802.1p bits), IP and MAC criteria. The characteristics of the forwarding class meters are defined within the policy as to the number of forwarding class meters for unicast traffic and the meter characteristics (like CIR, PIR, etc.). Each of the forwarding classes can be associated with different unicast parameters. A service ingress QoS policy also defines up to three (3) meters per forwarding class to be used for multipoint traffic for multipoint services. There can be up to 32 meters in total per Service ingress QOS policies. In the case of the VPLS, four types of forwarding are supported (which is not to be confused with forwarding classes); unicast, multicast, broadcast, and unknown. Multicast, broadcast, and unknown 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.

An access egress policy is similar to a SAP egress policy as defined in the 7750 SR, 7450 ESS, 7710 SR series of products. The difference is the point of attachment. An access egress policy is applied on the physical port as opposed to the logical port (SAP) for SAP egress policy. An access egress QoS policy maps the traffic egressing out on the customer facing ports into various queues and marks the traffic accordingly. The FCs are mapped onto the queues. There are 8 queues at the port level. FC-to-queue mapping is static and is not configurable. The number of queues are static and there are always 8 queues at the port level. An access egress policy also defines how to remark the forwarding class to IEEE 802.1p bits in the customer traffic.

For 7210 SAS-M and 7210 SAS-T devices configured to operate in access-uplink mode, there are two types of network QoS policies, one applied to a network IP interface and the other type is applied to a network port. Network QoS policies are applied to IP interfaces .On ingress, the policy applied to an IP interface maps incoming MPLS LSP EXP values to forwarding class and profile state for the traffic received from the core network. On egress, the policy maps forwarding class and profile state to MPLS LSP EXP values for traffic to be transmitted into the core network. The network policy applied to a network port maps incoming IP packets, DSCP or Dot1p values, to the forwarding class and the profile state for the traffic received from the core network. On egress, the policy maps forwarding class and profile state to DSCP and/or Dot1p values for IP traffic to be transmitted into the core network.

For 7210 SAS-M and 7210 SAS-T devices configured to operate in access uplink port, network QoS policies apply to access uplink ports. On ingress, the policy applied to an IP interface maps incoming Dot1p values to forwarding class and profile state for the traffic received from the core network. On egress, the policy maps forwarding class and profile state to Dot1p values for traffic to be transmitted into the core network.

Network queue policies are applied on egress to network ports when operating in network mode and to access-uplink ports when operating in access-uplink mode. The policies define the forwarding class queue characteristics for these entities. The FCs are mapped onto the queues. There are 8 queues at the port level. FC-to-queue mapping is static and is not configurable. The number of queues are static and there are always 8 queues at the port level.

Service ingress, access egress, and network QoS policies are defined with a scope of either *template* or *exclusive*. Template policies can be applied to multiple entities (such as SAPs and ports) whereas exclusive policies can only be applied to a single entity.

One service ingress QoS policy can be applied to a specific SAP. One access egress QoS policy can be applied to the access port. One network QoS policy can be applied to a specific IP interface or network port based on the type of network QoS policy when operating in network mode. One network QoS policy can be applied to a access-uplink port when operating in access-uplink mode. A network QoS policy defines both ingress and egress behavior. One network queue policy can be applied to the network port or a access-uplink port.

If no QoS policy is explicitly applied to a SAP, port or interface, a default QoS policy is applied.

A summary of the major functions performed by the QoS policies is listed in Table 3.

Table 3: QoS Policy Types and Descriptions

Policy Type	Device Operating Mode	Applied at…	Description	Page
Service Ingress	Network mode Or access-uplink mode	SAP ingress	• Defines up to 16 forwarding class meters and meter parameters for traffic classification. • Defines match criteria to map flows to the meters based on any one of the criteria (IP or MAC).	51
Access Egress	Network mode Or access-uplink mode	Access port	• Defines up to 8 forwarding class queues and queue parameters for traffic classification. • Maps forwarding classes to the queues. • Defines FC to remarking values. • Defines CIR levels and PIR weights that determines how the queue gets prioritized by the scheduler.	51
Network (of type’ip-interface’)	Network mode	IP interface	Packets are marked using QoS policies on edge devices. Invoking a QoS policy on a network port allows for the packets that match the policy criteria to be remarked. • Used for classification/marking of MPLS packets. • At ingress, defines MPLS LSP-EXP to FC mapping and 12 meters used by FCs. • At egress, defines FC to MPLS LSP-EXP marking.	27
Network (of type’port’)	Network mode	Network and Hybrid Ports	• Used for classification/marking of IP packets. • At ingress, defines DSCP or Dot1p to FC mapping and 8 meters. • At egress, defines FC to DSCP or Dot1p marking or both.	
Network	Access uplink mode	Access uplink	• Used for classification/marking of IP packets. • At ingress, defines Dot1p to FC mapping and 8 meters. • At egress, defines FC to Dot1p marking.	

Table 3: QoS Policy Types and Descriptions (Continued)

Policy Type	Device Operating Mode	Applied at…	Description	Page
Network Queue	Network mode	Network Ports and Hybrid Ports	• Defines forwarding class mappings to network queues and queue characteristics for the queues.	35
	Access-uplink mode	Access-uplink Ports		
Slope	Network mode	Access ports, Network ports and Hybrid ports	• Enables or disables the high-slope, low-slope, and non-TCP parameters within the egress pool.	72
	Access-uplink mode	Access ports and Access-uplink ports		
Port scheduler	Network mode	Access ports, Network ports and Hybrid ports	• Defines the parameters for the port scheduler.	76
	Access-uplink mode	Access ports and Access-uplink ports		

Service and Network QoS Policies

The QoS mechanisms within the 7210 SAS M are specialized for the type of traffic on the interface. For customer interfaces, there is service ingress and access egress traffic, and for IP interfaces, there is network ingress and network egress traffic (Figure 1).

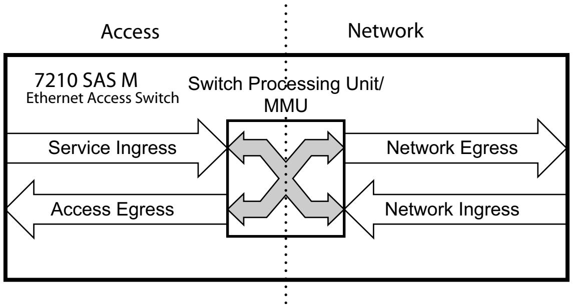

Figure 1: 7210 SAS-M Traffic Types Operating in Network Mode

When operating in access-uplink mode, the QoS mechanisms available are similar to network mode, expect that network ingress and network egress traffic is associated with access-uplink interfaces instead of network IP interface or network port (as shown in Figure 2).

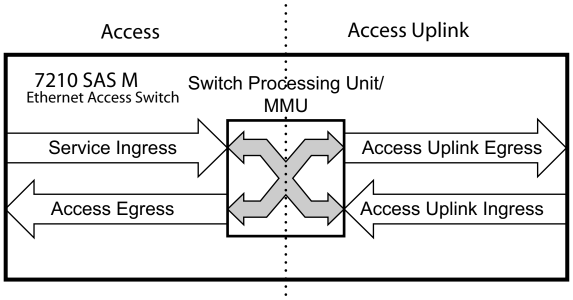

Figure 2: 7210 SAS-M Traffic Types for Access Uplink Mode

The 7210 SAS uses the following QoS policies applied to a SAP or a network port or an access port or an access-uplink port to define queuing, queue attributes, policer/meter attributes and QoS marking interpretation.

The 7210 SAS supports four types of service and network QoS policies:

- Service ingress QoS policies
- Access egress QoS policies

- Network QoS policies
- Network Queue QoS policies

Network QoS Policies in Network Mode

The following functionalities of Network QoS policies in Network mode are:

1. Two types of network QoS policies can be defined, **ip-interface** and **port**. By default, when a network QoS policy is created, it is an **ip-interface** type.
2. A network QoS policy of type **ip-interface** is created in the **configure>qos>network** *network-policy-id* **create** context.
3. A network QoS policy of type **port** is created in the **configure>qos>network** *network-policy-id* **network-policy-type port create** context.
4. When a network QoS policy of type **ip-interface** is applied to an IP interface, it is used for classification of MPLS packets based on LSP-EXP bits.
5. When a network QoS policy of type **port** is applied to a network and hybrid port, it is used for classification of IP packets based on the DSCP or Dot1p bits.

Network QoS policies (**ip-interface** type) define ingress forwarding class meters and maps traffic to those meters for IP interfaces. When a network QoS policy is created, it always has two meters defined that cannot be deleted, one for all the unicast traffic and one for all the multipoint traffic. These meters exist within the definition of the policy. The meters only get noticed in the hardware when the policy is applied to an IP interface. It also defines the forwarding class to EXP bit marking, on the egress mode.

A network QoS policy defines both the ingress and egress handling of QoS on the network IP interface and network port. The following functions are defined for network policy type **ip-interface**:

- Ingress
  - → Defines EXP value mapping to forwarding classes.
  - → Defines forwarding class to meter mapping.
- Egress
  - → Defines the forwarding class to EXP value markings.
  - → Remarking of QoS bits can be enabled or disabled.
    Note that FC to DSCP marking is used to mark only IP traffic sent out through that port if marking is enabled and FC to Dot1p marking is used to mark IP and MPLS traffic sent out through that port, if marking is enabled.

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

- A unique network QoS policy ID.
- Egress forwarding class to EXP value mappings for each forwarding class.
- A default ingress forwarding class and in-profile/out-of-profile state.

- At least one default unicast forwarding class meter. The parameters that can be configured for a meter are discussed in Meter Parameters on page 38.
- At least one multipoint forwarding class meter.

Optional network QoS policy elements include:

- Additional unicast meters up to a total of 11.
- Additional multipoint meters up to 11.
- EXP value to forwarding class and profile state mappings for all EXP values received.

Network policy ID 2 is reserved as the default network QoS policy of type IP interface. The default policy cannot be deleted or changed.

Default network QoS policy 2 is applied to all IP interfaces which do not have another network QoS policy explicitly assigned.

The network QoS policy applied at network egress (for example, on an IP interface) determines how or whether the profile state is marked in packets transmitted into the service core network. If the profile state is marked in the service core packets, out-of-profile packets are preferentially dropped over in-profile packets at congestion points in the core network. For network egress, traffic remarking in the network QoS policy is disabled. Table 5 lists the default mapping of forwarding class to EXP values.

Table 4: Default Network QoS Policy(type = ip-interface) Egress Marking

FC-ID	FC Name	FC Label	Egress EXP Marking	
			In-Profile	Out-of-Profile
7	Network Control	nc	111 - 7	111 - 7
6	High-1	h1	110 - 6	110 - 6
5	Expedited	ef	101 - 5	101 - 5
4	High-2	h2	100 - 4	100 - 4
3	Low-1	l1	011 - 3	010-2
2	Assured	af	011-3	010 - 2
1	Low-2	l2	001 - 1	001 - 1
0	Best Effort	be	000 - 0	000 - 0

For network ingress, Table 5 lists the default mapping of EXP values to forwarding class and profile state for the default network QoS policy. Color aware policing is supported on network ingress.

Table 5: Default Network QoS Policy (type = ip-interface) EXP to FC Mapping

EXP Value	7210 FC Ingress	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

“port” Type Network QoS Policy

Network QoS policy of type **port** defines ingress forwarding class meters and maps traffic to those meters for only IP traffic received on network and hybrid ports. When a network policy of this type is created it has a single unicast meter which cannot be deleted. These meters exist within the definition of the policy. The meters get instantiated in hardware, only when the policy is applied to a network port. It also defines the forwarding class to DSCP and/or Dot1p marking to be used for packets sent out through that port.

A network QoS policy of type port defines both the ingress and egress handling of QoS on the network port.

The following functions are defined:

- Ingress
  - → Defines DSCP or Dot1p value mapping to forwarding classes. Only one type supported, such as DSCP or Dot1p, per policy.
  - → Defines forwarding class to meter mapping.
- Egress
  - → Specifies remark policy that defines forwarding class to DSCP or Dot1p (or both) value markings.

→ Remarking of QoS bits is always disabled

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

- A unique network QoS policy ID and network-policy-type set to **port**.
- Egress forwarding class to DSCP or Dot1p (or both) value mappings for each forwarding class.
- A default ingress forwarding class and in-profile/out-of-profile state.
- At least one default unicast forwarding class meter. The parameters that can be configured for a meter are discussed in Meter Parameters on page 25.

Optional network QoS policy elements include:

- Additional unicast meters up to a total of 8.
- A DSCP or Dot1p (or both) value to forwarding class and profile state mappings for all DSCP or Dot1p values received.

Network policy ID 1 is reserved as the default network QoS policy of type port. The default policy cannot be deleted or changed.

The default network QoS policy is applied to all network ports which do not have another network QoS policy explicitly assigned.

Table 6 lists the default mapping of forwarding class to Dot1p and DSCP values.

Table 6: Default Network QoS Policy of type 'port' Egress Marking

FC-ID	FC Name	FC Label	Egress DSCP Marking		Egress Dot1p Marking	
			In-Profile	Out-of-Profile	In-Profile	Out-of-profile
7	Network Control	nc	nc2	nc2	111 - 7	111 - 7
6	High-1	h1	nc1	nc1	110-6	110-6
5	Expedited	ef	ef	ef	101-5	101-5
4	High-2	h2	af41	af41	100-4	100-4
3	Low-1	l1	af21	af22	011-3	010-2

Table 6: Default Network QoS Policy of type 'port' Egress Marking

FC-ID	FC Name	FC Label	Egress DSCP Marking		Egress Dot1p Marking	
			In-Profile	Out-of-Profile	In-Profile	Out-of-profile
2	Assured	af	af11	af12	011-3	010-2
1	Low-2	l2	cs1	cs1	001-1	001-1
0	Best Effort	be	be	be	000-0	000-0

Table 7 lists the default mapping of Dot1p/DSCP values to forwarding class and profile state for the default network QoS policy of type port, for network ingress. Color aware policing is supported on network ingress.

Table 7: Default Network QoS Policy of Type Port - Dot1p/DSCP to FC Mapping

DSCP Value	Dot1p Value	FC Ingress	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

Network QoS Policies for Access-uplink Mode

Network QoS policies of type ‘port’ define ingress forwarding class meters and maps traffic to those meters for access uplink ports. When a network QoS policy is created, it always has two meters/policers defined that cannot be deleted, one for the all unicast traffic and one for all multipoint traffic. These meters exist within the definition of the policy. The meters only get instantiated in hardware when the policy is applied to an access uplink port. It also defines the forwarding class to priority bit marking, on the egress.

A network QoS policy of type ‘port’ defines both the ingress and egress handling of QoS on the access uplink ports. The following functions are defined:

- Ingress
  - → Defines Dot1p value mapping to forwarding classes (DSCP is not available for use)
  - → Defines forwarding class to meter mapping.
- Egress
  - → Defines the forwarding class to Dot1p value markings.
  - → Remarking of QoS bits can be enabled or disabled.

The required elements to be defined in a network QoS policy of type ‘port’ are:

- A unique network QoS policy ID.
- Egress forwarding class to Dot1p value mappings for each forwarding class.
- A default ingress forwarding class and in-profile/out-of-profile state.
- At least one default unicast forwarding class meter. The parameters that can be configured for a meter are discussed in Meter Parameters on page 38.
- At least one multipoint forwarding class meter.

Optional network QoS policy elements include:

- Additional unicast meters up to a total of 11.
- Additional multipoint meters up to 11.
- Dot1p value to forwarding class and profile state mappings for all Dot1p values received.

Network policy ID 1 is reserved as the default network QoS policy of type ‘port’. The default policy cannot be deleted or changed. The default network QoS policy is applied to all access uplink ports which do not have another network QoS policy explicitly assigned. The network QoS policy applied at network egress (for example, on an access uplink port) determines how or if the profile state is marked in packets transmitted into the service core network. If the profile state is marked in the service core packets, out-of-profile packets are preferentially dropped over in-profile packets at congestion points in the core network. For network egress, traffic remarking in the network QoS policy is always enabled. Table 8 lists the default mapping of forwarding class to Dot1p values.

Table 8: Default Network QoS Policy of Type ‘port’ used for Egress Marking on Access-uplink Ports

FC-ID	FC Name	FC Label	DiffServ Name	Egress Dot1p Marking	
				In-Profile	Out-of-Profile
7	Network Control	nc	NC2	111-7	111-7
6	High-1	h1	NC1	110-6	110-6
5	Expedited	ef	EF	101-5	101-5
4	High-2	h2	AF4	100-4	100-4
3	Low-1	l1	AF2	011-3	010-2
2	Assured	af	AF1	011-3	010-2
1	Low-2	l2	CS1	00-1	001-1
0	Best Effort	be	BE	000-0	000-0

For network ingress, Table 9 lists the default mapping of Dot1p values to forwarding class and profile state for the default network QoS policy. Color aware policing is supported on ingress for access-uplink ports.

Table 9: Default Network QoS Policy of Type ‘port’ used for Dot1p to FC on Access-uplink Ports

Dot1pValue	7210 FC Ingress	Profile
0	be	Out
1	l2	In
2	af	Out
3	af	In
4	h2	In
5	ef	In

Table 9: Default Network QoS Policy of Type ‘port’ used for Dot1p to FC on Access-uplink Ports (Continued)

Dot1pValue	7210 FC Ingress	Profile
6	h1	In
7	nc	In

Network Queue QoS Policies

Network queue policies define the network forwarding class queue characteristics. Network queue policies are applied on egress on network and hybrid ports for 7210 SAS-M operating in network mode or access uplink ports for 7210 SAS-M and 7210 SAS-T devices operating in access uplink mode. The system allocates 8 queues for the network port and FCs are mapped to these 8 queues. All policies uses eight queues like the default network queue policy.

On 7210 SAS-M, the network queues on hybrid ports are used for MPLS traffic, IP traffic and SAP traffic sent out of IP interfaces and SAPs configured on hybrid ports.

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

- Peak Information Rate (PIR) as a percentage of egress port bandwidth
- Committed Information Rate (CIR) as a percentage of egress port bandwidth

Network queue policies are identified with a unique policy name which conforms to the standard 7210 SAS alphanumeric naming conventions.

The system default network queue policy is named **default** and cannot be edited or deleted. CBS values cannot be provisioned. Table 10 describes the default network queue policy definition.

Table 10: Default Network Queue Policy Definition. (for 7210 SAS-M configured in Network mode)

Forwarding Class	Queue	Definition
`Network-Control (nc)`	Queue 8	• PIR = 100% • CIR = 10% • CBS = 12.5
`High-1 (h1)`	Queue 7	• PIR = 100% • CIR = 10% • CBS = 12.5%
`Expedited (ef)`	Queue 6	• PIR = 100% • CIR = 100% • 12.5%
`High-2 (h2)`	Queue 5	• PIR = 100% • CIR = 100% • CBS = 12.5%

Table 10: Default Network Queue Policy Definition. (for 7210 SAS-M configured in Network mode) (Continued)

Forwarding Class	Queue	Definition (Continued)
`Low-1 (l1)`	Queue 4	• PIR = 100% • CIR = 25% • CBS = 12.5%
`Assured (af)`	Queue 3	• PIR = 100% • CIR = 25% • CBS = 12.5%
`Low-2 (l2)`	Queue 2	• PIR = 100% • CIR = 25% • CBS = 12.5%
`Best-Effort (be)`	Queue 1	• PIR = 100% • CIR = 0% • CBS = 12.5%

Table 11: Default Network Queue Policy Definition (for 7210 SAS-M and 7210 SAS-T configured in access uplink mode)

Forwarding Class	Queue	Definition
`Network-Control (nc)`	Queue 8	• PIR = 100% • CIR = 10% • CBS = 7%
`High-1 (h1)`	Queue 7	• PIR = 100% • CIR = 10% • CBS = 7%
`Expedited (ef)`	Queue 6	• PIR = 100% • CIR = 100% • CBS = 21%
`High-2 (h2)`	Queue 5	• PIR = 100% • CIR = 100% • CBS = 21%

Table 11: Default Network Queue Policy Definition (for 7210 SAS-M and 7210 SAS-T configured in access uplink mode) (Continued)

Forwarding Class	Queue	Definition (Continued)
`Low-1 (l1)`	Queue 4	• PIR = 100% • CIR = 25% • CBS = 7%
`Assured (af)`	Queue 3	• PIR = 100% • CIR = 25% • CBS = 21%
`Low-2 (l2)`	Queue 2	• PIR = 100% • CIR = 25% • CBS = 7%
`Best-Effort (be)`	Queue 1	• PIR = 100% • CIR = 0% • CBS = 7%

Meter Parameters

This section describes the meter parameters provisioned on access and network meters provisioned on IP interfaces (for 7210 SAS-M in Network mode) or access uplink (7210 SAS-M and 7210 SAS-T in access uplink mode) for QoS.

The meter parameters are:

- Meter ID on page 38
- Committed Information Rate on page 38
- Peak Information Rate on page 39
- Adaptation Rule for Meters on page 39
- Committed Burst Size on page 41
- Maximum Burst Size on page 41
- Meter Counters on page 42
- Meter Modes on page 42

Meter ID

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

Committed Information Rate

The committed information rate (CIR) for a meter is the long term average rate at which traffic is considered as conforming traffic or in-profile traffic. The higher the rate, the greater the throughput user can expect. The user will be able to burst above the CIR and up to PIR for brief periods of time. The time and profile of the packet is decided based on the burst sizes as explained in the following sections.

When defining the CIR for a meter, the value specified is the administrative CIR for the meter. The 7210 SAS M has a number of native rates in hardware that it uses to determine the operational CIR for the meter. The user has some control over how the administrative CIR is converted to an operational CIR should the hardware not support the exact CIR and PIR combination specified. Refer to the interpretation of the administrative CIR in Adaptation Rule for Meters on page 39.

The CIR for meter is provisioned on service ingress and network ingress within service ingress QoS policies and network QoS policies, respectively.

Peak Information Rate

The peak information rate (PIR) defines the maximum rate at which packets are allowed to exit the meter. It does not specify the maximum rate at which packets may enter the meter; this is governed by the meter's ability to absorb bursts and is defined by its maximum burst size (MBS).

When defining the PIR for a meter, the value specified is the administrative PIR for the meter. The 7210 SAS M has a number of native rates in hardware that it uses to determine the operational PIR for the meter. The user has some control over how the administrative PIR is converted to an operational PIR should the hardware not support the exact CIR and PIR combination specified. Refer to the interpretation of the administrative PIR in Adaptation Rule for Meters on page 39.

The PIR for meter is provisioned on service ingress and access uplink port or network port ingress within service ingress QoS policies and network QoS policies, respectively

Adaptation Rule for Meters

The adaptation rule provides the QoS provisioning system with the ability to adapt the administrative rates provisioned for CIR and PIR, to derive the operational rates based on the underlying capabilities of the hardware. The administrative CIR and PIR rates are translated to actual operational rates enforced by the hardware meter. The rule provides a constraint, when the exact rate is not available due to hardware capabilities.

The hardware rate step-size is provided in Table 12:

Table 12: Supported Hardware rates and burst step sizes for CIR and PIR values

Rate (kbits_sec)	Burst (kbits_burst)	Rate Step Size (bits)	Burst Step Size (bits)
0-4194296	0-16773	8000	4096
4194297-8388592	16774-33546	16000	8192
8388593-16777184	33547-67092	32000	16384
16777185-33554368	67093-134184	64000	32768
33554369-67108736	134185-268369	128000	65536
67108737-134217472	268370-536739	256000	131072
134217473-268434944	536739-1073479	512000	262144
268434945-536869888	1073480-16384	1024000	524288

T

The system attempts to find the best operational rate depending on the defined constraint. The supported constraints are listed below:

- Minimum: Find the next multiple of step-size that is equal to or greater than the specified rate.
- Maximum: Find the next multiple of step-size that is equal to or less than the specified rate.
- Closest: Find the next multiple of step-size that is closest to the specified rate.

Hardware supports rates to be in the multiple of 8 kbps, the system will attempt to find the best operational rate depending on the defined constraint. The supported constraints are:

- Minimum: Find the next multiple of 8 kbps that is equal to or higher than the specified rate.
- Maximum: Find the next multiple of 8 kbps that is equal to or less than the specified rate.
- Closest: Find the next multiple of 8 kbps that is closest to the specified rate.

Table 13 lists the rate values configured in the hardware when different PIR or CIR rates are specified in the CLI.

Table 13: Administrative Rate Example

Administrative Rate	Operation Rate (Min)	Operation Rate (Max)	Operation Rate (Closest)
8	8	8	8
10	16	8	8
118085	11808	11800	11808
46375	46376	46368	46376

If user has configured any value greater than 0 and less than 8 then operation rate configured on hardware would be 8 kbps irrespective of the constraint used.

Note:

- The burst size configured by the user affects the rate step-size used by the system. The system uses the step size in a manner that both the burst-size and rate parameter constraints are met. For example, if the rate specified is less than 4Gbps but the burst size configured is 17Mbits, then the system uses rate step-size of 16Kbits and burst step-size of 8192bits (refer to Table 12, row#2)
- In prior releases of 7210 SAS-T CBS and MBS of meter max was 16384, now the max max value is 2146959

Committed Burst Size

The committed burst size parameter specifies the maximum burst size that can be transmitted by the source at the CIR while still complying with the CIR. If the transmitted burst is lower than the CBS value then the packets are marked as in-profile by the meter to indicate that the traffic is complying meter configured parameters.

The operational CBS set by the system is adapted from the user configured value by using the minimum constraint.

Maximum Burst Size

For trTCM, the maximum burst size parameter specifies the maximum burst size that can be transmitted by the source at the PIR while complying with the PIR. If the transmitted burst is lower than the MBS value then the packets are marked as out-profile by the meter to indicate that the traffic is not complying with CIR, but complying with PIR.

For srTCM, the maximum burst size parameter specifies the maximum burst size that can be transmitted by the source while not complying with the CIR. If the transmitted burst is lower than the MBS value then the packets are marked as out-profile by the meter to indicate that the traffic is not complying with CIR.

If the packet burst is higher than MBS then packets are marked as red are dropped.

The operational MBS set by the system is adapted from the user configured value by using the minimum constraint.

Meter Counters

The 7210 SAS M maintains following counters for meters within the system for granular billing and accounting. Each meter maintains the following counters:

- Counters for packets or octets marked as in-profile by meter
- Counters for packets or octets marked as out-of-profile by meter

Meter Modes

The 7210 SAS M supports following meter modes:

- srtcm: Single Rate Three Color Marking
- trtcm: Two Rate Three Color Marking
- trtcm1:Two Rate Three Color Marking1 (Applicable only for Service Ingress QoS Policies)
- trtcm2:Two Rate Three Color Marking2 (Applicable only for Service Ingress QoS Policies)

In srtcm the CBS and MBS Token buckets are replenished at single rate, that is, CIR where as in case of trtcm CBS and MBS buckets are individually replenished at CIR and PIR rates, respectively. trtcm1 implements the policing algorithm defined in RFC2698 and trtcm2 implements the policing algorithm defined in RFC4115.

Color Aware Policing

The 7210 SAS M supports Color Aware policing at the network ingress, where as at service ingress policing is color blind. In color aware policing user can define the color of the packet using the classification and feed those colored packets to the meter. A color aware meter would treat those packets with respect to the color defined.

- If the packet is pre-colored as in-profile (or also called as Green colored packets) then depending on the burst size of the packet meter can either mark it in-profile or out-profile.
- If the packet is pre-colored as out-profile (also called as Yellow colored packets) then even if the packet burst is lesser than the current available CBS, it would not be marked as in-profile and remain as out-profile.
- If the packet burst is higher than the MBS then it would be marked as Red and would be dropped by meter at ingress.

The profile marked by the meter is used to determine the packets eligibility to be enqueued into a buffer at the egress (when a slope policy is configured at the egress).

QoS Overrides

The QoS Override feature support on access SAP allows the user to override the meter parameters such as CBS, MBS, Rate (CIR and PIR), Mode, and Adaptation rule (CIR and PIR) at the SAP context.

The values are taken from the SAP-Ingress policy, when the meter parameter values are not overridden.

Meter Override commands are supported on all types of access SAP.

Configuration guidelines of QoS Override

The configuration guidelines of QoS Override are:

- QoS override commands can be used only for the meters or policers defined in the SAP ingress policy.
- QoS override commands are not allowed when the attached policy is of an exclusive type.
- QoS override commands are not allowed on Mirror destination SAPs.
- QoS override commands are not allowed when ToD is attached to the SAP.
- On 7210 SAS-M and 7210 SAS-T access-uplink mode, QoS override commands are not supported for ingress and egress QoS policies used with access-uplink SAPs and ports.
- On 7210 SAS-M (network mode), QoS override commands are not supported ingress and egress QoS policies used with network IP interfaces and network ports.

Configuring Meter Override parameters

The following example displays the meter override parameter configuration:

```
*7210SAS>config>service>epipe>sap>ingress# info
----------------------------------------------
                    qos 13
                    meter-override
                        meter 1 create
                            mode trtcm2
                            adaptation-rule pir max cir max
                            cbs 300
                            mbs 200
                            rate cir 300 pir 400
                        exit
                    exit
----------------------------------------------
*A:7210SAS>config>service>epipe>sap>ingress#
```

Queue Parameters

This section describes the queue parameters provisioned on access ports and access uplink network port’s queues for QoS (for 7210 SAS-M and 7210 SAS-T in access uplink mode).

The queue parameters are:

- Queue ID on page 46
- Committed Information Rate on page 47
- Peak Information Rate on page 48
- Adaptation Rule for Queues on page 49
- Committed Burst Size on page 51

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. On 7210 SAS M, the queue ID is not a user configurable entity but the queue ID is statically assigned to the 8 Queues on the port according to FC-QID map table shown in Table 31.

Committed Information Rate

The committed information rate (CIR) for a queue performs two distinct functions:

1. Minimum bandwidth guarantees — Egress queues CIR setting provides the bandwidth which will be given to this queue as compared to other queues on the port competing for a share of the available link bandwidth. The queue CIR does not necessarily guarantee bandwidth in all scenarios and also depends on factors such as CIR oversubscription and link port bandwidth capacity. For each packet in an egress 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 queue is considered in-profile. If the current rate is above the threshold, the queue is considered out-of-profile. This in and out profile state of queue is linked to scheduler prioritizing behavior as discussed below.
2. Scheduler queue priority metric — The scheduler serving a group of egress queues prioritizes individual queues based on their current CIR and PIR states. Queues operating below their CIR are always served before those queues operating at or above their CIR.

Queues at the egress never marks the packets as in-profile or out-profile based on the queue CIR, PIR values. The in-profile and out-profile state of the queue interacts with the scheduler mechanism and provides the minimum and maximum bandwidth guarantees.

When defining the CIR for a queue, the value specified is the administrative CIR for the queue. The user has some control over how the administrative CIR is converted to an operational CIR should the hardware not support the exact CIR and PIR combination specified. The interpretation of the administrative CIR is discussed below in Adaptation Rule for Queues on page 49

Although the 7210 SAS is flexible in how the CIR can be configured, there are conventional ranges for the CIR based on the forwarding class of a queue. A access egress queue associated with the high-priority class normally has the CIR threshold equal to the PIR rate although the 7210 SAS allows the CIR to be provisioned to any rate below the PIR should this behavior be required.

The CIR for a queue is provisioned on egress within access egress QOS policy.

The CIR for the network port queues (for 7210 SAS-M in network mode) and access uplink port queues (for 7210 SAS-M and 7210 SAS-T in access uplink mode) are defined within network queue policies based on the forwarding class. The CIR for the network queues is specified as a percentage of the network interface bandwidth.

Peak Information Rate

The peak information rate (PIR) 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. The actual transmission rate of a egress queue depends on more than just its PIR. Each queue is competing for transmission bandwidth with other queues. Each queue's PIR, CIR and the relative priority and/or weight of the scheduler serving the queue, all combine to affect a queue's ability to transmit packets.

The PIR is provisioned on egress service queues within access egress QoS policies.

The PIR for network queues are defined within network queue policies based on the forwarding class. The PIR for the network queues is specified as a percentage of the network interface bandwidth.

When defining the PIR for a queue or meter, the value specified is the administrative PIR for the queue.The user has some control over how the administrative PIR is converted to an operational PIR should the hardware not support the exact CIR and PIR values specified. The interpretation of the administrative PIR is discussed below in Adaptation Rule for Queues on page 49

Adaptation Rule for Queues

The adaptation rule provides the QoS provisioning system with the ability to adapt specific CIR and PIR defined administrative rates to the underlying capabilities of the hardware the queue will be created on to derive the operational rates. The administrative CIR and PIR rates are translated to actual operational rates enforced by the hardware queue. The rule provides a constraint used when the exact rate is not available due to hardware implementation trade-offs.

For the CIR and PIR parameters individually, the system will attempt to find the best operational rate depending on the defined constraint. The supported constraints are:

- Minimum — Find the hardware supported rate that is equal to or higher than the specified rate.
- Maximum — Find the hardware supported rate that is equal to or lesser than the specified rate.
- Closest — Find the hardware supported rate that is closest to the specified rate.

Depending on the hardware upon which the queue is provisioned, the actual operational CIR and PIR settings used by the queue will be dependant on the method the hardware uses to implement and represent the mechanisms that enforce the CIR and PIR rates.

The 7210 SAS E uses a single rate step value of to define the granularity for both the CIR and PIR rates The adaptation rule controls the method the system uses to choose the rate step based on the administrative rates defined by the **rate** command.

For the supported CIR/PIR range values 0 to 1Gb, the same hardware rate is show in Table 15 or the supported CIR/PIR range values 0 to 10Gb for a 10-Gig Port, the same hardware rate is show in Table 16.

Table 14: Supported Hardware Rates and CIR/PIR Values

Hardware Rate Steps	Rate Range
Kb/sec	0 to 1 Gb/sec

Table 15: Supported Hardware Rates and CIR/PIR Values

Hardware Rate Steps	Rate Range (kbps)
8 Kb/sec	0 - 16770 kbps
16kbps	16780 - 33540 kbps
32kbps	33550 - 67090 kbps
64kbps	67100 - 134180 kbps

Table 15: Supported Hardware Rates and CIR/PIR Values (Continued)

Hardware Rate Steps	Rate Range (kbps)
128kbps	134190 - 268360 kbps
256kbps	268370 - 536730 kpbs
512kbps	536740 - 1000000 kbps

Table 16: Supported Hardware Rates and CIR/PIR Values for 10-Gig Port

Hardware Rate Steps	Rate Range
8 Kb/sec	0 - 16770 kbps
16kbps	16780 - 33540 kbps
32kbps	33550 - 67090 kbps
64kbps	67100 - 134180 kbps
128kbps	134190 - 268360 kbps
256kbps	268370 - 536730 kpbs
512kbps	536740 - 1073470 kbps
1024kbps	1073480 - 10000000 kbps

To illustrate how the adaptation rule constraints **minimum**, **maximum** and **closest** are evaluated in determining the operational CIR or PIR for the 7210 SAS, assume there is a queue where the administrative CIR and PIR values are 90Kbps and 150 Kbps, respectively.

If the adaptation rule is **minimum**, the operational CIR and PIR values will be 96 Kbps and 152 Kbps respectively, as it is the native hardware rate greater than or equal to the administrative CIR and PIR values.

If the adaptation rule is **maximum**, the operational CIR and PIR values will be 88 Kbps and 144 Kbps.

If the adaptation rule is **closest**, the operational CIR and PIR values will be 88 Kbps and 152 Kbps, respectively, as those are the closest matches for the administrative values that are even multiples of the 8 Kbps rate step.

Committed Burst Size

The committed burst size (CBS) parameters specify the amount of buffers that can be drawn from the reserved buffer portion of the queue’s buffer pool. 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 CBS for the queues is not configurable entity for the access, network ports and access uplink ports. The CBS value for the queues is set to appropriate default values which takes care of specific FC needs in terms of maintaining the differential treatment.

Service Ingress QoS Policies

Service ingress QoS policies define ingress service forwarding class meters and map flows to those meters. When a service ingress QoS policy is created, it always has two meters defined that cannot be deleted: one for the all unicast traffic and one for all multipoint traffic. These meters exist within the definition of the policy. The meters only get instantiated in hardware when the policy is applied to a SAP. In the case where the service does not have multipoint traffic, the multipoint meters will not be instantiated.

In the simplest service ingress QoS policy, all traffic is treated as a single flow and mapped to a single meter, and all flooded traffic is treated with a single multipoint meter. 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.
- The number of classification and meter resources to allocate for this policy.
- Allocates resources from the ingress internal CAM resource pool for use for service ingress QoS policies. Additionally, allocate resources to the appropriate classification match criteria.
- At least one default forwarding class meter. The parameters that can be configured for a meter are discussed in Meter Parameters on page 38.

Optional service ingress QoS policy elements include:

- Additional unicast meters up to a total of 8.
- Additional multipoint meters up to 31.
- QoS policy match criteria to map packets to a forwarding class.

Each meter or a queue can have unique meter or queue parameters to allow individual policing or shaping of the flow mapped to the forwarding class. The figure below depicts service traffic being classified into three different forwarding classes.

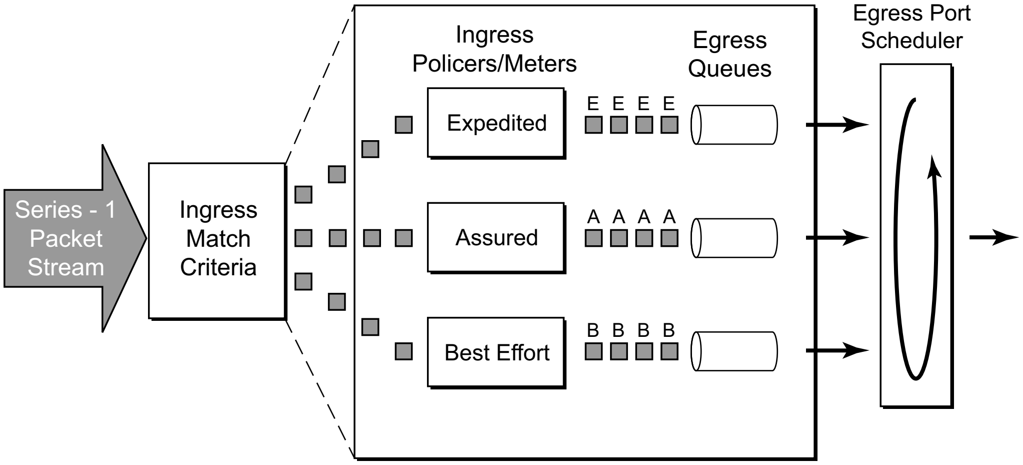

Figure 3: Traffic Queuing Model for Forwarding Classes

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 is subject to a classification policy provisioned.

Table 17 lists the classification rules that are available. Only a single classification policy can be provisioned for an entity.

The IP and MAC match criteria can be very basic or quite detailed. IP and MAC match criteria are constructed from policy entries. An entry is identified by a unique, numerical entry ID. A single entry cannot contain more than one match value for each match criteria. Each match entry has an action which specifies: the forwarding class of packets that match the entry.

The entries are evaluated in numerical order based on the entry ID from the lowest to highest ID value. The first entry that matches all match criteria has its action performed.

Table 17: Service Ingress QoS Policy IP Match Criteria in 7210 SAS-M network mode

IP Criteria	
• DSCP value (available for SAPs in VPLS, VLL, PBB Epipe I-SAP, PBB VPLS I-SAP, IES and VPRN services)	IP source and mask, IP destination and mask, IP protocol, TCP/UDP source port, TCP/UDP destination port, (available only for SAPs in VPLS, VLL, PBB Epipe I-SAP, PBB VPLS I-SAP, IES and VPRN services)

Table 19: Service Ingress QoS Policy MAC Match Criteria

MAC Criteria
• IEEE 802.1p/Dot1p value/mask, Source MAC address/mask, Destination MAC address/mask, EtherType Value/Mask (available for VLL, VPLS, PBB (Epipe I-SAP, VPLS I-SAP, B-SAP), IES and VPRN services.

Table 20: **Service Ingress QoS Policy IPv6 Match Criteria in SAS-M network mode**

IPv6 Criteria	
• DSCP value (available for SAPs in VPLS, VLL, and PBB services)	IPv6 128-bit source and mask, IPv6 128-bit destination and mask, IP protocol/next-header, TCP/UDP source port, TCP/UDP destination port, (available only for SAPs in VPLS, VLL, PBB Epipe I-SAP, PBB VPLS I-SAP)

IP Criteria	
• DSCP value (available for access SAPs in VPLS, VLL, and IES services)	IP source and mask, IP destination and mask, IP protocol, TCP/UDP source port, TCP/UDP destination port, (available only for access SAPs in VPLS, VLL, and IES services)

Table 21: Service Ingress QoS Policy IPv6 Match Criteria in 7210 SAS-M and 7210 SAS-T access-uplink mode

IPv6 Criteria	
• DSCP value (available for SAPs in VPLS, and VLL services)	IPv6 128-bit source and mask, IPv6 128-bit destination and mask, IP protocol/next-header, TCP/UDP source port, TCP/UDP destination port, (available only for SAPs in VPLS and VLL services)

Table 22: Service Ingress QoS Policy MAC Match Criteria in 7210 SAS-M and 7210 SAS-T access-uplink mode

MAC Criteria	
• IEEE 802.1p/Dot1p value/mask, Source MAC address/mask, Destination MAC address/mask, EtherType Value/Mask (available for VLL, VPLS, and IES services.	

The MAC match criteria that can be used for an Ethernet frame depends on the frame’s format. See Table 23.

Table 23: MAC Match Ethernet Frame Types

Frame Format	Description
802.3	IEEE 802.3 Ethernet frame. Only the source MAC, destination MAC and IEEE 802.1p value are compared for match criteria.
Ethernet-II	Ethernet type II frame where the 802.3 length field is used as an Ethernet type (Etype) value. Etype values are two byte values greater than 0x5FF (1535 decimal).

Table 24 lists the criteria that can be matched for the various MAC frame types.

Table 24: MAC Match Criteria Frame Type Dependencies

Frame Format	Source MAC	Dest MAC	IEEE 802.1p Value	Etype Value
802.3	Yes	Yes	Yes	No
ethernet-II	Yes	Yes	Yes	Yes

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

The default service ingress policy is implicitly applied to all SAPs which do not explicitly have another service ingress policy assigned. In the default policy no queues are defined. All traffic is mapped to the default forwarding class which uses a meter by default. The characteristics of the default policy are listed in Table 25.

Table 25: Default Service Ingress Policy ID 1 Definition

Characteristic	Item	Definition
Meters	Meter 1	1 (one) meter all unicast traffic: • Forward Class: best-effort (be) • CIR = 0 • PIR = max (4000000 kbps in case of a LAG with four member ports) • MBS, CBS = default (values derived from applicable policy)

Table 25: Default Service Ingress Policy ID 1 Definition (Continued)

Characteristic	Item	Definition
	Meter 11	1 (one) meter for all multipoint traffic: • CIR = 0 • PIR = max (4000000 kbps in case of a LAG with four member ports) • MBS, CBS = default (values derived from applicable policy)
Flows	Default Forwarding Class (be)	1 (one) flow defined for all traffic: • All traffic mapped to best-effort (be)

The available ingress CAM hardware resources can be allocated as per user needs for use with different QoS classification match criteria. By default, the system allocates resources to maintain backward compatibility with release 4.0. Users can modify the resource allocation based on their need to scale the number of entries or number of associations (that is, number of SAPs using a policy that uses a particular match criterion). If no resources are allocated to a particular match criteria used in the policy, then the association of that policy to a SAP will fail. Allocation of classification entries also allocates meter resources, used to implement the per FC per traffic type policing function. Please refer to the Resource Allocation for Service Ingress QoS policies on page 216 to know more about resource usage and allocation to SAP ingress policies.

An aggregate SAP shaper is available for use per SAP. The aggregate shaper limits the rate of unicast queued traffic across all the FCs configured on SAP ingress.

Hierarchical Ingress Policing

Hierarchical ingress policing allows the users to specify the amount of traffic admitted into the system per SAP. It also allows the user to share the available bandwidth per SAP among the different FCs of the SAP. For example, user can allow the packets classified as Internet data to use the entire SAP bandwidth when other forwarding classes do not have traffic.

It provides an option to configure SAP aggregate policer per SAP on SAP ingress. The user should configure the PIR rate of the aggregate policer. The user can optionally configure the burst size of the aggregate policer.

The aggregate policer monitors the traffic on different FCs and determines if the packet has to be forwarded to an identified profile or dropped. The final disposition of the packet is based on the operating rate of the following:

- Per FC policer
- Per SAP aggregate policer

For more information on the final color assigned of the packet, refer to the command description of "aggregate-meter-rate" command in the 7210 SAS M Services Guide.

A new meter mode “trtcm2” (RFC 4115) is introduced for use only on SAP ingress. When the SAP aggregate policer is configured, the per FC policer can be only configured in “trtcm2” mode. The existing meter mode “trtcm” is re-named as “trtcm1” (RFC 2698). The meter modes “srtCM” and “trtcm1” are used in the absence of aggregate meter.

NOTE: Before use of per SAP aggregate policer/meter, meter resources must be allocated using the CLI command config> system> resource-profile> ingress-internal-tcam> sap-aggregate-meter. Change to the amount of resources allocated for SAP aggregate meter requires a reboot of the node to take effect. For more information, see the 7210 Basic System Guide.

Access Egress QoS Policies

An access egress policy defines the queue and marking characteristics for the traffic egressing towards the customer on the access ports. There are 8 queues always available at the access port and FCs are mapped into these 8 Queues. By configuring appropriate queue shape rates the individual FC traffic can be managed so that each FC traffic is well within SLA limits and does not impact the serviceability of other FCs.

Access egress QoS policies define access queues and map forwarding class flows to queues. There are 8 queues always available per access port and all forwarding classes traffic is mapped into these separate 8 queue as per Table 31, Forwarding Class to Queue-ID Map, on page 81. To define a basic access egress QoS policy, the following are required:

- A unique service access QoS policy ID.
- A QoS policy scope of template or exclusive.
- The parameters that can be configured for a queue are discussed in Queue Parameters on page 46.
- IEEE 802.1p priority value remarking based on forwarding class.

  In the 7210 SAS-M in network mode, 7210 SAS-M and 7210 SAS-T access-uplink mode, remarking of dot1p or DSCP or both bits by default is disabled. It can be enabled by the **remarking** command with options to remark dot1p/dscp/both present under access-egress context. In 7210 SAS-M network mode, user is provided with an option to remark Dot1p or DSCP or both. In 7210 SAS-M and 7210 SAS-T access-uplink mode, user is provided with an option to remark Dot1p bits only.

The forwarding class determination per service egress packet is determined at ingress. If the packet ingressed the service on the same router, the service ingress classification rules determine the forwarding class of the packet. In network mode, if the packet was received over a service transport tunnel on a network port, the forwarding class is typically determined by in the MPLS LSP EXP bits. For 7210 SAS-M and 7210 SAS-T in access uplink mode, if the packet was received on a access-uplink port, the forwarding class is determined by the Dot1p bits in the outer tag of the QinQ encapsulation.

Access egress QoS policy ID 1 is reserved as the default access ports which do not have another access egress policy explicitly assigned. The characteristics of the default policy are listed in the following table.

Table 26: Default Access Egress Policy ID 1 Definition

Characteristic	Item	Definition
Queues	Queue 1-8	1 (one) queue defined for each traffic class
Network-Control (nc)	Queue 8	• CIR=0 • PIR=max (line rate) • CBS=default (values derived for optimal buffer usage)
High-1 (h1)	Queue7	• CIR=0 • PIR=max (line rate) • CBS=default (values derived for optimal buffer usage)
Expedited (ef)	Queue 6	• CIR = 0 • PIR = max (line rate) • CBS = default (values derived for optimal buffer usage)
High-2 (h2)	Queue 5	• CIR = 0 • PIR = max (line rate) • CBS = default (values derived for optimal buffer usage)
Low-1 (l1)	Queue 4	• CIR = 0 • PIR = max (line rate) • CBS = default (values derived for optimal buffer usage)
Assured (af)	Queue 3	• CIR = 0 • PIR = max (line rate) • CBS = default (values derived for optimal buffer usage)
Low-2 (l2)	Queue 2	• CIR = 0 • PIR = max (line rate) • CBS = default (values derived for optimal buffer usage)
Best-Effort (be)	Queue 1	• CIR = 0 • PIR = max (line rate) • CBS = default (values derived for optimal buffer usage)
Flows	Default Action	All FCs are mapped to corresponding Queues and Dot1p values are marked as follows:

Table 26: Default Access Egress Policy ID 1 Definition (Continued)

Characteristic	Item	Definition	
		In-Profile	**Out-Profile**
Network-Control (nc)		7	7
High-1(h1)		6	6
Expedited (ef)		5	5
High-2 (h2)		4	4
Low-1 (l1)		3	3
Assured (af)		2	2
Low-2 (l2)		1	1
Best-Effort (be)		0	0

Buffer Pools

Buffer pools cannot be created or deleted in the 7210 SAS. The default pools created by the system are distributed among various ports. The 7210 SAS-M, when operating in network mode and access-uplink mode, only supports port egress buffer pools by default.The egress buffer pools are distributed as network egress buffer pool and access egress buffer pools. When the decommission entries are not configured, during system initialization, based on the maximum number of ports to be supported for access and network, the total buffer is distributed into the access egress buffer pool and the network egress buffer pool. The distribution of the buffers into access and network egress pools take care of the buffer requirements at the port level for various queue shaping/ scheduling mechanisms and for various packet sizes varying from 64 bytes to jumbo frames. Each port on the system gets a equal portion of the available buffers. From the buffers allocated to a port, each queue gets its CBS amount of buffers. The remaining buffers are allocated towards the shared MBS pool per port. All the queues of the port can use the buffers from the shared MBS pool.

Using decommission command for Buffer Allocation on 7210 SAS-M and 7210 SAS-T devices

Note: The platforms that support using decommission command for buffer allocation are 7210 SAS-M in both access-uplink and network mode, all variants of 7210 SAS-M – namely 7210 SAS-M 24F, 7210 SAS-M 24F 2XFP (ETR and non-ETR), with or without the CES MDA and the 2x10G MDA, and 7210 SAS-T. On 7210 SAS-M variants that support the 2 x10G MDA, it is possible to decommission the 10G ports on the MDA or to allocate more buffers to the 10G ports on the MDA.

This feature enables the user to make efficient use of the available port egress queue buffer pool by allocating queue buffers of the unused ports to ports. Services cannot be configured on the unused ports as software takes away all the queue buffer resources from these ports that need increased amount of buffers to handle larger bursts. This allows the operators who use limited number of ports to deploy services, to increase the amount of queue buffers allocated to them by decommissioning ports that are not used to deploy services.

The amount of credit of queue buffers received by a port is used to increase the MBS portion of the buffer pool of the port. This allows any queue on the port to use the buffers, if needed. The CBS portion of the queue is not modified with this feature.

Note: The system has to be rebooted after decommissioning of ports for the queue buffers to be reallocated and the configuration to take effect.

The users have an option to specify the groups of ports which receives the credit of queue buffers freed up using the decommission command. With this option, the user can specify a port or group of ports which receives the credit of queue buffers. For example, it is possible for the user to configure decommissioning of 4 fixed copper ports and allocate the freed queue buffers to the remaining copper ports in the system or decommission 5 fiber ports and allocate the freed up queue buffers to the 10G XFP ports, and so on. This mechanism allows the operators to provide higher amount of queue buffers to a specific port or a group of ports, allowing them to pick and choose ports that need the extra buffers for burst absorption. The user is allowed to increase the per port MBS pool limit so that more buffers are available to absorb larger bursts, at the cost of decommissioning ports which are not used to configure services.

Note on Buffer allocation on 7210 SAS-M

On 7210 SAS-M, each queue is allocated with a small fixed amount of buffers towards the CBS (Committed burst size) and each port is allocated with a shared pool of buffers towards the MBS (Maximum Burst Size). The per queue CBS portion of buffers guarantees that the queue does not starve due to lack of buffers and allows for line-rate throughput through the node. The buffers allocated towards the MBS pool, allows each port to handle some amount of burst. Per port MBS pool/portion of buffers is shared by all the queues of the port and allows any queue or a small group of queues of the port to absorb larger bursts assuming that, not all the queues receive burst simultaneously. In a typical network, the router/switch in the ingress traffic is usually a mix of packets of different sizes and different flows burst at different time intervals, thus allowing 7210 SAS-M to provide better burst absorption capability per queue.

The hardware implements an algorithm to handle requests for allocation of buffers from the MBS pool assuming that not all the ports and queues burst at the same time. This allows some queues to utilize a larger portion of the buffers when it is available, allowing them to handle larger bursts. At the same time, the algorithm ensures that all the queues get fair share of the buffers, so that the throughput on those ports is not affected. When hardware receives a packet, before it decides to queue up the packet on the egress queue of the destination port, it determines the discard threshold for the queue based on the oversubscription factor and the total amount of free buffers available at that point of time. The queue’s discard threshold is higher, if the amount of free buffers available is larger (which indicates other queues on the node have lesser congestion), allowing the queue to absorb larger bursts. The queue’s discard threshold is lower, if there is lesser amount of free buffers available (which indicates that other queues are heavily congested on the node), which results in the packet being dropped. At the same time, algorithm allocates the available free buffers to queues which are using lesser amount of buffers or not using any buffers. This allows equal sharing of available buffers and maintains a good throughput for less congested queues.

Note on Buffer allocation on 7210 SAS-T

The buffer allocation on 7210 SAS-T is different from what is available on 7210 SAS-M. 7210 SAS-T has 2MB of packets buffers and it provides for 2 modes of operation. In one mode, the MBS pool is a shared across all queues on all ports (that is, referred to as per node from now on) and in the other mode, the MBS pool is shared across all queues of a single port (that is, referred to as per port from now on).

Per node MBS pool

In the per node mode, each of the 8 queues available on a port, is allocated a CBS amount of committed buffers. The remaining amount of buffers is allocated towards the MBS pool that is available for sharing among all the queues across all the ports of the node. In other words the MBS pool is per node unlike the per port MBS pool on the 7210 SAS-M. **Note**: The system internal ports, such as internal loopback port used for mirroring, port loopback with mac-swap, and others are allocated some buffers. Additionally, some buffers are reserved for internal use. The 7210 SAS-T hardware implements a similar algorithm as the 7210 SAS-M to provide access to the per node MBS pool of buffers. For more information, see Note on Buffer allocation on 7210 SAS-M on page 62.

Per port MBS pool

To allow operators better control over which ports get larger portion of queue buffers, the operator is provided with an option to use per-port MBS pool (like what is available on 7210 SAS-M) and decommission ports. The decommissioning of ports is only allowed when the node is booted with the option to use per-port MBS pool.

With the decommissioning feature, the user is provided with an option to make efficient use of the available port egress queue buffer pool by allocating queue buffers of the unused ports to in-use ports. It allows the user to specify the unused front-panel ports which cannot be used to deploy any services. The software does not allocate any queue buffers to these unused ports and assigns it to a specific port or a group of ports. The user is provided with a CLI command to decommission a port and make it unavailable to deploy services. This mechanism allows operators who use limited number of ports to deploy services, to increase the amount of queue buffers allocated to them by decommissioning ports that will not be used to deploy any services.

The user has an option to specify the groups of ports which will receive the credit of queue buffers freed up using the decommission command. With this option, the user can specify a port or group of ports which receives the credit of queue buffers. For example, it is possible for the user to configure decommissioning of 4 fixed copper ports and allocate the freed queue buffers to the remaining copper ports in the system or decommission 5 fiber ports and allocate the freed up queue buffers to the 10G XFP ports, and so on. This mechanism allows the operators to provide higher amount of queue buffers to a specific port or a group of ports, allowing them to pick and choose ports that need the extra buffers for burst absorption.

The amount of credit of queue buffers received by a port is used to increase the MBS portion of the buffer pool of the port. This allows any queue on the port to use the buffers, if need be. The CBS portion of the queue is not modified with this feature. The system has to be rebooted after decommissioning of ports for the queue buffers to be reallocated and the configuration to take effect.

Configuration guidelines for use of ‘Decommission’ commands on 7210 SAS-M and 7210 SAS-T devices

- The CLI command “*configure>system>resource-profile>decommission>entry*” allows the user to configure the list of ports to be decommissioned and the list of ports that need more buffers. The system does not allocate any packet buffers to the ports which are decommissioned. For more information, see the CLI command description for details on the functionality provided by the command.
- Packet buffers are added to the MBS pool of the port (the MBS pool is shared by the 8 queues on the port) and the CBS portion of the queues are not modified.
- The user can modify the list of ports or update to the list of ports specified with the decommission command (and also entry command) when the node is up, but the changes are effected by software only after a reboot of the 7210 SAS-M node.
- The software maintains two lists of entries, one is the current list of ports and another which has been modified by the user and takes effect only after the next reboot. These lists can be displayed using the show command. The configuration file always stores the list of entries as configured by the user, so that when rebooted the modified entries and new entries (if any) takes effect.
- A port must be in administrative down (shutdown) state before it is in a decommission entry. An attempt to configure a port which is administratively up (no shutdown) state results in an error. The administrative state or the operational state of the port is not affected by configuring the port in a decommission entry.
- The decommissioned port cannot be used in any service configuration or as a loopback port. An attempt to do so results in an error.
- The decommissioned port must not be configured with BOF parameter, ‘no-service-ports’.
- Buffer allocation to a port should is possible for access ports, network ports or hybrid ports. In other words, irrespective of port mode, it is possible to assign more buffer resources to the port.
- The user needs to ensure that enough buffers are available for the internal loopback ports or front-panel ports assigned for loopback. It is not recommended to take away buffers allocated to these ports and assign it to other ports. This might cause unintended behavior of the system. The system software does not check for this, but expects users to ensure this through proper configuration.

- During system boot up, while executing the commands in the configuration file software checks if the no-service-ports are configured under the decommission entries. If there is match, software throws an error and stops execution of further commands in the configuration file. When this happens, user needs to correct the configuration file or the BOF file, to either remove the ports from the decommission entries or not configure them as no-service-ports in the BOF, save the BOF file or the configuration file based on where the change was made and reboot the node.
- On 7210 SAS-T, the decommission command takes affect only if the per port MBS pool is in use, that is, the user needs to configure the CLI command "*configure>configure> system> resource-profile> qos> mbs-pool port"*, before using the decommission port feature.

The following configuration sample shows the ports to be decommissioned and the ports that need more buffers.

```
A:7210SAS>config>system>res-prof>decom# info detail
----------------------------------------------
entry 15 port 1/2/1,1/2/2 to 1/1/2
entry 23 port 1/1/5 to 1/1/3
----------------------------------------------
A:7210SAS>config>system>res-prof>decom#
```

Note: For more information on the decommission CLI commands, see the "7210 SAS OS Basics System User Guide".

Slope Policies

The available buffer space is partitioned into buffer pools. The buffers for a queue are allocated from a single buffer pool. On 7210 SAS-M (network mode and access-uplink mode), buffer pools are created for access port egress, network port egress (in network mode) and access uplink port egress (in access uplink mode). In 7210 SAS-T, the buffer allocation is done as described above in the section on Buffer Allocation.

Slope policies define the RED slope characteristics as a percentage of pool size for the pool on which the policy is applied.

On 7210 SAS-M (network mode and access-uplink mode) default buffer pools exist (logically) at the port levels.

- Access egress pool
- Network egress pool (in network mode)
- Access uplink egress pool (in access uplink mode)

By default, each queue on the port is associated with slope-policy **default** which disables the high-slope, low-slope, and non-TCP slope within the pool.

On 7210 SAS-M (network mode and access-uplink mode) Access, anetwork pools (in network mode) and access uplink pools (in access uplink mode) are created at the port level; creation is dependent on the physical port mode (network , access, or access uplink).

Note: If WRED is not configured, then taildrop is used.

RED Slopes In Network and Access-uplink Mode

Operation and Configuration

On 7210 SAS-M (network mode and access-uplink mode) each queue provides user an option to configure high-priority RED slope a non-TCP RED slope,and a low-priority RED slope or use 2 slopes - high-priority RED slope and a low-priority RED slope per queue. On 7210 SAS-T, each queue, supports a high-priority RED slope and a low-priority RED slope.

The high-priority RED slope manages access to the shared portion of the buffer pool for high-priority or in-profile packets. The low-priority RED slope manages access to the shared portion of the buffer pool for low-priority or out-of-profile packets. The non-TCP slope manages access to the shared portion of the buffer pool for non-TCP packets (such as MPLS packets received on network ingress).

By default, the high-priority, low-priority , and non-TCP RED slopes are disabled.

The WRED uses average queue lengths, queue thresholds provisioned, and drop probablility to calculate the packet’s eligibility to be enqueued. The committed portion of the buffer pool is exclusively used by a queue to enqueue traffic within committed rate.

For the queues within a buffer pool, packets are either queued using committed burst size (CBS) buffers or shared buffers. The CBS buffers are simply buffer memory that has been allocated to the queue while the queue depth is at or below its CBS threshold. The amount of CBS assigned to all queues is dependent upon the number of queues created, the setting of the default CBS as defined in the policy, and any CBS values set per queue within a QoS policy. However, from a functional perspective, the buffer pool does not keep track of the total of the CBS assigned to queues serviced by the pool. CBS subscription on the pool is an administrative function that must be monitored by the queue provisioner.

For access and network buffer pools, the percentage of the buffers that are to be reserved for CBS buffers is configured by the software (cannot be changed by user). This setting indirectly assigns the amount of shared buffers on the pool. This is an important function that controls the ultimate average and total shared buffer utilization value calculation used for RED slope operation. The CBS setting can be used to dynamically maintain the buffer space on which the RED slopes operate.

When a queue depth exceeds the queue’s CBS, packets received on that queue must contend with other queues exceeding their CBS for shared buffers. To resolve this contention, the buffer pool uses two RED slopes to determine buffer availability on a packet by packet basis. A packet that was either classified as high priority or considered in-profile is handled by the high-priority RED slope. This slope should be configured with RED parameters that prioritize buffer availability over packets associated with the low-priority RED slope. Packets that had been classified as low priority or out-of-profile are handled by this low-priority RED slope.

The following is a simplified overview of how a RED slope determines shared buffer availability on a packet basis:

1. The RED function keeps track of shared buffer utilization and shared buffer average utilization.
2. At initialization, the utilization is 0 (zero) and the average utilization is 0 (zero).
3. When each packet is received, the current average utilization is plotted on the slope to determine the packet’s discard probability.
4. A random number is generated associated with the packet and is compared to the discard probability.
5. The lower the discard probability, the lower the chances are that the random number is within the discard range.
6. If the random number is within the range, the packet is discarded which results in no change to the utilization or average utilization of the shared buffers.
7. A packet is discarded if the utilization variable is equal to the shared buffer size or if the utilized CBS (actually in use by queues, not just defined by the CBS) is oversubscribed and has stolen buffers from the shared size, lowering the effective shared buffer size equal to the shared buffer utilization size.
8. If the packet is queued, a new shared buffer average utilization is calculated using the time-average-factor (TAF) for the buffer pool. The TAF describes the weighting between the previous shared buffer average utilization result and the new shared buffer utilization in determining the new shared buffer average utilization. (See Tuning the Shared Buffer Utilization Calculation on page 69.)
9. The new shared buffer average utilization is used as the shared buffer average utilization next time a packet’s probability is plotted on the RED slope.
10. When a packet is removed from a queue (if the buffers returned to the buffer pool are from the shared buffers), the shared buffer utilization is reduced by the amount of buffers returned. If the buffers are from the CBS portion of the queue, the returned buffers do not result in a change in the shared buffer utilization.

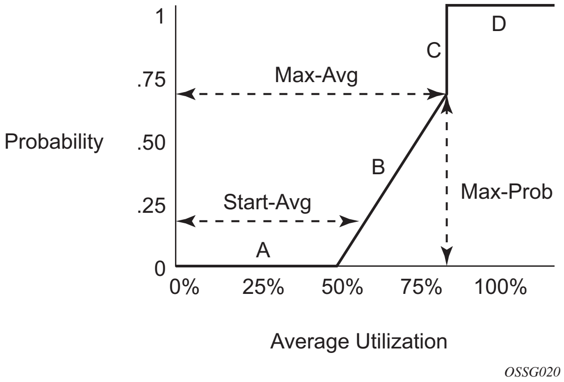

Figure 4: RED Slope Characteristics

A RED slope itself is a graph with an X (horizontal) and Y (vertical) axis. The X-axis plots the percentage of shared buffer average utilization, going from 0 to 100 percent. The Y-axis plots the probability of packet discard marked as 0 to 1. The actual slope can be defined as four sections in (X, Y) points (Figure 4):

1. Section A is (0, 0) to (start-avg, 0). This is the part of the slope that the packet discard value is always zero, preventing the RED function from discarding packets when the shared buffer average utilization falls between 0 and start-avg.
2. Section B is (start-avg, 0) to (max-avg, max-prob). This part of the slope describes a linear slope where packet discard probability increases from zero to max-prob.
3. Section C is (max-avg, max-prob) to (max-avg, 1). This part of the slope describes the instantaneous increase of packet discard probability from max-prob to one. A packet discard probability of 1 results in an automatic discard of the packet.
4. Section D is (max-avg, 1) to (100%, 1). On this part of the slope, the shared buffer average utilization value of max-avg to 100% results in a packet discard probability of 1.

Plotting any value of shared buffer average utilization will result in a value for packet discard probability from 0 to 1. Changing the values for start-avg, max-avg and max-prob allows the adaptation of the RED slope to the needs of the access or network queues using the shared portion of the buffer pool, including disabling the RED slope.

Tuning the Shared Buffer Utilization Calculation

The 7210 SAS Mallows tuning the calculation of the Shared Buffer Average Utilization (SBAU) after assigning buffers for a packet entering a queue as used by the RED slopes to calculate a packet’s drop probability. The 7210 SAS M implements a time average factor (TAF) parameter in the buffer policy which determines the contribution of the historical shared buffer utilization and the instantaneous Shared Buffer Utilization (SBU) in calculating the SBAU. The TAF defines a weighting exponent used to determine the portion of the shared buffer instantaneous utilization and the previous shared buffer average utilization used to calculate the new shared buffer average utilization. To derive the new shared buffer average utilization, the buffer pool takes a portion of the previous shared buffer average and adds it to the inverse portion of the instantaneous shared buffer utilization (SBU). The formula used to calculated the average shared buffer utilization is:

$$SBAU_n = \left(SBU \times \frac{1}{2^{TAF}}\right) + \left(SBAU_{n-1} \times \frac{2^{TAF} - 1}{2^{TAF}}\right)$$

where:

$SBAU_n$ = Shared buffer average utilization for event n

$SBAU_{n-1}$ = Shared buffer average utilization for event (n-1)

SBU = The instantaneous shared buffer utilization

TAF = The time average factor

Table 27 shows the effect the allowed values of TAF have on the relative weighting of the instantaneous SBU and the previous SBAU ($SBAU_{n-1)}$ has on the calculating the current SBAU ($SBAU_n$).

Table 27: TAF Impact on Shared Buffer Average Utilization Calculation

TAF	2^{TAF}	Equates To	Shared Buffer Instantaneous Utilization Portion	Shared Buffer Average Utilization Portion
0	2^0	1	1/1 (1)	0 (0)
1	2^1	2	1/2 (0.5)	1/2 (0.5)
2	2^2	4	1/4 (0.25)	3/4 (0.75)
3	2^3	8	1/8 (0.125)	7/8 (0.875)
4	2^4	16	1/16 (0.0625)	15/16 (0.9375)
5	2^5	32	1/32 (0.03125)	31/32 (0.96875)
6	2^6	64	1/64 (0.015625)	63/64 (0.984375)
7	2^7	128	1/128 (0.0078125)	127/128 (0.9921875)
8	2^8	256	1/256 (0.00390625)	255/256 (0.99609375)

Table 27: TAF Impact on Shared Buffer Average Utilization Calculation (Continued)

TAF	2^{TAF}	Equates To	Shared Buffer Instantaneous Utilization Portion	Shared Buffer Average Utilization Portion
9	2^9	512	1/512 (0.001953125)	511/512 (0.998046875)
10	2^{10}	1024	1/1024 (0.0009765625)	1023/2024 (0.9990234375)
11	2^{11}	2048	1/2048 (0.00048828125)	2047/2048 (0.99951171875)
12	2^{12}	4096	1/4096 (0.000244140625)	4095/4096 (0.999755859375)
13	2^{13}	8192	1/8192 (0.0001220703125)	8191/8192 (0.9998779296875)
14	2^{14}	16384	1/16384 (0.00006103515625)	16383/16384 (0.99993896484375)
15	2^{15}	32768	1/32768 (0.000030517578125)	32767/32768 (0.999969482421875)

The value specified for the TAF affects the speed at which the shared buffer average utilization tracks the instantaneous shared buffer utilization. A low value weights the new shared buffer average utilization calculation more to the shared buffer instantaneous utilization. When TAF is zero, the shared buffer average utilization is equal to the instantaneous shared buffer utilization. A high value weights the new shared buffer average utilization calculation more to the previous shared buffer average utilization value. The TAF value applies to all high and low priority RED slopes for ingress and egress buffer pools controlled by the buffer policy.

Slope Policy Parameters

The elements required to define a slope policy are:

- A unique policy ID.
- On 7210 SAS-M, choose whether the three slopes per queue must be used or two slopes must be used. On 7210 SAS-T, only two slopes per queue is available.
- The high and low RED slope shapes for the buffer pool: settings for the high-priority and low-priority RED slopes.
- The RED slope shapes for the buffer-pool, that is, settings for the RED slopes:
  - → If 3 slopes are used, then user needs to configure high-priority TCP slope, low - priority TCP slope and non-TCP slope parameters.
  - → If two slopes are used, then user needs to configure high-priority slope and low - priority slope parameters.

All slopes are available per queue and the following parameters are configurable for each slope:

- start-avg
- max-avg
- max-prob
- Time average factor (TAF)

A slope policy is defined with generic parameters so that it is not inherently an access or a network policy. A slope policy defines access egress buffer management properties, when it is associated with an access port buffer pool and network egress buffer management properties, when it is associated with a network port buffer pool.

Each access egress buffer pool and network egress pool can be associated with only one slope policy ID.

Slope policy ID **default** is reserved for the default slope policy. The default policy cannot be deleted or changed. The default slope policy is implicitly applied to all access and network buffer pools which do not have another slope policy explicitly assigned.

Table 28 lists the default values for the default slope policy.

Table 28: Default Slope Policy Definition (for 7210 SAS-M configured in Network mode)

Parameter	Description	Setting
Policy ID	policy ID	default (for default policy)
High (RED) slope	Administrative state	Shutdown

Table 28: Default Slope Policy Definition (for 7210 SAS-M configured in Network mode)

Parameter	Description	Setting
	start-avg	70% utilization
	max-avg	90% utilization
	max-prob	75%
Low (RED) slope	Administrative state	Shutdown
	start-avg	50% utilization
	max-avg	75% utilization
	max-prob	75%

Table 28: Default Slope Policy Definition (for 7210 SAS-M configured in Network mode)

Parameter	Description	Setting
Non-TCP (RED) slope	Administrative State	Shutdown
	start-avg	50% utilization
	max-avg	75% utilization
	max-prob	75%

CPU Queues

The packets that are destined to the CPU are prioritized based on the application. Some of the applications that are prioritized are Layer 2 data packets (copy of which is sent to CPU for MAC learning), EFM, CFM, STP, LACP, OSPF, IS-IS, RSVP, TLDP, and so on.

The packets destined to the CPU are classified internally and are placed into the correct queue. These packets are rate-limited to prevent DoS attacks. The software programs the classification entries to identify these packets and assigns appropriate bandwidth and priority to them. It is not configurable by the user.

Port Scheduler Policies

Port scheduler policies control the traffic behavior on a per-port basis. Associated with each egress port is a set of eight class of service (CoS) queues and a default port-scheduler-policy named “default”. This default policy makes the port to behave in strict mode. The default policy cannot be modified. The user can attach another policy to the port to change its scheduling behavior. The scheduler that provides the arbitration across the eight CoS queues is a scheduler that is configured in a variety of modes. A major aspect of the arbitration mechanism is the ability to provide minimum and maximum bandwidth guarantees. This is accomplished by tightly integrating a network queue and access egress policies into the scheduler. After the packets are mapped into a COS queue, they are forwarded/conditioned using one of these schedulers (such as Strict Priority (SP), Round-Robin (RR), Weighted Round-Robin (WRR), Weighted Deficit Round-Robin (WDRR), (WRR+SP, WDRR+SP). The traffic shaping aspect is tightly integrated with the scheduler.

Scheduler Modes

The scheduling modes interact with the minimum and maximum bandwidth CoS queue and maximum bandwidth egress port shaping specifications. Each egress port may be configured to have a specific scheduling mode. The scheduler first services the queues to meet their CIR and then services the queues to meet the PIR. There are five possibilities as follows:

- Strict priority scheduling across CoS queues — The strict priority scheduler provides strict priority access to the egress port across the CoS queue from highest CoS queue index (7) to the lowest (0). The purpose of the strict priority scheduler is to provide lower latency service to the higher CoS classes of traffic. In this mode, the scheduler services the queues in order of their prority in both the CIR and PIR loop.

Table 29: Minimum and Maximum Bandwidth Meters Example

QoS Queue Name	Minimum Bandwidth	Maximum Bandwidth
7	10 Mbps	1 Gbps
6	10 Mbps	1 Gbps
5	50 Mbps	1 Gbps
4	50 Mbps	1 Gbps
3	50 Mbps	1 Gbps
2	50 Mbps	1 Gbps
1	50 Mbps	1 Gbps
0	50 Mbps	1 Gbps

Displayed in Table 29, CoS queues 7 and 6 each have a minimum bandwidth specification of 10 Mbps, whereas the remaining QoS queues have a minimum bandwidth specification of 50 Mbps. All CoS queues have a maximum bandwidth specification of 1 Gbps. The goal of these settings is to guarantee the minimum bandwidth settings for each of the queues while also allowing each CoS queue to fully use the egress port capability by having the maximum bandwidth setting at 1 Gbps. The strict priority scheduler mode provides low latency service for CoS queues 6 and 7 while their minimum bandwidth guarantees are being satisfied.

- Round robin scheduling across CoS queues — The round robin scheduler mode provides round robin arbitration across the CoS queues. The scheduler visits each backlogged CoS queue, servicing a single packet at each queue before moving on to the next one. The purpose of the round robin scheduler is to provide fair access to the egress port bandwidth (at a packet level). This works best when packet sizes are approximately comparable. In this mode, the scheduler services the queues in round-robin for both the CIR and the PIR loop.
- Weighted round robin (WRR) — In WRR mode, the scheduler provides access to each CoS queue in round robin order.When the scheduler is providing access to a particular queue, it services a configurable number of back-to-back packets before moving on to the subsequent CoS queue. A value of strict is used to designate that a particular queue be considered to be a part of a hybrid Strict + WRR configuration. The values 1 to 15 are used to indicate the number of back-to-back packets to be serviced when the scheduler is servicing a particular CoS queue. If the weight specified is N, but if the number of packets in the queue is lesser than N, the scheduler continues working and moves on to the next backlogged queue. In this mode, with no strict queues configured, the scheduler services the queues in round robin in the CIR loop. The configured weights are not considered in the CIR loop. The weights are used only in the PIR loop.
- Weighted deficit round robin (WDRR) scheduling— An inherent limitation of the WRR mode is that bandwidth is allocated in terms of packets. WRR works well if the average packet size for each CoS queue flow is known.WDRR aims at addressing this issue. WDRR provides a bandwidth allocation scheduler mode that takes into account the variably-sized packet issue by maintaining sufficient state information when arbitrating across the CoS queues. In this mode, with no strict queues configured, the scheduler services the queues in round-robin in the CIR loop. The configured weights are not considered in the CIR loop. The weights are used only in the PIR loop. A weight value of 1 to 15 can be configured for each queue. Based on the weights provided respective amount of bytes is de-queued from the queue. A value of 0 is used to designate that a particular queue be considered to be a part of a hybrid Strict + WDRR configuration. If a weight value of 1 is given for queue 1 and 5 is given for queue 2, then we will see traffic out of the port in the ratio of 1:5 between the queues (1 and 2), provided no traffic is flowing in the other queues. A weight value of 1 will actually pump out 2Kbytes from that queue, a value of 5 will pump out 10 Kbytes. Twice of the weight value given will be pumped out.
- Strict + WRR/WDRR — If the WRR/WDRR weight associated with a particular CoS queue is set to strict, the queue is considered to be in a strict priority mode. This set of

strict priority queues is serviced first in the order of their CoS numbering (higher numbered CoS queue receives service before smaller numbered queues). In this mode, the scheduler services the strict queues first and then the queues configured with weights in both the CIR and PIR loop. The scheduler ensures that it meets the CIR of all the queues (both strict queues and queues with weight), if bandwidth is available before scheduling the queues in the PIR loop. If multiple queues are configured as strict, the higher-priority strict queues are serviced first before the lower priority strict queues in both the CIR and the PIR loop. The weights configured for the queues are only considered during the PIR loop.

CPU Queues

The packets that are destined to the CPU are prioritized based on the application. Some of the applications that are prioritized are Layer 2 data packets (a copy of which is sent to CPU for MAC learning), EFM, CFM, STP, LACP, ICMP, etc. The CPU provides eight queues from BE (0) to NC (7). The packets destined to the CPU are classified internally and are put into the correct queue.

These packets are rate-limited to prevent DoS attacks. The software programs the classification entries to identify these packets and assigns appropriate bandwdith and priority to them. It is not configurable by the user.

Egress Port Rate Limiting

The 7210 SAS supports port egress rate limiting. This features allows the user to limit the bandwidth available on the egress of the port to a value less than the maximum possible link bandwidth. It also allows the user to control the amount of burst sent out.

Forwarding Classes

7210 SAS devices support multiple forwarding classes and class-based queuing, so the concept of forwarding classes is common to all of the QoS policies.

Each forwarding class (also called Class of Service (CoS)) is important only in relation to the other forwarding classes. A forwarding class provides network elements a method to weigh the relative importance of one packet over another in a different forwarding class.

Queues are created for a specific forwarding class to determine the manner in which the queue output is scheduled. The forwarding class of the packet, along with the in-profile or out-of-profile state, determines how the packet is queued and handled (the per hop behavior (PHB)) at each hop along its path to a destination egress point. 7210 SAS devices support eight (8) forwarding classes (Table 30).

Table 30: Forwarding Classes

FC-ID	FC Name	FC Designation	DiffServ Name	Notes
7	Network Control	NC	NC2	Intended for network control traffic.
6	High-1	H1	NC1	Intended for a second network control class or delay/jitter sensitive traffic.
5	Expedited	EF	EF	Intended for delay/jitter sensitive traffic.
4	High-2	H2	AF4	Intended for delay/jitter sensitive traffic.
3	Low-1	L1	AF2	Intended for assured traffic. Also is the default priority for network management traffic.
2	Assured	AF	AF1	Intended for assured traffic.
1	Low-2	L2	CS1	Intended for BE traffic.
0	Best Effort	BE	BE	

Note that Table 30 presents the default definitions for the forwarding classes. The forwarding class behavior, in terms of ingress marking interpretation and egress marking, can be changed by a Network QoS Policies in Network Mode on page 27. All forwarding class queues support the concept of in-profile and out-of-profile.

Forwarding-Class To Queue-ID Map

There are 8 forwarding classes supported on 7210 SAS M. Each of these FC is mapped to a specific queue. By mapping FC to different queues the differential treatment is imparted to various classes of traffic.

In the7210 SAS M, there are only 8 queues available at the port level. These 8 queues are created by default per port. Users cannot create or delete the queues or the queue ID. Only the queue parameters can be changed. The queue-id is not a configurable entity and queue ID 1 to 8 are, by default, used to identify these 8 queues available on the port. The 8 queues are available both on the access and network ports. Queue parameters for these 8 queues can be configured as part of the access egress QoS policy which is applied on the access ports and network queue policy which is applied on the network ports.

The queue ID 1 to 8 are assigned to each of the 8 queues. Queue-ID 8 is the highest priority and queue-id 1is the lowest priority. FCs are correspondingly mapped to these queue IDs according to their priority. The stystem defined map is as shown in Table 31.

Table 31: Forwarding Class to Queue-ID Map

FC-ID	FC Name	FC Designation	Queue-ID
7	Network control	NC	8
6	High-1	H1	7
5	Expedited	EF	6
4	High-2	H2	5
3	Low-1	L1	4
2	Assured	AF	3
1	Low-2	L2	2
0	Best-Effort	BE	1

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 access egress QoS policy, two default network QoS policy (one each for network qos policy of type ip-interface and of type port) and two default port scheduler policy. Only one ingress QoS policy and one egress QoS policy can be applied to a SAP, IP interface, network port, or access uplink ports.

When you create a new QoS policy, default values are provided for most parameters with the exception of the policy ID, descriptions. Each policy has a scope, default action, a description, and meters for ingress policies and queues for egress policies. The queue is associated with a forwarding class.

QoS policies can be applied to the following service types:

- Epipe — Only SAP ingress policies are supported on an Epipe service access point (SAP).
- VPLS — Only SAP ingress policies are supported on a VPLS SAP.
- VPRN — SAP ingress policies are supported on a VPRN SAP.

QoS policies can be applied to the following entities:

- Access egress policies on access ports
-
- Network QoS policy on access uplinknetwork port (in network mode) or access uplink port (in access uplink mode)
- Network queue policy (egress) on access uplinknetwork port (in network mode) or access uplink port (in access uplink mode).

QoS prioritizes traffic according to the forwarding class and uses congestion management to control access ingress, access egress, and network traffic (network port or access-uplink port) , enqueuing packets according to their priority (color).

QoS Policy Entities for Hybrid port

- Network queue policies are supported for queue configuration of egress queues on hybrid ports. These egress queues are shared by traffic sent out of SAPs and network IP interfaces configured on hybrid port.
- Network qos (type == ip-interface) policies are supported for network IP interfaces on hybrid ports. The behavior is similar to the existing behavior for network IP interfaces on network ports. It supports per IP interface ingress classification and policing, and egress marking (only EXP marking for MPLS traffic).

- Network qos (type == port) policies are supported for hybrid ports. The behavior is similar to existing behavior for network ports. It supports per port ingress classification and policing, and egress marking (Dot1p and/or DSCP marking).
- SAP ingress QoS policies are supported for SAPs configured on Hybrid ports. The behavior is similar to existing behavior for access SAP ingress. It supports per SAP ingress classification and policing.
- For marking traffic sent out of SAPs and IP traffic sent out of IP interfaces configured on hybrid port, user needs to use the network qos policy of type 'port', with an option to mark Dot1p, DSCP, or both.
  NOTE that if DSCP marking or both is specified, then all the traffic, including the traffic sent out of SAPs configured in a L2 services, will be marked with IP DSCP.

Configuration Notes

The following information describes QoS implementation caveats:

- Creating additional QoS policies is optional.
- Default policies are created for service ingress, access service egress, network, network-queue, slope, and port scheduler.
- Associating a service or access uplink or IP interface or network ports with a QoS policy other than the default policy is optional.

Port Level Egress Rate-Limiting

In This Section

This section provides information to configure port level egress-rate using the command line interface.

Topics in this section include:

Overview

Egress port rate limiting allows the device to limit the traffic that egresses through a port to a value less than the available link bandwidth. This feature is supported on the 7210 SAS-Series platforms.

Applications

This feature is useful when connecting the 7210 SAS to an Ethernet-over-SDH (EoSDH) (or microwave) network, where the network allocates predetermined bandwidth to the nodes connecting into it, based on the transport bandwidth requirement. When connecting to such a network it is important that the traffic sent into the SDH node does not exceed the configured values, since the SDH network does not have QoS capabilities and buffers required to prioritize the ingress traffic.

Egress rate attributes include:

- Allows for per port configuration of the maximum egress port rate, using the egress-rate CLI command.
- Ethernet ports configured asaccess, access uplink and networksupport this feature.
- The port scheduler distributes the available maximum egress bandwidth based on the CIR/PIR configuration parameters provisioned for the queues.
- Provides support for a burst parameter to control the amount of burst the egress port can generate.
- When ports are members of a LAG, all the ports use the same value for the egress-rate and the max-burst parameters.
- If frame overhead accounting is enabled, then queue scheduler accounts for the Ethernet frame overhead.

Effect of Port Level Rate-Limiting on Network Queue Functionality

- When an egress-rate sub-rate value is given, the network queue (on network ports or access uplink ports) rates that are specified using percentages will use the egress-rate value instead of the port bandwidth to configure the appropriate queue rates. Configuration of egress port rate to different values will result in a corresponding dynamic adjustment of rates for the queues configured on network ports, or access uplink ports.
- When the egress-rate sub-rate value is set, CBS/MBS of the associated network queues will not change.

Basic Configurations

To apply port level rate-limiting, perform the following:

- The **egress-rate** command is present in the ***A:Dut-1>config>port>ethernet** context.
- The **egress-rate** configures the maximum rate (in kbps) for the port. The value should be between 1 and 1000000 kbps and between 1 and 10000000 kbps for 10G port.
- The **max-burst** command configures a maximum-burst (in kilo-bits) associated with the egress-rate. This is optional parameter and if not defined then, by default, it is set to 64kb for a 1G port and 66kb for a 10G port. User cannot configure max-burst without configuring egress-rate. The value should be between 64 and 16384 or default.
- By default there is no egress-rate command set on port. By default egress-rate for a port is maximum (equal to line-rate).
- On 10G port, if ERL configured is more than 8Gig it is recommended to configure burst value higher than 80kbits to avoid packet drops.

The following displays the egress-rate configuration for a port:

```
*A:Dut-1>config>port# info
----------------------------------------------
        ethernet
            egress-rate 120000 max-burst 234
        exit
        no shutdown
----------------------------------------------
*A:Dut-1>config>port#
```

Modifying Port Level Egress-Rate Command

To modify egress-rate parameters you can simply apply a egress-rate command with new egress-rate and max-burst value.

The following displays the egress-rate configuration for a port:

```
*A:Dut-1>config>port# ethernet egress-rate 10000 max-burst default
*A:Dut-1>config>port# info
----------------------------------------------
        ethernet
            egress-rate 10000
        exit
        no shutdown
----------------------------------------------
*A:Dut-1>config>port#
```

Removing Port Level Egress-Rate Command

To remove egress-rate command from a port, use the **no** option with the **egress-rate** command. The rate for the egress-rate option and max-burst should not be used in this case.

CLI Syntax: `config>port>ethernet# no egress-rate`

The following displays the removal of egress-rate configuration from a port:

```
*A:Dut-1>config>port# no ethernet egress-rate
*A:Dut-1>config>port# info
----------------------------------------------
        ethernet
        exit
        no shutdown
----------------------------------------------
*A:Dut-1>config>port#
```

Default Egress-Rate Values

By default no egress-rate is configured for a port.

Port Level Egress-Rate Command Reference

Command Hierarchies

Configuration Commands

```
config
    — port
        — ethernet
            — egress-rate sub-rate [max-burst size-in-kbits]
            — no egress-rate
```

Show Commands

```
show
    — port [port-id]
```

Configuration Commands

egress-rate

Syntax **egress-rate** *sub-rate* **[max-burst** *size-in-kbits***]**
no egress-rate

Context config>port>ethernet

Description This command configures maximum rate and corresponding burst value for a port. The egress-rate is configured as kbps while max-burst is configured as kilo-bits while max-burst should be between 64 and 16384 or default.

The **no** form of the command removes egress-rate from the port.

Default No egress-rate and max-burst is configured for the port.

Parameters *sub-rate* — Specifies an integer value between 1 and 1000000 kbps and between 1 and 10000000 kbps for 10G port.

max-burst *size-in-kbits* **—** Specifies an integer value, in kilo-bits, between 64 and 16384 or default.

Show Commands

port

Syntax **port** [*port-id*]

Context show

Description This command displays Egress-Rate and Max-Burst value set for port along with other details of the port.

Parameters *port-id* — Displays information about the specific port ID.

Sample Output

```
*A:Dut-1>config>port>ethernet# show port 1/1/23
=============================================================================
Ethernet Interface
=============================================================================
Description        : 10/100/Gig Ethernet SFP
Interface          : 1/1/23                    Oper Speed       : 100 mbps
Link-level         : Ethernet                  Config Speed     : 1 Gbps
Admin State        : up                        Oper Duplex      : full
Oper State         : up                        Config Duplex    : full
Physical Link      : Yes                       MTU              : 9212
IfIndex            : 36405248                  Hold time up     : 0 seconds
Last State Change  : 03/12/2001 03:31:09       Hold time down   : 0 seconds
Last Cleared Time  : N/A

Configured Mode    : network                   Encap Type       : null
Dot1Q Ethertype    : 0x8100                    QinQ Ethertype   : 0x8100
Net. Egr. Queue Pol: default                   Access Egr. Qos *: n/a
Egr. Sched. Pol    : default                   Network Qos Pol  : 1
Auto-negotiate     : true                      MDI/MDX          : MDX
Accounting Policy  : None                      Collect-stats    : Disabled
Egress Rate        : 100000                    Max Burst        : 8000

Down-when-looped   : Disabled                  Keep-alive       : 10
Loop Detected      : False                     Retry            : 120

Configured Address : 00:f7:d6:5e:98:18
Hardware Address   : 00:f7:d6:5e:98:18
Cfg Alarm          :
Alarm Status       :

Transceiver Data

Transceiver Type   : SFP
Model Number       : 3HE00062AAAA01  ALA  IPUIAEHDAA6
TX Laser Wavelength: 0 nm                      Diag Capable     : no
Connector Code     : Unknown                   Vendor OUI       : 00:90:65
```

```
Manufacture date   : 2008/09/11                 Media            : Ethernet
Serial Number      : PEB2WGH
Part Number        : FCMJ-8521-3-A5
Optical Compliance : GIGE-T
Link Length support: 100m for copper

===============================================================================
Traffic Statistics
===============================================================================
                                                   Input                 Output
-------------------------------------------------------------------------------
Octets                                          15028477                   3236
Packets                                            16729                     19
Errors                                                 0                      0
===============================================================================
* indicates that the corresponding row element may have been truncated.

===============================================================================
Port Statistics
===============================================================================
                                                   Input                 Output
-------------------------------------------------------------------------------
Unicast Packets                                    11611                     17
Multicast Packets                                    359                      0
Broadcast Packets                                   4759                      2
Discards                                               0                      0
Unknown Proto Discards                                 0
===============================================================================

===============================================================================
Ethernet-like Medium Statistics
===============================================================================

Alignment Errors :                   0  Sngl Collisions  :                   0
FCS Errors       :                   0  Mult Collisions  :                   0
SQE Test Errors  :                   0  Late Collisions  :                   0
CSE              :                   0  Excess Collisns  :                   0
Too long Frames  :                   0  Int MAC Tx Errs  :                   0
Symbol Errors    :                   0  Int MAC Rx Errs  :                   0
===============================================================================
*A:MTU-T2>config>port>ethernet#
```

Frame Based Accounting

In This Section

This section provides information to configure frame-based accounting using the command line interface.

Topics in this section include:

Overview

This feature when enabled let QoS policies to accounts for the Ethernet frame overhead (for example, it accounts for the IFG (inter-frame gap) and the preamble). Typically, the IFG and preamble constitutes about 12 + 8 = 20 bytes. The overhead for Ethernet ports uses this value.

A configurable CLI command enables accounting of the frame overhead at ingress or egress. This is a system wide parameter and affects the behavior of the ingress meter or egress rate. When disabled, the queue rates and egress-rate do not account for the Ethernet frame overhead. By default frame-based accounting is disabled for bothingress and egress.

Effects of Enabling Ingress Frame Based Accounting on Ingress Meter Functionality

To enable system-wide consistency in configuring QoS queue and meter rate parameters, the meters used on the system ingress might need to account for Ethernet frame overhead. Network ingress and service ingress meters account for Ethernet frame overhead. A configurable CLI command can enable or disable the frame overhead accounting. This is a system-wide parameter affecting the behavior of all the meters in the system.

Effects of Enabling Egress Frame Based Accounting on Network Queue Functionality

If frame overhead consideration is enabled, then queue scheduler accounts for the Ethernet frame overhead. The maximum egress bandwidth accounts for the Ethernet frame overhead (it accounts for the IFG (inter-frame gap) and the preamble). Typically, the IFG and preamble constitutes about 12 + 8 = 20 bytes. The overhead for Ethernet ports uses this value.

A configurable CLI command enables accounting of the frame overhead. This is a system wide parameter and affects the behavior of all egress queues (when frame-based-accounting is enabled on egress port (network ports or access-uplink ports, as applicable), the associated queues also account for frame overhead implicitly). When disabled, the egress-rate command does not account for the Ethernet frame overhead.

Accounting and Statistics

Accounting logs and statistics do not account for frame overhead.

Basic Configurations

To enable frame-based accounting, you must perform the following:

- The **frame-based-accounting** command is in the ***A:Dut-1> config>qos>frame-based-accounting** context.
- The **ingress-enable** command enables frame-based-accounting for ingress metering.
- The **egress-enable** command enables frame-based-accounting for egress queue rates, scheduler and port level egress-rate.

The following displays the frame-based accounting configuration:

```
*A:Dut-1>config>qos>frame-based-accounting# info detail
----------------------------------------------
            no ingress-enable
            no egress-enable
----------------------------------------------
*A:Dut-1>config>qos>frame-based-accounting#
```

Enabling and Disabling Frame-Based Accounting

To enable frame-based-accounting for ingress, you can simply use the **ingress-enable** command and to enable frame-based-accounting on egress use the **egress-enable** command. To disable frame-based-accounting for ingress, execute the **no ingress-enable** command and to disable frame-based-accounting on egress, execute the **no egress-enable** command.

CLI Syntax: `config>qos>frame-based-accounting`

The following output displays the enabling of frame-based-accounting:

```
*A:Dut-1>config>qos>frame-based-accounting# ingress-enable
*A:Dut-1>config>qos>frame-based-accounting# egress-enable
*A:Dut-1>config>qos>frame-based-accounting# info
----------------------------------------------
            ingress-enable
            egress-enable
----------------------------------------------
*A:Dut-1>config>qos>frame-based-accounting#
```

The following output displays the disabling of frame-based-accounting:

```
*A:Dut-1>config>qos>frame-based-accounting# no ingress-enable
*A:Dut-1>config>qos>frame-based-accounting# no egress-enable
*A:Dut-1>config>qos>frame-based-accounting# info detail
----------------------------------------------
            no ingress-enable
            no egress-enable
----------------------------------------------
*A:Dut-1>config>qos>frame-based-accounting#
```

Default Frame-Based-Accounting Values

By default frame-based-accounting is disabled for both ingress and egress.

Frame Based Accounting Command Reference

Command Hierarchies

Configuration Commands

```
config
    — qos
        — frame-based-accounting
            — [no] egress-enable
            — [no] ingress-enable
```

egress-enableingress-enable

Show Commands

```
show
    — qos
        — access-egress [policy-id] [association|detail]
        — network  [policy-id] [detail]
        — network-queue [network-queue-policy-name] [detail]
        — port-scheduler-policy [port-scheduler-policy-name] [association]
        — sap-ingress [policy-id] [association|match-criteria|detail]
```

Configuration Commands

egress-enable

Syntax [**no**] **egress-enable**

Context config>qos>frame-based-accounting

Description This command enables the frame-based-accounting for access-egress, network-queue, port scheduler, SAP or Network Aggregate Rate and port-level egress-rate.

The **no** form of the command disables frame-based-accounting for all egress QoS.

Default disabled

ingress-enable

Syntax [**no**] **ingress-enable**

Context config>qos>frame-based-accounting

Description This command enables the frame-based-accounting for sap-ingress and network QoS.

The **no** form of the command disables frame-based-accounting for sap-ingress and network QoS.

Default disabled

Show Commands

sap-ingress

Syntax **sap-ingress** [*policy-id*] [association|match-criteria|detail]

Context show>qos

Description This command displays accounting status of a sap-ingress policy along with other details of the policy. When frame-based-accounting is enabled accounting is shown as frame-based otherwise packet-based.

Parameters *policy-id* — Displays information about the specific policy ID.

Sample Output

```
A:7210-SAS>config>qos>access-egress#  show qos sap-ingress 1

===============================================================================
QoS Sap Ingress
===============================================================================
-------------------------------------------------------------------------------
Sap Ingress Policy (1)
-------------------------------------------------------------------------------
Policy-id                 : 1                 Scope                : Template
Default FC                : be
Criteria-type             : None              Sub-Criteria-type    : None
Accounting                : packet-based
Classifiers Allowed       : 4                 Meters Allowed       : 2
Classifiers Reqrd (VPLS)  : 2                 Meters Reqrd (VPLS)  : 2
Classifiers Reqrd (EPIPE) : 1                 Meters Reqrd (EPIPE) : 1
Description    : Default SAP ingress QoS policy.

===============================================================================
A:7210-SAS>config>qos>access-egress#
```

network

Syntax **network** [*policy-id*] [**detail**]

Context show>qos

Description This command displays the accounting status of a network qos policy along with other details of the policy. When frame-based-accounting is enabled accounting is shown as frame-based otherwise packet-based.

Parameters *policy-id* — Displays information about the specific policy ID.

Sample Output

```
*A:7210-SAS# show qos network 1

===============================================================================
QoS Network Policy
===============================================================================
-------------------------------------------------------------------------------
Network Policy (1)
-------------------------------------------------------------------------------
Policy-id      : 1
Egr Remark     : False
Forward Class  : be                           Profile      : Out
Scope          : Template                     Policy Type  : port
Accounting     : packet-based
Description    : Default network-port QoS policy.
-------------------------------------------------------------------------------
Meter Mode     CIR Admin CIR Rule   PIR Admin   PIR Rule    CBS Admin MBS Admin
-------------------------------------------------------------------------------
1     TrTcm1_CA   0         closest       max       closest   def       def


-------------------------------------------------------------------------------
FC              UCastM         MCastM
-------------------------------------------------------------------------------
No FC-Map Entries Found.

===============================================================================
*A:7210-SAS>#
```

access-egress

Syntax **access-egress** [*policy-id*] [**association|detail**]

Context show>qos

Description This command displays accounting status of an access-egress policy along with other details of the policy. When frame-based-accounting is enabled accounting is shown as frame-based otherwise packet-based.

Parameters *policy-id* — Displays information about the specific policy ID.

association — Displays the policy associations.

detail — Displays the policy information in detail.

Sample Output

```
*A:Dut-1# show qos access-egress 1
===============================================================================
QoS Access Egress
===============================================================================
-------------------------------------------------------------------------------
Policy-id      : 1                           Scope        : Template
Remark         : False
Accounting     : frame-based
Description    : Default Access egress QoS policy.
===============================================================================
*A:Dut-1#
```

network-queue

Syntax **network-queue** [*network-queue-policy-name*] [**detail**]

Context show>qos

Description This command displays accounting status of a network-queue policy along with other details of the policy. When frame-based-accounting is enabled accounting is shown as frame-based otherwise packet-based.

Parameters *network-queue-policy-name* — Displays information about the specific Network queue policy.

detail — Displays the detailed policy information.

Sample Output

```
*A:Dut-1# show qos network-queue default
===============================================================================
QoS Network Queue Policy
===============================================================================
-------------------------------------------------------------------------------
Network Queue Policy (default)
-------------------------------------------------------------------------------
Policy         : default
Accounting     : frame-based
Description    : Default network queue QoS policy.
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Port-id : 1/1/6
Port-id : 1/1/7
Port-id : 1/1/8
Port-id : 1/1/9
Port-id : 1/1/10
Port-id : 1/1/11
Port-id : 1/1/12
Port-id : 1/1/13
Port-id : 1/1/14
Port-id : 1/1/15
Port-id : 1/1/16
Port-id : 1/1/17
Port-id : 1/1/18
Port-id : 1/1/20
Port-id : 1/1/21
Port-id : 1/1/22
Port-id : 1/1/23
```

```
Port-id : 1/1/24
===============================================================================
*A:Dut-1#
```

port-scheduler-policy

Syntax **port-scheduler-policy** [*port-scheduler-policy-name*] [**association**]

Context show>qos

Description This command displays accounting status of a port-scheduler policy along with other details of the policy. When frame-based-accounting is enabled accounting is shown as frame-based otherwise packet-based.

Parameters *port-scheduler-policy-name* — Displays information about the specific port scheduler policy.

association — Displays the associations of the port scheduler policy.

Sample Output

```
*A:Dut-1# show qos port-scheduler-policy default
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : default
Description       : Default Port Scheduler policy.
Accounting        : frame-based
Mode              : STRICT
Last changed      : 08/06/2001 18:36:04
Number Of Queues  : 8
```

Network QoS Policies

In This Section

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

Topics in this section include:

Overview

Network QoS Policy in Network Mode

The network QoS policy consists of an ingress and egress component. When 7210 SAS-M is operating in network mode, there are two types of network QoS policies, network QoS policy of type **port** and network QoS policy of type **ip-interfac**e. A **port** network policy is applied to network and hybrid ports, used for classification/remarking of IP traffic using DSCP or Dot1p values. Either DSCP or Dot1p can be used for ingress classification but not both. Both DSCP and Dot1p can be configured at egress for remarking. The **ip-interface** type network policy is applied to IP Interface, used for classification/remarking of MPLS traffic using EXP values. Note that the FC to Dot1p marking values configured on the port, is also used to mark the Dot1p in the VLAN tag, if any, used for MPLS traffic.

The ingress component of the policy defines how EXP, DSCP or Dot1p 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 7210 SAS . From release 4.0, the profile mapping is defined using a new policy mpls-lsp-exp-profile-map. The **mpls-lsp-exp-profile-map** defines the mapping between the LSP EXP bits and the profile (in or out) to be associated with a packet. The mapping on each **ip-interface** or **port** defaults to the mappings defined in the default network QoS policy until an explicit policy is defined for the IP interface or port.It also defines the rate-limiting parameters for the traffic mapped to each forwarding classes. Traffic mapped to each forwarding class can be rate limited using separate meters for each unicast and multipoint traffic (multipoint is used only for IP Interface for MPLS traffic).

The total number of QoS resources, that is ingress classification entries and policers, available for use with IP interfaces is limited. The software allocates these resources to an IP interface on a first come first serve basis. The number of resources used per IP interface limits the total number of IP interfaces configured on the system (the total number of IP interfaces allowed is also subject to a system limit).

The egress component of the network QoS policy defines the LSP EXP, DSCP or Dot1p bits marking values associated with each forwarding class.

By default, network qos policy remarking is always disabled. If the egressing packet originated on an ingress SAP, the egress EXP bit marking based on the forwarding class and the profile state. The default map of FC-EXP marking is as shown in default network qos policy, policy id 2. All non-default network qos policies inherits the FC-EXP map.

By default, all ports configured in network mode use Default network policy "1" and all network port IP interfaces use Default network policy "2". Default network policies "1" and "2" cannot be modified or deleted.

Network **policy-id 2** exists as the default policy that is applied to all IP interface by default. The network **policy-id 2** cannot be modified or deleted. It defines the default LSP EXP-to-FC mapping and default meters for unicast and multipoint meters for the ingress MPLS packets. For the egress, it defines eight forwarding classes which defines LSP EXP values and the packet marking criteria.

Network QoS Policy in Access Uplink Mode

The network QoS policy consists of an ingress and egress component. For 7210 SAS-M and 7210 SAS-T devices operating in access-uplink mode, network policy of 'port' is available for use. The ingress component of the policy defines how Dot1p bits are mapped to internal forwarding class and profile state (DSCP is not available for use). The forwarding class and profile state define the Per Hop Behavior (PHB) or the QoS treatment through the system. The mapping on each access uplink port defaults to the mappings defined in the default network QoS policy until an explicit policy is defined for the access uplink ports. It also defines the rate-limiting parameters for the traffic mapped to each forwarding classes. Traffic mapped to each forwarding class can be rate limited using separate meters for each unicast and multipoint traffic.

The egress component of the network QoS policy defines the Dot1p bits marking values associated with each forwarding class. By default, network qos policy remarking is always disabled. If the egressing packet originated on an ingress SAP, the egress QoS policy also defines the Dot1p bit marking based on the forwarding class and the profile state. The default map of FC-Dot1p marking is as shown in default network qos policy of type 'port', policy-id 1. All non-default network qos policies inherits the FC-Dot1p map.

Network policy-id 1 exists as the default policy and is applied to access uplink ports.The network policy-id 1 cannot be modified or deleted. It defines the default Dot1p-to-FC mapping and Dot1pto-FC mapping and default meters for unicast and multipoint meters for the ingress. For the egress, it defines eight forwarding classes and 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 IP interface 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 devices, refer to CLI Usage chapter in the OS Basic System Configuration Guide.

Normal QoS Operation

The following types of QoS mapping decisions are applicable on a network IP interface when operating in network mode.

- MPLS LSP EXP value mapping to FC (if defined)
- Default QoS mapping
- MPLS LSP EXP mapping to profile

The default QoS mapping always exists on an IP interface and every received packet will be mapped to this default if another explicitly defined matching entry does not exist.

The following types of QoS mapping decisions are applicable on a network port when operating in network mode:

- Ethernet Dot1P and IP DSCP value mapping (if defined) for use with IP packets
- Default QoS mapping

The default QoS mapping always exists on network port and every received packet will be mapped to this default if another explicitly defined matching entry does not exist.

The following types of QoS mapping decisions are applicable on an access-uplink port when operating in access-uplink mode:

- Ethernet Dot1P value mapping (if defined)
- Default QoS mapping

The default QoS mapping always exists on an ingress access uplink port and every received packet will be mapped to this default if another explicitly defined matching entry does not exist.

Network Qos Policy (ip-interface type) Functionality

The following behavior is supported with use of network IP interface qos policies for LDP and RSVP(with FRR/PHP) MPLS LSPs:

- LSPs setup using LDP uses a global mpls-lsp-exp-profile-map policy. By default, the system assigns a default mpls-lsp-exp-profile-map policy. User has an option to change the global policy to use. A new policy mpls-lsp-exp-profile-map policy allows the user to assign different profile value for MPLS EXP bits for MPLS packets received over different IP interface. This is helpful for use with primarily RSVP LSP with FRR 1:1. For LDP LSPs or when using FRR facility it is recommended to use a single mpls-lsp-exp-profile-map policy for all IP interfaces.
- The new policy separate the profile mapping and FC mapping. The FC to use is always picked from the network policy. Using the EXP to FC mapping configured in the network policy. EXP to profile mapping is picked up from the "mpls-lsp-exp-profile" policy associated with the network qos policy.
- Each IP interface can define a unique network policy for it use, each possibly using a different mapping for MPLS LSP EXP bits to forwarding class (FC). It allows for use of more than 32 distinct network policies, provided network classification resources are available for use.
- If user receives traffic on RSVP LSP and LDP LSP with the same value in the EXP bits, the system provides the same QoS treatment. The system always uses the FC and the meter from the network Qos policy for all MPLS traffic received on an IP interface irrespective of whether its LDP or RSVP LSP.

DSCP Marking CPU Generated Traffic

DSCP marking for CPU generated traffic is not configurable by the user. The default values are given in Table 32:

Note: RSVP, TLDP, OSPF and IS-IS protocols are not supported on 7210 SAS-M devices configured in Access uplink mode.

Table 32: DSCP and Dot1p Marking

Protocol	IPv4	DSCP Marking	Dot1P Marking	Default FC	DSCP Values	DOT1P Values
OSPF	Yes	Yes	Yes	NC	48	7
ISIS	Yes	Yes	Yes	NC	-	7
TLDP	Yes	Yes	Yes	NC	48	7
RSVP	Yes	Yes	Yes	NC	48	7
SNMP	Yes	Yes	Yes	H2	34	4
NTP	Yes	Yes	Yes	NC	48	7
TELNET	Yes	Yes	Yes	H2	34	4
FTP	Yes	Yes	Yes	H2	34	4
TFTP	Yes	Yes	Yes	H2	34	4
SYSLOG	Yes	Yes	Yes	H2	34	4
TACACS	Yes	Yes	Yes	H2	34	4
RADIUS	Yes	Yes	Yes	H2	34	4
SSH	Yes	Yes	Yes	H2	34	4
ICMP Req	Yes	Yes	Yes	NC	0	7
ICMP Res	Yes	Yes	Yes	NC	0	7
ICMP Unreach	Yes	Yes	Yes	NC	0	7
SCP	Yes	Yes	Yes	H2	34	4
STP	NA	NA	Yes	NC	-	7
CFM	NA	NA	Yes	NC	-	7
ARP	NA	NA	Yes	NC	-	7

Table 32: DSCP and Dot1p Marking (Continued)

Protocol	IPv4	DSCP Marking	Dot1P Marking	Default FC	DSCP Values	DOT1P Values
Trace route	Yes	Yes	Yes	NC	0	7
TACPLUS	Yes	Yes	Yes	H2	34	4
DNS	Yes	Yes	Yes	H2	34	4
BGP	Yes	Yes	Yes	NC	48	7

Note: DSCP and Dot1P values in the table are applicable when remarking is disabled at port level.

Default DSCP Mapping Table

```
DSCP Name  DSCP Value   DSCP Value DSCP Value   Label
           Decimal      HexadecimalBinary
=============================================================
Default    0            0x00       0b000000     be
nc1        48           0x30       0b110000     h1
nc2        56           0x38       0b111000     nc
ef         46           0x2e       0b101110     ef
af11       10           0x0a       0b001010     assured
af12       12           0x0c       0b001100     assured
af13       14           0x0e       0b001110     assured
af21       18           0x12       0b010010     l1
af22       20           0x14       0b010100     l1
af23       22           0x16       0b010110     l1
af31       26           0x1a       0b011010     l1
af32       28           0x1c       0b011100     l1
af33       30           0x1d       0b011110     l1
af41       34           0x22       0b100010     h2
af42       36           0x24       0b100100     h2
af43       38           0x26       0b100110     h2

default*   0
```

*The default forwarding class mapping is used for all DSCP names/values for which there is no explicit forwarding class mapping.

Basic Configurations

A basic network QoS policy must conform to the following:

- Each network QoS policy must have a unique policy ID.
- Specify the default-action.
- Have a QoS policy scope of template or exclusive.
- Have at least one default unicast forwarding class meter.
- Have at least one multipoint forwarding class meter.

Create a Network QoS Policy

Configuring and applying QoS policies other than the default policy is optional. A default network policy of the type ‘ip-interface’ is applied .

To create an network QoS policy of type ip-interface when operating in network mode, define the following:

- A network policy ID value. The system will not dynamically assign a value.
- Set the network-policy-type parameter to be ip-interface.
- Include a description. The description provides a brief overview of policy features.
- You can modify egress LSP EXP marking map. Otherwise, the default values are applied.
  - → Remarking — When enabled, this command remarks ALL packets that egress on the specified network port. The remarking is based on the forwarding class to LSP EXP bit mapping defined under the egress node of the network QoS policy.
  - → Forwarding class criteria — The forwarding class name represents an egress queue. Specify forwarding class criteria to define the marking criteria of packets flowing through it.
  - → LSP EXP — The EXP value is used for all MPLS labeled packets requiring marking that egress on this forwarding class queue that are *in* or *out* of profile.
- Ingress criteria — Specifies the EXP to forwarding class mapping for all packets.
  - → Default action — Defines the default action to be taken for packets that have an undefined EXP bits set. The default-action specifies the forwarding class to which such packets are assigned.
  - → LSP EXP — Creates a mapping between the EXP bits of the network ingress traffic and the forwarding class. Ingress traffic that matches the specified EXP bits will be assigned to the corresponding forwarding class.

User has an option to specify the mapping of the LSP EXP bits to a profile (in/out). Ingress traffic that matches the specified EXP bits will be assigned the corresponding profile.

To create an network QoS policy of type **port** when oprating in network mode, define the following:

- A network policy ID value. The system will not dynamically assign a value.
- Set the network-policy-type parameter to 'port'
- Include a description. The description provides a brief overview of policy features.
- You can modify egress DSCP and Dot1p marking map. Otherwise, the default values are applied.
  - → Remarking — When enabled, this command remarks ALL packets that egress on the specified network port. The remarking is based on the forwarding class to DSCP bit mapping defined under the egress node of the network QoS policy for all IP traffic and forwarding class to Dot1p bit mapping for all IP and MPLS traffic.
  - → Forwarding class criteria — The forwarding class name represents an egress queue. Specify forwarding class criteria to definethe marking criteria of packets flowing through it.
  - → DSCP and Dot1p — The DSCP and Dot1p value is used for all packets requiring marking that egress on this forwarding class queue that are in or out of profile.
- Ingress criteria — Specifies either DSCP or Dot1p (but not both) to forwarding class mapping for all packets.
  - → Default action — Defines the default action to be taken for packets that have an undefined DSCP or Dot1p bits set. The default-action specifies the forwarding class to which such packets are assigned.
  - → DSCP or Dot1p — Creates a mapping between the DSCP or Dot1p bits of the network ingress traffic and the forwarding class. Ingress traffic that matches the specified DSCP or Dot1p bits will be assigned to the corresponding forwarding class.

To create an network QoS policy of type port when operating in access-uplink mode, define the following:

- A network policy ID value. The system will not dynamically assign a value.
- Set the network-policy-type parameter to 'port'
- Include a description. The description provides a brief overview of policy features.
- You can modify egress Dot1p marking map. Otherwise, the default values are applied.
  - → Remarking — When enabled, this command remarks ALL packets that egress on the specified network port. The remarking is based on the forwarding class to Dot1p bit mapping.

  - → Forwarding class criteria — The forwarding class name represents an egress queue. Specify forwarding class criteria to define the marking criteria of packets flowing through it.
  - → Dot1p — The Dot1p value is used for all packets requiring marking that egress on this forwarding class queue that are in or out of profile.
- Ingress criteria — Specifies Dot1p to forwarding class mapping for all packets.
  - → Default action — Defines the default action to be taken for packets that have an undefined DSCP or Dot1p bits set. The default-action specifies the forwarding class to which such packets are assigned.
  - → Dot1p — Creates a mapping between the Dot1p bits of the access uplink port ingress traffic and the forwarding class. Ingress traffic that matches the specified Dot1p bits will be assigned to the corresponding forwarding class.

Use the following CLI syntax to create a network QoS policy (for 7210 SAS-M in network mode):

CLI Syntax:
```
config>qos#
 network policy-id [network-policy-type network-policy-type]
    description description-string
    scope {exclusive|template}
    egress
       remarking
       fc {be|l2|af|l1|h2|ef|h1|nc}
          lsp-exp-in-profile mpls-exp-value
          lsp-exp-out-profile mpls-exp-value
       default-action fc {fc-name} profile {in|out}
       lsp-exp lsp-exp-value fc fc-name profile {in | out}
       fc {fc-name}
          meter {meter-id}
          multicast-meter {id}
       meter meter-id [multipoint]
          adaptation-rule cir {closest | max | min} pir {clos-
             est | max | min}
          cbs {size-in-kbits}
          mbs {size-in-kbits}
          mode {trtcm | srtcm}
          rate cir cir-rate-in-kbps [pir pir-rate-in-kbps]
          mpls-lsp-exp-profile policy-id
```

Use the following CLI syntax to create a network QoS policy for 7210 SAS-M and 7210 SAS-T in access uplink mode:

CLI Syntax:
```
config>qos#
 network policy-id [network-policy-type network-policy-type]
    description description-string
```

```
scope {exclusive|template}
egress
   remarking
   fc {be|l2|af|l1|h2|ef|h1|nc}
      dot1p-in-profile dot1p-priority
      dot1p-out-profile dot1p-priority
   default-action fc {fc-name} profile {in|out}
   dot1p dot1p-priority fc {fc-name} profile {in|out}
   fc {fc-name}
      meter {meter-id}
      multicast-meter {id}
   meter meter-id [multipoint]
      adaptation-rule cir {closest | max | min} pir {clos-
         est | max | min}
      cbs {size-in-kbits}
      mbs {size-in-kbits}
      mode {trtcm | srtcm}
   rate cir cir-rate-in-kbps [pir pir-rate-in-kbps]
```

```
config>qos>network# info
----------------------------------------------
            description "Network Qos policy 200"
            ingress
                meter 1 create
                exit
                meter 9 multipoint create
                exit
            exit
            egress
                remarking
            exit
----------------------------------------------
A:ALA-10config>qos>network#
```

CLI Syntax:

```
config>router
interface interface-name
   qos network-policy-id
```

CLI Syntax:

```
network port (in network mode)
 config> port
    ethernet
       network
          qos network-policy-id
```

CLI Syntax:

```
access uplink port (in access-uplink mode)
 config>port
    ethernet
       access
          uplink
          qos network-policy-id
```

The following output displays the configuration for router interface ALA-1-2 with network policy 600 applied to the network IP interface.

```
A:ALA-7>config>router# info
#------------------------------------------
echo "IP Configuration"
#------------------------------------------
...
     interface "ALA-1-2"
        address 10.10.4.3/24
        qos 600
     exit
...
----------------------------------------------
A:ALA-7>config>router#
```

Default Network Policy Values

The default network policy for IP interfaces is identified as policy-id **2**. Default policies cannot be modified or deleted. The following displays default network policy parameters:

Table 33: Network Policy Defaults for Policy Type IP Interface

Field	Default
description	Default network QoS policy.
scope	template
ingress	
default-action	fc be profile out (default action profile out is applicable only for port policies and not for ip-interface policies)
mpls-lsp-exp-profile	1
egress	
remarking	no
fc af:	
lsp-exp-in-profile	3
lsp-exp-out-profile	2
fc be:	
lsp-exp-in-profile	0
lsp-exp-out-profile	0
fc ef:	
lsp-exp-in-profile	5
lsp-exp-out-profile	5
fc h1:	
lsp-exp-in-profile	6
lsp-exp-out-profile	6
fc h2:	
lsp-exp-in-profile	4

Table 33: Network Policy Defaults for Policy Type IP Interface (Continued)

Field	Default
lsp-exp-out-profile	4
fc l1:	
lsp-exp-in-profile	3
lsp-exp-out-profile	2
fc l2:	
lsp-exp-in-profile	1
lsp-exp-out-profile	1
fc nc:	
lsp-exp-in-profile	7
lsp-exp-out-profile	7

Table 34: Default Network QoS Policy of Type IP Interface, LSP EXP to FC Mapping on Ingress

LSP EXP Value	7210 FC Ingress	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

The default network policy for port is identified as policy-id 1. Default policies cannot be modified or deleted. The following output displays the parameters for default network policy of type **port** when in network mode of operation:

```
*A:ALA>config>qos>network# info detail
----------------------------------------------
```

```
description "Default network-port QoS policy."
scope template
ingress
    default-action fc be profile out
    meter 1 create
        mode trtcm
        adaptation-rule cir closest pir closest
        rate cir 0 pir max
        mbs default
        cbs default
    exit
    dscp be fc be profile out
    dscp ef fc ef profile in
    dscp cs1 fc l2 profile in
    dscp nc1 fc h1 profile in
    dscp nc2 fc nc profile in
    dscp af11 fc af profile in
    dscp af12 fc af profile out
    dscp af41 fc h2 profile in
exit
egress
    no remarking
    fc af
        dscp-in-profile af11
        dscp-out-profile af12
        dot1p-in-profile 3
        dot1p-out-profile 2
    exit
    fc be
        dscp-in-profile be
        dscp-out-profile be
        dot1p-in-profile 0
        dot1p-out-profile 0
    exit
    fc ef
        dscp-in-profile ef
        dscp-out-profile ef
        dot1p-in-profile 5
        dot1p-out-profile 5
    exit
    fc h1
        dscp-in-profile nc1
        dscp-out-profile nc1
        dot1p-in-profile 6
        dot1p-out-profile 6
    exit
    fc h2
        dscp-in-profile af41
        dscp-out-profile af41
        dot1p-in-profile 4
        dot1p-out-profile 4
    exit
    fc l1
        dscp-in-profile af21
        dscp-out-profile af22
        dot1p-in-profile 3
        dot1p-out-profile 2
    exit
    fc l2
```

```
                    dscp-in-profile cs1
                    dscp-out-profile cs1
                    dot1p-in-profile 1
                    dot1p-out-profile 1
                exit
                fc nc
                    dscp-in-profile nc2
                    dscp-out-profile nc2
                    dot1p-in-profile 7
                    dot1p-out-profile 7
                exit
            exit
----------------------------------------------
*A:ALA>config>qos>network#

A:SAS-M>config>qos>network# info
----------------------------------------------
            description "Default network QoS policy."
            ingress
                meter 1 create
                exit
                meter 9 multipoint create
                exit
                lsp-exp 0 fc be
                lsp-exp 1 fc l2
                lsp-exp 2 fc af
                lsp-exp 3 fc af
                lsp-exp 4 fc h2
                lsp-exp 5 fc ef
                lsp-exp 6 fc h1
                lsp-exp 7 fc nc
            exit
            egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
----------------------------------------------
*A:SAS-M>config>qos>network#
```

Service Management Tasks

Deleting QoS Policies

A network policy is associated by default with IP interfaces and network ports for 7210 SAS-M operating in network mode. A network policy is associated by default with access uplink ports for 7210 SAS-M and 7210 SAS-T in access uplink mode.

You can replace the default policy with a non-default policy, but you cannot remove default policies from the configuration. When you remove a non-default policy, the policy association reverts to the appropriate default network policy.

Remove a Policy from the QoS Configuration

To delete a network policy, enter the following commands:

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

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.

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

The following output displays the copied policies:

```
A:ALA-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
...
---------------------------------------------
A:ALA-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 network ports or IP interfaces or access uplink ports 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. The number of meters (TP) used are: 5 (Meters 1,2,3,9,12).

Resource Allocation for Network QoS policy

This section describes the allocation of QoS resources for network QoS policy (for type=ip interface only).

When an IP interface is created, a default network QoS policy is applied. For the default policy, two meters and two classification entries in hardware are allocated.

The resources are allocated to a network policy, only when a port is configured for the IP interface.

For every FC in use, the system allocates two classification entries in hardware. If multiple matchcriteria entries map to the same FC, then each of these are allocated two classification entries in hardware. For example, if there are two match-criteria entries that map to FC ‘af’, then a total of four classification entries are allocated in hardware and if there are four match-criteria entries that map to FC ‘af’, then a total of 8 classification entries are allocated in hardware.

For every meter or policer in use, the system allocates one meter in hardware. A meter or policer is considered to be in use when it is associated with an FC in use.

The number of IP interfaces allowed is limited to number of resources available in hardware, subject to system limit (a maximum of 64 IP interfaces are allowed). The system reserves a total of 512 classification entries and 256 meters in hardware for use by network policy associated with an IP interface.

For computing the number of QoS resources used by an IP interface:

- Determine number of match-criteria entries used to identify the FC.
- Determine number of FCs to use.

Only the FCs used by the match-criteria classification entries are to be considered for the 'number of FCs'. Therefore are referred to as ‘FC in use’.

Use the following rules to compute the number of classification entries per FC in use:

If a FC is in use and is created without explicit meters, use default meter#1 for unicast traffic and default meter #9 for all other traffic types (that is, broadcast, multicast and unknown-unicast). This requires two classification entries in hardware.

If a FC is in use and is created with an explicit unicast meter, use that meter for unicast traffic and use default meter #9 for all other traffic types. This requires two classification entries in hardware.

If a FC is in use and is created with an explicit unicast meter and explicit multicast meter, use the unicast meter for unicast traffic and multicast meter for all other kinds of traffic. This requires two classification entries in hardware.

Given the number of match criteria and the number of FCs used, use the equation given below to arrive at total number of classification entries per policy (for example TC):

$TC= \Sigma\ 2 * E(i)$

$i=nc,h1,ef,h2,l1,af,l2,be$

Where,

E(i) is the number of match- criteria entries that classify packets to FCi. For 7210 platforms, the maximum number of classification entries per policy can be 64 (including default).

2 is the number of classification entries that are required by FCi.

Note: In any case, only 2 classification entries are used per FC in a network policy, as only two traffic-types are supported.

Determine number of policers or meters to use (for example TP). A maximum of 12 meters per network policy is available.

Only those meters that are associated with FCs need to be considered for number of meters. Note, that only FCs in use are considered.

Network QoS Policies Resource Usage Examples

NOTE: In the examples below the profile configuration is not shown. In practice, user needs to configure the mpls-lsp-exp-profile policy and associate it with the network policy. Association of a profile policy with the network qos policy does not change the resource calculation methodology show below.

Example 1

```
network 1 network-policy-type ip-interface create
     description “network-policy-1”
            ingress
                default-action fc be
                meter 1 create
                exit
                meter 9 multipoint create
                exit
            exit
     egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
```

The number of classification entries (TC) used is calculated, as follows:

(2 * 0)nc + (2 * 0)h1 + (2 * 0)ef + (2 * 0)h2 + (2 * 0)l1 + (2 * 0)af + (2 * 0)l2 + (2 * 1)be = 2

The number of meters (TP) used are: 2 (meter 1 and 9).

Example 2

```
network 2 network-policy-type ip-interface create
     description “network-policy-2”

            ingress
```

```
                default-action fc be
                meter 1 create
                exit
                meter 2 create
                exit
                meter 9 multipoint create
                exit
                meter 12 multipoint create
                exit
                fc "af" create
                    meter 2
                    multicast-meter 12
                exit
                lsp-exp 2 fc af
            exit
            egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
exit
```

The number of classification entries (TC) used is calculated, as follows:

(2 * 0)nc + (2 * 0)h1 + (2 * 0)ef + (2 * 0)h2 + (2 * 0)l1 + (2 * 1)af + (2 * 0)l2 + (2 * 1)be = 4

The number of meters (TP) user are: 4 (Meters 1,2,9,12)

Example 3

```
network 3 network-policy-type ip-interface create
     description “network-policy-3”
            ingress
                default-action fc be
                meter 1 create
                exit
                meter 2 create
                exit
                meter 9 multipoint create
                exit
                meter 12 multipoint create
                exit
                fc "af" create
                    meter 2
                    multicast-meter 12
                exit
                fc "be" create
                    meter 2
                    multicast-meter 12
                exit
                lsp-exp 2 fc af
            exit
            egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
exit
```

The number of classification entries (TC) used are calculated, as follows:

(2 * 0)nc + (2 * 0)h1 + (2 * 0)ef + (2 * 0)h2 + (2 * 0)l1 + (2 * 1)af + (2 * 0)l2 + (2 * 1)be = 4

The number of meters (TP) user are: 2 (Meters 2,12).

Example 4

```
network 4 network-policy-type ip-interface create
     description “network-policy-4”
            ingress
                default-action fc be
                meter 1 create
                exit
                meter 9 multipoint create
                exit
                lsp-exp 1 fc l2
                lsp-exp 2 fc af
                lsp-exp 3 fc af
                lsp-exp 4 fc h2
                lsp-exp 5 fc ef
                lsp-exp 6 fc h1
                lsp-exp 7 fc nc
            exit
            egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
exit
```

The number of Filter-Entries (TC) used is calculated, as follows:

(2 * 1)nc + (2 * 1)h1 + (2 * 1)ef + (2 * 1)h2 + (2 * 0)l1 + (2 * 2)af + (2 * 1)l2 + (2 * 1)be = 16

The number of meters (TP) used are: 2 (Meters 1,9).

Example 5

```
network 5 network-policy-type ip-interface create
     description “network-policy-5”
            ingress
                default-action fc be
                meter 1 create
                exit
                meter 2 create
                exit
                meter 9 multipoint create
                exit
                meter 12 multipoint create
                exit
                fc "af" create
                exit
                fc "be" create
                exit
                fc "ef" create
                exit
                fc "h1" create
                exit
                fc "h2" create
                exit
                fc "l2" create
                exit
                fc "nc" create
                exit
                lsp-exp 1 fc l2
                lsp-exp 2 fc af
                lsp-exp 3 fc af
                lsp-exp 4 fc h2
                lsp-exp 5 fc ef
                lsp-exp 6 fc h1
                lsp-exp 7 fc nc
            exit
            egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
```

The number of classification entries (TC) used is calculated, as follows:

(2 * 1)nc + (2 * 1)h1 + (2 * 1)ef + (2 * 1)h2 + (2 * 0)l1 + (2 * 2)af + (2 * 1)l2 + (2 * 1)be = 16

The number of meters (TP) used are: 2 (Meters 1,9 – Note that meters 2 and 12 are not accounted for, since its not associated with any FC).

Example 6

```
network 6 network-policy-type ip-interface create
     description “network-policy-6”

            ingress
                default-action fc be
                meter 1 create
                exit
                meter 2 create
                exit
                meter 3 create
                exit
                meter 9 multipoint create
                exit
                meter 12 multipoint create
                exit
                fc "af" create
                    meter 2
                    multicast-meter 12
                exit
                fc "be" create
                exit
                fc "ef" create
                exit
                fc "h1" create
                    meter 3
                exit
                fc "h2" create
                exit
                fc "l2" create
                exit
                fc "nc" create
                    meter 3
                exit
                lsp-exp 1 fc l2
                lsp-exp 2 fc af
                lsp-exp 3 fc af
                lsp-exp 4 fc h2
                lsp-exp 5 fc ef
                lsp-exp 6 fc h1
                lsp-exp 7 fc nc
            exit
            egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
exit
```

The number of classification entries (TC) used is calculated, as follows:

(2 * 1)nc + (2 * 1)h1 + (2 * 1)ef + (2 * 1)h2 + (2 * 0)l1 + (2 * 2)af + (2 * 1)l2 + (2 * 1)be = 16

The number of meters (TP) used are: 5 (Meters 1,2,3,9,12).

Example 7

```
network 2 network-policy-type ip-interface create
            description "Default network QoS policy."
            scope template
            ingress
                default-action fc be
                meter 1 create
                    mode trtcm
                    adaptation-rule cir closest pir closest
                    rate cir 0 pir max
                    mbs default
                    cbs default
                exit
                meter 9 multipoint create
                    mode trtcm
                    adaptation-rule cir closest pir closest
                    rate cir 0 pir max
                    mbs default
                    cbs default
                exit
                lsp-exp 0 fc be
                lsp-exp 1 fc l2
                lsp-exp 2 fc af
                lsp-exp 3 fc af
                lsp-exp 4 fc h2
                lsp-exp 5 fc ef
                lsp-exp 6 fc h1
                lsp-exp 7 fc nc
            exit
            egress
                no remarking
                fc af
                    lsp-exp-in-profile 3
                    lsp-exp-out-profile 2
                exit
                fc be
                    lsp-exp-in-profile 0
                    lsp-exp-out-profile 0
                exit
                fc ef
                    lsp-exp-in-profile 5
                    lsp-exp-out-profile 5
                exit
                fc h1
                    lsp-exp-in-profile 6
                    lsp-exp-out-profile 6
                exit
                fc h2
                    lsp-exp-in-profile 4
                    lsp-exp-out-profile 4
                exit
                fc l1
                    lsp-exp-in-profile 3
                    lsp-exp-out-profile 2
                exit
                fc l2
                    lsp-exp-in-profile 1
                    lsp-exp-out-profile 1
                exit
                fc nc
                    lsp-exp-in-profile 7
                    lsp-exp-out-profile 7
                exit
            exit
exit
```

The number of classification entries (TC) used is: 2.

The number of meters (TP) used is: 2.

Example 8

```
network 8 network-policy-type ip-interface create
     description “network-policy-8”
            ingress
                default-action fc nc
                meter 1 create
                exit
                meter 2 create
                exit
                meter 3 create
                exit
                meter 4 create
                exit
                meter 5 create
                exit
                meter 7 multipoint create
                exit
                meter 8 multipoint create
                exit
                meter 9 multipoint create
                exit
                meter 12 multipoint create
                exit
                fc "af" create
                    meter 2
                    multicast-meter 12
                exit
                fc "ef" create
                    meter 4
                    multicast-meter 8
                exit
                fc "h2" create
                exit
                fc "l2" create
                    meter 3
                    multicast-meter 7
                exit
                fc "nc" create
                    meter 4
                    multicast-meter 8
                exit
                lsp-exp 1 fc l2
                lsp-exp 3 fc af
                lsp-exp 5 fc ef
                lsp-exp 7 fc nc
            exit
            egress
                fc af
                exit
                fc be
                exit
                fc ef
                exit
                fc h1
                exit
                fc h2
                exit
                fc l1
                exit
                fc l2
                exit
                fc nc
                exit
            exit
exit
```

The number of classification entries (TC) used is calculated, as follows:

> (2 * 2)nc + (2 * 0)h1 + (2 * 1)ef + (2 * 0)h2 + (2 * 0)l1 + (2 * 1)af + (2 * 1)l2 + (0 * 0)be = 10

The numbers of meters (TP) used is: 6 (Meters 2, 3, 4, 7, 8, 12).

Network QoS Policy Command Reference

Command Hierarchies

- Configuration Commands (for network mode operation) on page 139
- Operational Commands (for network mode or access-uplink mode of operation) on page 141
- Show Commands (for network mode or access-uplink mode of operation) on page 142

Configuration Commands (for network mode operation)

```
config
    — qos
        — [no] mpls-lsp-exp-profile-map policy-id [create]
            — description description-string
            — no description
            — lsp-exp lsp-exp-value profile {in|out}
            — no lsp-exp
        — [no] use-global-mpls-lsp-exp-profile policy-id
```

```
config
    — qos
        — [no] network network-policy-id [create] [network-policy-type { ip-interface |  port} ]
            — description description-string
            — no description
            — scope {exclusive | template}
            — no scope
            — egress
                — [no] fc fc-name
                    — no dot1p-in-profile dot1p-priority
                    — no dot1p-in-profile
                    — no 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
                — [no] remark policy-id
                — remarking {use-dot1p | use-dscp | all }
                — no remarking
            — ingress
                — default-action fc fc-name profile {in | out}
```

- — **dot1p** *dot1p-priority* **fc** *fc-name* **profile** {**in** | **out**}
- — **no dot1p**
- — [**no**] **fc** *fc-name* [**create**]
  - — **meter** *meter-id*
  - — **no meter**
  - — **multicast-meter** *meter-id*
  - — **no multicast-meter**
- — **dscp** *dscp-name* **fc** *fc-name* **profile** {**in** | **out**}
- — **no dscp** *dscp-name*
- — **lsp-exp** *lsp-exp-value* **fc** *fc-name*
- — **no lsp-exp**
- — **meter** *meter-id* [**multipoint**] [**create**]
- — **no meter** *meter-id*
  - — **adaptation-rule** [**cir** *adaptation-rule*] [**pir** *adaptation-rule*]
  - — **no adaptation-rule**
  - — **cbs** *size-in-kbits*
  - — **no cbs**
  - — **mbs** *size-in-kbits*
  - — **no mbs**
  - — **mode** *mode*
  - — **no mode**
  - — **rate** *cir-rate-in-kbps* [**pir** *pir-rate-in-kbps*]
  - — **no rate**
- — **[no] mpls-lsp-exp-profile** *policy-id*

Configuration Commands in Access-uplink Mode

```
config
    — qos
        — [no] network network-policy-id [network-policy-type] {ip-interface|port} (port supported only in
           7210 SAS-M in access-uplink mode) (For 7210 SAS-T, by default this command is of type port)]
            — description description-string
            — no description
            — no scope {exclusive | template}
            — egress
                — [no] fc fc-name
                — dot1p-in-profile
                — no dot1p-in-profile
                — dot1p-out-profile
                — no dot1p-out-profile
                — [no] remarking
            — ingress
                — default-action fc fc-name profile {in | out}
                — dot1p dot1p-priority fc fc-name profile {in | out}
                — no dot1p dot1p-priority
                — [no] fc fc-name [create]
                    — meter meter-id
                    — no meter
                    — multicast-meter meter-id
                    — no multicast-meter
                — meter meter-id [multipoint] [create]
                — no meter meter-id
                    — adaptation-rule [cir adaptation-rule] [pir adaptation-rule]
                    — no adaptation-rule
                    — cbs size-in-kbits
                    — no cbs
                    — mbs size-in-kbits
                    — no mbs
                    — mode {trtcm1 | trtcml2 | srtcm}
                    — no mode
                    — rate cir-rate-in-kbps [pir pir-rate-in-kbps]
                    — no rate
```

Operational Commands (for network mode or access-uplink mode of operation)

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

Show Commands (for network mode or access-uplink mode of operation)

```
show
     — qos
             — network policy-id [detail]
             — mpls-lsp-exp-profile [policy-id] [detail]
```

Configuration Commands

Generic Commands

description

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

Context config>qos>network *policy-id*
config>qos>mpls-lsp-exp-profile-map

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

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

The **no** form of this command removes any description string from the context.

Default No description is associated with the configuration context.

Parameters *description-string* — 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.

Operational Commands

copy

Syntax **copy network** *src-pol dst-pol* [**overwrite**]

Context config>qos

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

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.

Parameters **network** *src-pol dst-pol* — 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.

Values 1 — 65535

overwrite — Specifies to replace the existing destination policy. 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.

```
SR>config>qos# copy network 1 427
MINOR: CLI Destination "427" exists use {overwrite}.
SR>config>qos# copy network 1 427 overwrite
```

scope

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

Context config>qos>network *policy-id*

Description This command configures the network policy scope as exclusive or template.

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 one interface. If a policy with an exclusive scope is assigned to a second interface an error message is generated. If the policy is removed from the exclusive interface, it will become available for assignment to another exclusive interface.
The system default policies cannot be put into the exclusive scope. An error will be generated if scope exclusive is executed in any policies with a policy-id equal to 1.

template — When the scope of a policy is defined as template, the policy can be applied to multiple interfaces on the router.

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.

Network QoS Policy Commands

network

Syntax [**no**] **network** *network-policy-id* [create] [**network-policy-type** { **ip-interface** | **port**}] (for 7210 SAS-M in network mode)

Context config>qos

Description This command creates or edits a QoS network policy. The network policy defines the treatment packets receive as they ingress and egress the network port.

The QoS network policy consists of an ingress and egress component. The ingress component of the policy defines how LSP 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 7210 SAS. 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. It also defines the rate-limiting parameters for the traffic mapped to each forwarding classes. Traffic mapped to each forwarding class can be rate limited using separate meters for each uni-cast and multipoint traffic.

The egress component of the network QoS policy defines forwarding class and profile state to LSP EXP values for traffic to be transmitted into the core network. If the egressing packet originated on an ingress SAP, the parameter is always enabled for the networkport, the egress QoS policy also defines the Dot1p bit marking based on the forwarding class and the profile state.

Network **policy-id 2** exists as the default policy that is applied to all IP interface by default. The network **policy-id 2** cannot be modified or deleted. It defines the default LSP EXP-to-FC mapping and default meters for unicast and multipoint meters for the ingress MPLS packets. For the egress, it defines eight forwarding classes which defines LSP EXP values and the packet marking criteria.

Network policy-id 1 exists as the default policy that is applied to all network ports by default. This default policy cannot be modified or deleted. It defined the default DSCP-to-FC mapping and default unicast meters for ingress IP traffic. For the egress, if defines the forwarding class to Dot1p and DSCP values and the packet marking criteria.

If a new network policy is created (for instance, policy-id 3), only the default action, default meters for unicast and multipoint traffic and egress forwarding class parameters are identical to the default policy. A new network policy does not contain the default LSP EXP-to-FC mapping for network QoS policyof type **ip-interface** or the DSCP-to-FC mapping (for network QoSpolicy of type **port**). The default network policy can be copied (use the copy command) to create a new network policy that includes the default ingress LSP EXP or DSCP to FC mapping (as appropriate). You can modify parameters or use the **no** modifier to remove an object from the configuration.

Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all network ports 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 network policy. A policy cannot be deleted until it is removed from all entities where it is applied. The default network **policy** *policy-id* 1 cannot be deleted.

Default System Default Network Policy 1

Parameters *network-policy-id* — The policy-id uniquely identifies the policy on the 7210 SAS.

Default none

Values 1— 65535

network-policy-type — The type of the policy, either **ip-interface** or **port**. It defines where this network policy can be applied.

ip-interface — Specifies only EXP-based classification rules and marking values. It can only be associated with an IP interface. It can be used only when the device is operating in network mode.

port — Specifies only DSCP and Dot1p classification rules and marking values. It can only be associated with a port and is available for use when the device is operating in network mode.

mpls-lsp-exp-profile-map

Syntax **mpls-lsp-exp-profile-map policy-id [create]**
no mpls-lsp-exp-profile-map

Context config>qos

Description This command allows the user to create a new mpls-lsp-exp-profile-map policy. The policy specifies the profile to assign to the packet based on the MPLS LSP EXP bits value matched in the MPLS packet received on a network IP interface.

The assigned profile is available for use by the meter/policer associated with FC in the network policy attached to this IP interface.

The policy is associated with network policy attached to a network IP interface.

When ‘no ldp-use-local-fc-enable’ is set, system creates the mpls-lsp-exp-profile-map automatically with same ID as the network policy ID. The values that map the lsp-exp bits to a profile value can be modified by the user. The system deletes the policy when the associated network policy is deleted.

When ldp-use-local-fc-enable is set, system does not create the mpls-lsp-exp-profile-map policies by default (except for the default policy “1”). User is allowed to create, delete, modify, copy the policies. User needs to associate these policies with appropriate network policies as per their requirement.

Default 1 (default mpls-lsp-exp-profile-map policy “1”).

Parameters *policy-id* — The policy-id uniquely identifies the policy on the 7210 SAS.

Values 1— 65535

create — The keyword used to create a policy.

lsp-exp

Syntax **lsp-exp** *lsp-exp-value*
no lsp-exp

Context config>qos> mpls-lsp-exp-profile-map

Description This command creates a mapping between the LSP EXP bits of the network ingress traffic and the profile.

Ingress traffic that matches the specified LSP EXP bits will be assigned the corresponding profile.

Multiple commands can be entered to define the association of some or all eight LSP EXP bit values to the profile. For undefined values, packets are assigned the profile value out.

The no form of this command removes the association of the LSP EXP bit value to the profile value. The default profile value ‘out’ then applies to that LSP EXP bit pattern.

Default none

Parameters *lsp-exp-value* — The 3-bit LSP EXP bit value, expressed as a decimal integer.

Values 0 — 7

use-global-mpls-lsp-exp-profile

Syntax **use-global-mpls-lsp-exp-profile** *policy-id*
no use-global-mpls-lsp-exp-profile

Context config>qos

Description This command allows the user to associate the mpls-lsp-exp-profile-map policy for use with LDP LSPs. When color aware metering is in use for the IP interface, the policy specified here provides the profile to assign to the MPLS packets received on any of the network IP interface in use in the system. The MPLS EXP bits in the received packet are matched for assigning the profile.

When ‘no ldp-use-local-fc-enable’ is set, system sets it to the default value. User cannot modify it.

When ldp-use-local-fc-enable is set, on system boot-up sets it to the default value. User can modify it to use the policy of their choice.

For LDP LSP traffic, the system always uses the global mpls-lsp-exp-profile-map policy. For RSVP LSP traffic, system uses the mpls-lsp-exp-profile-map policy associated with the network policy. It is highly recommended to use a single mpls-lsp-exp-profile-map policy for all the network policies when FRR facility is in use for consistent QoS treatment.

The **no** form of the command sets the policy to default policy.

Default Default mpls-lsp-exp-profile-map policy “1” is used.

Parameters *policy-id* — The policy-id uniquely identifies the mpls-lsp-exp-profile-map policy to use.

Values 1 — 65535

mpls-lsp-exp-profile

Syntax **mpls-lsp-exp-profile policy-id [create]**
no mpls-lsp-exp-profile

Context config>qos>network>ingress

Description Specify the mpls-lsp-exp-profile-map policy to use for assigning profile values for packets received on this IP interface.

When ‘no ldp-use-local-fc-enable’ is set, this policy is managed by the system. User is not allowed to modify it. The system assigns the same policy ID as the network policy ID. It is cannot be modified by the user.

When ‘ldp-use-local-fc-enable’ is set, by default the system assigns the default policy ID “1”. User can create new policies and specify the new policy instead of the default policy.

Note: For LDP LSP traffic, the system always uses the global mpls-lsp-exp-profile-map policy. For RSVP LSP traffic, system uses the mpls-lsp-exp-profile-map policy associated with the network policy. It is highly recommended to use a single mpls-lsp-exp-profile-map policy for all the network policies when FRR facility is in use for consistent QoS treatment.

The **no** form of the command assigns the default policy.

Parameters *policy-id* — The policy-id uniquely identifies the policy on the 7210 SAS.

Values 1 — 65535

Network QoS Policy Commands (for 7210 SAS-M and 7210 SAS-T in access uplink mode)

network

Syntax **[no] network** *network-policy-id*

Context config>qos

Description This command creates or edits a QoS network policy. The network policy defines the treatment packets receive as they ingress and egress the access uplink port.

The QoS network policy consists of an ingress and egress component. The ingress component of the policy defines how Dot1p 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 7210 SAS. 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. It also defines the rate-limiting parameters for the traffic mapped to each forwarding classes. Traffic mapped to each forwarding class can be rate limited using separate meters for each uni-cast and multipoint traffic.

The egress component of the network QoS policy defines the queuing parameters associated with each forwarding class. There are eight queues per port on the egress. Each of the forwarding classes is associated with a queue on each access uplink port. This queue gets all the parameters defined within the default network QoS policy 1 until an explicit policy is defined for the network interfaceaccess uplink port. If the egressing packet originated on an ingress SAP, the parameter is always enabled for the access uplink port, the egress QoS policy also defines the Dot1p bit marking based on the forwarding class and the profile state.

The network policy-id 1 cannot be modified or deleted. It defines the default Dot1p-to-FC mapping and

Dot1p-to-FC mapping and default meters for unicast and multipoint meters for the ingress. For the egress, it defines eight forwarding classes which represent individual queues and the packet marking criteria.

If a new network policy is created (for instance, policy-id 2), only the default action, default meters for unicast and multipoint traffic and egress forwarding class parameters are identical to the default policy. A new network policy does not contain the default Dot1p-to-FC mapping for network QoS policy of type port). The default network policy can be copied (use the copy command) to create a new network policy that includes the default ingress Dot1p or DSCP to FC mapping (as appropriate).

You can modify parameters or use the no modifier to remove an object from the configuration.

Any changes made to an existing policy, using any of the sub-commands, will be applied immediately to all access uplink ports 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 network policy. A policy cannot be deleted until it is removed from all entities where it is applied. The default network policy policy-id 1 cannot be deleted.

Default System Default Network Policy 1

Parameters *network-policy-id* — The policy-id uniquely identifies the policy on the 7210 SAS.

Default none

Values 1— 65535

Network Ingress QoS Policy Commands

ingress

Syntax **ingress**

Context config>qos>network *policy-id*

Description This command is used to enter the CLI node that creates or edits policy entries that specify the lsp-exp value to forwarding class mapping for all MPLS packets.

When pre-marked packets ingress on a network port, the QoS treatment through the 7210 SAS-based on the mapping defined under the current node.

default-action

Syntax **default-action fc** *fc-name* [**profile** {**in** | **out**}]

Context config>qos>network>ingress

Description This command defines or edits the default action to be taken for packets that have an undefined LSP EXP (only on 7210 SAS-M network mode) or dot1p bits (for 7210 SAS-M and 7210 SAS-T in access uplink mode) bits set. The **default-action** command specifies the forwarding class to which such packets are assigned.

Multiple default-action commands will overwrite each previous default-action command.

Default default-action fc be profile out

Parameters **fc** *fc-name* — Specify the forwarding class name. All packets with LSP EXP (only on 7210 SAS-M network mode) or dot1p bits (for 7210 SAS-M and 7210 SAS-T in access uplink mode) bits that is not defined will be placed in this forwarding class.

Default None, the fc name must be specified

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, on network ingress, the meter/policer supports color-aware policing/metering. The value of the profile parameter is used to provide the color to the meter. Value of 'in' indicates 'Green' color OR in-profile packet to the meter and value of 'out' indicates 'Yellow' color OR out-of-profile packet to the meter operating in color-aware mode. Based on the configured meter rates, the final profile for the packet is determined. The final color is used for subsequent processing of the packet in the system. On egress, in case of congestion, the in-profile packets are preferentially queued over the out-of-profile packets. The profile can be specified in 3.0 release

Default None

Values in, out

dot1p

Syntax **dot1p** *dot1p-priority* **fc** *fc-name* **profile** {**in** | **out**}
no dot1p

Context config>qos>network>ingress

Description This command explicitly sets the forwarding class or enqueuing priorityand profile of the packet when a packet is marked with a *dot1p-priority* specified. Adding a dot1p rule on the policy forces packets that match the *dot1p-priority* specified to overridebe assigned to the forwarding class and enqueuing priorityand profile of the packet based on the parameters included in the Dot1p rule.

The *dot1p-priority* is derived from the most significant three bits in the IEEE 802.1Q or IEEE 802.1P header. The three dot1p bits define 8 Class-of-Service (CoS) values commonly used to map packets to per-hop Quality-of-Service (QoS) behavior.

The **no** form of this command removes the explicit dot1p classification rule from the policy. Removing the rule on the policy immediately removes the rule on all ingress SAPsports using the policy.

Parameters *dot1p-priority* — 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 *dot1p-value*, the previous forwarding class is completely overridden by the new parameters .

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 — 7

fc *fc-name* — The value given for the *fc-name* parameter 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** *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`

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

Default none, the profile name must be specified.

meter

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

Context config>qos>network>ingress

Description This command enables the context to configure an ingress Network QoS policy meter. The meter command allows the creation of multipoint meters. Only multipoint meters can receive ingress packets that need to be sent to multiple destinations.

Multipoint meters are for traffic bound to multiple destinations. Within non-multipoint services, such as Epipe services, all traffic is considered unicast due to the nature of the service type. Multicast and broadcast-destined traffic in an Epipe service will not be mapped to a multipoint service meter.

The no form of this command removes the meter-id from the Network ingress QoS policy and from any existing Ports using the policy. If any forwarding class forwarding types are mapped to the meter, they revert to their default meters. When a meter is removed, any pending accounting information for each port meter created due to the definition of the meter in the policy is discarded.

Default meter 1 (for unicast traffic)

meter 9 multipoint (for all other traffic, other than unicast traffic)

Parameters *meter-id* — Specifies the meter-id that uniquely identifies the meter within the policy. This is a required parameter each time the meter command is executed.

Values For network policy of type ip-interface: 1 — 12 (except 9, the default multipoint meter)
For network policy of type port: 1 — 8

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

The meter must be created as multipoint. The **multipoint** designator cannot be defined after the meter 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 meter to edit *meter-id* parameters.

Values multipoint or not present

Default Not present (the meter is created as non-multipoint)

meter

Syntax **meter** *meter-id*
no meter

Context config>qos>network>ingress>fc

Description This command overrides the default unicast forwarding type meter mapping for **fc** *fc-name*. The specified meter-id must exist within the policy as a non-multipoint meter before the mapping can be made. Once the forwarding class mapping is executed, all unicast traffic on a port using this policy is forwarded using the meter-id.

The **no** form of this command sets the unicast (point-to-point) meter-id back to the default meter for the forwarding class (meter 1).

Default meter 1

Parameters *meter-id* — Specifies the meter-id. The specified parameter must be an existing, non-multipoint meter defined in the **config>qos>network>ingress** context.

Values 1 — 12

multicast-meter

Syntax **multicast-meter** *meter-id*
no multicast-meter

Context config>qos>network>ingress>fc

Description This command overrides the default multicast forwarding type meter mapping for **fc** *fc-name*. The specified meter-id must exist within the policy as a multipoint meter before the mapping can be made. Once the forwarding class mapping is executed, all multicast traffic on a port using this policy is forwarded using the meter-id.

This command can only be used with a network policy of type **ip-interface**.

The **no** form of the command sets the multicast forwarding type meter-id back to the default meter for the forwarding class.

Default 9

Parameters *meter-id* — Specifies the multicast meter. The specified parameter must be an existing, multipoint meter defined in the **config>qos>network>ingress** context.

Values 1— 12

dscp

Syntax **dscp** *dscp-name* **fc** *fc-name* **profile** {**in** | **out**}
no dscp

Context config>qos>network *policy-id*>ingress

Description This command creates a mapping between the DiffServ Code Point (DSCP) of the network ingress traffic and the forwarding class.

Ingress traffic that matches the specified DSCP will be assigned to the corresponding forwarding class. Multiple commands can be entered to define the association of some or all sixty-four DiffServ code points to the forwarding class. For undefined code points, packets are assigned to the forwarding class specified under the **default-action** command.

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.

Default none

Parameters *dscp-name* — The name of the DiffServ code point to be associated with the forwarding class. DiffServ code point can only be specified by its name and only an existing DiffServ code point can be specified. The software provides names for the well known code points.

The system-defined names available are as follows. The system-defined names must be referenced as all lower case exactly as shown in the first column in Table 35 and Table 36 below.

Additional names to code point value associations can be added using the '**dscp-name** *dscp-name dscp-value*' command.

The actual mapping is being done on the *dscp-value*, not the *dscp-name* that references the *dscp-value*. If a second *dscp-name* that references the same *dscp-value* is mapped within the policy, an error will occur. The second name will not be accepted until the first name is removed.

Table 35: Default DSCP Names to DSCP Value Mapping Table

DSCP Name	DSCP Value Decimal	DSCP Value Hexadecimal	DSCP Value Binary
nc1	48	0x30	0b110000
nc2	56	0x38	0b111000
ef	46	0x2e	0b101110
af41	34	0x22	0b100010
af42	36	0x24	0b100100
af43	38	0x26	0b100110
af31	26	0x1a	0b011010
af32	28	0x1c	0b011100
af33	30	0x1d	0b011110
af21	18	0x12	0b010010
af22	20	0x14	0b010100
af23	22	0x16	0b010110
af11	10	0x0a	0b001010
af12	12	0x0c	0b001100
af13	14	0x0e	0b001110
default	0	0x00	0b000000

Table 36: Default Class Selector Code Points to DSCP Value Mapping Table

DSCP Name	DSCP Value Decimal	DSCP Value Hexadecimal	DSCP Value Binary
cs7	56	0x38	0b111000
cs6	48	0X30	0b110000
cs5	40	0x28	0b101000
cs4	32	0x20	0b100000

Table 36: Default Class Selector Code Points to DSCP Value Mapping Table (Continued)

DSCP Name	DSCP Value Decimal	DSCP Value Hexadecimal	DSCP Value Binary
`cs3`	`24`	`0x18`	`0b011000`
`cs2`	`16`	`0x10`	`0b010000`
`cs1`	`08`	`0x8`	`0b001000`

fc *fc-name* **—** Enter this required parameter to specify the *fc-name* with which the code point will be associated.

Default none, for every DSCP value defined, the forwarding class must be indicated.

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

profile {**in** | **out**} **—** Enter this required parameter to indicate whether the DiffServ code point value is the in-profile or out-of-profile value.

NOTE 1: DSCP values mapping to forwarding classes Expedited (ef), High-1 (h1) and Network-Control (nc) can only be set to in-profile.

NOTE 2: DSCP values mapping to forwarding class ‘be’ can only be set to out-of-profile.

Default None, for every DSCP value defined, the profile must be indicated. If a DSCP value is not mapped, the default-action forwarding class and profile state will be used for that value.

Values in, out

lsp-exp

Syntax **lsp-exp** *lsp-exp-value* **fc** *fc-name*
no lsp-exp *lsp-exp-value*

Context config>qos>network *policy-id*>ingress

Description This command creates 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. Multiple commands can be entered to define the association of some or all eight LSP EXP bit values to the forwarding class. For undefined values, packets are assigned to the forwarding class specified under the **default-action** command.

The **no** form of this command removes the association of the LSP EXP bit value to the forwarding class. The **default-action** then applies to that LSP EXP bit pattern.

Default none

Parameters *lsp-exp-value* — Specify the LSP EXP values to be associated with the forwarding class.

Default None, the lsp-exp command must define a value.

Values 0 to 7 (Decimal representation of three EXP bit field)

fc *fc-name* **—** Enter this required parameter to specify the fc-name that the EXP bit pattern will be associated with.

Default None, the lsp-exp command must define a fc-name.

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

adaptation-rule

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

Context config>qos>network>ingress>meter

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the meter is provisioned in hardware. For the CIR and PIR parameters, individually the system attempts to find the best operational rate depending on the defined constraint.

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

Default **adaptation-rule cir closest pir closest**

Parameters *adaptation-rule* — Specifies the adaptation rule to be used while computing the operational CIR or PIR value.

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

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

max **—** The **max** (maximum) option is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR/CIR will be the next multiple of 8 kbps that is equal to or lesser than the specified rate.

min **—** The **min** (minimum) option is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR/CIR will be the next multiple of 8 kbps that is equal to or higher than the specified rate.

closest **—** The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR/CIR will be the next multiple of 8 kbps (that is closest to the specified rate.

cbs

Syntax **cbs** *size-in-kbits*
no cbs

Context config>qos>network>ingress>meter

Description This command provides a mechanism to override the default reserved tokens for the meter. The committed burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the CBS value then the packets are marked as in-profile by the meter to indicate that the traffic is complying meter configured parameters.

The no form of this command returns the CBS size to the default value.

Default default

Parameters *size-in-kbits* — Specifies the size parameter is an integer expression of the number of kilobits reserved for the meter. For example, if a value of 10KBits is desired, then enter the value 10.

Values 4 — 2146959, default

mbs

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

Context config>qos>network>ingress>meter

Description This command provides the explicit definition of the maximum amount of tokens allowed for a specific meter. The value is given in kilobits and overrides the default value for the context.

In case of trTCM, the maximum burst size parameter specifies the maximum burst size that can be transmitted by the source at the PIR while complying with the PIR. If the transmitted burst is lower than the MBS value then the packets are marked as out-profile by the meter to indicate that the traffic is not complying with CIR, but complying with PIR.

In case of srTCM, the maximum burst size parameter specifies the maximum burst size that can be transmitted by the source while not complying with the CIR. The transmitted burst is lower than the MBS value then the packets are marked as out-profile by the meter to indicate that the traffic is not complying with CIR.

If the packet burst is higher than MBS then packets are marked as red are dropped by the meter.

The **no** form of this command returns the MBS size assigned to the meter to the default value.

Default default

Parameters *size-in-kbits* — This parameter is an integer expression of the maximum number of kilobits of burst allowed for the meter. For example, for a value of 100 Kbits, enter the value 100.

Values 4 — 2146959, default

mode

Syntax **mode** *mode*
no mode

Context config>qos>network>ingress>meter

Description This command defines the mode of the meter. The mode can be configured as Two Rate Three Color Marker (trTCM) or Single Rate Three Color Marker (srTCM). The mode command can be executed at anytime.

The **no** form of the command sets the default mode to be trtcm.

Default trtcm

Parameters **trtcm1 —** Meters the packet stream and marks the packets either green, yellow, or red. A packet is marked red if it exceeds the PIR. Otherwise, it is marked either yellow or green depending on whether it exceeds or does not exceed the CIR. The trTCM1 is useful, for example, for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate.

srtcm — Meters a packet stream and marks its packets either green, yellow, or red. Marking is based on a CIR and two associated burst sizes, a CBS and an Maximum Burst Size (MBS). A packet is marked green if it doesn't exceed the CBS, yellow if it does exceed the CBS, but not the cir and red otherwise. The srTCM is useful, for example, for ingress policing of a service, where only the length, not the peak rate, of the burst determines service eligibility.

rate

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

Context config>qos>network>ingress>meter

Description This command defines the administrative PIR and CIR parameters for the meter.

The rate command can be executed at anytime, altering the PIR and CIR rates for all meters created through the association of the Network QoS policy with the meter-id.

The **no** form of the command returns all meter instances created with this meter-id to the default PIR and CIR parameters (max, 0).

NOTE: The value of rates are represented in 1000 kilobits per second and bursts are represented as 1024 kilobits per second.

Default rate 0 pir max — The max default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The max value is mutually exclusive to the pir-rate value.

Parameters **cir** *cir-rate-in-kbps* — The cir parameter overrides the default administrative CIR used by the meter. When the rate command has not been executed or the cir parameter is not explicitly specified, the default CIR (0) is assumed.

Values 0 — 20000000, max

pir *pir-rate-in-kbps* **—** Defines the administrative PIR rate, in kilobits, for the meter. When this rate command is executed, the PIR setting is optional.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.

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

Values — 20000000, max

Network Egress QoS Policy Commands

egress

Syntax **egress**

Context config>qos>network *policy-id*

Description This command is used to enter the CLI node that creates or edits egress policy entries that specify the forwarding class to marking map to be instantiated when this policy is applied to the network IP interface, network port or access-uplink port.

The forwarding class and profile state mapping to appropriate marking values for all packets are defined in this context.

In network mode of operation, the system supports use of forwarding class mapping to EXP bits for IP interface, forwarding class mapping to DSCP and Dot1p bits for network ports. In access-uplink mode of operation it allows the user to specify the FC mapping to Dot1p bits for access-uplink ports.

All out-of-profile service packets are marked with the corresponding out-of-profile value at network egress. All the in-profile service ingress packets are marked with the corresponding in-profile value based on the forwarding class they belong.

fc

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

Context config>qos>network>egress

Description This command specifies the forwarding class name. The forwarding class name represents an egress queue. The **fc** *fc-name* represents a CLI parent node that contains sub-commands or parameters describing the marking criteria of packets flowing through it. The **fc** command overrides the default parameters for that forwarding class to the values defined in the network default policy. Appropriate default parameters are picked up based on whether the network-policy-type is port or ip-interface.

The **no** form of this command removes the forwarding class LSP EXP/Dot1p/DSCP map associated with this fc, as appropriate. The forwarding class reverts to the defined parameters in the default network policy. If the *fc-name* is removed from the network policy that forwarding class reverts to the factory defaults.

Default Undefined forwarding classes default to the configured parameters in the default network policy policy-id 1.

Parameters *fc-name* — The case-sensitive, system-defined forwarding class name for which policy entries will be created.

Default none

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

Network Egress QoS Policy Forwarding Class Commands

fc

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

Context config>qos>network>ingress
config>qos>network>egress

Description This command creates a class instance of the forwarding class. Once the fc-name is created, classification actions can be applied and it can be used in match classification criteria.

The **no** form of the command removes all the explicit meter mappings for fc-name forwarding types. The meter mappings revert to the default meters for fc-name.

Default Undefined forwarding classes default to the configured parameters in the default **policy** *policy-id* 1.

Parameters *fc-name* — The case-sensitive, system-defined forwarding class name for which policy entries will be created.

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

create — The keyword used to create the forwarding class. The **create** keyword requirement can be enabled/disabled in the **environment>create** context.

dot1p-in-profile

Syntax **dot1p-in-profile** *dot1p-priority*
no dot1p-in-profile

Context config>qos>network>egress>fc *fc-name*

Description This command specifies dot1p in-profile mappings.

The **no** form of the command reverts to the default in-profile *dot1p-priority* setting for policy-id 1.

Parameters *dot1p-priority* — 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 *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 — 7

dot1p-out-profile

Syntax **dot1p-out-profile** *dot1p-priority*
no dot1p-out-profile

Context config>qos>network>egress>fc *fc-name*

Description This command specifies dot1p out-profile mappings.

The **no** form of the command reverts to the default out-profile *dot1p-priority* setting for policy-id 1.

Parameters *dot1p-priority* — 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 *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 — 7

dscp-in-profile

Syntax **dscp-in-profile** *dscp-name*
no dscp-in-profile

Context config>qos>network *policy-id*>egress>fc *fc-name*

Description This command specifies the in-profile DSCP name for the forwarding class. The corresponding DSCP value will be used for all IP packets requiring marking the egress on this forwarding class queue that are in profile.

When multiple DSCP names are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command reverts to the factory default in-profile dscp-name setting for policy-id 1.

Parameters *dscp-name* — System- or user-defined, case-sensitive *dscp-name*.

Default none

Values Any defined system- or user-defined *dscp-name*

dscp-out-profile

Syntax **dscp-out-profile** *dscp-name*
no dscp-out-profile

Context config>qos>network *policy-id*>egress>fc *fc-name*

Description This command specifies the out-of-profile DSCP name for the forwarding class. The corresponding DSCP value will be used for all IP packets requiring marking the egress on this forwarding class queue that are out-of-profile.

When multiple DSCP names are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command reverts to the factory default out-of-profile dscp-name setting for policy-id 1.

Parameters *dscp-name* — System- or user-defined, case-sensitive *dscp-name.*

Default none

Values Any defined system- or user-defined *dscp-name*

lsp-exp-in-profile

Syntax **lsp-exp-in-profile** *lsp-exp-value*
no lsp-exp-in-profile

Context config>qos>network *policy-id*>egress>fc *fc-name*

Description This command specifies the in-profile LSP EXP value for the forwarding class. The EXP value will be used for all LSP labeled packets requiring marking the egress on this forwarding class queue that are in-profile.

When multiple EXP values are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command reverts to the factory default in-profile EXP setting.

Default

Policy-id 2:	Factory setting
Policy-id 3 — 65535:	Policy-id setting

Parameters *lsp-exp-value* — The 3-bit LSP EXP bit value, expressed as a decimal integer.

Default none

Values 0 — 7

lsp-exp-out-profile

Syntax **lsp-exp-out-profile** *lsp-exp-value*
no lsp-exp-out-profile

Context config>qos>network *policy-id*>egress>fc *fc-name*

Description This command specifies the out-of-profile LSP EXP value for the forwarding class. The EXP value will be used for all LSP labeled packets requiring marking the egress on this forwarding class queue that are out-of-profile.

When multiple EXP values are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command reverts to the factory default out-of-profile EXP setting.

Default

Policy-id 2:	Factory setting
Policy-id 3 — 65535:	Policy-id setting

Parameters *mpls-exp-value* — The 3-bit MPLS EXP bit value, expressed as a decimal integer.

Default none

Values 0 — 7

remarking

Syntax [**no**] **remarking**

Context config>qos>network *policy-id*>egress

Description This command remarks network egress traffic. The remarking is based on the forwarding class to LSP EXP/Dot1p/DSCP bit mapping defined under the egress node of the network QoS policy in network mode. In access-uplink mode, the remarking is based on the forwarding class to Dot1p bit mappings defined under the egress node of the network QoS policy.

On network egress in network mode, for MPLS packets, only LSP EXP and Dot1p values can be marked. The LSP EXP mapping is defined in the network policy of type **ip-interface** and the Dot1p mapping can be defined in the network policy of type **port**.

On network egress in network mode, for IP packets, DSCP and Dot1p values can be marked. The Dot1p and DSCP values can be configured in the network policy of type **port**.

Normally, packets that ingress on network ports have, in case of MPLS packets, LSP EXP bit set by an upstream router. The packets are placed in the appropriate forwarding class based on the LSP EXP to forwarding class mapping. The LSP EXP bits of such packets are not altered as the packets egress this router, unless remarking is enabled.

Remarking can be required if this SAS-M is connected to a different DiffServ domain where the EXP forwarding class mapping is different.

Typically, no remarking is necessary when all devices are in the same DiffServ domain. The network QoS policy supports an egress flag that forces remarking of packets that were received on network IP interfaces. This provides the capability of remarking without regard to the ingress state of the IP interface on which a packet was received. The effect of the setting of the egress network remark trusted state on each type of ingress IP interface and trust state is shown in the following table.

Ingress IP Interface Type and Trust State	Egress Network IP Interface Trust Remark Disabled (Default)	Egress Network IP Interface Trust Remark Enabled
Network Non-Trusted	Egress Remarked	Egress Remarked
Network Trusted (Default)	Egress Not Remarked	Egress Remarked

The remark trusted state has no effect on packets received on an ingress IP interface.

The remark trusted state is not applicable for network policies of type **port**.

In access-uplink mode, on access-uplink port egress, only Dot1p values can be marked for QinQ packets. The Dot1p mapping is defined in the network policy of type port.

The **no** form of this command reverts to the default behavior.

Default **no remarking** — Remarking disabled in the Network QoS policy.

Show Commands

network

Syntax **network** [*policy-id*] [**detail**]

Context show>qos

Description This command displays network policy information.

Parameters *policy-id* — Displays information for the specific policy ID.

Default all network policies

Values 1 — 65535

detail — Includes information about ingress and egress EXP bit mappings and network policy interface associations. (for 7210 SAS-M in Network mode)

detail — Includes information about ingress and egress Dot1p bit mappings and network policy interface associations (for 7210 SAS-M and 7210 SAS-T in access uplink mode)

Network QoS Policy Output Fields — The following table describes network QoS Policy output fields.

Table 37: Show QoS Network Output Fields

Label	Description
`Policy-Id`	The ID that uniquely identifies the policy.
`Remark`	`True` — Remarking is enabled for all packets that egress this router where the network policy is applied. The remarking is based on the forwarding class to EXP bit mapping defined under the egress node of the network QoS policy.
`Description`	A text string that helps identify the policy's context in the configuration file.
`Forward Class/ FC Name`	Specifies the forwarding class name.
`Profile`	`Out` — Specifies the EXP marking for the packets which are out-of-profile, egressing on this queue. `In` — Specifies the EXP markings for in-profile packets egressing this queue.

Table 37: Show QoS Network Output Fields (Continued)

Label	Description
Accounting	Packet-based — Specifies that the meters associated with this policy do not account for packet framing overheads (such as Ethernet the Inter Frame Gap (IFG) and the preamble), while accounting for the bandwidth to be used by this flow. Frame-based — Specifies that the meters associated with this policy account for the packet framing overheads (such as for Ethernet the IFG and preamble), while accounting the bandwidth to be used by the flow.
Profile policy	Displays the profile policy ID.
Global Prof	Displays the global profile policy ID for LDP packets.
EXP Bit Mapping:	
Out-of-Profile	Displays the EXP value used for out-of-profile traffic.
In-Profile	Displays the EXP value used for in-profile traffic.
Interface	Displays the interface name.
IP Addr	Displays the interface IP address.
Port-Id	Specifies the physical port identifier that associates the interface.

```
A:qos1# show qos network
=========================================================================
Network Policies
=========================================================================
Policy-Id            Remark LerUseDscp Description
-------------------------------------------------------------------------
1                    False  False      Default network-port QoS policy.
2                    False  False      Default network QoS policy.
=========================================================================
A:qos1#

*A:ALA# show qos network 1 detail
===============================================================================
QoS Network Policy
===============================================================================
Network Policy (1)
-------------------------------------------------------------------------------
Policy-id      : 1                             Remark       : False
Forward Class  : be                            Profile      : Out
Attach Mode    : l2                            Config Mode  : l2+mpls
Scope          : Template                      Policy Type  : port
Accounting     : packet-based
Description    : Default network-port 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
af41                                    h2                              In
-------------------------------------------------------------------------------
Dot1p Bit Map                         Forwarding Class                Profile
-------------------------------------------------------------------------------
No Matching Entries
-------------------------------------------------------------------------------
Meter Mode   CIR Admin   CIR Rule   PIR Admin   PIR Rule    CBS       MBS
-------------------------------------------------------------------------------
1     TrTcm_CA  0         closest       max       closest   32        128
-------------------------------------------------------------------------------
FC                  UCastM         MCastM
-------------------------------------------------------------------------------
No FC-Map Entries Found.
-------------------------------------------------------------------------------
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

FC Value       : 1                            FC Name      : l2
- DSCP Mapping
Out-of-Profile : cs1                          In-Profile   : cs1

- Dot1p 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   : 3

FC Value       : 3                            FC Name      : l1
- DSCP Mapping
Out-of-Profile : af22                         In-Profile   : af21

- Dot1p Mapping
Out-of-Profile : 2                            In-Profile   : 3

FC Value       : 4                            FC Name      : h2
- DSCP Mapping
Out-of-Profile : af41                         In-Profile   : af41

- Dot1p 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

FC Value       : 6                            FC Name      : h1
- DSCP Mapping
Out-of-Profile : nc1                          In-Profile   : nc1

- Dot1p 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
-------------------------------------------------------------------------------
Interface Association
-------------------------------------------------------------------------------
No Interface Association Found.
-------------------------------------------------------------------------------
Port Attachments
-------------------------------------------------------------------------------
Port-id : 1/1/1
Port-id : 1/1/2
Port-id : 1/1/3
Port-id : 1/1/4
Port-id : 1/1/5
Port-id : 1/1/6
Port-id : 1/1/7
Port-id : 1/1/8
Port-id : 1/1/9
Port-id : 1/1/10
Port-id : 1/1/11
Port-id : 1/1/12
Port-id : 1/1/13
Port-id : 1/1/14
Port-id : 1/1/16
Port-id : 1/1/17
Port-id : 1/1/18
Port-id : 1/1/20
Port-id : 1/1/21
Port-id : 1/1/22
Port-id : 1/1/23
Port-id : 1/1/24
===============================================================================
*A:ALA#


*A:ALA# show qos network 2 detail
===============================================================================
QoS Network Policy
===============================================================================
Network Policy (2)
-------------------------------------------------------------------------------
```

```
Policy-id      : 2                            Remark       : False
Forward Class  : be                           Profile      : Out
Attach Mode    : mpls                         Config Mode  : mpls
Scope          : Template                     Policy Type  : IpInterface
Accounting     : packet-based
Profile Policy : 1
Global Prof  : 1
Description    : Default network QoS policy.

-------------------------------------------------------------------------------
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
-------------------------------------------------------------------------------
Meter Mode   CIR Admin   CIR Rule   PIR Admin   PIR Rule    CBS       MBS
-------------------------------------------------------------------------------
1     TrTcm_CA  0         closest       max       closest   32        128
9     TrTcm_CA  0         closest       max       closest   32        128
-------------------------------------------------------------------------------
FC                  UCastM         MCastM
-------------------------------------------------------------------------------
No FC-Map Entries Found.
-------------------------------------------------------------------------------
Egress Forwarding Class Queuing
-------------------------------------------------------------------------------
FC Value       : 0                            FC Name      : be
- LSP EXP Bit Mapping
Out-of-Profile : 0                            In-Profile   : 0

FC Value       : 1                            FC Name      : l2
- LSP EXP Bit Mapping
Out-of-Profile : 1                            In-Profile   : 1

FC Value       : 2                            FC Name      : af
- LSP EXP Bit Mapping
Out-of-Profile : 2                            In-Profile   : 3

FC Value       : 3                            FC Name      : l1
- LSP EXP Bit Mapping
Out-of-Profile : 2                            In-Profile   : 3

FC Value       : 4                            FC Name      : h2
- LSP EXP Bit Mapping
Out-of-Profile : 4                            In-Profile   : 4

FC Value       : 5                            FC Name      : ef
- LSP EXP Bit Mapping
Out-of-Profile : 5                            In-Profile   : 5

FC Value       : 6                            FC Name      : h1
- LSP EXP Bit Mapping
Out-of-Profile : 6                            In-Profile   : 6
```

```
FC Value       : 7                            FC Name      : nc
- LSP EXP Bit Mapping
Out-of-Profile : 7                            In-Profile   : 7
-------------------------------------------------------------------------------
Interface Association
-------------------------------------------------------------------------------
Interface      : system
IP Addr.       : n/a                          Port Id      : system
Interface      : in-band-management
IP Addr.       : 10.135.25.189/24             Port Id      : 1/1/23
-------------------------------------------------------------------------------
Port Attachments
-------------------------------------------------------------------------------
No Matching Entries
===============================================================================
*A:ALA#


For SAS-MX:
*A:qos1# show qos network 1001 detail
===============================================================================
QoS Network Policy
===============================================================================
-------------------------------------------------------------------------------
Network Policy (1001)
-------------------------------------------------------------------------------
Policy-id      : 1001                         Remark       : False
Forward Class  : be                           Profile      : In
Attach Mode    : mpls                         Config Mode  : mpls
Scope          : Template                     Policy Type  : IpInterface
Accounting     : packet-based
Description    : ip-interface-type
-------------------------------------------------------------------------------
LSP EXP Bit Map                         Forwarding Class                Profile
-------------------------------------------------------------------------------
0                                       be                              Out
1                                       l2                              Out
2                                       af                              In
3                                       l1                              Out
4                                       h2                              In
5                                       ef                              Out
6                                       h1                              Out
7                                       nc                              In
-------------------------------------------------------------------------------
Meter Mode   CIR Admin  CIR Rule   PIR Admin   PIR Rule    CBS Admin MBS Admin
             CIR Oper              PIR Oper                CBS Oper  MBS Oper
-------------------------------------------------------------------------------
1     TrTcm_CA  4000      closest       8000      closest   def       def
                4000                    8000                def       500
2     TrTcm_CA  4000      closest       7000      closest   16384     16384
                4000                    7000                16000     16000
3     TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
4     TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
5     TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
6     TrTcm_CA  4000      closest       7000      closest   def       def
```

```
                4000                    7000                def       500
7     TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
8     TrTcm_CA  7000      closest       7000      closest   def       def
                7000                    7000                def       500
9     TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
10    TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
11    TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
12    TrTcm_CA  4000      closest       7000      closest   def       def
                4000                    7000                def       500
-------------------------------------------------------------------------------
FC                  UCastM         MCastM
-------------------------------------------------------------------------------
l2                  2              def
af                  3              def
l1                  4              def
h2                  5              12
ef                  6              11
h1                  7              10
nc                  8              9
-------------------------------------------------------------------------------
Egress Forwarding Class Queuing
-------------------------------------------------------------------------------
FC Value       : 0                            FC Name      : be
- LSP EXP Bit Mapping
Out-of-Profile : 0                            In-Profile   : 0

FC Value       : 1                            FC Name      : l2
- LSP EXP Bit Mapping
Out-of-Profile : 1
...
===============================================================================
*A:qos1#
```

Table 38: Show QoS Network Output Fields

Label	Description
`Policy-Id`	The ID that uniquely identifies the policy.
`Remark`	`True` — Remarking is enabled for all packets that egress this router where the network policy is applied. The remarking is based on the forwarding class to Dot1p bit mapping defined under the egress node of the network QoS policy.
`Description`	A text string that helps identify the policy's context in the configuration file.

`Forward Class/`
`FC Name`
	Specifies the forwarding class name.

Table 38: Show QoS Network Output Fields (Continued)

Label	Description
Profile	Out — Specifies the Dot1p marking for the packets which are out-of-profile, egressing on this queue. In — Specifies the Dot1p markings for in-profile packets egressing this queue.
Accounting	Packet-based — Specifies that the meters associated with this policy do not account for packet framing overheads (such as Ethernet the Inter Frame Gap (IFG) and the preamble), while accounting for the bandwidth to be used by this flow. Frame-based — Specifies that the meters associated with this policy account for the packet framing overheads (such as for Ethernet the IFG and preamble), while accounting the bandwidth to be used by the flow.
Dot1p Bit Mapping:	
Out-of-Profile	Displays the Dot1p value used for out-of-profile traffic.
In-Profile	Displays the Dot1p value used for in-profile traffic.
Port-Id	Specifies the physical port identifier that associates the interface.

```
*A:SAS-M-A0-2>show>qos# network 1 detail

===============================================================================
QoS Network Policy
===============================================================================
-------------------------------------------------------------------------------
Network Policy (1)
-------------------------------------------------------------------------------
Policy-id      : 1
Egr Remark     : False
Forward Class  : be                           Profile      : Out
Scope          : Template                     Policy Type  : port
Accounting     : packet-based
Description    : Default network-port 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
af41                                    h2                              In
```

```
-------------------------------------------------------------------------------
Dot1p 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
-------------------------------------------------------------------------------
Meter Mode     CIR Admin CIR Rule   PIR Admin   PIR Rule    CBS Admin MBS Admin
-------------------------------------------------------------------------------
1     TrTcm1_CA   0         closest       max       closest   def       def


-------------------------------------------------------------------------------
FC              UCastM         MCastM
-------------------------------------------------------------------------------
No FC-Map Entries Found.


-------------------------------------------------------------------------------
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

FC Value       : 1                            FC Name      : l2
- DSCP Mapping
Out-of-Profile : cs1                          In-Profile   : cs1

- Dot1p 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   : 3

FC Value       : 3                            FC Name      : l1
- DSCP Mapping
Out-of-Profile : af22                         In-Profile   : af21

- Dot1p Mapping
Out-of-Profile : 2                            In-Profile   : 3

FC Value       : 4                            FC Name      : h2
- DSCP Mapping
Out-of-Profile : af41                         In-Profile   : af41
```

```
- Dot1p 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

FC Value       : 6                            FC Name      : h1
- DSCP Mapping
Out-of-Profile : nc1                          In-Profile   : nc1

- Dot1p 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


-------------------------------------------------------------------------------
Port Attachments
-------------------------------------------------------------------------------
Port-id : 1/1/3
Port-id : 1/1/4
Port-id : 1/1/5
Port-id : 1/1/6
Port-id : 1/1/7
Port-id : 1/1/8
Port-id : 1/1/9
Port-id : 1/1/10
Port-id : 1/1/11
Port-id : 1/1/12
Port-id : 1/1/13
Port-id : 1/1/14
Port-id : 1/1/15
Port-id : 1/1/16
Port-id : 1/1/17
Port-id : 1/1/18
Port-id : 1/1/19
Port-id : 1/1/20
Port-id : 1/1/21
Port-id : 1/1/22
Port-id : 1/1/23
Port-id : 1/1/24
===============================================================================
*A:SAS-M-A0-2>show>qos#
```

mpls-lsp-exp-profile

Syntax **mpls-lsp-exp-profile-map [***policy-id***] [detail]**

Context show>qos

Description This command displays profile policy information.

Parameters *policy-id* — Displays information for the specific policy ID.

Values 1 — 65535

detail — Displays detail policy information.

Table 39: Show QoS Network Output Fields

Label	Description
`Profile Map-id`	Displays the profile Map ID.
`Description`	A text string that helps identify the policy's context in the configuration file.
`Exp`	Displays the EXP. values
`Profile`	Specifies the marking of the packets as in-profile or out-of-profile.
`Network Policy Id`	Displays the Network policy ID with which the mpls-lsp-exp-profile is associated.

Output

```
*A:7210-SAS>show>qos# mpls-lsp-exp-profile-map 1

===============================================================================
QoS MPLS LSP EXP Profile Maps
===============================================================================
-------------------------------------------------------------------------------
Profile Map-id     : 1
Description        : Default MPLS LSP EXP Profile Map policy

-------------------------------------------------------------------------------
Exp       Profile
-------------------------------------------------------------------------------
0         Out
1         In
2         Out
3         In
4         In
5         In
6         In
```

```
7         In
===============================================================================
*A:7210SAS>show>qos# mpls-lsp-exp-profile-map 1 detail

===============================================================================
QoS MPLS LSP EXP Profile Maps
===============================================================================
-------------------------------------------------------------------------------
Profile Map-id     : 1
Description        : Default MPLS LSP EXP Profile Map policy

-------------------------------------------------------------------------------
Exp       Profile
-------------------------------------------------------------------------------
0         Out
1         In
2         Out
3         In
4         In
5         In
6         In
7         In

-------------------------------------------------------------------------------
Network Policy Associations
-------------------------------------------------------------------------------
Network Policy Id             : 2
-------------------------------------------------------------------------------
===============================================================================
*A:7210-SAS>show>qos#
```

Network Queue QoS Policies

In This Section

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

Topics in this section include:

Overview

Network Queue policies define the egress network queuing for the traffic egressing on the network ports (for 7210 SAS-M in network mode) and access uplink ports (for 7210 SAS-M and 7210 SAS-T in access uplink mode). Network queue policies are used at the Ethernet port and define the bandwidth distribution for the various FC traffic egressing on the Ethernet port.

There is one default network queue policy. Each policy always has 8 queues in both network mode and access uplink mode**.** Each of these queues are shared by unicast and multicast traffic. The default policies can be copied but they cannot be deleted or modified. The default policy is identified as **network-queue default**. Default network queue policies are applied to all network ports in network mode and access uplink ports in access uplink mode. You must explicitly create and then associate other network queue QoS policies.

Basic Configurations

A basic network queue QoS policy must conform to the following:

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

Create 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 all network ports (for7210 SAS-M in Network mode) and access uplink ports (for 7210 SAS-M and 7210 SAS-T in access uplink mode).

To create an network queue policy, define the following:

- Enter a network queue policy name. The system will not dynamically assign a name.
- Include a description. The description provides a brief overview of policy features.
- FCs are mapped to 8 queues available at the port according to Table 31, Forwarding Class to Queue-ID Map, on page 81.

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

CLI Syntax:
```
config>qos
  network-queue policy-name
     description description-string
     queue queue-id
        rate cir cir-percent [pir pir-percent]
        adaptation-rule [cir adaptation-rule] [pir adaptation-
           rule]
```

```
*A:Dut-B>config>qos>network-queue# info detail
----------------------------------------------
            description "Default network queue QoS policy."
            queue 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 2
                rate cir 25 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 3
                rate cir 25 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 4
```

```
                rate cir 25 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 5
                rate cir 100 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 6
                rate cir 100 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 7
                rate cir 10 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 8
                rate cir 10 pir 100
                adaptation-rule cir closest pir closest
            exit
----------------------------------------------
*A:Dut-B>config>qos>network-queue#
```

Applying Network Queue Policies

Apply network queue policies to the following entities:

- Ethernet Ports

Ethernet Ports

Use the following CLI syntax to apply a network queue policy to an Ethernet port in network mode of operation.

The network-queue policy can only be applied on a network port.

CLI Syntax:
```
config>port#
   ethernet
```

```
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
    port 1/1/1
        ethernet
            mode network
            network
                    queue-policy "nq1-cbs"
                exit
            exit
        exit
        no shutdown
    exit
```

Use the following CLI syntax to apply a network queue policy to an Ethernet port in access-uplink mode of operation.

CLI Syntax:
```
config>port#
   ethernet
          access
             uplink
             queue-policy policy-name
```

```
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
port 1/1/1
     ethernet
          mode access uplink
               access
                    uplink
                         queue-policy "nq1-cbs"
                    exit
               exit
          exit
          no shutdown
```

```
                exit
```

Default Network Queue Policy Values

The default network queue policies are identified as policy-id **default**. The default policies cannot be modified or deleted. The following displays default policy parameters:

```
A:qos1# show qos network-queue default detail
===============================================================================
QoS Network Queue Policy
===============================================================================
Network Queue Policy (default)
-------------------------------------------------------------------------------
Policy         : default
Accounting     : packet-based
Description    : Default network queue QoS policy.

-------------------------------------------------------------------------------
Queue CIR        PIR       CBS
      CIR Rule   PIR Rule
-------------------------------------------------------------------------------
1      0         100       12.50
       closest   closest
2      25        100       12.50
       closest   closest
3      25        100       12.50
       closest   closest
4      25        100       12.50
       closest   closest
5      100       100       12.50
       closest   closest
6      100       100       12.50
       closest   closest
7      10        100       12.50
       closest   closest
8      10        100       12.50
       closest   closest

-------------------------------------------------------------------------------
FC    UCastQ
-------------------------------------------------------------------------------
be     1
l2     2
af     3
l1     4
h2     5
ef     6
h1     7
nc     8

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Port-id : 1/1/4
Port-id : 1/1/8
Port-id : 1/1/9
Port-id : 1/1/10
Port-id : 1/1/12
Port-id : 1/1/13
```

```
Port-id : 1/1/14
Port-id : 1/1/15
Port-id : 1/1/16
Port-id : 1/1/17
Port-id : 1/1/18
Port-id : 1/1/19
Port-id : 1/1/20
Port-id : 1/1/21
Port-id : 1/1/22
Port-id : 1/1/23
Port-id : 1/1/24
Port-id : lag-1
===============================================================================
A:qos1#
```

The following displays default policy parameters for 7210 SAS-M:

```
*A:Dut-C>config>qos>network-queue# info detail
----------------------------------------------
            description "Default network queue QoS policy."
            queue 1
                rate 0 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 2
                rate 25 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 3
                rate 25 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 4
                rate 25 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 5
                rate 100 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 6
                rate 100 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 7
                rate 10 pir 100
                adaptation-rule cir closest pir closest
            exit
            queue 8
                rate 10 pir 100
                adaptation-rule cir closest pir closest
            exit
----------------------------------------------
```

```
*A:Dut-C>config>qos>network-queue#
```

```
*7210SAS>config>qos>network-queue# info detail
----------------------------------------------
            description "Default hybrid queue QoS policy."
            queue 1
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
            queue 2
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
            queue 3
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
            queue 4
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
            queue 5
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
            queue 6
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
            queue 7
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
            queue 8
                port-parent cir-level 1 pir-weight 1
                rate cir 0 pir 100
                adaptation-rule cir closest pir closest
                queue-mgmt "default"
            exit
----------------------------------------------
*7210SAS>config>qos>network-queue#
```

Use the following CLI syntax to apply a network queue policy to an Ethernet port in access-uplink mode of operation.

CLI Syntax:

```
config>port#
 ethernet
       access
          uplink
          queue-policy policy-name
```

```
#--------------------------------------------------
echo "Port Configuration"
#--------------------------------------------------
port 1/1/1
     ethernet
          mode access uplink
               access
                    uplink
                         queue-policy "nq1-cbs"
                    exit
               exit
          exit
          no shutdown
     exit
```

Service Management Tasks

This section discusses the following service management tasks:

- Deleting QoS Policies on page 193
- Copying and Overwriting QoS Policies on page 194
- Editing QoS Policies on page 196

Deleting QoS Policies

A network queue policy is associated by default with all network ports (for SAS-M in Network mode) and access uplink ports (for SAS-M and 7210 SAS-T in access uplink mode). 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**.

A network-queue policy cannot be deleted until it is removed from all network ports where it is applied.

To delete a user-created network queue policy, enter the following commands:

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.

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

Example: `config>qos# copy network-queue nq1-cbs nq2-cbs`

The following output displays the copied policies

```
*A:card-1>config>qos# info
#--------------------------------------------------
echo "QoS Slope and Queue Policies Configuration"
#--------------------------------------------------
.......
        network-queue "nq1-cbs" create
            queue 1
                rate cir 0 pir 32
                adaptation-rule cir max
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
            exit
            queue 5
            exit
            queue 6
                rate cir 0 pir 4
            exit
            queue 7
                rate cir 3 pir 93
            exit
            queue 8
                rate cir 0 pir 3
            exit
        exit
        network-queue "nq2-cbs" create
            queue 1
                rate cir 0 pir 32
                adaptation-rule cir max
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
            exit
            queue 5
            exit
            queue 6
                rate cir 0 pir 4
            exit
            queue 7
                rate cir 3 pir 93
            exit
            queue 8
                rate cir 0 pir 3
            exit
        exit
----------------------------------------------
*A:card-1>config>qos# info
```

Editing QoS Policies

You can change existing policies, except the default policies, and entries in the CLI. The changes are applied immediately to all ports 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 on page 141
- Operational Commands on page 142
- Show Commands on page 142

Configuration Commands

```
config
    — qos
        — network-queue policy-name [create]
            — description description-string
            — no description
            — queue queue-id
                — adaptation-rule [cir adaptation-rule] [pir adaptation-rule]
                — no adaptation-rule
                — adaptation-rule
                — rate [cir cir-percent] [pir pir-percent]
                — no rate
```

Operational Commands

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

Show Commands

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

Configuration Commands

Generic Commands

description

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

Context config>qos>network-queue

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

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

The **no** form of this command removes any description string from the context.

Default No description is associated with the configuration context.

Parameters *description-string* — 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.

Operational Commands

copy

Syntax **copy network-queue** *src-name dst-name* [**overwrite**]

Context config>qos

Description This command copies or overwrites existing network queue QoS policies to another network queue policy ID.

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.

Parameters **network-queue** *src-name dst-name* **—** 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.

overwrite — specifies to replace the existing destination policy. 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.

```
SR>config>qos# copy network-queue nq1 nq2
MINOR: CLI Destination "nq2" exists - use {overwrite}.
SR>config>qos# copy network-queue nq1 nq2 overwrite
```

Network Queue QoS Policy Commands

network-queue

Syntax [**no**] **network-queue** *policy-name* [**create**]

Context config>qos

Description This command creates a context to configure a network queue policy. Network queue policies on the Ethernet port define network egress queuing.

Default default

Parameters *policy-name* — The name of the network queue 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.

create — Mandatory keyword to create a network queue policy.

Network Queue QoS Policy Queue Commands

queue

Syntax **queue** *queue-id*

Context config>qos>network-queue

Description This command enables the context to configure a QoS network-queue policy queue.

The FCs are mapped to these queues as per Table 31, Forwarding Class to Queue-ID Map, on page 81. Only one FC can be mapped to one queue. Queue-id 8 is the highest priority and Queue-id 1 is the lowest priority. Queue carry both the unicast and multicast traffic and no segregation is done. The hardware port scheduler prioritizes the queue according to the priority for each queue. High priority traffic should be mapped to high priority FC. Mapping traffic to high priority FC does not necessarily guarantee high priority treatment since the scheduler policy can influence the relative priority among the queues.

The no form of this command is not supported.

Parameters *queue-id* — The *queue-id* 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 — 8

adaptation-rule

Syntax **adaptation-rule** [**cir** *adaptation-rule*] [**pir** *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 **pir** and **cir** apply.

Default adaptation-rule cir closest pir closest

Parameters *adaptation-rule* — Specifies the adaptation rule to be used while computing the operational CIR or PIR value.

Values **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 **pir** 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.

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

The system creates and associates a port-scheduler with every access port on the system. Every queue within a SAP is associated with the port scheduler available on the port on which the SAP is created. This command provides the context to configure the queue parameters ‘cir-level’ and ‘pir-weight’. The port scheduler uses these parameters to apportion the bandwidth to all the queues competing for the available bandwidth.

The no form of the command sets the cir-level and pir-weight to default values.port-parent cir-level 1 pir-weight 1Specifies the priority of the queue with respect to other queues. The priority of the queue is used only in the CIR loop. Level "8" is the highest priority and level "1" is the lowest priority.

Default In the PIR loop, the priority of the queues cannot be configured. The system assigns the priority to the queues based on the cir-level associated with the queue.Specifies the relative weight of the queue with respect to the other queues. The weight parameter is used only in the PIR loop. If a queues level parameter is set to ‘8’, the weight parameter is ignored by the system.

rate

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

Context config>qos>network-queue>queue

Description This command defines the administrative Peak Information Rate (PIR) and the administrative Committed Information Rate (CIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets through the port. 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. The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth.

The rate command can be executed at anytime, altering the PIR and CIR rates for all queues created on the access ports.

The **no** form of the command returns all queues created with the *queue-id* by association with the QoS policy to the default PIR and CIR parameters (100, 0).

Parameters

cir *percent* **—** Defines the percentage of the guaranteed rate allowed for the queue. When the **rate** command is executed, a valid CIR setting must be explicitly defined. When the **rate** command has not been executed, the default CIR of **0** is assumed. Fractional values are not allowed and must be given as a positive integer.

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

Values 0 — 100

Default 0

pir *percent* **—** Defines the percentage of the maximum rate allowed for the queue. When the **rate** command is executed, the PIR setting is optional. When the **rate** command has not been executed, or the PIR parameter is not explicitly specified, the default PIR of 100 is assumed. Fractional values are not allowed and must be given as a positive integer.

Values 1— 100 percent

100Show Commands

network-queue

Syntax **network-queue** [*network-queue-policy-name*] [**detail**]

Description This command displays network queue policy information.

Context show>qos

Parameters *network-queue-policy-name* — The name of the network queue 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.

detail — Includes each queue’s rates and adaptation-rule and & cbs details. It also shows FC to queue mapping details.

Table 40: Network Queue Labels and Descriptions

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.
`Associations`	Displays the physical port identifier where the network queue policy is applied.
`Queue`	Displays the queue ID.
`CIR`	Displays the committed information rate.
`PIR`	Displays the peak information rate.
`CBS`	Displays the committed burst size.
`FC`	Displays FC to queue mapping.

```
*A:card-1# show qos network-queue nq1
===============================================================================
QoS Network Queue Policy
-------------------------------------------------------------------------------
Network Queue Policy (nq1)
-------------------------------------------------------------------------------
Policy          : nq1
Accounting      : packet-based
-------------------------------------------------------------------------------
```

```
Associations
-------------------------------------------------------------------------------
Port-id : 1/1/20
===============================================================================
*A:card-1#

*A:card-1# show qos network-queue nq1 detail
===============================================================================
QoS Network Queue Policy
===============================================================================
Network Queue Policy (nq1)
-------------------------------------------------------------------------------
Policy         : nq1
Accounting     : packet-based
Description    : this is a network-queue policy
-------------------------------------------------------------------------------
Queue CIR        PIR       CBS
      CIR Rule   PIR Rule
-------------------------------------------------------------------------------
1      0         100       12.50
       closest   closest
2      0         100       12.50
       closest   closest
3      0         100       12.50
       closest   closest
4      0         100       12.50
       closest   closest
5      0         100       12.50
       closest   closest
6      0         100       12.50
       closest   closest
7      0         100       12.50
       closest   closest
8      0         100       12.50
       closest   closest
-------------------------------------------------------------------------------
FC    UCastQ
-------------------------------------------------------------------------------
be     1
l2     2
af     3
l1     4
h2     5
ef     6
h1     7
nc     8
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Port-id : 1/1/20
===============================================================================
*A:card-1#
*A:card-1# show qos network-queue default detail
===============================================================================
QoS Network Queue Policy
-------------------------------------------------------------------------------
Network Queue Policy (default)
-------------------------------------------------------------------------------
Policy         : default
```

Service Ingress QoS Policies

In This Section

This section provides information to configure SAP ingress QoS policies using the command line interface.

Topics in this section include:

- Overview on page 208
- Basic Configurations on page 222
- Service Management Tasks on page 273
- Service Ingress Policy Configuration Considerations on page 215
- Allocation of QoS Resources for a SAP Ingress Policy on page 217

Overview

There is one default service ingress policy. The default policy has two classification resources and one meter (the num-qos-classifiers set to value "2"). No queues are allocated by default. SAP ingress policies with policing is supported for SAPs configured on access ports and hybrid ports. The default policies can be copied but cannot be deleted. The default policies are identified as policy ID 1.

The default policies are applied to the appropriate interface, by default. For example, the default SAP ingress policy is applied to access ingress 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 your 7210 SAS devices, refer to the CLI Usage chapter in the 7210 SAS OS Basic System Configuration Guide.

Default SAP Ingress Policy

```
*A:7210-SAS>config>qos>sap-ingress# info detail
----------------------------------------------
            description "Default SAP ingress QoS policy."
            num-qos-classifiers 2
            scope template
            meter 1 create
                mode trtcm1
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
                mbs default
                cbs default
            exit
            default-fc "be"
----------------------------------------------
*A:7210-SAS>config>qos>sap-ingress#
```

SAP Ingress Policy Defaults

Table 41: SAP Ingress Policy Defaults

Field	Default
description	“Default SAP ingress QoS policy.”
scope	template
num-qos-classifiers	2
meter	1
mode	trtcm1
adaptation-rule	cir closest pir closest
rate	pir = max, cir= 0
cbs	Default
mbs	Default
default-fc	be

Use of Index file by SAP QoS Ingress policy

7210 uses an index file to store the map which indicates the QoS resource allocation to SAPs. This file is used on reboot to ensure that all the SAPs that were created successfully before reboot can be created again on a reboot. Without an index file the system does not ensure this (that is, without an index file it is possible that all the SAPs that were configured successfully, may fail on a reboot after saving the configuration file). The file is stored in the flash. On reboot if the file is found, the system allocates resources as per the stored map. If the file is not found the system implements a best-fit algorithm and tries to allocate resources for all the SAPs on a first-come-first-served basis (Note : There is no guarantee that resources will be allocated to all SAPs). Hence, when the file is not present it is possible that configuration saved, does not execute successfully after the reboot.

NOTE: The index file used for QoS map is different from the one used for storing Interface indexes.

Use of the keyword “multipoint” for default meter “11”

The system allows sharing of a single meter for both unicast and multipoint traffic. The user can configure any of the available meters for multipoint traffic. The use of 'multipoint’ keyword during meter creation is deprecated, except for use with meter “11” as described in the following paragraphs.

When the “**multipoint”** keyword is specified with meter "11" the software interprets it to be the default multipoint meter. The default multipoint meter is used for all FCs that do not have explicit multipoint meters configured.The software does the appropriate resource checks to ensure that resources needed to use multipoint meter with all the FCs are available before allowing this change.

Note 1: When num-qos-resources is set to a value of ‘2’, default multipoint meter "11" cannot be used as only a single meter is available for use.

Note 2: When associating a meter with a FC for BUM traffic, the software does not validate if the meter is a multipoint meter thus allowing user to use a single meter for unicast and BUM traffic. This implies efficient use of SAP ingress qos resources.From release 4.0R4 onwards when the "multipoint" keyword is used, software throws a warning indicating that it is an obsolete CLI command and it is not saved in the configuration file deprecating the use of multipoint keyword with any meter other than the default.

Examples of usage of multipoint meter:

Example 1:

```
*7210-SAS>config>qos# sap-ingress 12 create
*7210-SAS>config>qos>sap-ingress$ info
----------------------------------------------
            num-qos-classifiers 4
            meter 1 create
            exit
----------------------------------------------
*7210-SAS>config>qos>sap-ingress$
```

All FCs in the SAP ingress policy use the default meter 1 (for all traffic types). If the command “**configure qos sap-ingress <id> meter 11 multipoint create**” is executed, it attaches the default meter "11" with all the FCs defined in the SAP ingress policy.

After this configuration, all the FCs in this policy use two meters, default meter "1" to meter unicast traffic for all the FCs and meter "11" to meter BUM traffic for all the FCs. In this specific example, since only default FC “be” is in use, the multipoint meter will be used to meter BUM traffic associated with default FC “be”.

After the change the policy is as displayed in the example below:

```
*7210-SAS>config>qos# sap-ingress 12
*7210-SAS>config>qos>sap-ingress$ info
----------------------------------------------
             num-qos-classifiers 4
             meter 1 create
             exit
meter 11 multipoint create
----------------------------------------------
*7210-SAS>config>qos>sap-ingress$
```

Delete the multipoint meter "11" to remove all the FCs associated with the multicast-meter (assuming all the FCs are using the default multicast meter and do not have any other multicast meter explicitly configured). Execute the command “**configure qos sap-ingress <id> no meter 11**” , this disassociates meter "11" from the FCs and now the FCs use only meter "1" (if no other meter configured explicitly).

Example 2:

```
*7210-SAS>config>qos# sap-ingress 12
*7210-SAS>config>qos>sap-ingress$ info
----------------------------------------------
configure> qos> sap-ingress 10 create
     meter 1 create
     exit
     meter 3 create
     exit
     default-fc be
     fc be
          meter 3
          multicast-meter 3
     exit
     fc af
          meter 3
     exit
exit
----------------------------------------------
```

Starting with the above policy, if the user now executes the command "**configure qos sap-ingress <id> meter 11 multipoint create**", the FC "be" continues to use meter "3" and the FC "af" uses meter "11" for BUM traffic. In the above example, if the user were to execute "**configure qos sap-ingress <id> fc be no multicast-meter**", then the default meter “11” is used for FC "be" too.

Example 3:

```
----------------------------------------------
configure> qos> sap-ingress 10 create
     meter 1 create
     exit
     meter 3 create
     exit

     default-fc be

     fc be
          meter 3
          unknown-meter 3
     exit
exit
----------------------------------------------
```

On execution of the command "**configure qos sap-ingress <id> meter 11 multipoint create**", FC "be" unknown-unicast traffic type will continue to use meter 3 and broadcast and multicast traffic type will use meter “11”.

In the above example, if initially a broadcast-meter was configured in the sap-ingress policy and then followed by execution of the command "**configure qos sap-ingress <id> meter 11 multipoint create**", then FC be changes to use meter “11” for multicast traffic and broadcast traffic continue to use meter “3” for unknown-unicast traffic and meter “3” for unicast traffic.

In the above example, if the user executes "**configure qos sap-ingress <id> fc be no unknown-meter**", then meter "3" is used for all traffic types classified to FC “be”. But, if the default meter "11" is defined in the policy, then FC “be” uses meter “11” for BUM traffic.

Service Ingress Meter Selection Rules

The following are rules for meter selection by different traffic types under various configurations for VPLS services:

- In the default policy, only meter “1” is defined. All FC and all traffic types use meter “1” by default. Meter “11” is not created by default and is not available for use.

Sample configuration:

```
*7210-SAS>config>qos# sap-ingress 1 create // Default policy
*7210-SAS>config>qos>sap-ingress$ info
----------------------------------------------
num-qos-classifiers 2
meter 1 create
exit
----------------------------------------------
*7210-SAS>config>qos>sap-ingress$
```

The following describes the usage of meters when meter “11” is not configured in the policy:

- If a FC is created without explicit meters, the default meter “1” is used for unicast traffic and for multipoint traffic types (such as broadcast, multicast and unknown-unicast traffic).
- If a FC is created with an explicit unicast meter, that meter is used for unicast traffic and for multipoint traffic types (such as broadcast, multicast and unknown-unicast traffic).
- If a FC is created with an explicit unicast meter and explicit broadcast meter, use these meters for unicast and broadcast traffic respectively and use the unicast meter for all other traffic types.
- If a FC is created with an explicit unicast meter and explicit multicast meter, use the unicast meter for unicast traffic and multicast meter for all other traffic types.

- If a FC is created with an explicit unicast meter, an explicit broadcast meter, and an explicit multicast meter, use these meters for unicast, broadcast and multicast traffic types respectively. Unknown unicast traffic type will use the explicitly defined multicast meter.
- If a FC is created with an explicit unicast meter, an explicit broadcast meter, an explicit unknown-unicast meter, and an explicit multicast meter, use these meters for unicast, broadcast, unknown-unicast and multicast traffic types respectively.

The following describes the usage of meters when meter “11” is defined in the policy:

- If a FC is created without explicit meters, use the default meter “1” for unicast traffic and default meter “11” for all other traffic types (such as broadcast, multicast and unknown-unicast).
- If a FC is created with an explicit unicast meter, use that meter for unicast traffic and use default meter “11” for all other traffic types.
- If a FC is created with an explicit unicast meter and explicit broadcast meter, use these meters for unicast and broadcast traffic respectively and use meter “11” for all other traffic types.
- If a FC is created with an explicit unicast meter and explicit multicast meter, use the unicast meter for unicast traffic and multicast meter for all other kinds of traffic.
- If a FC is created with an explicit unicast meter, an explicit broadcast meter, and an explicit multicast meter, user these meters for unicast, broadcast and multicast traffic types respectively. Unknown unicast traffic type will use the explicitly defined multicast meter.
- If a FC is created with an explicit unicast meter, an explicit broadcast meter, an explicit unknown-unicast meter, and an explicit multicast meter, use these meters for unicast, broadcast, unknown-unicast and multicast traffic types respectively.

The following are rules for meter selection for Epipe and VPRN services:

- A multipoint meter cannot be used. A multipoint meter configured in a policy is not used when the policy is applied to a SAP in an Epipe service.
- All FCs associated with a meter always use the unicast meter.

Service Ingress Policy Configuration Considerations

The *num-qos-classifiers* parameter cannot be modified when the policy is in use (for example, when it is associated with a SAP). Other parameters in the SAP ingress policy can be changed.

When changing other parameters (for example, fc meter map or fc classification match criteria entries) for a policy which is in use, the system recomputes the resources required due to accomodate the change. If the resources required exceeds the configured value for *num-qos-classifiers*, then the change is not allowed.

If more resources are needed than what is configued in *num-qos-classifiers* for a existing policy, then the following options are available.

- Copy the existing policy to a new policy, modify the *num-qos-classifiers* parameter, modify the match criteria entries suitably, and finally modify the SAP configuration to associate it with the new policy.
- Ensure the existing policy is not in use by any SAP (if required change the SAP configuration to disable the use of the QoS policy with the **no qos** form of the command), change all the required parameters and finally modify the SAP configuration to use the policy again.

  Note that both these options have side-effects, for example, it resets the statistics associated with the meters and can potentially cause existing traffic classification not to take effect. But, the system will ensure that default policy is in use during the intermittent time when a policy changes are being made following the steps given above.

- In releases prior to release 3.0R1, the software always the computes the number of resources (like classifiers and meters) required by a policy assuming it will be used in a VPLS service. This allows the policy to be applied to either an Epipe or VPLS service.
- From release 3.0R1 onwards, on creation of SAP ingress policy, software does not compute the number of resources required by a policy and validate it against resources available in the system. The software validates the resources needed only when the SAP ingress policy is attached to a SAP. If enough resources are available the association succeeds, else the software fails the CLI command. Based on the service (i.e. Either VLL, VPLS, and so on.) the SAP is configured in, for the same SAP ingress policy the amount of resources required is different. The software validates that the amount of qos resources specfied with the command num-qos-classifiers is sufficient for the match criteria, forwarding class and service specified and the resources are available in hardware. On failure of the validation, the software disallows the association of the SAP ingress policy with the SAP.
- The match criteria type (that is, mac-criteria, ipv4-criteria and ipv6-criteria) cannot be changed when the SAP ingress QoS policy is in use. For example - if the match-criteria is set to ipv4-criteria and the policy is associated with a SAP then the ipv6-criteria or mac-criteria cannot be enabled in the same policy. If there is a need to change the criteria, then

user must remove the association and then change the SAP ingress policy to use the new match criteria. For SAPs configured in VPRN services, the computation of resources is similar to an SAP configured in an Epipe service.

Please see the section on "Resource Allocation for Service Ingress QoS policies on page 216" for more information.

Resource Allocation for Service Ingress QoS policies

The available global pool of ingress internal CAM hardware resources can be allocated as per user needs for use with different features such as SAP ingress QoS policy, ingress ACLs, etc. SAP ingress QoS can be allocated classification and meter resources for use from this pool. Further on, resources can be allocated for different SAP ingress QoS policy classification match criteria, based on the operator needs. Users can modify the resource allocated to scale the number of entries available per match criteria or scale the number of SAPs. The resources from the global ingress internal CAM pool are allocated in chunks with fixed number of entries. For 7210 SAS-M , each chunk allows for 512 classification entries and 256 meters. The number of chunks to be allotted for SAP ingress QoS policy is specified using the CLI command configure> system> resource-profile> ingress-internal-tcam> qos-sap-ingress-resource.

User can specify a limit for the amount of resources required for SAP ingress QoS policies and also an option to limit the amount of resources used per match criteria supported for SAP ingress QoS policies. A given chunk can be used for either MAC criteria or IP criteria or IPv6 criteria. Allocation of classification entries also allocates meter/policer resources, used to implement per FC per traffic type policing.

By default, the system allocates resources for SAP ingress QoS policies to maintain backward compatibility with release 4.0 and allocates resources for MAC criteria and IP criteria (by setting it to 'max'). Setting the value to ‘max’ allows each match criteria to use the available SAP ingress QoS resources on first-come-first-served model. By default, software does not allocate resources for use by ingress IPv6 filters. Before associating an IPv6 SAP ingress policy to a SAP, resources must be allocated. Until resources are allocated for use by IPv6 filters, software fails all attempts to associate an IPv6 filter policy with a SAP.

When the user allocates resources for use by SAP ingress QoS policies using the CLI command configure> system> resource-profile> qos-sap-ingress-resource, the system allocates resources in chunks of 512 entries. The usage of these entries by different type of match criteria is given below:

- **mac-criteria (any) -** User needs to allocate resources for mac-criteria from the SAP ingress QoS resource pool by using the command “configure> system> resource-profile> ingress-internal-tcam> qos-sap-ingress-resource> mac-match-enable" before using SAP ingress policies with mac-criteria. Every entry configured in the SAP ingress QoS policy using the mac-criteria uses one (1) entry from the chunks in the hardware.

For example: Assume a SAP Ingress QoS policy is configured to use mac-criteria with 50 entries and uses “configure> system> resource-profile> ingress-internal-tcam> qos-sap-ingress-resource> mac-match-enable 1”, to configure one chunk for use by mac-criteria (allowing a total of 512 entries for use by policies using mac-criteria). In this case, the user can have 10 SAPs using mac-criteria SAP ingress policy and consumes 500 entries.

- **ipv4-criteria (any) -** The usage is same as the mac-criteria. Resources need to be allocated using the command “configure> system> resource-profile> ingress-internal-tcam> qos-sap-ingress-resource> ipv4-match-enable". Additionally,IPv4 criteria can share the entries allocated for IPv6 criteria. The software automatically allocates entries from an IPv6 criteria slice to IPv4 criteria policies, if there are no entries available in the allocated IPv4 criteria chunks and there are no chunks available for allocation to IPv4 criteria from the SAP ingress QoS resource pool. The number of hardware entries taken up by an IPv4 criteria entry when using the IPv6 criteria chunks is the same as required by an entry using IPv6 criteria (see below for details).
- **ipv6-criteria (any) -** User needs to allocate resources from the SAP ingress QoS resource pool for ipv6-criteria by using the command “configure> system> resource-profile> ingress-internal-tcam> qos-sap-ingress-resource> ipv6-ipv4-match-enable" before using IPv6 criteria and num-qos-classifiers must specify the ipv6 keyword. Every ipv4 criteria match entry or ipv6 criteria match entry configured in the QoS policy using ipv6-criteria uses two (2) entries from the chunks allocated for use by ipv6-criteria (128-bit) in the hardware. Software allocates entries from the ipv6-criteria pool if the SAP ingress QoS policy uses both ipv6-criteria entries and ipv4-criteria (any or IPv4 DSCP) entries or if the SAP ingress QoS policy uses only IPv6 criteria any or if the SAP ingress QoS policy uses ipv4 criteria any and there are no resources available in the IPv4 criteria (as explained above).

For example: Assume a QoS policy is configured to use ipv6-criteria with 50 entries and using “configure>system> resource-profile> ingress-internal-tcam> qos-sap-ingress-resource> ipv4-ipv6-128-match-enable 1”, user configures one chunk for use by ipv6-criteria. This allows for a total of 256 entries for use by SAPs using SAP ingress QoS policies with ipv6-critiera (as each IPv6 entry uses 2 entries in hardware). In this example, user can have five (5) SAPs using this policy and consuming 250 entries in total. These resources can be shared with policies that use IPv4 criteria, though it consumes 2 entries in hardware consumed per IPv4 criteria entry. It allows user to make use of spare IPv6 resources for IPv4 criteria policies, though if user plans to have a larger number of IPv4 criteria policies they are better off allocating more resources for use with IPv4 criteria.

Note when a chunk is allocated to IPv6 criteria, software automatically adjusts the number of available entries in that chunk to 256, instead of 512, since 2 entries are needed to match IPv6 fields. The number of meters available does not reduce though and 256 meters are available for use.

- **dot1p-only, IPv4 dscp-only, IPv6 dscp-only and Default SAP Ingress QoS policies -** User can use the option 'dot1p-only' or dscp-only', if they plan to use only dot1p bits or only DSCP bits for SAP ingress classification. This typically allows for efficient use of available hardware resources and better scaling. SAP ingress policies that use only Dot1p bits or only IPv4/IPv6 DSCP and Default SAP ingress QoS policies bits can use the resources from chunks currently allocated for use by either IP-criteria or MAC-criteria or IPv6 criteria. There are some special cases noted below for allocation of resources for default, dot1p-only and dscp-only SAP ingress policies:

→ If there are no chunks available for accommodating a SAP that is associated with default or dot1p-only or a dscp-only SAP ingress policy, the software allocates resources against mac-criteria if the SAP is configured in a VLL or VPLS service. The software uses the required number of entries for this policy. The remaining entries is available for SAPs that use mac-criteria or that use only dot1p or only ipv4/ipv6 DSCP or that use default policy.

→ If there are no chunks available for accommodating a SAP that is associated with default, dot1p-only or a dscp-only SAP ingress policy, the software allocates resources against ipv4-criteria if the SAP is configured in an IES or a VPRN service. The software uses the required number of entries for this policy. The remaining entries is available for SAPs that use ipv4-criteria or that use only ipv4/ipv6 DSCP or only dot1p criteria or that use default policy.

The SAP ingress resource chunks referred to in this section is different from the resources specified using the command 'num-qos-classifiers'. num-qos-classifiers set the limit on the resources needed per SAP ingress QoS policy. The above resources set the maximum limit on the resources available for use by all the SAP ingress policies in use simultaneously on the system. The software manages the resource chunks allocated to SAP ingress QoS policy pool and allocates the entries in the chunks when a SAP ingress QoS policy is associated with a SAP. In other words, a SAP specifies the amount of QoS resources it needs, using the 'num-qos-resources' CLI command (in the SAP ingress policy) and the software allocates the resources required by a SAP from the chunks depending on whether the SAP ingress policy uses ip-criteria or mac-criteria or ipv6-criteria.

The users can use “tools> dump> system-resources” command to know the current usage and availability. One or more entries per chunk are reserved for system use.

For 7210 SAS-M , each chunk allows for 256 classification entries and 128 meters.

Computation of resources used per SAP ingress policy

The user is allowed to configure the number of classification entries the SAP requires (for example: TQ).

Number of meters allocated automatically by system = TQ / 2 (up to a maximum of 32 meters).

To calculate the number of SAPs allowed, assume all configured to use ‘TQ’ QoS resources per SAP.

Number of SAPs allowed = maximum classification entries / TQ.

NOTE: The number of SAPs arrived at using the equation above is subject to system limits. The above equation is used to derive the limit on the number of SAPs due to QoS resources only.

The user is allowed to mix and match SAPs with different QoS resources (that is, using different values of TQ).

The following determines the number of QoS resources to be allocated for an SAP:

- Number of match-criteria entries used to identify the FC.
- Number of FCs to use and number of traffic-types to be policed per FC.
- The amount of hardware classification resources needed per entry configured by the user (refer to the section "Resource Allocation for Service Ingress QoS policies on page 216" to know about resources needed per match entry. It varies based on different match criteria in use).

Only those FCs that are in use by the match-criteria classification entries are considered for the number of FCs. Therefore, these FCs are referred to as ‘FC in use’.

Given the number of traffic types to use per 'FC in use', the following rules apply for a SAP in a VPLS service to arrive at number of classification entries per FC in use:

- If a FC is in use and is created without explicit meters, use default meter #1 for unicast traffic and for all other traffic types (that is, broadcast, multicast and unknown-unicast). This requires one classification entry in hardware. This assumes default mulitpoint meter #11 is not created by the user.
- If a FC is in use and is created without explicit meters, use default meter #1 for unicast traffic and default meter #11 (assuming meter “11” is created by the user), for all other traffic types (that is, broadcast, multicast and unknown-unicast). This requires two classification entries in hardware.
- If a FC is in use and is created with an explicit unicast meter, use that meter for unicast traffic and for all other traffic types (that is, broadcast, multicast and unknown-unicast). This requires one classification entries in hardware. This assumes default multipoint meter “11” is not created by the user.
- If a FC is in use and is created with an explicit unicast meter, use that meter for unicast traffic and use default meter #11 (assuming meter “11” is created by the user) for all other traffic types. This requires two classification entries in hardware.

- If a FC is in use and is created with an explicit unicast meter and explicit broadcast meter, use these meters for unicast and broadcast traffic respectively and use the unicast meter for all other traffic types (that is, multicast and unknown-unicast). This requires two classification entries in hardware. This assumes that the default multipoint meter #11 is not created by the user.
- If a FC is in use and is created with an explicit unicast meter and explicit broadcast meter, use these meters for unicast and broadcast traffic respectively and use meter #11 (assuming meter 11 is created by the user) for all other traffic types. This requires three classification entries in hardware.
- If a FC is in use and is created with an explicit unicast meter and explicit multicast meter, use the unicast meter for unicast traffic and multicast meter for all other kinds of traffic. This requires two classification entries in hardware.
- If a FC is in use and is created with an explicit unicast meter, an explicit broadcast meter, and an explicit multicast meter, use these meters for unicast, broadcast and multicast traffic types respectively. Unknown unicast traffic type will use the explicitly defined multicast meter. This requires three classification entries in hardware.

For calculating the number of classification entries per FC for a SAP in a VLL or vprn service, the following rules apply:

- Multipoint meters cannot be used. Multipoint meter configured in a policy is not used when the policy is applied to a SAP in an Epipe service.
- All FCs in use and associated with a meter always use the unicast meter. Therefore, all FCs in use utilize only one classification entry in the hardware.

Apply the rules to determine the number of classification entries per FC (only for the FCs in use) using the following equation:

$$C(i)=\Sigma FCi(unicast)+FCi(multicast)+FCi(broadcast)+FCi(unknown\_unicast)$$

$$i=nc,h1,ef,h2,l1,af,l2,be$$

where FCi (unicast), FCi (multicast), FCi (broadcast), and FCi (unknown-unicast) are set to a value of 1 if this FC uses classifier to identify traffic-type unicast, multicast, broadcast and unknown-unicast respectively. FCi (unicast), FCi (multicast), FCi (broadcast), and FCi (unknown-unicast) are set to a value of 0 if this FC does not use a classifier to identify this traffic-type.

If the user does not configure meters explicitly for the FC and meter “11” is not created, the default unicast meter is used for all traffic types and therefore, only one classification entry in hardware is required by the FC. If the user does not configure meters explicitly for the FC and meter “11” is created, the default unicast meter and multicast meter are used. Therefore by default, two classification entries in hardware are required by a FC.

Taking into account the number of match criteria and the number of FCs used, use the equation given below to arrive at total number of classification entries per policy, for example:

$TC = \Sigma\ E(i) * C(i)$

$i = nc, h1, ef, h2, l1, af, l2, be$

where:

- E(i) is the number of match-criteria entries that classify packets to FCi. For 7210 platforms, the maximum number of classification entries per policy can be 64 (including default).
- C(i) is the number of classification entries that are required by FCi to identify different traffic types.

Determine the number of policers or meters to use (for example TP). A maximum of 32 meters per policy are available.

Only those meters associated with FCs are considered for number of meters. Note that only 'FCs in use' is considered.

Total QoS resources required (for example TQ) = max ((TC), (2 * TP)).

The number obtained is rounded off to next multiple of “2” greater than TQ obtained above.

The user configures value TQ using CLI command **num-qos-classifiers**.

Basic Configurations

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

- Have a unique service ingress QoS policy ID.
- Allocates number of classifier and meter resources needed for use
- Have a QoS policy scope of template or exclusive.
- Have at least one default unicast forwarding class meter.
- Use of multipoint forwarding class meter is optional.

Create Service Ingress QoS Policies

Configuring and applying QoS policies is optional. If no QoS policy is explicitly applied to a SAP, a default QoS policy is applied.

- Service Ingress QoS Policy on page 223

Service Ingress QoS Policy

To create an service ingress policy, define the following:

- A policy ID value. The system will not dynamically assign a value.
- Include a description. The description provides a brief overview of policy features.
- Specify *num-qos-classifiers* parameter. The default value is 2.
- Specify 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.
- Define forwarding class parameters.
    - → Modify the unicast-meter default value to override the default unicast forwarding type meter mapping for **fc** *fc-name*.
    - → Modify the **multicast-meter** default value to override the default multicast forwarding type meters mapping for **fc** *fc-name*.
    - → Modify the **unknown-meter** default value to override the default unknown unicast forwarding type **meter** mapping for **fc** *fc-name*.
    - → Modify the **broadcast-meter** default value to override the default broadcast forwarding type **meter** mapping for **fc** *fc-name*.
- Specify IPv4/IPv6 or MAC criteria. You can define IPv4/IPv6 and MAC-based SAP ingress policies to select the appropriate ingress meter and corresponding forwarding class for matched traffic.
- A SAP 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.

The following displays an service ingress policy configuration:

```
A:ALA-7>config>qos>sap-ingress# info
----------------------------------------------
...
        sap-ingress 100 create
            description "Used on VPN sap"
...
----------------------------------------------
A:ALA-7>config>qos>sap-ingress#
```

Service Ingress QoS Meter

To create service ingress meter parameters, define the following:

- A new meter ID value — The system will not dynamically assign a value.
- Meter parameters — Ingress meters support the definition of either srTCM (Single Rate Tri-Color Meter) or trTCM (Two Rate Tri-Color Meter), CIR/PIR, CBS/MBS parameters.

The following displays an ingress meter configuration:

```
A:ALA-7>config>qos# info
#------------------------------------------
echo "QoS Policy Configuration"
#------------------------------------------
...
sap-ingress 100 create
     description "Used on VPN sap"
     meter 1 create
     exit
     meter 11 multipoint create
          exit
     meter 2 create
          rate cir 11000
     exit
     meter 3 create
          cbs 32
          rate 11000
     exit
     meter 4 create
          rate 1
     exit
     meter 5 create
          cbs 64
          mbs 128
          rate cir 1500 pir 1500
     exit
     meter 6 create
          mode srtcm
          rate cir 2500 pir 2500
     exit
     meter 7 create
          cbs 256
          mbs 512
          rate cir 100 pir 36
     exit
     meter 8 create
          cbs 256
          mbs 512
          rate cir 11000
     exit
     meter 9 create
          rate cir 11000
     exit
     meter 10 create
          rate cir 1
```

```
    exit
    meter 12 create
        rate cir 1500 pir 1500
    exit
    meter 13 create
        rate cir 2500 pir 2500
    exit
    meter 14 create
        rate cir 36 pir 100
    exit
        meter 15 create
        rate cir 36 pir 100
    exit
    meter 16 create
        cbs 128
        mbs 256
        rate cir 36 pir 100
    exit
...
#------------------------------------------
A:ALA-7>config>qos#
```

SAP Ingress Forwarding Class (FC)

The following displays a forwarding class and precedence configurations:

```
A:ALA-7>config>qos# info
#------------------------------------------
...
     fc af create
          meter 1
          broadcast-meter 7
          unknown-meter 8
     exit
     fc be create
          meter 2
          unknown-meter 9
     exit
     fc ef create
          meter 3
          broadcast-meter 10
     exit
     fc h1 create
          meter 4
          multicast-meter 12
     exit
     fc h2 create
          meter 5
          broadcast-meter 13
          multicast-meter 14
          unknown-meter 15
     exit
     fc nc create
          meter 6
          broadcast-meter 16
          multicast-meter 10
          unknown-meter 11
     exit

...
#------------------------------------------
```

Service Ingress IP Match Criteria

When specifying SAP ingress match criteria, only one match criteria type can be configured in the SAP ingress QoS policy.

The following displays an ingress IP criteria configuration:

```
7210-SAS>config>qos>sap-ingress# info
----------------------------------------------
            num-qos-classifiers 32
            meter 1 create
            exit
            meter 11 multipoint create
            exit
            fc "h2" create
            exit
            ip-criteria any
                entry 16 create
                    description "test"
                    match
                    exit
                    action fc "be"
                exit
            exit
----------------------------------------------
7210-SAS>config>qos>sap-ingress#

7210-SAS>config>qos>sap-ingress# info
----------------------------------------------
            num-qos-classifiers 4
            meter 1 create
            exit
            meter 11 multipoint create
            exit
            ip-criteria dscp-only
                entry 30 create
                    match
                    exit
                    action fc "l2"
                exit
            exit
----------------------------------------------
7210-SAS>config>qos>sap-ingress#
```

Service Ingress MAC Match Criteria

Both IP criteria and MAC criteria cannot be configured in the same SAP ingress QoS policy.

To configure service ingress policy MAC criteria, define the following:

- A new entry ID value. Entries must be explicitly created. The system will not dynamically assign entries or a value.
- The action to associate the forwarding class with a specific MAC criteria entry ID.
- A description. The description provides a brief overview of policy features.

The following displays an ingress MAC criteria configuration:

```
7210-SAS>config>qos>sap-ingress# info
----------------------------------------------
            description "test"
            num-qos-classifiers 16
            meter 1 create
            exit
            meter 11 multipoint create
            exit
            mac-criteria dot1p-only
                entry 25 create
                    match
                    exit
                    no action
                exit
            exit
            default-fc "h1"
----------------------------------------------
7210-SAS>config>qos>sap-ingress#
```

Service Ingress QoS Policies Resource Usage Examples

The resource calculation shown for VLL is also applicable for VPRN services.

Example 1

```
sap-ingress 10 create
     description“example-policy-1”
     num-qos-classifiers   8
     meter 1 create
          rate cir 0 pir max
     exit
     meter 11 multipoint create
          rate cir 0 pir max
     exit
meter 3 create
          rate cir100 pir 100
     exit
     scope template
     default-fc be
     fc   be create
          meter3
     exit
     fc   af create
          meter1
     exit
     fc   l1 create
          meter 3
     exit
     fc   h2 create
          meter3
     exit
     mac-criteria dot1p-only
          entry 1 create
               match dot1p 7
               action fc af
          exit
          entry 2 create
               match dot1p 5
               action fc l1
          exit
          entry 3 create
               match dot1p 6
               action fc h2
          exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, compute the number of classification entries per FC as follows:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter, need an entry to identify this traffic type explicitly. Another entry is needed to classify broadcast, multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl1 = 1 + 0 + 1 + 0 = 2
FCaf = 1 + 0 + 1 + 0 = 2
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the equation, calculate the total classification entries used by this policy, as follows:

> TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (1 * 2)h2 + (1 * 2)l1 + (1 * 2)af + (0 * 0)l2 + (1 * 2)be = 8 (since three explicit match criteria entries are used to map traffic to each of FC H2, FC L1, and FC AF along with a default classification entry for FC BE).

The total number of meters used = 3 (since FCs use meter #1, meter #3 and meter #11).

Hence, in this example, **num-qos-classifiers 8** is used (maximum of (8, (2 * 3))).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, total classification entries used = 4 and meters used = 2.

As can be seen here, using the same policy for Epipe SAP can lead to inefficient use of resources. Hence, it is recommended to create a different policy with the required number of resources (that is, with **num-qos-classifiers 4**)

Example 1a (Default multipoint meter 11 is not used):

```
sap-ingress 10 create
         description  “example-policy”
         num-qos-classifiers 4

         meter 1  create
              rate cir 0 pir max
         exit
         meter 3 create
              rate cir 100 pir 100
         exit

         scope template

         default-fc  be
```

```
                fc be  create
                    meter 3
                exit
                fc af  create
                    meter 1
                exit
                fc l1  create
                    meter 3
                exit
                fc h2  create
                    meter 3
                exit
                mac-criteria dot1p-only
                entry 1 create
                    match dot1p 7
                    action fc af
                exit
                entry 2  create
                    match dot1p 5
                    action fc l1
                exit
                entry 3  create
                    match dot1p  6
                    action fc h2
                exit
            exit
        exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, compute the number of classification entries per FC as follows:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
```

Since this FC uses unicast meter for all traffic types, we need an entry to classify all traffic types to this FC explicitly.

```
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the equation, calculate the total classification entries used by this policy, as follows:

TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (1 * 1)h2 + (1 * 1)l1 + (1 * 1)af + (0 * 0)l2 + (1 *1)be = 4 (since three explicit match criteria entries are used to map traffic to each of FC H2, FC L1, and FC AF along with a default classification entry for FC BE).

The total number of meters used = 2 (since FCs use meter #1 and meter #3).

Hence, in this example, num-qos-classifiers 4 is used (maximum of (4, (2 * 2))). Hence, use of unicast meter for all traffic-types allows for use QoS resources efficiently.

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, total classification entries used = 4 and meters used = 2.

As can be seen here, using the same policy for Epipe SAP can lead to inefficient use of resources. Hence, it is recommended to create a different policy with the required number of resources (that is, with num-qos-classifiers 4).

Example 2

```
sap-ingress 10 create
     description“example-policy-1”
     num-qos-classifiers16
     meter 1 create
          rate cir 0 pir max
     exit
     meter 11 multipoint create
          rate cir 0 pir max
     exit
     meter 3 create
          rate cir100 pir 100
     exit
     meter 2 create
          rate cir 1 pir 20
     exit
     scope template
     default-fc be
     fc   be create
          meter 3
          broadcast-meter 2
     exit
     fc   af create
          meter 3
          broadcast-meter 2
     exit
     fc   l1 create
          meter 3
          broadcast-meter 2
     exit
     fc   h2 create
          meter 3
          broadcast-meter 2
     exit
     mac-criteria dot1p-only
          entry 1 create
               match dot1p 7
               action fc af
          exit
          entry 2 create
               match dot1p 5
               action fc l1
          exit
          entry 3 create
               match dot1p 6
               action fc h2
          exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, classification entries used per FC as:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
```

```
FCh2 = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast meter and broadcast meter, two entries are needed to identify these traffic types explicitly. Another entry is needed to classify multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl1 = 1 + 1 + 1 + 0 = 3
FCaf = 1 + 1 + 1 + 0 = 3
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 1 + 1 + 0 = 3
```

Using the above equation, to get the total classification entries used = 12 (since three explicit match criteria entries map to each of FC H2, L1, and AF along with a default classification rule for BE).

The number of meters used = 3 (since FCs use only meter #2, meter #3 and meter #11).

Hence, in this example **num-qos-classifiers 16** is used (i.e. maximum of (12, (2*3))).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, to get total classification entries used = 4 and Meters used = 1.

As can be seen here, using the same policy for Epipe SAP can lead to inefficient use of resources. Hence, it is recommended to create a different policy with the required number of resources (i.e. with **num-qos-classifiers 4**)

Example 2a (Default multipoint meter "11" is not used):

```
sap-ingress 10 create
     description  “example-policy-1”
     num-qos-classifiers  8

     meter 1 create
          rate cir 0 pir max
     exit
     meter 3 create
          rate cir  100 pir 100
     exit
     meter 2 create
          rate cir 1 pir 20
     exit
     scope template
     default-fc be
     fc be  create
          meter  3
          broadcast-meter 2
     exit
     fc af  create
          meter  3
          broadcast-meter 2
     exit
     fc l1  create
          meter  3
          broadcast-meter 2
     exit
     fc h2  create
          meter  3
          broadcast-meter 2
     exit
     mac-criteria dot1p-only
     entry  1  create
          match dot1p  7
          action fc af
     exit
     entry 2  create
          match dot1p 5
          action fc l1
     exit
     entry 3 create
          match dot1p  6
          action fc h2
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, classification entries used per FC as:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter for unicast, multicast, unknown-unicast traffic and broadcast meter for broadcast traffic, hence two entries are needed.

```
FCl1 = 1 + 0 + 1 + 0 = 2
FCaf = 1 + 0 + 1 + 0 = 2
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the above equation, to get the total classification entries used = 8 (since three explicit match criteria entries map to each of FC H2, L1, and AF along with a default classification rule for BE).

The number of meters used = 2 (since FCs use only meter #2 and meter #3).

Hence, in this example num-qos-classifiers 8 is used (that is, maximum of (8, (2*2))).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, to get total classification entries used = 4 and Meters used = 1. As can be seen here, using the same policy for Epipe SAP can lead to inefficient use of resources. Hence, it is recommended to create a different policy with the required number of resources (that is,with num-qos-classifiers 4)

Example 3

```
sap-ingress 10 create
     description“example-policy-2”
     num-qos-classifiers 16
     meter 1 create
          rate cir 100 pir 100
     exit
     meter11 multipoint create
          rate cir 1 pir 20
     exit
     meter 3 create
          rate cir 100 pir 100
     exit
     meter 2 create
          rate cir 1 pir 20
     exit
     meter 4 create
          rate cir 10 pir 100
     exit
     meter 5 create
          rate cir 10 pir 10
     exit
     scope template
     default-fc be
     fc   af create
          meter 3
          broadcast-meter 2
          multicast-meter  4
     exit
     fc   l1 create
          meter 3
          broadcast-meter 2
     exit
     fc   h2 create
          meter 3
          broadcast-meter 2
     exit
     fc   h1 create
          meter 5
          broadcast-meter 4
          multicast-meter  4
          unknown-meter  4
     exit
     mac-criteria dot1p-only
          entry 1 create
               match dot1p7
               action fc af
          exit
          entry 2 create
               match dot1p 5
               action fc l1
          exit
          entry 3 create
               match dot1p6
               action fc h2
          exit
          entry 4 create
```

```
              match dot1p 3
              action fc h1
         exit
exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the classification entries used per FC are:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 1 + 1 + 1 + 1 = 4
```

Since this FC uses unicast, broadcast, multicast and unknown-unicast meter, four entries are needed to identify these traffic types explicitly.

```
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast meter and broadcast meter, two entries are needed to identify these traffic types explicitly. Another entry if needed to classify multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl1 = 1 + 1 + 1 + 0 = 3
```

Since this FC uses only unicast meter, an entry is needed to identify this traffic type explicitly. Another entry is needed to classify broadcast, multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCaf = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the above equation, the total classification entries used = 15 and meters used = 6.

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following results:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 1 + 0 + 0 + 0 = 1
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, the total classification entries used = 5 and meters used = 3 (since all FCs used only meter #1, meter #3 and meter #5).

Example 3a (Default multipoint meter "11" is not used):

```
sap-ingress 10 create
     description  “example-policy-2”
     num-qos-classifiers  12
     meter 1 create
          rate cir 100 pir 100
     exit
     meter 3 create
          rate cir 100 pir 100
     exit
     meter  2 create
          rate cir 1 pir 20
     exit
     meter 4 create
          rate cir 10 pir 100
     exit
     meter 5 create
          rate cir 10 pir 10
     exit
     scope template
     default-fc   be
     fc af  create
          meter  3
          broadcast-meter 2
          multicast-meter 4
     exit
     fc l1  create
          meter  3
          broadcast-meter 2
     exit
     fc h2  create
          meter  3
          broadcast-meter 2
     exit
     fc h1  create
          meter 5
          broadcast-meter 4
          multicast-meter 4
          unknown-meter 4
     exit
     mac-criteria dot1p-only
     entry  1  create
          match dot1p  7
          action fc af
     exit
     entry 2  create
          match dot1p 5
          action fc l1
     exit
     entry 3  create
          match dot1p  6
          action fc h2
     exit
     entry 4  create
```

```
          match dot1p 3
          action fc h1
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the classification entries used per FC are:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 1 + 1 + 1 + 1 = 4
```

Since this FC uses unicast, broadcast, multicast and unknown-unicast meter, four entries are needed to identify these traffic types explicitly.

```
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter and broadcast meter, two entries are needed to identify these traffic types explicitly. multicast and unknown-unicast traffic use the same resource as the unicast traffic.

```
FCl1 = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter and broadcast meter, two entries are needed to identify these traffic types explicitly. multicast and unknown-unicast traffic use the same resource as the unicast traffic.

```
FCaf = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Since no explicit meters are configured for FC be, it uses meter 1 for all traffic types and needs one entry is needed to identify these traffic types.

Using the above equation, the total classification entries used = 12 and meters used = 5. The num-qos-classifiers can be set to 12 (the minimum value).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following results:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 1 + 0 + 0 + 0 = 1
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
```

```
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, the total classification entries used = 5 and meters used = 3 (since all FCs used only meter #1, meter #3 and meter #5). For epipe service a policy with num-qos-resources set to 6 can be used.

Example 4

```
sap-ingress 10 create
     description“example-policy-3”
     num-qos-classifiers 32
     meter 1 create
          rate cir100 pir 100
     exit
     meter11 multipoint create
          rate cir 1 pir 20
     exit
     meter 3 create
          rate cir100 pir 100
     exit
     meter 2 create
          rate cir 1 pir 20
     exit
     meter 4 create
          rate cir 10 pir 100
     exit
     meter 5 create
          rate cir 10 pir 10
     exit
     meter 6 create
          rate cir 11 pir 100
     exit
     meter 8 create
          rate cir 20 pir 100
     exit
     scope template
     default-fc be
     fc   af create
          meter 3
          broadcast-meter 2
          multicast-meter  4
     exit
     fc   l1 create
          meter 3
          broadcast-meter 2
     exit
     fc   h2 create
          meter 3
          broadcast-meter 2
     exit
     fc   h1 create
          meter 5
          broadcast-meter 4
          multicast-meter  4
          unknown-meter  4
     exit
     fc   ef create
          meter 6
          broadcast-meter 2
          multicast-meter  8
     exit
     fc   nc create
          meter 6
          broadcast-meter 2
          multicast-meter 8
     exit
     mac-criteria dot1p-only
          entry 1 create
               match dot1p 4
               action fc af
          exit
          entry 2 create
               match dot1p 5
               action fc l1
          exit
          entry 3 create
               match dot1p 6
               action fc h2
          exit
          entry 4 create
               match dot1p 3
               action fc h1
          exit
          entry 5 create
               match dot1p 2
               action fc ef
          exit
          entry 6 create
               match dot1p 7
               action fc nc
          exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, compute the classification entries per FC as:

```
FCnc = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCh1 = 1 + 1 + 1 + 1 = 4
```

Since this FC uses unicast, broadcast, multicast and unknown-unicast meter, four entries are needed to identify these traffic types explicitly.

```
FCef = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCh2 = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast meter and broadcast meter, two entries are needed to identify these traffic types explicitly. Another entry is needed to classify multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl1 = 1 + 1 + 1 + 0 = 3
FCaf = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the above equation, the total classification entries used = 21 and meters used = 8.

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 1 + 0 + 0 + 0 = 1
FCh1 = 1 + 0 + 0 + 0 = 1
FCef = 1 + 0 + 0 + 0 = 1
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, the total classification entries used = 7 and meters used = 4.

As can be seen here, using the same policy for Epipe SAP can lead to inefficient use of resources. Hence, it is recommended to create a different policy with the required number of resources (i.e. with **num-qos-classifiers 8**)

Example 4a (Default multipoint meter "11" is not used):

```
sap-ingress 10 create
     description  “example-policy-3”
     num-qos-classifiers  20
     meter 1 create
          rate cir 100 pir 100
     exit
     meter 3 create
          rate cir  100 pir 100
     exit
     meter 2 create
          rate cir 1 pir 20
     exit
     meter 4 create
          rate cir 10 pir 100
     exit
     meter 5 create
          rate cir 10 pir 10
     exit
```

```
meter 6 create
     rate cir 11 pir 100
exit
meter 8 create
     rate cir 20 pir 100
exit

scope template

default-fc  be
fc af  create
     meter  3
     broadcast-meter 2
     multicast-meter 4
exit
fc l1  create
     meter 3
     broadcast-meter 2
exit
fc h2 create
     meter 3
     broadcast-meter 2
exit
fc h1 create
     meter 5
     broadcast-meter 4
     multicast-meter 4
     unknown-meter 4
exit
fc ef  create
     meter 6
     broadcast-meter 2
     multicast-meter 8
exit
fc nc  create
     meter 6
     broadcast-meter 2
     multicast-meter 8
exit
mac-criteria dot1p-only
entry  1  create
     match dot1p  4
     action fc af
exit
entry  2  create
     match dot1p 5
     action fc l1
exit
entry  3   create
     match dot1p  6
     action fc h2
exit
entry  4  create
     match dot1p 3
     action fc h1
exit
entry   5  create
     match dot1p 2
     action fc ef
     exit
     entry   6  create
          match dot1p 7
          action fc nc
     exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, compute the classification entries per FC as:

```
FCnc = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCh1 = 1 + 1 + 1 + 1 = 4
```

Since this FC uses unicast, broadcast, multicast and unknown-unicast meter, four entries are needed to identify these traffic types explicitly.

```
FCef = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCh2 = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast meter and broadcast meter, two entries are needed to identify these traffic types explicitly. multicast and unknown-unicast traffic of the same FC use the unicast resources (both meter and classification entry).

```
FCl1 = 1 + 1 + 1 + 0 = 3
FCaf = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Since this FC uses a single meter for all traffic-types only a single meter and single entry is needed.

Using the above equation, the total classification entries used = 20 and meters used = 7, num-qos-classifiers to use is 20 (the minimum value).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 1 + 0 + 0 + 0 = 1
FCh1 = 1 + 0 + 0 + 0 = 1
FCef = 1 + 0 + 0 + 0 = 1
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, the total classification entries used = 7 and meters used = 4.

As can be seen here, using the same policy for Epipe SAP can lead to inefficient use of resources. Hence, it is recommended to create a different policy with the required number of resources (that is,with num-qos-classifiers 8).

Example 5

```
sap-ingress 10 create
     description“example-policy-3”
     num-qos-classifiers 32
     meter 1 create
          rate cir100 pir 100
     exit
     meter 11 multipoint create
          rate cir 1 pir 20
     exit
     meter 3 create
          rate cir 100 pir 100
     exit
     meter 2 create
          rate cir 1 pir 20
     exit
     meter 4 create
          rate cir 10 pir 100
     exit
     meter 5 create
          rate cir 10 pir 10
     exit
     meter 6 create
          rate cir 11 pir 100
     exit
     meter 8 create
          rate cir 20 pir 100
     exit
     scope template
     default-fc be
     fc   af create
          meter 3
          broadcast-meter 2
          multicast-meter  4
     exit
     fc   l1 create
          meter 3
          broadcast-meter 2
     exit
     fc   h2 create
          meter 3
          broadcast-meter 2
     exit
     fc   h1 create
          meter 5
          broadcast-meter 4
          multicast-meter  4
          unknown-meter  4
     exit
     fc   ef create
     exit
     fc   nc create
          meter 6
          broadcast-meter 2
          multicast-meter 8
     exit
     mac-criteria dot1p-only
```

```
          entry 1 create
               match dot1p 4
               action fc af
          exit
          entry 2 create
               match dot1p 5
               action fc l1
          exit
          entry 3 create
               match dot1p 6
               action fc h2
          exit
          entry 4 create
               match dot1p 3
               action fc h1
          exit
          entry 5 create
               match dot1p 2
               action fc ef
          exit
          entry 6 create
               match dot1p 7
               action fc nc
          exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, get the classification entries used per FC:

```
FCnc = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCh1 = 1 + 1 + 1 + 1 = 4
```

Since this FC uses unicast, broadcast, multicast and unknown-unicast meter, four entries are needed to identify these traffic types explicitly.

```
FCef = 1 + 0 + 1 + 0 = 2
```

Since no meters are explicitly configured, this FC uses the appropriate default meters all the traffic types (i.e. unicast traffic uses unicast meter #1 and broadcast, multicast, and unknown-unicast traffic uses multipoint meter #11.

```
FCh2 = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast meter and broadcast meter, two entries are needed to identify these traffic types explicitly. Another entry is needed to classify multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl1 = 1 + 1 + 1 + 0 = 3
```

```
FCaf = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the above equation, the total classification entries used = 20 and meters used = 8.

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 1 + 0 + 0 + 0 = 1
FCh1 = 1 + 0 + 0 + 0 = 1
FCef = 1 + 0 + 0 + 0 = 1
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, to get the total classification entries used = 7 and meters used = 4.

Example 6

```
sap-ingress 10 create
     description“example-policy-1”
     num-qos-classifiers 16

     meter 1 create
          rate cir 0 pir max
     exit
     meter 11 multipoint create
          rate cir 0 pir max
     exit
     meter 3 create
          rate cir100 pir 100
     exit
     meter 4 create
          rate cir 10  pir 50
     exit

     scope template

     default-fc      be
     fc   be create
          meter 3
     exit
     fc   af create
          meter 1
     exit
     fc   l1 create
          meter 3
          multicast-meter 4
     exit
     fc   h2 create
          meter 3
     exit

     mac-criteria dot1p-only
          entry 1 create
               match dot1p 7
               action fc af
          exit
          entry 2 create
               match dot1p 5
               action fc l1
          exit
          entry 3 create
               match dot1p 6
               action fc h2
          exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the following number of classification entries per FC:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
```

```
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 1 + 0 = 2
FCl1 = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter and multicast meter, an entry is needed to identify these traffic types explicitly. Broadcast and unknown-unicast traffic is also classified using the same entry as multicast and use the same meter.

```
FCaf = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter, an entry is needed to identify these traffic types explicitly. Another entry is needed to classify broadcast, multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the above equation, the total classification entries used = 8 and meters used = 4.

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 1 + 0 + 0 + 0 = 1
FCl1 = 1 + 0 + 0 + 0 = 1
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, the total classification entries used = 4 and meters used = 2.

Example 7

```
sap-ingress 10 create
     num-qos-classifiers 8
     meter 1 create
     exit
     meter 11 multipoint create
     exit
     meter 3 create
     exit
     meter 4 create
     exit
     fc be create
          meter 1
          broadcast-meter 11
          mulitcast-meter   4
     exit
     fc af create
          meter 3
     exit
     default-fc be
     match entry 1
          dot1p 7 fc af
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the following number of classification entries per FC are:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter, an entry is needed to identify these traffic types explicitly. Another entry is needed entry to classify broadcast, multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

Using the above equation, the total classification entries used = 5 and meters used = 4.

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
```

```
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, the total classification entries used = 2 and meters used = 2.

Example 8

```
sap-ingress 10 create
     num-qos-classifiers16
     meter 1 create
     exit
     meter 11 multipoint create
     exit
     meter 3 create
     exit
     meter 4 create
     exit
     fc be create
          meter 1
          broadcast-meter 11
          mulitcast-meter   4
     exit
     fc af create
          meter 3
     exit
     default-fc be
     mac-criteria dot1p-only
     entry 1 create
          match dot1p 7 7
          action fc af
     exit
          dot1p 7 fc af
     exit
     match entry 2
          dot1p 5 fc af
     exit
     match entry 3
          dot1p 3 fc af
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the following number of classification entries per FC:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 1 + 0 = 2
```

Since this FC uses unicast meter, an entry is needed to identify these traffic types explicitly. Another entry is needed to classify broadcast, multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

Using the equation, calculate the total classification entries used by this policy, as follows

TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (3 * 2)af + (0 * 0)l2 + (1 * 3)be = 9

The number of meters used in this policy = 4.

Hence, in this example **num-qos-classifiers 16** is used (i.e. maximum of (9, (2 * 4))).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the equation, calculate the total classification entries used by this policy, as follows:

(0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (3 * 1)af + (0 * 0)l2 + (1 * 1)be = 4

The number of meters used in this policy = 2.

Example 9

```
sap-ingress 10 create
     num-qos-classifiers 256
     meter 1 create
     exit
     meter 11 multipoint create
     exit
     meter 3 create
     exit
     meter 4 create
     exit
     fc be create
          meter 1
          broadcast-meter 11
          mulitcast-meter   4
     exit
     fc af create
          meter 3
          broadcast-meter 11
          multicast-meter   4
     exit
     default-fc be
     ip-criteria  dscp-only
     entry 1  create
          match dscp cp1
          action fc af
     exit
     entry 2  create
          match dscp cp2
          action fc af
     exit
     entry 3 create
          match dscp cp3
          action fc af
     exit
     entry 4  create
          match dscp cp4
          action fc af
     exit
     entry 5  create
          match dscp cp5
          action fc af
     exit
     entry 6  create
          match dscp cp6
          action fc af
     exit
     entry 7   create
          match dscp cp7
          action fc af
     exit
     entry 8   create
          match dscp cs1
          action fc af
     exit
     entry 9   create
          match dscp cp9
          action fc af
     exit
     entry 10   create
          match dscp af11
          action fc af
     exit
     entry 11   create
          match dscp cp11
          action fc af
     exit
     entry 12   create
          match dscp af12
          action fc af
     exit
     entry 13   create
          match dscp cp13
          action fc af
     exit
     entry 14   create
          match dscp af13
          action fc af
     exit
     entry 15   create
          match dscp cp15
          action  fc af
     exit
     entry 16   create
          match dscp  cs2
          action fc af
     exit
     entry 17   create
          match dscp cp17
          action fc af
     exit
     entry 18   create
          match dscp af21
          action  fc af
     exit
     entry 19   create
          match dscp cp19
          action fc af
     exit
     entry 20  create
          match dscp af22
          action fc af
     exit
     entry 21   create
          match dscp cp21
          action fc af
     exit
     entry 22   create
          match dscp af23
          action  fc af
     exit
     entry 23   create
          match dscp cp23
          action fc af
     exit
     entry 24   create
```

```
                         match dscp cs3
                         action  fc af
                    exit
                    entry 25   create
                         match dscp cp25
                         action fc af
                    exit
                    entry 26   create
                         match dscp af31
                         action  fc af
                    exit
                    entry 27   create
                         match dscp cp27
                         action fc af
                    exit
                    entry 28   create
                         match dscp af32
                         action fc af
                    exit
                    entry 29   create
                         match dscp cp29
                         action fc af
                    exit
                    entry 30   create
                         match dscp af33
                         action fc af
                    exit
                    entry 31   create
                         match dscp cp31
                         action fc af
                    exit
                    entry 32   create
                         match dscp cs4
                         action fc af
                    exit
                    entry 33   create
                         match dscp cp33
                         action fc af
                    exit
                    entry 34   create
                         match dscp af41
                         action fc af
                    exit
                    entry 35   create
                         match dscp cp35
                         action fc af
                    exit
                    entry 36   create
                         match dscp af42
                         action fc af
                    exit
                    entry 37   create
                         match dscp cp37
                         action  fc af
                    exit
                    entry 38   create
                         match dscp af43
                         action fc af
                    exit
```

```
     entry 39   create
          match dscp cp39
          action fc af
     exit
     entry 40   create
          match dscp cs5
          action fc af
     exit
     entry 41   create
          match dscp cp41
          action  fc af
     exit
     entry 42   create
          match dscp cp42
          action fc af
     exit
     entry 43    create
          match dscp cp43
          action  fc af
     exit
     entry 44   create
          match dscp cp44
          action fc af
     exit
     entry 45    create
          match dscp cp45
          action fc af
     exit
     entry 46   create
          match dscp ef
          action  fc af
     exit
     entry 47   create
          match dscp cp47
          action  fc af
     exit
     entry 48  create
          match dscp nc1
          action fc af
     exit
     entry 49 create
          match dscp cp49
          action fc af
     exit
     entry 50 create
          match dscp cp50
          action fc af
     exit
exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the following number of classification entries per FC:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
```

```
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 1 + 0 = 3
```

Since this FC uses unicast meter, an entry is needed to identify these traffic types explicitly. Another entry is needed to classify broadcast, multicast and unknown-unicast traffic type to the same FC and use the default meter #11.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter.

Using the equation, calculate the total classification entries used by this policy, as follows:

> TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (50 * 3)af + (0 * 0)l2 + (1 * 3)be = 153

The number of meters used in this policy = 4.

Hence, in this example num-qos-classifiers 256 is used (maximum of (153, (2 * 4)) = 153, rounded off to the next multiple of 2 will be 154).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, e the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the equation, calcuate the total classification entries used by this policy, as follows:

> (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (50 * 1)af + (0 * 0)l2 + (1 * 1)be = 51

The number of meters used in this policy = 2.

Hence for Epipe SAP it is recommended to define another sap-ingress policy with num-qos-classifiers 64 is used (i.e. maximum of (51, (2 * 2)) = 51, rounded off to the next multiple of 2 will be 52).

Example 9a (Default multipoint meter "11" is not used):

```
sap-ingress 10 create
    num-qos-classifiers  154
```

```
meter 1 create
exit
meter 3 create
exit
meter 4 create
exit
meter 11 create
exit

fc be  create
     meter 1
     broadcast-meter 11
     multicast-meter 4
exit
fc af  create
     meter 3
     broadcast-meter 11
     multicast-meter 4
exit
default-fc be

ip-criteria  dscp-only
entry 1  create
     match dscp cp1
     action fc af
exit
entry 2  create
     match dscp cp2
     action fc af
exit
entry 3 create
     match dscp cp3
     action fc af
exit
entry 4  create
     match dscp cp4
     action fc af
exit
entry 5  create
     match dscp cp5
     action fc af
exit
entry 6  create
     match dscp cp6
     action fc af
exit
entry 7   create
     match dscp cp7
     action fc af
exit
entry 8   create
     match dscp cs1
     action fc af
exit
entry 9   create
     match dscp cp9
     action fc af
exit
entry 10   create
```

```
     match dscp af11
     action fc af
exit
entry 11   create
     match dscp cp11
     action fc af
exit
entry 12   create
     match dscp af12
     action fc af
exit
entry 13   create
     match dscp cp13
     action fc af
exit
entry 14   create
     match dscp af13
     action fc af
exit
entry 15   create
     match dscp cp15
     action  fc af
exit
entry 16   create
     match dscp  cs2
     action fc af
exit
entry 17   create
     match dscp cp17
     action fc af
exit
entry 18   create
     match dscp af21
     action  fc af
exit
entry 19   create
     match dscp cp19
     action fc af
exit
entry 20  create
     match dscp af22
     action fc af
exit
entry 21   create
     match dscp cp21
     action fc af
exit
entry 22   create
     match dscp af23
     action  fc af
exit
entry 23   create
     match dscp cp23
     action fc af
exit
entry 24   create
     match dscp cs3
     action  fc af
exit
```

```
entry 25   create
     match dscp cp25
     action fc af
exit
entry 26   create
     match dscp af31
     action  fc af
exit
entry 27   create
     match dscp cp27
     action fc af
exit
entry 28   create
     match dscp af32
     action fc af
exit
entry 29   create
     match dscp cp29
     action fc af
exit
entry 30   create
     match dscp af33
     action fc af
exit
entry 31   create
     match dscp cp31
     action fc af
exit
entry 32   create
     match dscp cs4
     action fc af
exit
entry 33   create
     match dscp cp33
     action fc af
exit
entry 34   create
     match dscp af41
     action fc af
exit
entry 35   create
     match dscp cp35
     action fc af
exit
entry 36   create
     match dscp af42
     action fc af
exit
entry 37   create
     match dscp cp37
     action  fc af
exit
entry 38   create
     match dscp af43
     action fc af
exit
entry 39   create
     match dscp cp39
     action fc af
     exit
     entry 40   create
         match dscp cs5
         action fc af
     exit
     entry 41   create
         match dscp cp41
         action  fc af
     exit
     entry 42   create
         match dscp cp42
         action fc af
     exit
     entry 43    create
         match dscp cp43
         action  fc af
     exit
     entry 44   create
         match dscp cp44
         action fc af
     exit
     entry 45    create
         match dscp cp45
         action fc af
     exit
     entry 46   create
         match dscp ef
         action  fc af
     exit
     entry 47   create
         match dscp cp47
         action  fc af
     exit
     entry 48  create
         match dscp nc1
         action fc af
     exit
     entry 49 create
         match dscp cp49
         action fc af
     exit
     entry 50 create
         match dscp cp50
         action fc af
     exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the following number of classification entries per FC:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are required to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter. Additionally note that meter 11 is not defined to be multipoint meter, but is used as a normal unicast meter.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast, broadcast and multicast meter, three entries are needed to identify these traffic types explicitly. Unknown-unicast traffic type is classified using the same entry as multicast traffic type and uses the same meter. Additionally note that meter 11 is not defined to be multipoint meter, but is used as a normal unicast meter.

Using the equation, calculate the total classification entries used by this policy, as follows:

TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (50 * 3)af + (0 * 0)l2 + (1 * 3)be = 153

The number of meters used in this policy = 4. Hence, in this example num-qos-classifiers 154 is used (maximum of (153, (2 * 4)) = 153, rounded off to the next multiple of 2 will be 154).

Hence, in this example num-qos-classifiers 154 is used (maximum of (153, (2 * 4)) = 153, rounded off to the next multiple of 2 will be 154).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the equation, calcuate the total classification entries used by this policy, as follows:

TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (50 * 1)af + (0 * 0)l2 + (1 * 1)be = 51

The number of meters used in this policy = 2.

Hence for Epipe SAP it is recommended to define another sap-ingress policy with num-qos-classifiers 52 is used (that is, maximum of (51, (2 * 2)) = 51, rounded off to the multiple of 2 will be 52).

Example 10

```
sap-ingress 10 create
     description“example-policy-1”
     num-qos-classifiers   4
     meter 1 create
          rate cir 0 pir max
     exit
     meter 11 multipoint create
          rate cir 0 pir max
     exit
     scope template
     default-fc l2
     fc   l2 create
          meter 1
     exit
     fc   af create
          meter 1
     exit
     mac-criteria any
          entry 1 create
               match dot1p 7
               action fc af
          exit
     exit
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, compute the number of classification entries per FC as follows:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 1 + 0 = 2
FCl2 = 1 + 0 + 1 + 0 = 2
FCbe = 0 + 0 + 0 + 0 = 2
```

Using the equation, calculate the total classification entries used by this policy, as follows:

TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (1 * 2)af + (1 * 2)l2 + (0 * 0)be = 4

The number of meters used = 2 (since both FCs use meter #1 and meter #11).

Hence, in this example **num-qos-classifiers 4** is used (i.e. maximum of (4, (2 * 2))).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
```

```
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 1 + 0 + 0 + 0 = 1
FCl2 = 1 + 0 + 0 + 0 = 1
FCbe = 0 + 0 + 0 + 0 = 0
```

Using the above equation, calculate the total classification entries used = 2 and meters used = 1.

As can be seen here, for Epipe SAP with the same amount of resources allocated one can have more FCs if need be.

Example 11

```
sap-ingress 10 create
     description“example-policy-1”
     num-qos-classifiers   4
     meter 1 create
          rate cir 0 pir max
     exit
     meter 11 multipoint create
          rate cir 0 pir max
     exit
     scope template
     default-fc be
exit
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, compute the number of classification entries per FC as follows:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 0 + 0 + 0 + 0 = 0
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the equation, calculate the total classification entries used by this policy, as follows:

TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (0 * 0)af + (1 * 2)l2 + (0 * 0)be = 2

The number of meters used = 2 (since default FC uses meter #1 and meter #11).

Hence, in this example **num-qos-classifiers 4** is used (i.e. maximum of (2, (2 * 2))).

If the same policy were to be used for a SAP in an Epipe service, then since all traffic is classified to a unicast traffic type and since only unicast meters are used, the following:

```
FCnc = 0 + 0 + 0 + 0 = 0
FCh1 = 0 + 0 + 0 + 0 = 0
FCef = 0 + 0 + 0 + 0 = 0
FCh2 = 0 + 0 + 0 + 0 = 0
FCl1 = 0 + 0 + 0 + 0 = 0
FCaf = 0 + 0 + 0 + 0 = 0
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 0 + 0 = 1
```

Using the above equation, total classification entries used = 1 and meters used = 1.

As can be seen here, for Epipe SAP with the same amount of resources allocated one can have more FCs if need be.

Applying Service Ingress Policies

Apply SAP ingress policies to the following service SAPs:

- Epipe
- VPLS
- VPRN

Epipe

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

```
A:ALA-7>config>service# info
----------------------------------------------
        epipe 6 customer 6 vpn 6 create
            description "Epipe service to west coast"
            sap 1/1/10:10 create
                exit
                egress
                    qos 105
                exit
            exit
        exit
----------------------------------------------
A:ALA-7>config>service#
```

VPLS

The following output displays a VPLS service configuration with SAP ingress policy 100.

```
A:ALA-7>config>service# info
----------------------------------------------
        vpls 700 customer 7 vpn 700 create
            description "test"
            stp
                shutdown
            exit
            sap 1/1/9:10 create
                ingress
                    qos 100
                exit
            exit
        exit
----------------------------------------------
A:ALA-7>config>service#
```

VPRN

The following output displays a VPRN service configuration.

```
A:ALA-7>config>service# info
----------------------------------------------
...
        vprn 1 customer 1 create
            autonomous-system 10000
            route-distinguisher 10001:1
            auto-bind ldp
            vrf-target target:10001:1
            interface "to-ce1" create
                address 11.1.0.1/24
                sap 1/1/10:1 create
                    ingress
                        qos 100
                    exit
                                   exit
            exit
            no shutdown
        exit
...
----------------------------------------------
A:ALA-7>config>service#
```

IES

The following output displays a IES service configuration.

```
A:ALA-7>config>service# info
----------------------------------------------
...
ies 1 customer 1 create
     interface "to-c1" create
         address 11.1.0.1/24
              sap 1/1/10:100 create
                   ingress
                        qos 100
                   exit
              exit
         exit
         no shutdown
     exit
...
----------------------------------------------
A:ALA-7>config>service#
```

Service Management Tasks

This section discusses the following service management tasks:

- Deleting QoS Policies on page 273
- Copying and Overwriting QoS Policies on page 274
- Remove a Policy from the QoS Configuration on page 275
- Editing QoS Policies on page 275

Deleting QoS Policies

Every service SAP is associated, by default, with the appropriate 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 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 they are applied.

```
A:ALA-7>config>qos# no sap-ingress 100
MINOR: CLI SAP ingress policy "100" cannot be removed because it is in use.
A:ALA-7>config>qos#
```

Remove a QoS Policy from Service SAP(s)

The following Epipe service output examples show that the SAP service ingress reverted to policy-id “**1**” when the non-default policies were removed from the configuration.

```
A:ALA-104>config>service>epipe# info detail
----------------------------------------------
         description "Distributed Epipe service to west coast"
                no tod-suite
                dot1ag
                exit
                ingress
                    qos 1
                    no filter
                exit
                egress
                    no filter
                exit
                no collect-stats
                no accounting-policy
                no shutdown
----------------------------------------------
A:ALA-7>config>service>epipe#
```

Copying and Overwriting QoS Policies

You can copy an existing service 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.

CLI Syntax: `config>qos# copy {sap-ingress}` *`source-policy-id dest-policy-id`* `[overwrite]`

```
*A:ALU-7210>config>qos# info
#--------------------------------------------------
echo "QoS Policy Configuration"
#--------------------------------------------------
        sap-ingress 100 create
            description "Used on VPN sap"
            meter 1 create
            exit
            meter 2 multipoint create
            exit
            meter 10 create
                rate cir 11000
            exit
            meter 11 multipoint create
            exit
        exit
        sap-ingress 101 create
            description "Used on VPN sap"
            meter 1 create
            exit
            meter 2 multipoint create
            exit
            meter 10 create
                rate cir 11000
            exit
            meter 11 multipoint create
            exit
        exit
        sap-ingress 200 create
            description "Used on VPN sap"
            meter 1 create
            exit
            meter 2 multipoint create
            exit
            meter 10 create
                rate cir 11000
            exit
            meter 11 multipoint create
            exit
        exit
----------------------------------------------
*A:ALU-7210>config>qos#
```

Remove a Policy from the QoS Configuration

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

Example: `config>qos# no sap-ingress 100`

Editing QoS Policies

You can change QoS existing policies and entries. 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 SAP QoS Policy Command Reference

Command Hierarchies

- Service Ingress QoS Policy CommandsOperational Commands
- Show Commands

Service Ingress QoS Policy Commands

```
config
    — qos
            — [no] sap-ingress policy-id
                    — default-fc  fc
                    — no default-fc
                    — description description-string
                    — no description
                    — [no] fc fc-name [create]
                            — broadcast-meter meter-id
                            — no broadcast-meter
                            — meter meter-id
                            — no meter
                            — multicast-meter meter-id
                            — no multicast-meter
                            — unknown-meter meter-id
                            — no unknown-meter
                    — [no] ip-criteria [any | dscp-only]
                            — [no] entry entry-id [create]
                                    — action [fc fc-name
                                    — no action
                                    — description description-string
                                    — no description
                                    — match [protocol protocol-id]
                                    — no match
                                            — dscp dscp-name
                                            — no dscp
                                            — dst-ip {ip-address/mask | ip-address netmask}
                                            — no dst-ip
                                            — dst-port fc {eq} dst-port-number
                                            — no dst-port
                                            — fragment {true | false}
                                            — no fragment
                                            — src-ip {ip-address/mask | ip-address netmask}
                                            — no src-ip
                                            — src-port {eq} src-port-number
                                            — no src-port
```

```
          — renum [old-entry-id new-entry-id]
— [no] ipv6-criteria [any | dscp-only] [IPv6 Match Criteria]
          — [no] entry entry-id [create]
                    — action [fc fc-name]
                    — no action
                    — description description-string
                    — no description
                    — match [next-header next-header]
                    — no match
                              — dscp dscp-name
                              — no dscp
                              — dst-ip {ipv6-address/prefix-length}
                              — no dst-ip
                              — dst-port {eq} dst-port-number}
                              — no dst-port
                              — src-ip {ipv6-address/prefix-length}
                              — no src-ip
                              — src-port {eq} src-port-number
                              — no src-port
          — renum [old-entry-id new-entry-id]
— [no] mac-criteria [any | dot1p-only]
          — [no] entry entry-id
                    — action [fc fc-name]
                    — no action
                    — description description-string
                    — no description
                    — [no] match
                              — dot1p dot1p-value [dot1p-mask]
                              — no dot1p
                              — dst-mac ieee-address [ieee-address-mask]
                              — no dst-mac
                              — etype 0x0600..0xffff
                              — no etype
                              — src-mac ieee-address [ieee-address-mask]
                              — no src-mac
                    — renum
— num-qos-classifiers [num-resources] [ipv6 | no-ipv6]
— meter meter-id [multipoint] [create]
— no meter meter-id
          — adaptation-rule [cir adaptation-rule] [pir adaptation-rule]
          — no adaptation-rule
          — cbs size-in-kbits
          — no cbs
          — mbs size-in-kbits
          — no mbs
          — mode {trtcm1 | trtcm2 | srtcm}
          — no mode
          — rate cir-rate-in-kbps [pir pir-rate-in-kbps]
          — no rate
— scope {exclusive | template}
— no scope
```

Operational Commands

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

Show Commands

```
show
     — qos
             — sap-ingress policy-id [association | match-criteria]
```

Configuration Commands

Generic Commands

description

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

Context config>qos>sap-ingress
config>qos>sap-ingress>ip-criteria>entry
config>qos>sap-ingress>mac-criteria>entry

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 No description is associated with the configuration context.

Parameters *description-string* — 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.

Operational Commands

copy

Syntax **copy sap-ingress** *src-pol dst-pol* [**overwrite**]

Context config>qos

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

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.

Parameters **sap-ingress** *src-pol dst-pol* **—** Indicates that the source policy ID and the destination policy ID are 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.

Values 1 — 65535

overwrite — Specifies to replace the existing destination policy. 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.

renum

Syntax **renum**

Context config>qos>sap-ingress>ip-criteria
config>qos>sap-ingress>mac-criteria

Description This command renumbers existing QoS policy criteria entries to properly sequence policy entries.

This can be required in some cases since the 7210 SAS exits when the first match is found and executes the actions in accordance with the accompanying action command. This requires that entries be sequenced correctly from most to least explicit.

Parameters

Default none

Values 1 — 64

Default none

Values 1 —64

Service Ingress QoS Policy Commands

sap-ingress

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

Context config>qos

Description This command is used to create or edit the ingress policy. The ingress policy defines the Service Level Agreement (SLA) enforcement service packets receive as they ingress a SAP. SLA enforcement is accomplished through the definition of meters that have Forwarding Class (FC), Committed Information Rate (CIR), Peak Information Rate (PIR), Committed Burst Size (CBS), and Maximum Burst Size (MBS) characteristics. The simplest policy defines a single queue that all ingress traffic flows through. Complex policies have multiple meters combined with specific IP or MAC match criteria that indicate which queue a packet will flow though.

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

SAP ingress policies can be defined with either IP headers as the match criteria or MAC headers as the match criteria. The IP and MAC criteria are mutually exclusive and cannot be part of the same SAP ingress policy. Only one service ingress policy can be provisioned.

The SAP ingress policy with *policy-id* 1 is a system-defined policy applied to services when no other policy is explicitly specified. The system SAP ingress policy can be modified but not deleted. The **no sap-ingress** command restores the factory default settings when used on *policy-id* 1. The default SAP ingress policy defines one meter associated with the best effort (be) forwarding class, with CIR of zero and PIR of line rate.

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 policy-id. Use the **config qos copy** command to maintain policies in this manner.

NOTE: Before associating a SAP ingress policy with a SAP, resources must be allocated using the CLI command config> system> resource-profile>ingress-internal-tcam> qos-sap-ingress-resource. Please read the Service Ingress Qos Policies Chapter above and the 7210 Basic Systems Guide for more information about this CLI command and resource allocation.

The **no sap-ingress** *policy-id* command deletes the SAP 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 policy-id 1.

Parameters *policy-id* — The *policy-id* uniquely identifies the policy.

Values 1 — 65535

create — Keyword used to create a sap ingress policy.

scope

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

Context config>qos>sap-ingress *policy-id*

Description This command configures the Service Ingress QoS policy scope as exclusive or template.

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 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.

template — When the scope of a policy is defined as template, the policy can be applied to multiple SAPs on the router.

Default QoS policies are configured with template scopes. An error is generated when the template scope parameter to exclusive scope on default policies is modified.

default-fc

Syntax **default-fc** *fc*

Context config>qos>sap-ingress

Description 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.

The default forwarding class is best effort (`be`). The **default-fc** settings are displayed in the **show configuration** and **save** output regardless of inclusion of the **detail** keyword.

Context be

Parameters *fc* **—** Specify the forwarding class name for the queue. The value given for *fc* must be one of the predefined forwarding classes in the system.

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

fc

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

Context config>qos>sap-ingress

Description The **fc** command creates a class instance of the forwarding class fc-name. Once the *fc-name* is created, classification actions can be applied and can be used in match classification criteria.

The **no** form of the command removes all the explicit queue mappings for *fc-name* forwarding types. The queue mappings revert to the default meters for *fc-name*.

Parameters *fc-name* — Specifies the forwarding class name for the queue. The value given for the fc-name must be one of the predefined forwarding classes for the system.

Values fc: class

class: be, l2, af, l1, h2, ef, h1, nc

Default None (Each class-name must be explicitly defined)

create — Mandatory keyword to create a forwarding class.

ip-criteria

Syntax [**no**] **ip-criteria [any|dscp-only]** *policy id*

Context config>qos>sap-ingress

Description IP criteria-based SAP ingress policies are used to select the appropriate ingress meter and corresponding forwarding class for matched traffic.

User can specify either 'any' or 'dscp-only' as the sub-criteria. The sub-criteria determines what fields can be used to match traffic. The resource allocation for classification is affected by the sub-criteria in use. Please see the section on SAP ingress resource allocation for L2 and L3 criteria for more information.

This command is used to enter the context to create or edit policy entries that specify IP criteria DiffServ code point.

7210 SAS OS implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. For this reason entries must be sequenced correctly from most to least explicit.

The **no** form of this command deletes all the entries specified under this node. Once IP criteria entries are removed from a SAP ingress policy, the IP criteria is removed from all services where that policy is applied.

Default dscp-only

Parameters **any —** -Specifies that entries can use any of the fields available under ip-criteria (Example - IP source, IP destination, IP protocol fields can be used) for matching

dscp-only — Specifies that entries can use only the DSCP field.

policy-id — -The policy-id that uniquely identifies the policy.

Values 1 — 65535

ipv6-criteria

Syntax **[no] ipv6-criteria [any | dscp-only]** *policy-id*

Context config>qos>sap-ingress

Description IPv6 criteria-based SAP ingress policies are used to select the appropriate ingress meters and corresponding forwarding class for matched traffic.

This command is used to enter the node to create or edit policy entries that specify IPv6 criteria such as IP quintuple lookup or DiffServ code point.

The 7210 OS implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. For this reason entries must be sequenced correctly from most to least explicit.

NOTE: Before associating a SAP ingress policy configured to use IPv6 criteria with a SAP, resources must be allocated using the CLI command config> system> resource-profile>ingress-internal-tcam> qos-sap-ingress-resource> ipv6-ipv4-match-enable. Please read the 7210 Basic Systems Guide for more information about this CLI command and resource allocation.

The no form of this command deletes all the entries specified under this node. Once ipv6-criteria entries are removed from a SAP ingress policy, the ipv6-criteria is removed from all services where that policy is applied.

Parameters **any —** -Specifies that entries can use any of the fields available under ipv6-criteria (Example - IPv6 source, IPv6 destination, IPv6 protocol fields can be used) for matching

dscp-only — Specifies that entries can use only the IPv6 DSCP field.

policy-id — -The policy-id that uniquely identifies the policy.

Values 1 — 65535

mac-criteria

Syntax [**no**] **mac-criteria [any|dot1p-only]** *policy id*

Context config>qos>sap-ingress

Description The **mac-criteria** based SAP ingress policies are used to select the appropriate ingress meters and corresponding forwarding class for matched traffic.

User can specify either 'any' or dot1p-only' as the sub-criteria. The sub-criteria determines what fields can be used to match traffic. The resource allocation for classification is affected by the sub-criteria in use. Please see the section on SAP ingress resource allocation for L2 and L3 criteria for more information.

This command is used to enter the node to create or edit policy entries that specify MAC criteria.

7210 SAS OS implementation will exit on the first match found and execute the actions in accordance with the accompanying action command. For this reason entries must be sequenced correctly from most to least explicit.

The **no** form of this command deletes all the entries specified under this node. Once mac-criteria entries are removed from a SAP ingress policy, the mac-criteria is removed from all services where that policy is applied.

Default any

Parameters **any —** .Specifies that entries can use any of the fields available under mac-criteria (Example - MAC source, MAC destination, MAC Ethertype, etc. fields can be used)

dot1p-only — Specifies that entries can use only the Dot1p field.

policy-id — -The policy-id that uniquely identifies the policy.

Values 1 — 65535

num-qos-classifiers

Syntax **num-qos-classifiers** [*num-resources*] [ipv6 | no-ipv6]

Context config>qos>sap-ingress>num-qos-classifiers

Description This command configures the number of classifiers the SAP ingress Qos policy can use. A user cannot modify this parameter when it is in use (i.e. applied to a SAP).

The num-resources parameter also determines the maximum number of meters that are available to this policy. The maximum number of meters available for use by the forwarding classes (FC) defined under this policy is equal to half the value specified in the parameter num-resources. Any of these meters is available for use to police unicast or multipoint traffic. Any of these meters is available for use by more than one FC (or a single meter is available for use by all the FCs).

The keyword 'ipv6' lets the user indicate that they plan to use the ipv6-criteria and the resources needed for this SAP ingress QoS policy must be allocated for the chunk allocated to IPv6 criteria.

Default num-resources is set to a default value of 2 and no-ipv6 is use as the default keyword.

Parameters *num-resources* — Specifies the number of resources planned for use by this policy

Values 2,4,6, 8, 16,10,.... 256 (multiples of “2” upto “256”)

ipv6 — keyword which lets the user indicate that they intend to use the ipv6-criteria and software must allocate resources from the chunks alloted to IPv6 criteria.

no-ipv6 — keyword which lets the user indicate that they do not intend to use the ipv6-criteria. Resources are then allocated from the chunk alloted to either IPv4 criteria or MAC criteria, depending on what criteria the user uses.

Service Ingress QoS Policy Forwarding Class Commands

broadcast-meter

Syntax **broadcast-meter** *meter-id*
no broadcast-meter

Context config>qos>sap-ingress>fc

Description This command overrides the default broadcast forwarding type meter mapping for **fc** *fc-name*. The specified *meter-id* must exist within the policy as a multipoint meter 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 *meter-id*.

The broadcast forwarding type usually tracks the multicast forwarding type definition. This command overrides that default behavior.

The **no** form of the command sets the broadcast forwarding type *meter-id* back to the default of tracking the multicast forwarding type meter mapping.

Parameters *meter-id* — Specifies an existing multipoint queue defined in the **config>qos>sap-ingress** context.

Values 2 to 32

Default 11

meter

Syntax **meter** *meter-id*
no meter

Context config>qos>sap-ingress>fc

Description This command overrides the default unicast forwarding type meter mapping for **fc** *fc-name*. The specified *meter-id* must exist within the policy as a non-multipoint meter before the mapping can be made. Once the forwarding class mapping is executed, all unicast traffic (this includes all traffic, even broadcast and multicast for services) on a SAP using this policy is forwarded using the *meter-id*.

The **no** form of this command sets the unicast (point-to-point) *meter-id* back to the default meter for the forwarding class (meter 1).

Parameters *meter-id* — Specifies an existing non-multipoint meter defined in the **config>qos>sap-ingress** context.

Values 1 — 32

multicast-meter

Syntax **multicast-meter** *meter-id*
no multicast-meter

Context config>qos>sap-ingress>fc

Context This command overrides the default multicast forwarding type meter mapping for **fc** *fc-name*. The specified *meter -id* must exist within the policy as a multipoint meter before the mapping can be made. Once the forwarding class mapping is executed, all multicast traffic on a SAP using this policy is forwarded using the *meter-id*.

The multicast forwarding type includes the **unknown** unicast forwarding type and the **broadcast** forwarding type unless each is explicitly defined to a different multipoint meter. When the unknown and broadcast forwarding types are left as default, they will track the defined meter for the multicast forwarding type.

The **no** form of the command sets the multicast forwarding type *meter-id* back to the default meter for the forwarding class. If the **broadcast** and **unknown** forwarding types were not explicitly defined to a multipoint meter, they will also be set back to the default multipoint meter (11).

Parameters *meter-id* — Specifies an existing multipoint queue defined in the **config>qos>sap-ingress** context.

Values 1— 32

Default 11

unknown-meter

Syntax **unknown-meter** *meter-id*
no unknown-meter

Context config>qos>sap-ingress>fc

Description This command overrides the default unknown unicast forwarding type meter mapping for **fc** *fc-name*. The specified *meter-id* must exist within the policy as a multipoint meter before the mapping can be made. Once the forwarding class mapping is executed, all unknown traffic on a SAP using this policy is forwarded using the *meter-id*.

The unknown forwarding type usually tracks the multicast forwarding type definition. This command overrides that default behavior.

The **no** form of this command sets the unknown forwarding type *meter-id* back to the default of tracking the multicast forwarding type meter mapping.

Parameters *meter-id* — Specifies an existing multipoint meter defined in the **config>qos>sap-ingress** context.

Values 1— 32

Default 11

Service Ingress QoS Policy Entry Commands

action

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

Context config>qos>sap-ingress>ip-criteria>entry
config>qos>sap-ingress>mac-criteria>entry

Description This mandatory command associates the forwarding class with specific IP or MAC criteria entry ID. The action command supports setting the forwarding class parameter. Packets that meet all match criteria within the entry have their forwarding class overridden based on the parameters included in the **action** parameters.

The **action** command must be executed for the match criteria to be added to the active list of entries.

Each time action is executed on a specific entry ID, the previous entered values for **fc** *fc-name* is overridden with the newly defined parameters.

The **no** form of the command removes the entry from the active entry list. Removing an entry on a policy immediately removes the entry from all SAPs using the policy. All previous parameters for the action is lost.

Default Action specified by the **default-fc**.

Parameters **fc** *fc-name* **—** The value given for **fc** *fc-name* must be one of the predefined forwarding classes in the system. Specifying the **fc** *fc-name* is required. When a packet matches the rule, the forwarding class is only overridden when the **fc** *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

entry

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

Context config>qos>sap-ingress>ip-criteria
config>qos>sap-ingress>mac-criteria

Description This command is used to create or edit an IP or MAC criteria entry for the policy. Multiple entries can be created using unique *entry-id* numbers.

The list of flow criteria is evaluated in a top down fashion with the lowest entry ID at the top and the highest entry ID at the bottom. If the defined match criteria for an entry within the list matches the information in the egress packet, the system stops matching the packet against the list and performs the matching entries reclassification actions. If none of the entries match the packet, the IP flow reclassification list has no effect on the packet.

An entry is not populated in the list unless the action command is executed for the entry. An entry that is not populated in the list has no effect on egress packets. If the action command is executed without any explicit reclassification actions specified, the entry is populated in the list allowing packets matching the entry to exit the list, preventing them from matching entries lower in the list. Since this is the only flow reclassification entry that the packet matched and this entry explicitly states that no reclassification action is to be performed, the matching packet will not be reclassified.

The **no** form of this command removes the specified entry from the policy. Entries removed from the policy are immediately removed from all services where that policy is applied.

Default none

Parameters *entry-id* — The *entry-id,* expressed as an integer, uniquely identifies a match criterion and the corresponding action. It is recommended that multiple entries be given *entry-ids* in staggered increments. This allows users to insert a new entry in an existing policy without requiring renumbering of all the existing entries.

An entry cannot have any match criteria defined (in which case, everything matches) but must have at least the keyword **action fc** *fc-name* for it to be considered complete. Entries without the action keyword will be considered incomplete and hence will be rendered inactive.

Default none

Values 1— 64

create — Required parameter when creating a flow entry when the system is configured to require the explicit use of the keyword to prevent accidental object creation. Objects may be accidentally created when this protection is disabled and an object name is mistyped when attempting to edit the object. This keyword is not required when the protection is disabled. The keyword is ignored when the flow entry already exists.

match

Syntax [**no**] **match** [**protocol** *protocol-id*]

Context config>qos>sap-ingress>ip-criteria>entry

Description This command creates a context to configure match criteria for SAP QoS policy match criteria. When the match criteria have been satisfied the action associated with the match criteria is executed.

Only a single match criteria (either MAC or IP) is allowed at any point of time.

Parameters **protocol** *protocol-id* — Specifies an IP protocol to be used as a SAP QoS policy match criterion.

The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17).

Values 0 — 255

match

Syntax **match**
no match

Context config>qos>sap-ingress>mac-criteria>entry

Description This command creates a context for entering/editing match MAC criteria for ingress SAP QoS policy match criteria. When the match criteria have been satisfied the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured then all criteria must be satisfied (AND function) before the action associated with the match will be executed.

A **match** context can consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

The **no** form of the command removes the match criteria for the *entry-id*.

match

Syntax **match** [**next-header** *next-header*]
no match

Context config>qos>sap-ingress>ipv6-criteria>entry

Description This command creates a context to configure match criteria for ingress SAP QoS policy match IPv6 criteria. When the match criteria have been satisfied the action associated with the match criteria is executed.

If more than one match criteria (within one match statement) are configured, then all criteria must be satisfied (AND function) before the action associated with the match is executed.

A **match** context can consist of multiple match criteria, but multiple **match** statements cannot be entered per entry.

It is possible that a SAP ingress policy includes the **dscp** map command, the **dot1p** map command, and an IPv6 match criteria. When multiple matches occur for the traffic, the order of precedence is used to arrive at the final action. The order of precedence is as follows:

1. 802.1p bits
2. DSCP
3. IP Quintuple or MAC headers

The **no** form of this command removes the match criteria for the *entry-id*.

Parameters **next-header** *next-header* — Specifies the next meader to match.

The protocol type such as TCP / UDP / OSPF is identified by its respective protocol number. Well-known protocol numbers include ICMP(1), TCP(6), UDP(17).

Values protocol numbers accepted in DHB: 0 — 42, 45 — 49, 52 — 59, 61 — 255
keywords: none, crtp, crudp, egp, eigrp, encap, ether-ip, gre, icmp, idrp, igmp, igp, ip, ipv6, ipv6-icmp, ipv6-no-nxt, isis, iso-ip, l2tp, ospf-igp, pim, pnni, ptp, rdp, rsvp, stp,

tcp, udp, vrrp
* — udp/tcp wildcard

IP QoS Policy Match Commands

dscp

Syntax **dscp**
no dscp

Context config>qos>sap-ingress>ip-criteria>entry>match

Description This command configures a DiffServ Code Point (DSCP) code point to be used for classification of packets from the specified FC.

The **no** form of this command removes the DSCP match criterion.

Default none

Parameters *dscp-name* — Specifies a dscp name that has been previously mapped to a value using the **dscp-name** command. The DiffServ code point can only be specified by its name.

Values 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

dst-ip

Syntax **dst-ip** {*ip-address/mask* | *ip-address netmask*}
no dst-ip

Context config>qos>sap-ingress>ip-criteria>entry>match
config>qos>sap-ingress>ipv6-criteria>entry>match

Description This command configures a destination address range to be used as a SAP QoS policy match criterion.

To match on the destination address, specify the address and its associated mask, e.g., 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 can also be used.

The **no** form of this command removes the destination IP address match criterion.

Default none

Parameters *ip-address* — The IP address of the destination IP or IPv6 interface. This address must be unique within the subnet and specified in dotted decimal notation.

Values ipv4-prefix: a.b.c.d
ipv4-prefix-length: 0 -- 32
ipv6-prefix: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H

d: [0..255]D
ipv6-prefix-length: 0 -- 128
netmask Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 - 255.255.255.255

dst-port

Syntax **dst-port** *fc* {**eq**} *dst-port-number*
dst-port range *start end*
no dst-port

Context config>qos>sap-ingress
config>qos>sap-ingress>ip-criteria>entry>match

Description This command configures a destination TCP or UDP port number or port range for a SAP QoS policy match criterion.

The **no** form of this command removes the destination port match criterion.

Default none

Parameters **eq** *dst-port-number* **—** The TCP or UDP port numbers to match specified as equal to (**eq**) to the destination port value specified as a decimal integer.

Values 1 — 65535 (decimal hex or binary)

range *start end* **—** The range of TCP or UDP port values to match specified as between the *start* and *end* destination port values inclusive.

Values 1 — 65535 (decimal hex or binary)

fragment

Syntax **fragment** {**true** | **false**}
no fragment

Context config>qos>sap-ingress>ip-criteria>entry>match

Description This command configures fragmented or non-fragmented IP packets as a SAP QoS policy match criterion.

The **no** form of this command removes the match criterion.

Default fragment false

Parameters **true —** Configures a match on all fragmented IP packets. A match will occur for all packets that have either the MF (more fragment) bit set OR have the Fragment Offset field of the IP header set to a non-zero value.

false — Configures a match on all non-fragmented IP packets. Non-fragmented IP packets are packets that have the MF bit set to zero and have the Fragment Offset field also set to zero.

src-ip

Syntax **src-ip** {*ip-address*/*mask* **|** *ip-address netmask*}
no src-ip

Context config>qos>sap-ingress>ip-criteria>entry>match
config>qos>sap-egress>ip-criteria>entry>match
config>qos>sap-ingress>ipv6-criteria>entry>match

Description This command configures a source IP or IPv6 address range to be used as an SAP QoS policy match criterion.

To match on the source IP or IPv6 address, specify the address and its associated mask, e.g. 10.1.0.0/16. The conventional notation of 10.1.0.0 255.255.0.0 can also be used.

The **no** form of the command removes the source IP or IPv6 address match criterion.

Default No source IP match criterion.

Parameters *ip-address* | *ipv6-address* — The IP or IPv6 address of the source IP interface. This address must be unique within the subnet and specified in dotted decimal notation.

Values ip-address: a.b.c.d
mask: 1 — 32
netmask a.b.c.d (dotted quad equivalent of mask length)

Values ipv4-prefix: a.b.c.d
ipv4-prefix-length: 0 -- 32
ipv6-prefix: x:x:x:x:x:x:x:x (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
x: [0..FFFF]H
d: [0..255]D
ipv6-prefix-length: 0 -- 128
netmask Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 - 255.255.255.255

mask — The subnet mask length, expressed as an integer or in dotted decimal notation.

Values 0 — 32

netmask — Specify the subnet mask in dotted decimal notation.

Values a.b.c.d (dotted quad equivalent of mask length)

src-port

Syntax **src-port** {**eq**} *src-port-number*
src-port range *start end*
no src-port

Context config>qos>sap-ingress>ip-criteria>entry>match

Description This command configures a source TCP or UDP port number or port range for a SAP QoS policy match criterion.

The **no** form of this command removes the source port match criterion.

Default No src-port match criterion.

Parameters **eq** *src-port-number* **—** The TCP or UDP port numbers to match specified as equal to (**eq**) to the source port value specified as a decimal integer.

Values 1 — 65535 (decimal hex or binary)

range *start end* **—** The range of TCP or UDP port values to match specified as between the *start* and *end* source port values inclusive.

Values 1 — 65535 (decimal hex or binary)

Service Ingress MAC QoS Policy Match Commands

dot1p

Syntax **dot1p** *dot1p-value* [*dot1p-mask*]
no dot1p

Context config>qos>sap-ingress>mac-criteria>entry

Description The IEEE 802.1p value to be used as the match criterion.

Use the **no** form of this command to remove the dot1p value as the match criterion.

Default None

Parameters *dot1p-value* — Enter the IEEE 802.1p value in decimal.

Values 0 — 7

dot1pmask — This 3-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	D	4
Hexadecimal	0xH	0x4
Binary	0bBBB	0b100

To select a range from 4 up to 7 specify *p-value* of 4 and a *mask* of 0b100 for value and mask.

Default 7 (decimal) (exact match)

Values 1 — 7 (decimal)

dst-mac

Syntax **dst-mac** *ieee-address* [*ieee-address-mask*]
no dst-mac

Context config>qos>sap-ingress>mac-criteria>entry

Description Configures a destination MAC address or range to be used as a Service Ingress QoS policy match criterion.

The no form of this command removes the destination mac address as the match criterion.

Default none

Parameters *ieee-address* — The MAC address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — A 48-bit mask to match a range of MAC address values.

This 48-bit mask can be configured using the following formats:

Format Style	Format Syntax	Example
Decimal	`DDDDDDDDDDDDDD`	`281474959933440`
Hexadecimal	`0xHHHHHHHHHHHH`	`0xFFFFFF000000`
Binary	`0bBBBBBBB...B`	`0b11110000...B`

All packets with a source MAC OUI value of 00-03-FA subject to a match condition should be specified as: 0003FA000000 0x0FFFFF000000

Default 0xFFFFFFFFFFFF (hex) (exact match)

Values 0x00000000000000 — 0xFFFFFFFFFFFF (hex)

etype

Syntax **etype** *0x0600..0xffff*
no etype

Context config>qos>sap-ingress>mac-criteria>entry

Description Configures an Ethernet type II value to be used as a service ingress QoS policy match criterion.

The Ethernet type field is a two-byte field used to identify the protocol carried by the Ethernet frame. For e.g. 0800 is used to identify the IP v4 packets.

The Ethernet type field is used by the Ethernet version-II frames. IEEE 802.3 Ethernet frames do not use the type field. For IEEE 802.3 frames use the dsap, ssap or snap-pid fields as match criteria.

The snap-pid field, etype field, ssap and dsap fields are mutually exclusive and cannot be part of the same match criteria.

The no form of this command removes the previously entered etype field as the match criteria.

Default None

Parameters *etype-value* — The Ethernet type II frame Ethertype value to be used as a match criterion expressed in hexadecimal.

Values 0x0600 — 0xFFFF

src-mac

Syntax **src-mac** *ieee-address* [*ieee-address-mask*]
no src-mac

Context config>qos>sap-ingress>mac-criteria>entry

Description This command configures a source MAC address or range to be used as a service ingress QoS policy match criterion.

The **no** form of this command removes the source mac as the match criteria.

Default none

Parameters *ieee-address* — Enter the 48-bit IEEE mac address to be used as a match criterion.

Values HH:HH:HH:HH:HH:HH or HH-HH-HH-HH-HH-HH where H is a hexadecimal digit

ieee-address-mask — This 48-bit mask can be configured using:

This 48 bit mask can be configured using the following formats

Format Style	Format Syntax	Example
Decimal	`DDDDDDDDDDDDDD`	`281474959933440`
Hexadecimal	`0xHHHHHHHHHHHH`	`0x0FFFFF000000`
Binary	`0bBBBBBBB...B`	`0b11110000...B`

To configure all packets with a source MAC OUI value of 00-03-FA are subject to a match condition, then the entry should be specified as: 003FA000000 0xFFFFFF000000

Default 0xFFFFFFFFFFFF (hex) (exact match)

Values 0x00000000000000 — 0xFFFFFFFFFFFF (hex)

Service Meter QoS Policy Commands

meter

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

Context config>qos>sap-ingress

Description This command creates the context to configure an ingress service access point (SAP) QoS policy meter.

This command allows the creation of multipoint meters. Only multipoint meters can receive ingress packets that need flooding to multiple destinations. By separating the unicast for multipoint traffic at service ingress and handling the traffic on separate multipoint meters special handling of the multipoint traffic is possible. Each meter acts as an accounting and (optionally) policing device offering precise control over potentially expensive multicast, broadcast and unknown unicast traffic. Only the back-end support of multipoint traffic (between the forwarding class and the meter based on forwarding type) needs to be defined. The individual classification rules used to place traffic into forwarding classes are not affected. Meters must be defined as multipoint at the time of creation within the policy.

The multipoint meters 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 meter.

When an ingress SAP QoS policy with multipoint meters is applied to an Epipe SAP, the multipoint meters are not created.

Any billing or statistical queries about a multipoint meter on a non-multipoint service returns zero values. Any meter parameter information requested about a multipoint meter on a non-multipoint service returns the meter parameters in the policy. Multipoint meters would not be created for non-multipoint services.

The **no** form of this command removes the *meter-id* from the SAP ingress QoS policy and from any existing SAPs using the policy. Any forwarding class mapped to the meter, will revert to their default meters. When a meter is removed, any pending accounting information for each SAP meter created due to the definition of the meter in the policy is discarded.

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

Values 1 — 32

adaptation-rule

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

Context config>qos>sap-ingress>meter

Description This command defines the method used by the system to derive the operational CIR and PIR settings when the meter is provisioned in hardware. For the CIR and PIR parameters, individually the system attempts to find the best operational rate depending on the defined constraint.

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

Default **adaptation-rule cir closest pir closest**

Parameters *adaptation-rule* — Specifies the adaptation rule to be used while computing the operational CIR or PIR value.

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

max — The **max** (maximum) option is mutually exclusive with the **min** and **closest** options. When **max** is defined, the operational PIR/CIR will be the next multiple of 8 that is equal to or lesser than the specified rate.

min — The **min** (minimum) option is mutually exclusive with the **max** and **closest** options. When **min** is defined, the operational PIR/CIR will be the next multiple of 8 kbps that is equal to or higher than the specified rate.

closest — The **closest** parameter is mutually exclusive with the **min** and **max** parameter. When **closest** is defined, the operational PIR/CIR will be the next multiple of 8 kbps that is closest to the specified rate.

cbs

Syntax **cbs** *size-in-kbits*
no cbs

Context config>qos>sap-ingress>meter

Description This command provides a mechanism to override the default CBS for the meter. The committed burst size parameter specifies the maximum burst size that can be transmitted by the source while still complying with the CIR. If the transmitted burst is lower than the CBS value then the packets are marked as in-profile by the meter to indicate that the traffic is complying meter configured parameters.

The **no** form of this command returns the CBS size to the default value.

Default default

Parameters *size-in-kbits* — Specifies the size parameter is an integer expression of the number of kilobits reserved for the meter. For example, if a value of 100 KBits is desired, then enter the value 100. The bucket size is rounded off to the next highest 4096 bytes boundary.

Values 4 — 2146959, default

mbs

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

Context config>qos>sap-ingress>meter

Description This command provides the explicit definition of the maximum amount of tokens allowed for a specific meter. The value is given in Kilobits and overrides the default value for the context.

In case of trtcm, the maximum burst size parameter specifies the maximum burst size that can be transmitted by the source at the PIR while complying with the PIR. If the transmitted burst is lower than the MBS value then the packets are marked as out-profile by the meter to indicate that the traffic is not complying with CIR, but complying with PIR.

In case of srTCM, the MBS parameter specifies the maximum burst size that can be transmitted by the source while not complying with the CIR. The transmitted burst is lower than the MBS value then the packets are marked as out-profile by the meter to indicate that the traffic is not complying with CIR.

If the packet burst is higher than MBS then packets are marked as red are dropped by the meter.

The **no** form of this command returns the MBS size assigned to the meter to the value.

Default default

Parameters *size-in-kbits* — This parameter is an integer expression of the maximum number of Kilobits of buffering allowed for the meter. For example, for a value of 100 KBits, enter the value 100.

Values

Values 4— 2146959, default

mode

Syntax **mode** {**trtcm1** | **trtcm2** | **srtcm**}
no mode

Context config>qos>sap-ingress>meter

Description This command defines the mode of the meter. The mode can be configured as Two Rate Three Color Marker (trTCM1) or Single Rate Three Color Marker (srTCM). The mode command can be executed at anytime.

Note:

1. The meter counters are reset to zero when the meter mode is changed.
2. For more information on the interpretation of rate parameters when the meter mode is configured as "trtcm2", refer to the command description of the policer rate command.

The **no** form of the command sets the default mode **trtcm1**.

Default trtcm1

Parameters **trtcm1 —** Implements the policing algorithm defined in RFC2698. Meters the packet stream and marks its packets either green, yellow, or red. A packet is marked red if it exceeds the PIR. Otherwise, it is marked either yellow or green depending on whether it exceeds or doesn't exceed the CIR. The trTCM1 is useful, for example, for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate. Two token buckets are used, the CBS bucket and the MBS bucket. Tokens are added to the buckets based on the CIR and PIR rates. The algorithm deducts tokens from both the CBS and the MBS buckets to determine a profile for the packet.

trtcm2 — Implements the policing algorithm defined in RFC4115. Meters the packet stream and marks its packets either green, yellow, or red. A packet is marked red if it exceeds the PIR. Otherwise, it is marked either yellow or green depending on whether it exceeds or does not exceed the CIR. The trtcm2 is useful, for example, for ingress policing of a service, where a peak rate needs to be enforced separately from a committed rate. Two token buckets are used, the CBS bucket and the EBS bucket. Tokens are added to the buckets based on the CIR and EIR rates. The algorithm deducts tokens from either the CBS bucket (that is, when the algorithm identifies the packet as in-profile or green packet) or the EBS bucket (that is,when the algorithm identifies the packet as out-of-profile or yellow packet).

Note: In this mode, the value of the PIR rate configured by the user is used as the policer’s EIR rate.

srtcm — Meters an IP packet stream and marks its packets either green, yellow, or red. Marking is based on a CIR and two associated burst sizes, a CBS and an Maximum Burst Size (MBS). A packet is marked green if it doesn't exceed the CBS, yellow if it does exceed the CBS, but not the MBS, and red otherwise. The srTCM is useful, for example, for ingress policing of a service, where only the length, not the peak rate, of the burst determines service eligibility.

rate

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

Context config>qos>sap-ingress>meter

Description This command defines the administrative PIR and CIR parameters for the meter.

The rate command can be executed at anytime, altering the PIR and CIR rates for all meters created through the association of the SAP Ingress QoS policy with the meter-id.

Note: When the meter mode is configured in trtcm2 mode, the system interprets the PIR rate parameter as EIR for use by RFC 4115 algorithm.

The **no** form of the command returns all meters created with the meter-id by association with the QoS policy to the default PIR and CIR parameters (max, 0).

Default **rate cir 0 pir max** — The max default specifies the amount of bandwidth in kilobits per second (thousand bits per second). The max value is mutually exclusive to the *pir-rate* value.

Parameters **cir** *cir-rate-in-kbps* — The cir parameter overrides the default administrative CIR used by the meter. 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.

The actual CIR rate is dependent on the meter’s **adaptation-rule** parameters and the hardware.

Values 0 — 20000000, max

pir *pir-rate-in-kbps* **—** Defines the administrative PIR rate, in kilobits, for the meter. When this 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. When the **rate** command is executed, a PIR setting is optional.

Fractional values are not allowed and must be given as a positive integer.

The actual PIR rate is dependent on the meter's adaptation-rule parameters and the hardware.

Note: If the meter mode is configured as trtcm2, the system configures the policer's EIR rate, based on the value of the PIR rate configured by the user.

Values 0 — 20000000, max

Show Commands

sap-ingress

Syntax **sap-ingress** [*policy-id*] [**association | match-criteria**]

Context show>qos

Description This command displays SAP ingress QoS policy information.

Parameters *policy-id* — Displays information about the specific policy ID.

Default all SAP ingress policies

Values 1 — 65535

associations- — Displays the policy associations of the sap-ingress policy.

match-criterion- — Displays the match-criterion of the sap-ingress policy.

Sample Output

Show SAP Ingress Output — The following table describes SAP ingress show command output.

Label	Description
`Policy-Id`	The ID that uniquely identifies the policy.
`Scope`	`Exclusive` – Implies that this policy can only be applied to a single SAP. `Template` – Implies that 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`	Specifies the default forwarding class for the policy.
`Criteria-type`	`IP` – Specifies that an IP criteria-based SAP ingress policy is used to select the appropriate ingress meter and corresponding forwarding class for matched traffic. `MAC` – Specifies that a MAC criteria-based SAP is used to select the appropriate ingress meters and corresponding forwarding class for matched traffic.
`Meter`	Displays the meter ID.
Mode	Specifies the configured mode of the meter (trTcm1 or srTcm).

Label	Description (Continued)
CIR Admin	Specifies the administrative Committed Information Rate (CIR) parameters for the meters.
CIR Rule	min — The operational CIR for the meters will be equal to or greater than the administrative rate specified using the rate command. max — The operational CIR for the meter will be equal to or less than the administrative rate specified using the rate command. closest — The operational PIR for the meters will be the rate closest to the rate specified using the rate command without exceeding the operational PIR.
PIR Admin	Specifies the administrative Peak Information Rate (PIR) parameters for the meters.
PIR Rule	min — The operational PIR for the meter will be equal to or greater than the administrative rate specified using the rate command. max — The operational PIR for the meters will be equal to or less than the administrative rate specified using the rate command. closest — The operational PIR for the meters will be the rate closest to the rate specified using the rate command.
CBS	def — Specifies the default CBS value for the meters. value — Specifies the value to override the default reserved buffers for the meters.
MBS	def — Specifies the default MBS value. value — Specifies the value to override the default MBS for the meter.
UCastM	Specifies the default unicast forwarding type meters mapping.
MCastM	Specifies the overrides for the default multicast forwarding type meter mapping.
BCastM	Specifies the default broadcast forwarding type meters mapping.
UnknownM	Specifies the default unknown unicast forwarding type meters mapping.
Match Criteria	Specifies an IP or MAC criteria entry for the policy.

Label	Description (Continued)
Entry	
DSCP	Specifies a DiffServ Code Point (DSCP) name used for an ingress SAP QoS policy match.
FC	Specifies the entry’s forwarding class.
Src MAC	Specifies a source MAC address or range to be used as a Service Ingress QoS policy match.
Dst MAC	Specifies a destination MAC address or range to be used as a Service Ingress QoS policy match.
Dot1p	Specifies a IEEE 802.1p value to be used as the match.
Ethernet-type	Specifies an Ethernet type II Ethertype value to be used as a Service Ingress QoS policy match.
FC	Specifies the entry’s forwarding class.
Service Association	
Service-Id	The unique service ID number which identifies the service in the service domain.
Customer-Id	Specifies the customer ID which identifies the customer to the service.
SAP	Specifies the a Service Access Point (SAP) within the service where the SAP ingress policy is applied.
Classifiers required	Indicates the number of classifiers for a VPLS or Epipe service.
Meters required	Indicates the number of meters for a VPLS or Epipe service.
Sub-Criteria-type	Displays the configured sub-criteria-type

Sample Output

```
*A:Dut-G# show qos sap-ingress 100 detail

===============================================================================
QoS Sap Ingress
===============================================================================
-------------------------------------------------------------------------------
Sap Ingress Policy (100)
-------------------------------------------------------------------------------
Policy-id                 : 100               Scope                : Template
Default FC                : be
Criteria-type             : MAC
Sub-Criteria-type         :dot1p-only
```

```
Accounting                : packet-based
Classifiers Allowed       : 16                  Meters Allowed       : 8
Classifiers Reqrd (VPLS)  : 16                  Meters Reqrd (VPLS)  : 9 Exceeded
Classifiers Reqrd (EPIPE) : 8                   Meters Reqrd (EPIPE) : 8
Description    : (Not Specified)

-------------------------------------------------------------------------------
Meter Mode  CIR Admin    CIR Rule   PIR Admin   PIR Rule   CBS Admin MBS Admin
-------------------------------------------------------------------------------
1     TrTcm     0         closest       max       closest   def       def
2     TrTcm     0         closest       max       closest   def       def
3     TrTcm     0         closest       max       closest   def       def
4     TrTcm     0         closest       max       closest   def       def
5     TrTcm     0         closest       max       closest   def       def
6     TrTcm     0         closest       max       closest   def       def
7     TrTcm     0         closest       max       closest   def       def
8     TrTcm     0         closest       max       closest   def       def
9     TrTcm     0         closest       max       closest   def       def
10    TrTcm     0         closest       max       closest   def       def
11    TrTcm     0         closest       max       closest   def       def
12    TrTcm     0         closest       max       closest   def       def

-------------------------------------------------------------------------------
FC              UCastM         MCastM         BCastM         UnknownM
-------------------------------------------------------------------------------
l2              4              def            def            def
af              3              def            def            def
l1              5              def            def            def
h2              7              def            def            def
ef              2              def            def            def
h1              6              def            def            def
nc              8              def            def            def
-------------------------------------------------------------------------------
Match Criteria
-------------------------------------------------------------------------------
Entry                     : 1
Description    : (Not Specified)
Src MAC                   :                   Atm-Vci              : Disabled
Dst MAC                   :                   Dot1p                : 1/7
Ethernet-type             : Disabled
FC                        : af

Entry                     : 2
Description    : (Not Specified)
Src MAC                   :                   Atm-Vci              : Disabled
Dst MAC                   :                   Dot1p                : 2/7
Ethernet-type             : Disabled
FC                        : ef

Entry                     : 3
Description    : (Not Specified)
Src MAC                   :                   Atm-Vci              : Disabled
Dst MAC                   :                   Dot1p                : 3/7
Ethernet-type             : Disabled
FC                        : l1

Entry                     : 4
Description    : (Not Specified)
Src MAC                   :                   Atm-Vci              : Disabled
```

```
Dst MAC                   :                   Dot1p                : 4/7
Ethernet-type             : Disabled
FC                        : l2

Entry                     : 5
Description    : (Not Specified)
Src MAC                   :                   Atm-Vci              : Disabled
Dst MAC                   :                   Dot1p                : 5/7
Ethernet-type             : Disabled
FC                        : h1

Entry                     : 6
Description    : (Not Specified)
Src MAC                   :                   Atm-Vci              : Disabled
Dst MAC                   :                   Dot1p                : 6/7
Ethernet-type             : Disabled
FC                        : h2

Entry                     : 7
Description    : (Not Specified)
Src MAC                   :                   Atm-Vci              : Disabled
Dst MAC                   :                   Dot1p                : 7/7
Ethernet-type             : Disabled
FC                        : nc

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Service-Id                : 100 (Epipe)       Customer-Id          : 1
 - SAP : 1/1/1:100

===============================================================================
*A:Dut-G#


*A:qos1# show qos sap-ingress 102 detail
===============================================================================
QoS Sap Ingress
===============================================================================
Sap Ingress Policy (102)
-------------------------------------------------------------------------------
Policy-id          : 102                      Scope              : Template
Default FC         : be
Criteria-type             : MAC
Sub-Criteria-type         : dot1p-only
Accounting                : packet-based
Classifiers Allowed: 32                       Meters Allowed     : 16
Classifiers Used   : 32                       Meters Used        : 16
-------------------------------------------------------------------------------
Meter Mode  CIR Admin    CIR Rule   PIR Admin   PIR Rule   CBS       MBS
-------------------------------------------------------------------------------
1     TrTcm     100       closest       200       closest   32        128
2     TrTcm     100       closest       200       closest   32        128
3     TrTcm     100       closest       200       closest   32        128
4     TrTcm     100       closest       200       closest   32        128
5     TrTcm     100       closest       200       closest   32        128
6     TrTcm     100       closest       200       closest   32        128
7     TrTcm     100       closest       200       closest   32        128
8     TrTcm     100       closest       200       closest   32        128
```

```
9     TrTcm     100       closest       200       closest   32        128
10    TrTcm     100       closest       200       closest   32        128
11    TrTcm     100       closest       200       closest   32        128
12    TrTcm     100       closest       200       closest   32        128
13    TrTcm     100       closest       200       closest   32        128
14    TrTcm     100       closest       200       closest   32        128
15    TrTcm     100       closest       200       closest   32        128
16    TrTcm     100       closest       200       closest   32        128
-------------------------------------------------------------------------------
FC                  UCastM         MCastM         BCastM         UnknownM
-------------------------------------------------------------------------------
be                  1              11             16             16
l2                  8              16             16             16
af                  7              15             16             16
l1                  6              14             16             16
h2                  5              13             16             16
ef                  4              12             16             16
h1                  3              10             16             16
nc                  2              9              16             16
-------------------------------------------------------------------------------
Match Criteria
-------------------------------------------------------------------------------
Entry              : 1
Src MAC            :
Dst MAC            :                       Dot1p              : 7/7
Ethernet-type      : Disabled
FC                 : nc

Entry              : 2
Src MAC            :
Dst MAC            :                       Dot1p              : 6/7
Ethernet-type      : Disabled
FC                 : h1

Entry              : 3
Src MAC            :
Dst MAC            :                       Dot1p              : 5/7
Ethernet-type      : Disabled
FC                 : ef

Entry              : 4
Src MAC            :
Dst MAC            :                       Dot1p              : 4/7
Ethernet-type      : Disabled
FC                 : h2

Entry              : 5
Src MAC            :
Dst MAC            :                       Dot1p              : 3/7
Ethernet-type      : Disabled
FC                 : l1

Entry              : 6
Src MAC            :
Dst MAC            :                       Dot1p              : 2/7
Ethernet-type      : Disabled
FC                 : af

Entry              : 7
```

```
Src MAC            :
Dst MAC            :                          Dot1p              : 1/7
Ethernet-type      : Disabled
FC                 : l2
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Service-Id         : 102 (VPLS)               Customer-Id        : 1
 - SAP : 1/1/3:102
 - SAP : 1/1/7:102
===============================================================================
*A:qos1#
```

For SAS-MX:

```
*A:qos1# show qos sap-ingress 102 detail
===============================================================================
QoS Sap Ingress
===============================================================================
-------------------------------------------------------------------------------
Sap Ingress Policy (102)
-------------------------------------------------------------------------------
Policy-id          : 102                      Scope              : Template
Default FC         : be
Criteria-type             : MAC
Sub-Criteria-type         : dot1p-only
Accounting                : packet-based
Classifiers Allowed: 32                       Meters Allowed     : 16
Classifiers Used   : 32                       Meters Used        : 16
-------------------------------------------------------------------------------
Meter Mode  CIR Admin    CIR Rule   PIR Admin   PIR Rule   CBS Admin MBS Admin
            CIR Oper                PIR Oper               CBS Oper  MBS Oper
-------------------------------------------------------------------------------
1     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
2     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
3     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
4     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
5     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
6     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
7     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
8     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
9     TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
10    TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
11    TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
12    TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
13    TrTcm     100       closest       200       closest   def       def
```

```
                104                     200                 def       500
14    TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
15    TrTcm     100       closest       200       closest   def       def
                104                     200                 def       500
16    TrTcm     100       closest       200       closest   def       def
             104                   200              def      500
-------------------------------------------------------------------------------
FC                    UCastM         MCastM         BCastM         UnknownM
-------------------------------------------------------------------------------
be                    1              11             16             16
l2                    8              16             16             16
af                    7              15             16             16
l1                    6              14             16             16
h2                    5              13             16             16
ef                    4              12             16             16
h1                    3              10             16             16
nc                    2              9              16             16
-------------------------------------------------------------------------------
Match Criteria
-------------------------------------------------------------------------------
Entry               : 1
Src MAC             :
Dst MAC
===============================================================================
*A:qos1#
```

Access Egress QoS Policies

In This Section

This section provides information to configure Access Egress QoS policies using the command line interface.

Topics in this section include:

Overview

An access egress policy defines the queuing for the traffic egressing on the access ports. Access-egress queue policies are used at the Ethernet port and define the bandwidth distribution for the various FC/queue traffic egressing on the Ethernet port.

There is one default access egress policy which is identified as policy ID 1. Each policy has 8 queues available. The Forwarding Class to queue mapping is predefined and cannot be changed. The queue parameters like CIR, PIR, etc. can be modified. The default policy can be copied but they cannot be deleted or modified.

Basic Configurations

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

- Have a unique access egress QoS policy ID.
- Have a QoS policy scope of template or exclusive.
- Queue parameters can be modified, but not deleted.

Create Access Egress QoS Policies

Configuring and applying QoS policies is optional. If no QoS policy is explicitly applied to an access port, a default QoS policy 1 is applied.

Access Egress QoS Policy

To create an access egress policy, you must define the following:

- A new policy ID value. The system will not dynamically assign a value.
- Specify the scope. A QoS policy must be defined as having either an exclusive scope for use with a single port, or a template scope which enables its use with multiple access ports.
- Include a description. The description provides a brief overview of policy features.
- By default all FCs are mapped to 8 queues available at the port according to Table 31, Forwarding Class to Queue-ID Map, on page 81.
- Remark - By default, remarking is disabled. If remarking is enabled by default 'use-dot1p' is used and the Dot1p values in the customer packets which are egressing on this access

port are marked according to the FC-Dot1p marking map Table 26, Default Access Egress Policy ID 1 Definition, on page 59. The user has the option to specify either dot1p or dscp or both dot1p and dscp, needs to be used for marking the packets egressing the port.

- If the user wants to change the FC-Dot1p or/and dscp marking map, the forwarding class and the Dot1p or/and dscp marking values for the in-profile and out-profile packets must be specified.

The following displays the access egress QoS policy configuration:

```
Sample configuration with remarking set to "use-dscp":

*A:7210-SAS-M>config>qos>access-egress# info
----------------------------------------------
            description "policy-1"
            remarking use-dscp
            queue 1
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
            exit
            queue 5
                adaptation-rule cir max pir min
                rate cir 10000 pir 11690
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
            fc be create
            exit
----------------------------------------------
*A:7210-SAS-M>config>qos>access-egress#

Sample configuration with remarking set to "all":

*A:7210-SAS-M>config>qos>access-egress# info
----------------------------------------------
            description "policy-2"
            remarking all
            scope exclusive
            queue 1
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
                adaptation-rule cir max pir max
                rate cir 100000 pir 126583
            exit
            queue 5
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
            fc l2 create
            exit
----------------------------------------------
*A:7210-SAS-M>config>qos>access-egress#
```

Sample configuration with remarking set to "use-dot1p":

```
*A:7210-SAS-M>config>qos>access-egress# info
----------------------------------------------
            description "policy-3"
            remarking use-dot1p
            queue 1
            exit
            queue 2
            exit
            queue 3
                adaptation-rule cir min pir min
                rate cir 18689 pir 26794
            exit
            queue 4
            exit
            queue 5
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
            fc h2 create
                dot1p-in-profile 3
            exit
----------------------------------------------
*A:7210-SAS-M>config>qos>access-egress#
```

Modifying Access Egress QoS Queues

To modify access egress queue parameters specify the following:

- Queue ID value. 8 Queues are identified and are mapped as defined in Table 31, Forwarding Class to Queue-ID Map, on page 81.
- Queue parameters. Egress queues support configuration of CIR and PIR rates.

The following displays the access egress QoS policy configuration:

```
Sample configuration with remarking set to "use-dscp":

*A:7210-SAS-M>config>qos>access-egress# info
----------------------------------------------
            description "policy-1"
            remarking use-dscp
            queue 1
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
            exit
            queue 5
                adaptation-rule cir max pir min
                rate cir 10000 pir 11690
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
            fc be create
            exit
----------------------------------------------
*A:7210-SAS-M>config>qos>access-egress#

Sample configuration with remarking set to "all":

*A:7210-SAS-M>config>qos>access-egress# info
----------------------------------------------
            description "policy-2"
            remarking all
            scope exclusive
            queue 1
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
                adaptation-rule cir max pir max
                rate cir 100000 pir 126583
            exit
            queue 5
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
            fc l2 create
            exit
----------------------------------------------
*A:7210-SAS-M>config>qos>access-egress#
```

Sample configuration with remarking set to "use-dot1p":

```
*A:7210-SAS-M>config>qos>access-egress# info
----------------------------------------------
            description "policy-3"
            remarking use-dot1p
            queue 1
            exit
            queue 2
            exit
            queue 3
                adaptation-rule cir min pir min
                rate cir 18689 pir 26794
            exit
            queue 4
            exit
            queue 5
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
            fc h2 create
                dot1p-in-profile 3
            exit
----------------------------------------------
*A:7210-SAS-M>config>qos>access-egress#
```

Applying Access Egress QoS Policies

Apply access egress policies to the following entities:

- Ethernet ports

A policy can be applied to the ports that are in access mode.

Ethernet Ports

Use the following CLI syntax to apply a access-egress policy to an Ethernet port:

CLI Syntax:

```
config>port#
 ethernet access egress
    qos access-egress-policy-id
```

CLI Syntax:

```
config>port#
 ethernet access egress
    qos access-egress-policy-id
    sap-qos-marking disable
```

The following output displays the port configuration.

```
*A:card-1>config>port# info
----------------------------------------------
                 shutdown
                    ethernet
                        access
                            egress
                                qos 30
                            exit
                        exit
                    exit
----------------------------------------------
*A:card-1>config>port#
```

Default Access Egress QoS Policy Values

The default access egress policy is identified as policy-id 1. The default policy cannot be edited or deleted. The following displays default policy parameters:

```
*A:card-1>config>qos>access-egress# info detail
----------------------------------------------
            description "Default Access egress QoS policy."
            no remarking
            scope template
            queue 1
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
            exit
            queue 2
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
            exit
            queue 3
                adaptation-rule cir closest pir closest
                rate 0 pir max
            exit
            queue 4
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
            exit
            queue 5
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
            exit
            queue 6
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
            exit
            queue 7
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
            exit
            queue 8
                adaptation-rule cir closest pir closest
                rate cir 0 pir max
            exit
----------------------------------------------
*A:card-1>config>qos>access-egress#
```

Table 42: Access Egress Default Policy Details

Field	Default
description	“Default Access egress QoS policy.”
scope	template
queue 1	
adaptation-rule	adaptation-rule cir closest pir closest

Table 42: Access Egress Default Policy Details (Continued)

Field	Default
rate	cir 0 pir max
cbs	default = 8698 bytes
queue 2	
adaptation-rule	adaptation-rule cir closest pir closest
rate	0cir 0 pir max
cbs	default = 8698 bytes
queue 3	
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 8698 bytes
queue 4	
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 8698 bytes
queue 5	
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 8698 bytes
queue 6	
adaptation-rule	cir closest pir closest
rate	cir 0 pir max
cbs	default = 8698 bytes
queue 7	
adaptation-rule	cir closest pir closest
rate	cir 0 pir max
cbs	default = 8698 bytes
queue 8	

Table 42: Access Egress Default Policy Details (Continued)

Field	Default
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 8698 bytes
remarking	no

Table 43: Access Egress Default Policy Details (for 7210 SAS-M and 7210 SAS-T in access uplink mode)

Field	Default
description	“Default Access egress QoS policy.”
scope	template
queue 1	
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
queue 2	
adaptation-rule	adaptation-rule cir closest pir closest
rate	0cir 0 pir max
cbs	default = 3200 bytes
queue 3	
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
queue 4	
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
queue 5	

Table 43: Access Egress Default Policy Details (for 7210 SAS-M and 7210 SAS-T in access uplink mode) (Continued)

Field	Default
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
queue 6	
adaptation-rule	cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
queue 7	
adaptation-rule	cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
queue 8	
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
remarking	no

Table 44 lists the default forwarding class marking values when remarking is enabled on the access egress policy for 7210 SAS devices configured in network mode as well as access-uplink mode:

Table 44: Default FC Marking Values

Default FC value	Network mode	Access uplink mode
af:	dot1p-in-profile 2 dot1p-out-profile 2 dscp-in-profile af11 dscp-out-profile af12	dot1p-in-profile 2 dot1p-out-profile 2

Table 44: Default FC Marking Values (Continued)

Default FC value	Network mode	Access uplink mode
be:	dot1p-in-profile 0 dot1p-out-profile 0 dscp-in-profile be dscp-out-profile be	dot1p-in-profile 0 dot1p-out-profile 0
ef:	dot1p-in-profile 5 dot1p-out-profile 5 dscp-in-profile ef dscp-out-profile ef	dot1p-in-profile 5 dot1p-out-profile 5
h1:	dot1p-in-profile 6 dot1p-out-profile 6 dscp-in-profile nc1 dscp-out-profile nc1	dot1p-in-profile 6 dot1p-out-profile 6
h2:	dot1p-in-profile 4 dot1p-out-profile 4 dscp-in-profile af41 dscp-out-profile af41	dot1p-in-profile 4 dot1p-out-profile 4
l1:	dot1p-in-profile 3 dot1p-out-profile 3 dscp-in-profile af21 dscp-out-profile af22	dot1p-in-profile 3 dot1p-out-profile 3
l2:	dot1p-in-profile 1 dot1p-out-profile 1 dscp-in-profile cs1 dscp-out-profile cs1	dot1p-in-profile 1 dot1p-out-profile 1
nc:	dot1p-in-profile 7 dot1p-out-profile 7 dscp-in-profile nc2 dscp-out-profile nc2	dot1p-in-profile 7 dot1p-out-profile 7

Deleting QoS Policies

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

A QoS policy cannot be deleted until it is removed from all access ports where they are applied.

```
*A:card-1>config>qos# no access-egress 30
MINOR: CLI Could not remove Access egress policy "30" because it is in use.
```

Removing a Policy from the QoS Configuration

CLI Syntax: `config>qos# no access-egress` *`policy-id`*

Example:

```
config>qos# no access-egress 100
config>qos# no access-egress 1010
```

Access Egress QoS Policy Command Reference

Command Hierarchies

Configuration Commands

```
config
    — qos
            — access-egress policy-id [create]
            — no access-egress policy-id
                    — description description-string
                    — no description
                    — fc fc-name [create]
                    — no fc fc-name
                            — dot1p-in-profile dot1p-value
                            — no dot1p-in-profile
                            — dot1p-out-profile dot1p-value
                            — no dot1p-out-profile
                            — dscp-in-profile dscp-name
                            — no dscp-in-profile
                            — dscp-out-profile dscp-name
                            — no dscp-out-profile
                    —  queue queue-id
                            — adaptation-rule [cir adaptation-rule] [pir adaptation-rule]
                            — no adaptation-rule
                            — rate cir cir-rate [pir pir-rate]
                            — no rate
                    — remark policy-id
                    — no remark
                    — remarking {use-dot1p | use-dscp | all}
                    — no remarking
                    — scope {exclusive | template}
                    — no scope
```

Operational Commands

— **config**
  — **qos**
    — **copy sap-ingress** *src-pol dst-pol* **overwrite**

Show Commands

show
— **qos**
  — **access-egress** [*policy-id*] [**association**| **detail**]

Configuration Commands

Generic Commands

description

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

Context config>qos>access-egress

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

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

The **no** form of this command removes any description string from the context.

Default No description is associated with the configuration context.

Parameters *description-string* — 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.

access-egress

Syntax **access-egress** *policy-id* [**create**]
no access-egress *policy-id*

Context config>qos

Description This command is used to create or edit an access egress QoS policy. The egress policy defines the remark policy for the traffic egressing on the access port. Remarking is disabled by default on the access egress policies. The policy can be applied to multiple access ports. The access egress policy is common to services (SAPs) that are all egressing on a particular port.

Any changes made to an existing policy are applied to all access ports on which the policy is specified.

The system uses the access egress policy for marking only if the port with which this policy is associated is enabled for port-based marking (that is, the command sap-qos-marking is set to disable). When port-based marking is enabled, the system is capable of marking all the packets egressing out of the port with either dot1p or dscp or both (that is, both dot1p and dscp). If remarking is enabled and the remark policy is of type ‘dot1p’ or ‘dot1p-lsp-exp-shared’ then the dot1p bits are marked in the packet based on the FC to dot1p values specified in the remark policy. If remarking is enabled and the remark policy is of type ‘dscp’ then the IP DSCP bits are marked in the packet. If remarking is enabled and the remark policy is of type ‘dot1p-dscp’ then both dot1p and IP DSCP bits are marked in the packet.

Note: When port-based marking is enabled and marking for both dot1p and IP DSCP bits is configured, the system marks dot1p and IP DSCP bits for all the packets sent out of both L2 SAPs and L3 SAPs. It is recommended that if both L2 and L3 SAPs are configured on the same port, then remark policy of type dot1p, that marks only dot1p bits be used.

The **no** form of this command deletes the access-egress policy. A policy cannot be deleted until it is removed from all access ports where it is applied. When an access-egress policy is removed from an access port, the access port will revert to the default access-egress policy-id 1.

This command is used to create or edit a access egress QoS policy. The egress policy defines the queue parameters (CIR/PIR) for each of the forwarding class traffic as they egress on the access port. Policies in effect are templates that can be applied to multiple access ports as long as the scope of the policy is template. There are 8 queues always available per port for which parameters are configurable.

Parameters *policy-id* — The value that uniquely identifies the access-egress policy.

Values 1 — 65535

create — The keyword used to create an access-egress policy. The **create** keyword requirement can be enabled/disabled in the **environment**>**create** context.

fc

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

Context config>qos>access-egress

Description This command defines the **fc** node within the access egress QoS policy is used to contain the explicitly defined Dot1p marking commands for the *fc-name.*

Note that when the mapping for the *fc-name* and Dot1p marking is not defined, the node for *fc-name* is not displayed in the show configuration or save configuration output.

The **no** form of the command removes the explicit Dot1p marking commands for the *fc-name*.

fc-name **—** Specifies the forwarding class for which 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 an access-egress policy. The **create** keyword requirement can be enabled/ disabled in the **environment>create** context.

dot1p-in-profile

Syntax **dot1p-in-profile** *dot1p-value*
no dot1p-in-profile

Context config>qos>access-egress>fc

Description This command explicitly defines the egress IEEE 802.1P (Dot1p) bits marking for fc-name. All packets belonging to a particular FC that have either an IEEE 802.1Q or IEEE 802.1P encapsulation use the explicitly defined Dot1p-value. If the egress packets for fc-name are not IEEE 802.1Q or IEEE 802.1P encapsulated, the **dot1p** command has no effect. The dot1p-in-profile dot1p-value and dot1p-out-profile dot1p-value structure will add the capability to mark Dot1p on an egress access port the in and out of profile packets. If the user has not explicitly configured the FC-Dot1p map the marking of packets is still done according to Table 26, Default Access Egress Policy ID 1 Definition, on page 59. User can explicitly define the new Dot1P values using these commands.

The **no** form of the command sets the IEEE 802.1P or IEEE 802.1Q priority bits to default FC-Dot1P marking map as listed in Table 26, Default Access Egress Policy ID 1 Definition, on page 59.

Default not

Parameters *dot1p-value* — This value specifies the unique IEEE 802.1P value that will match the dot1p rule. If the command is executed multiple times with the same *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 — 7

dot1p-out-profile

Syntax **dot1p-out-profile** *dot1p-value*
no dot1p-out-profile

Context config>qos>access-egress>fc

Description This command explicitly defines the egress IEEE 802.1P (dot1p) bits marking for fc-name. All packets belonging to a particular FC that have either an IEEE 802.1Q or IEEE 802.1P encapsulation use the explicitly defined dot1p-value. If the egress packets for fc-name are not IEEE 802.1Q or IEEE 802.1P encapsulated, the **dot1p** command has no effect. The **dot1p-in-profile** *dot1p-value* and **dot1p-out-profile** *dot1p-value* commands will provide the capability to mark Dot1p on an egress access port for the in and out of profile packets. If the user has not explicitly configured this FC-Dot1p map the marking of packets is according to FC-Dot1P marking table as listed in Table 26, Default Access Egress Policy ID 1 Definition, on page 59. User can explicitly define the new Dot1P values using these commands.

The **no** form of the command sets the IEEE 802.1P or IEEE 802.1Q priority bits to default FC-Dot1P marking map as listed in Table 26, Default Access Egress Policy ID 1 Definition, on page 59.

Parameters *dot1p-value* — This value specifies the unique IEEE 802.1P value that will match the dot1p rule. If the command is executed multiple times with the same *dot1p-value*, the previous forwarding class and enqueuing priority is completely overridden by the new parameters or defined to be inherited when a forwarding class or enqueuing priority parameter is missing.

A maximum of eight dot1p rules are allowed on a single policy.

Values 0 — 7

dscp-out-profile

Syntax **dscp-out-profile** *dscp-name*
no dscp-out-profile

Context config>qos>access-egress>fc

Description This command specifies the out-of-profile DSCP name for the forwarding class. The corresponding DSCP value will be used for all IP packets requiring marking the egress on this forwarding class queue that are out-of-profile.

When multiple DSCP names are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The no form of this command reverts to the factory default out-of-profile dscp-name.

Parameters *dscp-name* — Specifies the DSCP name.

Values 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

dscp-in-profile

Syntax **dscp-in-profile** *dscp-name*
no dscp-in-profile

Context config>qos>access-egress>fc

Description This command specifies the in-profile DSCP name for the forwarding class. The corresponding DSCP value will be used for all IP packets requiring marking the egress on this forwarding class queue that are in profile.

When multiple DSCP names are associated with the forwarding class at network egress, the last name entered will overwrite the previous value.

The **no** form of this command reverts to the factory default in-profile dscp-name.

Parameters *dscp-name* — Specifies the DSCP name.

Values 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

queue

Syntax **queue** *queue-id*

Context config>qos>access-egress

Description This command creates the context to modify Queue parameters associated with a particular queue. The queue is identifiable by queue-id and FCs are mapped into the queues according to Table 31, Forwarding Class to Queue-ID Map, on page 81.

The **no** form of this command is not supported

Default none

Parameters *queue-id* — Specifies the access egress queue-id associated with an FC according to Table 31, Forwarding Class to Queue-ID Map, on page 81 .

Values 1 — 8

Access Egress Queue QoS Policy Commands

adaptation-rule

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

Context config>qos>access-egress>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 **cir** and **pir** apply.

Default adaptation-rule pir closest cir closest

Parameters *adaptation-rule* — Specifies the adaptation rule to be used while computing the operational CIR or PIR value.

Values **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.

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

rate

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

Context config>qos>access-egress>queue

Description This command defines the administrative Peak Information Rate (PIR) and the administrative Committed Information Rate (CIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets through the port. 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. The CIR defines the rate at which the system prioritizes the queue over other queues competing for the same bandwidth.

The rate command can be executed at anytime, altering the PIR and CIR rates for all queues created on the access ports.

The **no** form of this command returns all queues created with the queue-id by association with the QoS policy to the default PIR and CIR parameters (max, 0).

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

Values 0 — 1000000, **max**

7210 SAS-M 24F 2XFP (the M w/10G ports): 0 — 10000000, max

Default 0

pir-rate — Defines the administrative PIR rate, in kilobits, for the queue. When the **rate** command is executed, a PIR setting is optional. 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.

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

Values 1 — 1000000, **max**

7210 SAS-M 24F 2XFP (the M w/10G ports): 0 — 10000000, max

Default max

remark

Syntax **remark** *policy-id*
[**no**] **remark**

Context config>qos>access-egress

Description This command specifies the remarking policy for the access egress policy.

Only remark policy of type dot1p or dot1p-lsp-exp-shared or dscp or dot1p-dscp is allowed for use with access-egress policy.

Parameters *policy-id* — The value that uniquely identifies the remark policy.

Values 1 — 655353

remarking

Syntax [**no**] **remarking {use-dot1p|use-dscp|all}**
remarking

Context config>qos>access-egress
config>qos>network>egress

Description This command enables the system to remark egress packets sent out of access ports and hybrid ports. The user can specify if either dot1p, or dscp, or both needs to be used for marking the packets egressing the port.

The **no** form of the command disables remarking.

When 7210 SAS-M and 7210 SAS-T is operated in access-uplink mode, when remarking is enabled, only the FC to dot1p bit value specified by the user is used to mark all the traffic (L2 and IPv4 traffic) sent out of both access ports and access-uplink ports.

When 7210 SAS-M is operated in network mode, marking support is available as given below:

On access port egress, the behavior is as follows:

- If 'use-dot1p' is configured, then the dot1p bits are marked in the packet header for all traffic sent out of both L2 SAPs and L3 SAPs configured on that access port.
- If 'use-dscp' is configured, then the IP DSCP bits are marked in the packet header for IPv4 traffic sent out of both L2 and L3 SAPs configured on that access port. Note: DSCP marking also marks the IPv4 packets associated with SAPs configured in an L2 VPN service. To avoid this it is recommended to use only dot1p marking on access ports, when SAPs belonging to both L3 services and L2 VPN services are configured on the port.
- If 'all' is configured, then the Dot1p bits are marked in the packet header for all traffic (L2 and IPv4) sent out of both L2 and L3 SAPs and the IP DSCP bits are marked in the packet

header for all IPv4 traffic sent out of both L2 and L3 SAPs configured on that access port. Note: DSCP marking also marks the packets associated with SAPs configured in an L2 VPN service. To avoid this it is recommended to use only dot1p marking on access ports, when SAPs belonging to both L3 services and L2 VPN services are configured on the port.

On hybrid port egress, the behavior is as follows:

- If use-dot1p is configured, then the dot1p bits are marked in the packet header for all traffic sent out of both L2 SAPs and L3 SAPs configured on that hybrid port. The dot1p bits is also marked in the MPLS traffic and IP control and management traffic sent out of network IP interfaces configured on that hybrid port.
- If use-dscp is configured, then the IP DSCP bits are marked in the packet header for IPv4 traffic sent out of L3 SAPs configured on that hybrid port. The DSCP bits is also marked in the IP control and management traffic sent out of network IP interfaces configured on that hybrid port.
- If 'all' is configured, then the Dot1p bits are marked in the packet header for all traffic (L2 and IPv4) sent out of both L2 and L3 SAPs and the IP DSCP bits are marked in the packet header for all IPv4 traffic sent out of both L2 and L3 SAPs configured on that hybrid port. The dot1p bits is also marked in the MPLS traffic and IP control and management traffic sent out of network IP interfaces configured on that hybrid port. The DSCP bits is also marked only in the IP control and management traffic sent out of network IP interfaces configured on that hybrid port.

If remarking is enabled, by default 'use-dot1p' is used. Dot1p and DSCP values are marked according to Table 44, Default FC Marking Values, on page 325.

Default no remarking - Remarking is disabled by default

Parameters **use-dot1p —** If use-dot1p is configured, then for all the FCs only the configured dot1p values will be used.

use-dscp — If use-dscp is configured, then for all the FCs only the configured dscp values are used.

all — If all is configured, then for all the FCs both the dot1p and dscp values configured is used (if both have been provided).

scope

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

Context config>qos>access-egress

Description This command configures the scope as exclusive or template. The policy’s scope cannot be changed if the policy is applied to multiple ports.

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 one port. If a policy with an exclusive scope is assigned to a second interface an error message is generated. If the policy is removed from the exclusive interface, it will become available for assignment to another exclusive interface.
The system default policies cannot be put into the exclusive scope. An error will be generated if scope exclusive is executed in default access-egress policy (policy-id 1).

template — When the scope of a policy is defined as template, the policy can be applied to multiple ports on the router.

Default QoS policies are configured with template scope. An error is generated if you try to modify the scope parameter from **template** to exclusive **scope** on default policies.

Operational Commands

copy

Syntax **copy access-egress** *src-pol dst-pol* **[overwrite]**

Context config>qos

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

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.

Parameters **access-egress** *src-pol dst-pol* **—** Indicates that the source policy ID and the destination policy ID are 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.

Values 1 — 65535

overwrite — Specifies to replace the existing destination policy. Everything in the existing destination poicy 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.

Show Commands

access-egress

Syntax **access-egress** [*policy-id*] [**association | detail**]

Context show>qos

Description This command displays Access egress QoS policy information.

Parameters *policy-id* — Displays information about the specific policy ID. Displays all access-egress policies if no specific policy-id is entered.

Values 1 — 65535

association — Displays a list of ports on which the policy is applied.

detail — Displays detailed policy information including policy associations.

Access Egress Output — The following table describes Access egress show command output.

Label	Description
`Policy-Id`	The ID that uniquely identifies the policy.
`Remark`	True — Remarking is enabled for all packets that egress this router where the access egress QoS policy is applied. True — Remarking is enabled for all the Dot1q-tagged packets that egress the ports where the access-egress QoS policy is applied and remarking is enabled. The remarking is based on the forwarding class to explicit Dot1P bit mapping defined under the fc name. If explicit mapping FC-Dot1P map not defined marking is based on the default FC-Dot1P marking map as defined in Table 26, Default Access Egress Policy ID 1 Definition, on page 59. False — Remarking is disabled for the policy.
`Description`	A text string that helps identify the policy's context in the configuration file
`Forward Class/FC Name`	Specifies the forwarding class to Dot1p remarking value.
`Explicit/Default`	Explicit — Specifies the egress IEEE 802.1P (dot1p) bits marking for fc-name if explicitly configured.

Label	Description (Continued)
	Default —Specifies the default dot1p value according to FC-Dot1p marking map as defined in Table 26, Default Access Egress Policy ID 1 Definition, on page 59 if explicit values are not configured..
`CIR Admin`	Specifies 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. 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`	Specifies the administrative Peak Information Rate (PIR) parameters for the queue. The PIR defines the maximum rate that the queue can transmit packets through the access port.
`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 — Specifies that the CBS value reserved for the queue.
`Port-Id`	Specifies the physical port identifier that associates the access egress QoS policy.
`Accounting`	Specifies whether the accounting mode is packet-based or frame-based.
`Remark Type`	Displays the type of remarking enabled. It can be "use-dot1p ", "use-dscp" or "all"

Sample Output

```
A:7210-SAS>show>qos# access-egress 1

===============================================================================
QoS Access Egress
===============================================================================
-------------------------------------------------------------------------------
Policy-id      : 1                            Scope        : Template
Remark         : False                        Remark Type  : use-dot1p
Accounting     : packet-based
Description    : Default Access egress QoS policy.
===============================================================================
A:7210-SAS>show>qos#

A:7210-SAS>show>qos# access-egress 2 detail

===============================================================================
QoS Access Egress
===============================================================================
-------------------------------------------------------------------------------
Policy-id      : 2                            Scope        : Template
Remark         : True                         Remark Type  : use-dot1p
Accounting     : packet-based
Description    : (Not Specified)

-------------------------------------------------------------------------------
Queue     CIR Admin           PIR Admin           CBS
          CIR Rule            PIR Rule
-------------------------------------------------------------------------------
1         0                   max                 def
          closest             closest
2         0                   max                 def
          closest             closest
3         0                   max                 def
          closest             closest
4         0                   max                 def
          closest             closest
5         0                   max                 def
          closest             closest
6         0                   max                 def
          closest             closest
7         0                   max                 def
          closest             closest
8         0                   max                 def
          closest             closest

-------------------------------------------------------------------------------
FC Name        Queue-id    Explicit/Default       Explicit/Default
-------------------------------------------------------------------------------
be             1           Default  (in :0)       Default  (out :0)
l2             2           Default  (in :1)       Default  (out :1)
af             3           Default  (in :2)       Default  (out :2)
l1             4           Default  (in :3)       Default  (out :3)
h2             5           Default  (in :4)       Default  (out :4)
ef             6           Default  (in :5)       Default  (out :5)
h1             7           Default  (in :6)       Default  (out :6)
nc             8           Default  (in :7)       Default  (out :7)
```

```
-------------------------------------------------------------------------------
FC Name    Queue-id     DSCP In                 DSCP Out
-------------------------------------------------------------------------------
be             1           be                      be
l2             2           cs1                     cs1
af             3           af11                    af12
l1             4           af21                    af22
h2             5           af41                    af41
ef             6           ef                      ef
h1             7           nc1                     nc1
nc             8           nc2                     nc2

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
No Matching Entries

===============================================================================
A:7210-SAS>show>qos#
```

QoS Port Scheduler Policies

In This Section

This section provides information to configure port scheduler policies using the command line interface.

Topics in this section include:

- Overview on page 348
- Basic Configurations on page 349
- Service Management Tasks on page 351

Overview

Configuring Port Scheduler Policies

The **port-scheduler-policy** command creates a port scheduler template which may be assigned to an egress port. Only one port scheduler policy is allowed per port. There is a “default” port-scheduler policy (which services the queues of the port in a Strict order) associated with each port. To change the behavior, users can associate the port with another port-scheduler policy. The policy contains mode commands to set the mode of scheduling (RR, Strict, WRR, WDRR) and queue commands to set the weight of the queue (only 8 queues per port and queue settings only for WRR/WDRR modes). In WRR/WDRR, a **strict** option treats that particular queue as a strict queue, this leads to a hybrid mode of scheduling (WRR+Strict, WDRR+Strict).

Basic Configurations

A basic QoS port scheduler policy must conform to the following:

- Each QoS port scheduler policy must have a unique policy name.

Creating a QoS Port Scheduler Policy

To create a port scheduler policy, define the following:

- A port scheduler policy name.
- Include a description. The description provides a brief overview of policy features.

Use the following CLI syntax to create a QoS port scheduler policy.

Note that the **create** keyword is included in the command syntax upon creation of a policy.

CLI Syntax:
```
config>qos
 port-scheduler-policy port-scheduler-name [create]
    description description-string
    mode {strict | rr | wrr | wdrr}
    queue queue-id [strict | weight weight]
```

The following displays a port scheduler policy configuration example:

```
*A:card-1>config>qos>port-sched-plcy# info
----------------------------------------------
            mode WRR
            queue 1 weight 1
            queue 2 weight 3
            queue 3 weight 5
            queue 5 weight 5
            queue 6 weight 1
----------------------------------------------
*A:card-1>config>qos>port-sched-plcy#
```

Service Management Tasks

This section discusses the following service management tasks:

- Copying and Overwriting Scheduler Policies on page 351
- Editing QoS Policies on page 353

Copying and Overwriting Scheduler Policies

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

CLI Syntax: `config>qos> copy port-scheduler-policy` *`src-name dst-name`* `[overwrite]`

```
*A:Dut-1>config>qos# port-scheduler-policy psp create
*A:Dut-1>config>qos>port-sched-plcy# mode wdrr
*A:Dut-1>config>qos>port-sched-plcy# queue 1 weight 1
*A:Dut-1>config>qos>port-sched-plcy# queue 2 weight 2
*A:Dut-1>config>qos>port-sched-plcy# queue 3 weight 5
*A:Dut-1>config>qos>port-sched-plcy# info
----------------------------------------------
            mode wdrr
            queue 2 weight 2
            queue 3 weight 5
----------------------------------------------
*A:Dut-1>config>qos>port-sched-plcy# exit
*A:Dut-1>config>qos# exit
*A:Dut-1>config# qos copy port-scheduler-policy psp psp1
*A:Dut-1>config# qos copy port-scheduler-policy psp psp1
MINOR: CLI Destination "psp1" exists - use {overwrite}.

*A:Dut-1>config# show qos port-scheduler-policy
===============================================================================
Port Scheduler Policies
===============================================================================
Policy-Id                     Description                             Mode
-------------------------------------------------------------------------------
default                       Default Port Scheduler policy.         STRICT
psp                                                                   WDRR
psp1                                                                WDRR
===============================================================================
*A:Dut-1>config#


*A:Dut-1>config# show qos port-scheduler-policy psp
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : psp
Accounting        : packet-based
```

```
Mode              : WDRR
Last changed      : 04/12/2001 02:04:16
Queue 1 Weight:   : 1
Queue 2 Weight:   : 2
Queue 3 Weight:   : 5
Queue 4 Weight:   : 1
Queue 5 Weight:   : 1
Queue 6 Weight:   : 1
Queue 7 Weight:   : 1
Queue 8 Weight:   : 1
===============================================================================
*A:Dut-1>config#


*A:Dut-1>config# show qos port-scheduler-policy psp1
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : psp1
Accounting        : packet-based
Mode              : WDRR
Last changed      : 04/12/2001 02:05:00
Queue 1 Weight:   : 1
Queue 2 Weight:   : 2
Queue 3 Weight:   : 5
Queue 4 Weight:   : 1
Queue 5 Weight:   : 1
Queue 6 Weight:   : 1
Queue 7 Weight:   : 1
Queue 8 Weight:   : 1
===============================================================================
*A:Dut-1>config#
```

Editing QoS Policies

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.

QoS Port Scheduler Policy Command Reference

Command Hierarchies

- Port Scheduler Policy Configuration Commands on page 355
- Operational Commands on page 355
- Show Commands on page 355

Port Scheduler Policy Configuration Commands

```
config
    — qos
            — [no] port-scheduler-policy port-scheduler-name [create]
                    — description description-string
                    — no description
                    — mode {strict | rr | wrr | wdrr}
                    — no mode
                    — queue queue-id [strict | weight weight]
                    — no queue queue-id
```

Operational Commands

```
config
    — qos
            — copy port-scheduler-policy src-name dst-name [overwrite]
```

Show Commands

```
show
    — qos
            — port-scheduler-policy [port-scheduler-policy-name] [association]
```

Configuration Commands

Generic Commands

description

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

Context config>qos>port-scheduler-policy

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

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

The **no** form of this command removes any description string from the context.

Default No description is associated with the configuration context.

Parameters *description-string* — 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.

Operational Commands

copy

Syntax **copy port-scheduler-policy** *src-name dst-name* [**overwrite**]

Context config>qos

Description This command copies existing port scheduler QoS policy entries for a port scheduler QoS policy to another port scheduler QoS policy.

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.

If **overwrite** is not specified, an error will occur if the destination policy exists.

Parameters **port-scheduler-policy** *src-name dst-name* — Indicates that the source policy and the destination policy are port scheduler policy IDs. Specify the source policy that the copy command will attempt to copy from and specify the destination policy name to which the command will copy a duplicate of the policy.

overwrite — Forces the destination policy name to be copied as specified. When forced, everything in the existing destination policy will be completely overwritten with the contents of the source policy.

Port Scheduler Policy Commands

port-scheduler-policy

Syntax [**no**] **port-scheduler-policy** *port-scheduler-name* [**create**]

Context config>qos

Description The default scheduling done for a port is strict scheduling.When a port-scheduler policy is applied to a port , it overrides the default scheduling and determines the type of scheduling (Strict, RR, WRR, WDRR, WRR/WDRR + Strict) to be done between the 8 CoS queues of that particular port. When a port scheduler policy is detached from a port, the port reverts back to the default scheduling (strict).

The **no** form of the command removes the policy from the system.

Parameters *port-scheduler-name* — specifies an existing policy name. Each port-scheduler policy name should be unique and can go upto 32 ASCII characters in length.

create- **—** This keyword is used to create a port scheduler policy.

mode

Syntax **mode** {**strict | rr | wrr | wdrr**}
no mode

Context config>qos>port-sched-plcy

Description This command configures a particular mode of scheduling for the policy. For example, this implies that when a policy with a mode RR is applied to a port then that port will follow the round robin type of scheduling between its queues.

Parameters *mode* — Specifies the port scheduler policy mode.

strict — Strict scheduler mode
rr — Round Robin
wrr — Weighted Round Robin
wdrr — Weighted Deficit Round Robin

queue

Syntax **queue** *queue-id* [**strict |weight** *weight*]
no queue *queue-id*

Context config>qos>port-sched-plcy

Description This command configures a port scheduler queue. The queue and its weights can be configured only for WRR/WDRR modes. The weight specified in case of WRR corresponds to the number of packets that needs to be sent out in a cycle for that particular queue.

For WDRR, the weight specified is the ratio of traffic that will be sent out for that particular queue. For example, in WDRR, if a weight value for queue 1 is 1 and a weight value for queue 2 is 5, then traffic out of the port is in the ratio of 1:5 between the queues (1 and 2) provided no traffic is flowing in the other queues. If the keyword **strict** is specified in any of the queues, then that particular queue will be treated as strict. This set of strict priority queues is serviced first in the order of their CoS numbering (the higher numbered CoS queue receives service before smaller numbered queues).

The **no** form of the queue under a WRR/WDRR mode will set the queue weights to default (for example, 1).

Parameters *queue-id* — Specifies the queue ID.

Values 1 — 8 (8 is the highest)

strict — Specifies strict access.

weight *weight* **—** Specifies the number of packets in case of WRR and ratio of traffic out in WDRR.

Values 1 — 15

Show Commands

port-scheduler-policy

Syntax **port-scheduler-policy** [*port-scheduler-policy-name*] [**association**]

Context show>qos

Description This command displays port-scheduler policy information

Parameters *port-scheduler-policy-name* — Displays information for the specified existing port scheduler policy.

association — Displays associations related to the specified port scheduler policy.

Output **Show QoS Port Scheduler Output —** The following table describes the QoS port scheduler policy fields.

Label	Description
`Policy Name`	Displays the port scheduler policy name.
`Associations`	Displays associations related to the specified port scheduler policy.
`Mode`	Displays the port scheduler policy mode (STRICT, RR, WRR, WDRR).
`Accounting`	Displays whether the accounting mode is frame-based or packet-based
`Last Changed`	Displays the last time the configuration changed.
`Queue #`	Displays the weight of the queue if configured.

Sample Output

```
*A:Dut-1>config# show qos port-scheduler-policy
===============================================================================
Port Scheduler Policies
===============================================================================
Policy-Id                     Description                             Mode
-------------------------------------------------------------------------------
default                       Default Port Scheduler policy.          STRICT
psp                                                                   WDRR
psp1                                                                  WDRR
===============================================================================
*A:Dut-1>config#

*A:Dut-1>config# show qos port-scheduler-policy psp association
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : psp
Accounting        : packet-based
Mode              : WDRR

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
 - Port : 1/1/1

===============================================================================
*A:Dut-1>config#
*A:Dut-1>config# show qos port-scheduler-policy psp
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : psp
Accounting        : packet-based
Mode              : WDRR
Last changed      : 04/12/2001 02:04:16
Queue 1 Weight:   : 1
Queue 2 Weight:   : 2
Queue 3 Weight:   : 5
Queue 4 Weight:   : 1
Queue 5 Weight:   : 1
Queue 6 Weight:   : 1
Queue 7 Weight:   : 1
Queue 8 Weight:   : 1
===============================================================================
*A:Dut-1>config#
*A:card-1# show qos port-scheduler-policy default association
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : default
Description       : Default Port Scheduler policy.
Accounting        : packet-based
Mode              : STRICT

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
 - Port : 1/1/3
 - Port : 1/1/6
 - Port : 1/1/7
 - Port : 1/1/8
 - Port : 1/1/9
 - Port : 1/1/10
 - Port : 1/1/11
 - Port : 1/1/12
 - Port : 1/1/13
 - Port : 1/1/14
 - Port : 1/1/16
 - Port : 1/1/17
 - Port : 1/1/18
 - Port : 1/1/19
 - Port : 1/1/21
 - Port : 1/1/22
 - Port : 1/1/23
 - Port : 1/1/24
...
===============================================================================
*A:card-1#

*A:Dut-1>config# show qos port-scheduler-policy default
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : default
Description       : Default Port Scheduler policy.
Accounting        : packet-based
Mode              : STRICT
Last changed      : 04/11/2001 19:59:21
Number Of Queues  : 8
===============================================================================
*A:Dut-1>config#
```

Slope QoS Policies

In This Section

This section provides information to configure slope QoS policies using the command line interface.

Topics in this section include:

Overview

The buffer allocation on 7210 SAS-M and 7210 SAS-T is given above in the Chapter , QoS Policies, on page 20.

By default, each queue is associated with slope-policy default which disables the high-slope, low-slope and non-TCP slope parameters.

For information about the tasks and commands necessary to access the command line interface and to configure and maintain your 7210 SAS M, refer to CLI Usage chapter in the 7210 SAS M OS Basic System Configuration Guide.

Configuration Guidelines

For 7210 SAS-M Network Mode

Following slopes are used based on the traffic encapsulation:

- For traffic received with MPLS encapsulation (For example: MPLS traffic received on network port ingress, and others) non-TCP slope is used.
- For TCP traffic received with less than or equal to 2 VLAN tags (For example: VLAN ethernet traffic received on SAP ingress, and others) TCP- slopes (either high or low) is used.
- For non-TCP traffic received with less than or equal to 2 VLAN tags (For example: VLAN ethernet traffic received on SAP ingress, and others) non-TCP slope is used.
- For all traffic received with 3 or more VLAN tags (For example: VLAN ethernet traffic received on SAP ingress, and others) non-TCP slope is used.

For 7210 SAS-M Access-uplink mode

Following slopes are used based on the traffic encapsulation:

- For TCP traffic received with less than or equal to 2 VLAN tags (For example: VLAN ethernet traffic received on SAP ingress, and others) TCP- slopes (either high or low) is used.
- For non-TCP traffic received with less than or equal to 2 VLAN tags (For example: VLAN ethernet traffic received on SAP ingress, and others) non-TCP slope is used.
- For all traffic received with 3 or more VLAN tags (For example: VLAN ethernet traffic received on SAP ingress, and others) non-TCP slope is used.

WRED Slope enhancement

In 7210 SAS release 6.0, the user is provided with an option to use only 2 WRED slopes per queue (port egress queues), which allows differentiating in-profile and out-of-profile traffic flows. This is supported in both 7210 SAS-M access-uplink mode and network mode.

The following table compares the WRED slope used for different traffic flows. The slope does not get enabled by default. In order to maintain backward compatibility, the value is set to use 3 slopes (that is, tcp-non-tcp) and user has to change it explicitly to use 2 slopes on 7210 SAS-M nodes.

Table 45: Slope behavior table

Slopes	TCP-non-TCP slope option (Uses 3 WRED slopes per queue)	High-Low slope option (Uses 2 WRED slopes per queue)
SAP Ingress TCP/IP traffic (Number of VLAN tags <=2)	High-priority TCP slope or low-priority TCP slope, based on packet profile	High-priority or low-priority slope, based on packet profile
SAP Ingress non-TCP traffic (Number of VLAN tags does not matter)	Non-TCP slope - No in/out profile differentiation	High-priority or low-priority slope, based on packet profile
SAP Ingress TCP/IP traffic (Number of VLAN tags>2)	Non-TCP slope - No in/out profile differentiation	High-priority or low-priority slope, based on packet profile
MPLS LER originating traffic	High-priority TCP slope or low-priority TCP slope, based on packet profile	High-priority or low-priority slope, based on packet profile
MPLS LER terminating traffic	Non-TCP slope - No in/out profile differentiation	High-priority or low-priority slope, based on packet profile
MPLS LSR traffic	Non-TCP slope - No in/out profile differentiation	High-priority or low-priority slope, based on packet profile

WRED support on 7210 SAS-T access-uplink mode

On 7210 SAS-T, 2 WRED slopes are supported per queue, one each for in-profile or high-priority traffic and out-of-profile or low-priority traffic.

In 7210 SAS-T devices, the hardware supports a limited amount of profiles, out of which some are reserved for system internal use and the rest is available for user configuration. It is not possible to allocate a unique profile for each and every queue available on 7210 SAS-T. Multiple queues will need to share the same WRED profile. Software manages the allocation of hardware WRED profiles based on user configuration. It automatically allocates a single WRED hardware profile if multiple queues use the same slope parameters (that is, max-average, start-average, drop probability and time average factor). Only if these parameters differ, it allocates a different hardware WRED profile for use by the queue.

NOTE: The WRED state (For example: average queue size) per queue is maintained independently for each queue in hardware.

A WRED profile (that is, each high-slope and low-slope) allows to specify the slope parameters such as max-average, start-average, drop probability and time average factor (TAF).

Basic Configurations

A basic slope QoS policy must conform to the following:

- Each slope policy must have a unique policy ID.
- High slope, low slope and non-TCP slope are shut down (default).
- Default values can be modified but parameters cannot be deleted.

Create a Slope QoS Policy

Configuring and applying slope policies is optional. If no slope policy is explicitly applied to a port, a default slope policy is applied.

To create a new slope policy, define the following:

- A slope policy ID value. The system will not dynamically assign a value.
- Include a description. The description provides a brief overview of policy features.
- The high slope for the high priority Random Early Detection (RED) slope graph.
- The low slope for the low priority Random Early Detection (RED) slope graph.
- The non-TCP slope for the non-TCP Random Early Detection (RED) slope graph.
- The time average factor (TAF), a weighting exponent used to determine the portion of the shared buffer instantaneous utilization and shared buffer average utilization used to calculate the new shared buffer average utilization.

Use the following CLI syntax to configure a slope policy:

CLI Syntax:

```
config>qos
 slope-policy name
  description description-string
   high-slope
     start-avg percent
     max-avg percent
     max-prob percent
     no shutdown
  low-slope
     start-avg percent
     max-avg percent
     max-prob percent
     no shutdown
  non-tcp-slope
     start-avg percent
     max-avg percent
     max-prob percent
     no shutdown
  time-average-factor taf
```

The following displays the slope policy configuration (f:

```
A:ALA-7>config>qo>slope-policy# info
---------------------------------------------
            description "slope policy SlopePolicy1"
            high-slope
                no shutdown
            exit
            low-slope
                no shutdown
            exit
non-tcp-slope
              no shutdown
            exit
---------------------------------------------
A:ALA-7>config>qos>slope-policy#
```

Applying Slope Policies

- Ports

Apply slope policies to the egress buffer pool on the access and network ports.

Ports

The following CLI syntax examples may be used to apply slope policies to ports:

CLI Syntax:

```
config>port>access>egress>pool>slope-policy name
config>port>network>egress>pool>slope-policy name
```

Default Slope Policy Values

The default access egress and network egress policies are identified as policy-id “default”. The default policies cannot be edited or deleted. The following table displays default policy parameters:

Table 46: Slope Policy Defaults

Field	Default
description	Default slope policy
high (RED) slope	
Administrative state	shutdown
start-avg	70% utilization
max-avg	90% utilization
max-prob	75%
low (RED) slope	
Administrative state	shutdown
start-avg	50% utilization
max-avg	75% utilization
max-prob	75%
non-TCP (RED) slope	
Administrative state	shutdown
start-avg	50% utilization
max-avg	75% utilization
max-prob	75%

```
A:ALA>config>qos# slope-policy default
A:ALA>config>qos>slope-policy# info detail
----------------------------------------------
            description "Default slope policy."
            queue "1"
                high-slope
                    shutdown
                    start-avg 70
```

```
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
queue "2"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
queue "3"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
```

```
queue "4"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
queue "5"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
queue "6"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
```

```
                    max-prob 75
                exit
                time-average-factor 7
            exit
            queue "7"
                high-slope
                    shutdown
                    start-avg 70
                    max-avg 90
                    max-prob 75
                exit
                low-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                time-average-factor 7
            exit
            queue "8"
                high-slope
                    shutdown
                    start-avg 70
                    max-avg 90
                    max-prob 75
                exit
                low-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                time-average-factor 7
            exit
----------------------------------------------
A:ALA>config>qos>slope-policy#
```

Deleting QoS Policies

A slope policy is associated by default with access and network egress pools. A default policy may be replaced with a non-default policy, but a policy cannot be entirely removed from the configuration. When a non-default policy is removed, the policy association reverts to the default slope **policy** *policy-id* **default**. A QoS policy cannot be deleted until it is removed from all ports where it is applied.

```
ALA-7>config>qos# no slope-policy slopePolicy1
MINOR: QOS #1902 Slope policy has references
ALA-7>config>qos#
```

Ports

The following CLI syntax examples can be used to remove slope policies from MDA ports:

CLI Syntax:
```
config>port>access>egress>pool# no slope-policy name
config>port>network>egress>pool# no slope-policy name
```

Remove a Policy from the QoS Configuration

To delete a slope policy, enter the following command:

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

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.

CLI Syntax: `config>qos> copy {slope-policy}` *`source-policy-id dest-policy-id`* `[overwrite]`

The following output displays the copied policies for:

```
A:ALA-7210M>config>qos#
----------------------------------------------
...
      description "Default slope policy."
            queue "1"
                high-slope
                    shutdown
                    start-avg 70
                    max-avg 90
                    max-prob 75
                exit
                low-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                time-average-factor 7
            exit
            queue "2"
                high-slope
                    shutdown
                    start-avg 70
                    max-avg 90
                    max-prob 75
                exit
                low-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                time-average-factor 7
            exit
            queue "3"
                high-slope
                    shutdown
                    start-avg 70
                    max-avg 90
                    max-prob 75
                exit
                low-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                time-average-factor 7
            exit
            queue "4"
                high-slope
                    shutdown
                    start-avg 70
                    max-avg 90
                    max-prob 75
                exit
                low-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                time-average-factor 7
            exit
            queue "5"
                high-slope
                    shutdown
                    start-avg 70
                    max-avg 90
                    max-prob 75
                exit
                low-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
```

```
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
queue "6"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
queue "7"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    non-tcp-slope
        shutdown
        start-avg 50
        max-avg 75
        max-prob 75
    exit
    time-average-factor 7
exit
queue "8"
    high-slope
        shutdown
        start-avg 70
        max-avg 90
        max-prob 75
    exit
    low-slope
        shutdown
        start-avg 50
```

```
                    max-avg 75
                    max-prob 75
                exit
                non-tcp-slope
                    shutdown
                    start-avg 50
                    max-avg 75
                    max-prob 75
                exit
                time-average-factor 7
            exit
...
----------------------------------------------
A:ALA-7210M>config>qos#
```

Editing QoS Policies

You can change existing policies and entries in the CLI or NMS. 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.

Slope QoS Policy Command Reference

Command Hierarchies

Configuration Commands (for 7210 SAS-M in network mode and 7210 SAS-M and 7210 SAS-T access uplink mode)

```
config
    — qos
        — [no] slope-policy name
            — description description-string
            — no description
            — queue queue-id
                — [no] high-slope
                    — max-avg percent
                    — no max-avg
                    — max-prob percent
                    — no max-prob
                    — [no] shutdown
                    — start-avg percent
                    — no start-avg
                — [no] low-slope
                    — max-avg percent
                    — no max-avg
                    — max-prob percent
                    — no max-prob
                    — [no] shutdown
                    — start-avg percent
                    — no start-avg
                — [no] non-tcp-slope (Not supported for 7210 SAS-T, Only 2 WRED slopes are
                  supported per queue)
                    — max-avg percent
                    — no max-avg
                    — max-prob percent
                    — no max-prob
                    — [no] shutdown
                    — start-avg percent
                    — no start-avg
            — time-average-factor value
            — no time-average-factor
```

Operational Commands

```
config
    — qos
        — copy slope-policy src-name dst-name [overwrite]
```

WRED Commands

```
config
    — system
        — qos
            — no use-wred-slopes
            — use-wred-slopes slope-type
```

Show Commands

```
show
    — qos
        — slope-policy [slope-policy-name] [detail]
```

Configuration Commands

Generic Commands

description

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

Context config>qos>slope-policy

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

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

The **no** form of this command removes any description string from the context.

Default No description is associated with the configuration context.

Parameters *description-string* — 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.

Operational Commands

copy

Syntax **copy slope-policy** *src-name dst-name* [**overwrite**]

Context config>qos

Description This command copies existing QoS policy entries for a QoS policy-id to another QoS policy-id.

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.

Parameters **slope-policy —** 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.

overwrite — Specifies to replace the existing destination policy. 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.

```
ALA-7>config>qos# copy slope-policy default sp1
MINOR: CLI Destination "sp1" exists - use {overwrite}.
ALA-7>config>qos#overwrite
```

Slope Policy QoS Commands

slope-policy

Syntax [**no**] **slope-policy** *name*

Context config>qos

Description This command enables the context to configure a QoS slope policy.

Default slope-policy "default"

Parameters *name* — 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.

Slope Policy QoS Policy Commands

queue

Syntax **queue** *queue-id*

Context config>qos>slope-policy

Description This command sets the context to configure the high-priority, low-priority, and non-tcp slope parameters per queue.

Parameters *queue-id* — Specifies the ID of the queue for which the drop-rate is to be configured.

Values 1 — 8

high-slope

Syntax [**no**] **high-slope**

Context config>qos>slope-policy>queue

Description The **high-slope** context contains the commands and parameters for defining the high priority Random Early Detection (RED) slope graph. Each buffer pool supports a high priority RED slope for managing access to the shared portion of the buffer pool for high priority or in-profile packets.

The **high-slope** parameters can be changed at any time and the affected buffer pool high priority RED slopes will be adjusted appropriately.

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** node will not appear in save config and show config output unless the detail parameter is present.

low-slope

Syntax [**no**] **low-slope**

Context config>qos>slope-policy
config>qos>slope-policy>queue

Description The **low-slope** context contains the commands and parameters for defining the low priority Random Early Detection (RED) slope graph. Each buffer pool supports a low priority RED slope for managing access to the shared portion of the buffer pool for low priority or out-of-profile packets.

The **low-slope** parameters can be changed at any time and the affected buffer pool low priority RED slopes must be adjusted appropriately.

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** node will not appear in save config and show config output unless the detail parameter is present.

non-tcp-slope

Syntax [**no**] **non-tcp-slope**

Context config>qos>slope-policy>queue

Description This command configures non-tcp profile RED slope parameters.

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

time-average-factor

Syntax **time-average-factor** *value*
no time-average-factor

Context config>qos>slope-policy>queue

Description This command sets a weighting factor to calculate the new shared buffer average utilization after assigning buffers for a packet entering a queue. To derive the new shared buffer average utilization, the buffer pool takes a portion of the previous shared buffer average and adds it to the inverse portion

of the instantaneous shared buffer utilization. The time-average-factor command sets the weighting factor between the old shared buffer average

utilization and the current shared buffer instantaneous utilization when calculating the new shared buffer average utilization.

The TAF value applies to all high ,low priority and non-tcp packets WRED slopes for egress access and network buffer pools controlled by the slope policy.

The no form of this command restores the default setting.

Default 7 - Weighting instantaneous shared buffer utilization is 0.8%.

Parameters *value* — Represents the Time Average Factor (TAF), expressed as a decimal integer. The value specified for TAF affects the speed at which the shared buffer average utilization tracks the instantaneous shared buffer utilization. A low value weights the new shared buffer average utilization calculation more to the shared buffer instantaneous utilization, zero using it exclusively. A high value weights the new shared buffer average utilization calculation more to the previous shared buffer average utilization value.

Values 0 — 15

RED Slope Commands

max-avg

Syntax **max-avg** *percent*
no max-avg

Context config>qos>slope-policy>queue>high-slope
config>qos>slope-policy>queue>low-slope
config>qos>slope-policy>queue>non-tcp-slope

Description Sets the low priority or high priority or non-tcp Weighted Random Early Detection (WRED) slope position for the reserved and shared buffer average utilization value where the packet discard probability rises directly to one. The percent parameter is expressed as a percentage of the shared buffer size.

The **no** form of this command restores the max-avg value to the default setting. If the current startavg setting is larger than the default, an error will occur and the max-avg setting will not be changed to the default.

Default **max-avg 90** — High slope default is 90% buffer utilization before discard probability is 1.
max-avg 75 — Low slope default is 75% buffer utilization before discard probability is 1.
max-avg 75 — Non-tcp slope default is 75% buffer utilization before discard probability is 1.

Description *percent* — The percentage of the reserved and shared buffer space for the buffer pool 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.

Values 0 — 100

max-prob

Syntax **max-prob** *percent*
no max-prob

Context config>qos>slope-policy>queue>high-slope
config>qos>slope-policy>queue>low-slope
config>qos>slope-policy>queue>non-tcp-slope

Description Sets the low priority or high priority Random Early Detection (RED) slope position for the maximum non-one packet discard probability value before the packet discard probability rises directly to one. The percent 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.

The **no** form of this command restores the **max-prob** value to the default setting.

Default **max-prob 80** — 80% maximum drop probability corresponding to the **max-avg.**

Parameters *percent* — The maximum drop probability percentage corresponding to the **max-avg,** expressed as a decimal integer.

Values 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 25, 50, 75, 100

shutdown

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

Context config>qos>slope-policy>high-slope
config>qos>slope-policy>low-slope
config>qos>slope-policy>queue

Description This command enables or disables the administrative status of the Random Early Detection slope.

By default, all slopes are shutdown and have to be explicitly enabled (**no shutdown**).

The **no** form of this command administratively enables the RED slope.

Default **shutdown -** RED slope disabled implying a zero (0) drop probability.

start-avg

Syntax **start-avg** *percent*
no start-avg

Context config>qos>slope-policy>queue>high-slope
config>qos>slope-policy>queue>low-slope
config>qos>slope-policy>queue>non-tcp-slope

Description This command sets the low priority or high priority Random Early Detection (RED) slope position for the shared buffer average utilization value where the packet discard probability starts to increase above zero. The percent parameter is expressed as a percentage of the shared buffer size.

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.

Default max-avg 70 — High slope default is 70% buffer utilization.
max-avg 50 — Low slope default is 50% buffer utilization.
max-avg 50 — Non-tcp slope default is 50% buffer utilization.

Parameters *percent* — The percentage of the resrved and shared buffer space for the buffer pool at which the drop starts. The value entered must be lesser or equal to the current setting of max-avg. If the entered value is greater than the current value of max-avg, an error will occur and no change will take place.

Values 0 — 100

time-average-factor

Syntax **time-average-factor** *value*
no time-average-factor

Context config>qos>slope-policy>queue

Description This command sets a weighting factor to calculate the new shared buffer average utilization after assigning buffers for a packet entering a queue. To derive the new shared buffer average utilization, the buffer pool takes a portion of the previous shared buffer average and adds it to the inverse portion

of the instantaneous shared buffer utilization. The time-average-factor command sets the weighting factor between the old shared buffer average

utilization and the current shared buffer instantaneous utilization when calculating the new shared buffer average utilization.

The TAF value applies to all high ,low priority and non-tcp packets WRED slopes for egress access and network buffer pools controlled by the slope policy.

Values

WRED command

use-wred-slopes

Syntax **no use-wred-slopes**
use-wred-slopes *slope-type*

Context config>system>qos

Description The user is provided with an option to use 2 WRED slopes per queue or use 3 WRED slopes per queue. It is a global option which affects all the queues in the system. In other words, user can choose to use either 2 WRED slopes for all queues in the system or 3 WRED slopes for all queues in the system.

Using 3 WRED slopes per queue allows differentiating tcp in-profile traffic, tcp out-of-profile traffic, and non-tcp traffic. For non-tcp traffic both in and out profile use the same slope.

Using 2 WRED slopes per queue allows differentiating in-profile and out-of-profile traffic, without further differentiation of tcp and non-tcp traffic. All traffic, irrespective of tcp or non-tcp traffic, uses either in-profile slope or out-of-profile slope, depending on the profile assigned to the traffic by the ingress meters.

The no form of the command enables use of 3 WRED slopes per queue.

Default use-wred-slopes tcp-non-tcp to maintain backward compatibility.

Parameters **High and Low slope type —** When high-low is set, 2 slopes are used per queue. High priority/In-profile slope for all packets that are classified as in-profile by the ingress meter and Low priority/out-of-profile slope for all packets that are classified as out-of-profile by the ingress meter. The high-priority/in-profile WRED slope uses the values configured under **config> qos> slope-policy> high-slope**. The low-priority/out-of-profile WRED slope uses the values configured under **config> qos> slope-policy> low-slope**. The values configured under non-TCP WRED slope is ignored by the system.

TCP and Non-TCP slope type — There are 3 WRED slopes (High priority/In-profile TCP WRED slope, Low priority/out-of-profile TCP WRED slope, and non-TCP WRED slope) that are used per queue when TCP-non-tcp slope is set.

The non-TCP WRED slope is used for all packets classified as non-TCP packets on ingress, irrespective of the packet's profile or priority. Packets classified as TCP and determined to be high-priority/in-profile by the ingress meter, uses the high priority TCP WRED slope. This slope uses the values configured under **config> qos> slope-policy> high-slope**. Packets classified as TCP and determined to be low-priority/out-of-profile by the ingress meter, uses the low-priority TCP WRED slope. The low-priority/out-of-profile TCP WRED slope uses the values configured under **config> qos> slope-policy> low-slope**. The non-TCP WRED slope uses the values configured under **config> qos> slope-policy> non-tcp-slope**.

Show Commands

slope-policy

Syntax **slope-policy** [*slope-policy-name*] [**detail**]

Context show>qos

Description This command displays slope policy information.

Parameters *slope-policy-name* — The name of the slope policy.

detail — Displays detailed information about the slope policy.

Table 47: Show QoS Slope Policy Output Fields

Label	Description
`Policy`	The ID that uniquely identifies the policy.
`Description`	A string that identifies the policy's context in the configuration file.
`Time Avg`	The weighting between the previous shared buffer average utilization result and the new shared buffer utilization.
Slope Parameters	
`Start Avg`	Specifies the low priority or high priority RED slope position for the shared buffer average utilization value where the packet discard probability starts to increase above zero.
`Max Avg`	Specifies the percentage of the shared buffer space for the buffer pool at which point the drop probability becomes 1, expressed as a decimal integer
`Admin State`	`Up` — The administrative status of the RED slope is enabled. `Down` — The administrative status of the RED slope is disabled. Specifies the low priority or high priority RED slope position for the maximum non-one packet discard probability value before the packet discard probability rises directly to one.
`Max Prob.`	Specifies the high priority RED slope position for the maximum non-one packet discard probability value before the packet discard probability rises directly to one.

Sample Output

```
*A:SN12345678# show qos slope-policy 100
===============================================================================
QoS Slope Policy
===============================================================================
Policy         : 100
Description    : Slope policy 100
-------------------------------------------------------------------------------
Utilization                   State       Start-Threshold
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            70           90            75
Queue2          Down            70           90            75
Queue3          Down            70           90            75
Queue4          Down            70           90            75
Queue5          Down            70           90            75
Queue6          Down            70           90            75
Queue7          Down            70           90            75
Queue8          Down            70           90            75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
Non Tcp Slope
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
Time Avg Factor
-------------------------------------------------------------------------------
Queue Id   Time Avg Factor
-------------------------------------------------------------------------------
Queue1            7
Queue2            7
Queue3            7
Queue4            7
Queue5            7
```

```
Queue6            7
Queue7            7
Queue8            7
===============================================================================
*A:SN12345678# show qos slope-policy 100 detail


*A:SN12345678#
===============================================================================
QoS Slope Policy
===============================================================================
Policy         : 100
Description    : Slope policy 100
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            70           90            75
Queue2          Down            70           90            75
Queue3          Down            70           90            75
Queue4          Down            70           90            75
Queue5          Down            70           90            75
Queue6          Down            70           90            75
Queue7          Down            70           90            75
Queue8          Down            70           90            75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
Non Tcp Slope
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down            50           75            75
Queue2          Down            50           75            75
Queue3          Down            50           75            75
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
Time Avg Factor
-------------------------------------------------------------------------------
Queue Id   Time Avg Factor
-------------------------------------------------------------------------------
Queue1            7
Queue2            7
```

```
Queue3            7
Queue4            7
Queue5            7
Queue6            7
Queue7            7
Queue8            7
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Object Type Object Id     Application          Pool
-------------------------------------------------------------------------------
Port        1/1/13        Acc-Egr              default
===============================================================================
*A:SN12345678#

*A:SAST>config>qos>slope-policy>queue>$ show qos slope-policy "33" detail

===============================================================================
QoS Slope Policy
===============================================================================
Policy         : 33
Description    : (Not Specified)
-------------------------------------------------------------------------------
High Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1           Up              65           95            50
Queue2          Down             70           90            75
Queue3          Down             70           90            75
Queue4          Down             70           90            75
Queue5          Down             70           90            75
Queue6          Down             70           90            75
Queue7          Down             70           90            75
Queue8          Down             70           90            75
-------------------------------------------------------------------------------
Low Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1           Up              35           55            25
Queue2          Down             50           75            75
Queue3          Down             50           75            75
Queue4          Down             50           75            75
Queue5          Down             50           75            75
Queue6          Down             50           75            75
Queue7          Down             50           75            75
Queue8          Down             50           75            75
-------------------------------------------------------------------------------
Non Tcp Slope
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
QueueId        State      Start-Avg(%)   Max-Avg(%)   Max-Prob(%)
-------------------------------------------------------------------------------
Queue1          Down             50           75            75
Queue2          Down             50           75            75
Queue3          Down             50           75            75
```

```
Queue4          Down            50           75            75
Queue5          Down            50           75            75
Queue6          Down            50           75            75
Queue7          Down            50           75            75
Queue8          Down            50           75            75
-------------------------------------------------------------------------------
Time Avg Factor
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Queue Id   Time Avg Factor
-------------------------------------------------------------------------------
Queue1            7
Queue2            7
Queue3            7
Queue4            7
Queue5            7
Queue6            7
Queue7            7
Queue8            7

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Object Type Object Id     Application          Pool
-------------------------------------------------------------------------------
Port        1/1/1         Acc-Egr              default
Port        1/1/5         Acc-Egr              default

A:SAST>config>qos>slope-policy>queue>$ show
```

Standards and Protocol Support

Standards Compliance

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery

IEEE 802.1D Bridging

IEEE 802.1p/Q VLAN Tagging

IEEE 802.1s Multiple Spanning Tree

IEEE 802.1w Rapid Spanning Tree Protocol

IEEE 802.1X Port Based Network Access Control

IEEE 802.1ad Provider Bridges

IEEE 802.1ah Provider Backbone Bridges

IEEE 802.1ag Service Layer OAM

IEEE 802.3ah Ethernet in the First Mile

IEEE 802.3 10BaseT

IEEE 802.3ad Link Aggregation

IEEE 802.3ae 10Gbps Ethernet

IEEE 802.3ah Ethernet OAM

IEEE 802.3u 100BaseTX

IEEE 802.3z 1000BaseSX/LX ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks draft-ietf-disman-alarm-mib-04.txt IANA-IFType-MIB

IEEE8023-LAG-MIB ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

Protocol Support

BGP

RFC 1397 BGP Default Route Advertisement

RFC 1772 Application of BGP in the Internet

RFC 1997 BGP Communities Attribute

RFC 2385 Protection of BGP Sessions via MD5

RFC 2439 BGP Route Flap Dampening

RFC 2547 bis BGP/MPLS VPNs draft-ietf-idr-rfc2858bis-09.txt.

RFC 2918 Route Refresh Capability for BGP-4

RFC 3107 Carrying Label Information in BGP-4

RFC 3392 Capabilities Advertisement with BGP4

RFC 4271 BGP-4 (previously RFC 1771)

RFC 4360 BGP Extended Communities Attribute

RFC 4364 BGP/MPLS IP Virtual Private Networks (VPNs)(previously RFC 2547bis BGP/MPLS VPNs)

RFC 4760 Multi-protocol Extensions for BGP

RFC 4893 BGP Support for Four-octet AS Number Space

CIRCUIT EMULATION

RFC 4553 Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)

RFC 5086 Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)

RFC 5287 Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks

DHCP

RFC 2131 Dynamic Host Configuration Protocol (REV)

RFC 3046 DHCP Relay Agent Information Option (Option 82)

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)

RFC 2597 Assured Forwarding PHB Group (rev3260)

RFC 2598 An Expedited Forwarding PHB

RFC 2697 A Single Rate Three Color Marker

RFC 2698 A Two Rate Three Color Marker

RFC 4115 A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic

IPv6

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification

RFC 2461 Neighbor Discovery for IPv6

RFC 2462 IPv6 Stateless Address Auto configuration

RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification

RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

RFC 2740 OSPF for IPv6

RFC 3587 IPv6 Global Unicast Address Format

RFC 4007 IPv6 Scoped Address Architecture

RFC 4193 Unique Local IPv6 Unicast Addresses

RFC 4291 IPv6 Addressing Architecture

RFC 4552 Authentication/Confidentiality for OSPFv3

RFC 5095 Deprecation of Type 0 Routing Headers in IPv6

draft-ietf-isis-ipv6-05

draft-ietf-isis-wg-multi-topology-xx.txt

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 (ISIS) 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 3847 Restart Signaling for IS-IS – GR helper

RFC 4205 for Shared Risk Link Group (SRLG) TLV

MPLS - LDP

RFC 3037 LDP Applicability

RFC 3478 Graceful Restart Mechanism for LDP — GR helper

RFC 5036 LDP Specification

RFC 5283 LDP extension for Inter-Area LSP

RFC 5443 LDP IGP Synchronization

MPLS - General

RFC 3031 MPLS Architecture

RFC 3032 MPLS Label Stack Encoding

RFC 4379 Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures

RFC 4182 Removing a Restriction on the use of MPLS Explicit NULL

Multicast

RFC 1112 Host Extensions for IP Multicasting (Snooping)

RFC 2236 Internet Group Management Protocol, (Snooping)

RFC 3376 Internet Group Management Protocol, Version 3 (Snooping) [Only in 7210 SAS-M access-uplink mode]

NETWORK MANAGEMENT

ITU-T X.721: Information technology-OSI-Structure of Management Information

ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function

M.3100/3120 Equipment and Connection Models

TMF 509/613 Network Connectivity Model

RFC 1157 SNMPv1

RFC 1215 A Convention for Defining Traps for use with the SNMP

RFC 1907 SNMPv2-MIB

RFC 2011 IP-MIB

RFC 2012 TCP-MIB

RFC 2013 UDP-MIB

RFC 2096 IP-FORWARD-MIB

RFC 2138 RADIUS

RFC 2206 RSVP-MIB

RFC 2571 SNMP-FRAMEWORKMIB

RFC 2572 SNMP-MPD-MIB

RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB

RFC 2574 SNMP-USER-BASEDSMMIB

RFC 2575 SNMP-VIEW-BASEDACM-MIB

RFC 2576 SNMP-COMMUNITY-MIB

RFC 2665 EtherLike-MIB

RFC 2819 RMON-MIB

RFC 2863 IF-MIB

RFC 2864 INVERTED-STACK-MIB

RFC 3014 NOTIFICATION-LOGMIB

RFC 3164 Syslog

RFC 3273 HCRMON-MI

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-mpls-lsr-mib-06.txt

draft-ietf-mpls-te-mib-04.txt

draft-ietf-mpls-ldp-mib-07.txt

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 3623 Graceful OSPF Restart – GR helper

RFC 3630 Traffic Engineering (TE) Extensions to OSPF Version 2

RFC 2740 OSPF for IPv6 (OSPFv3) draft-ietf-ospf-ospfv3-update-14.txt

RFC 4203 Shared Risk Link Group (SRLG) sub-TLV

MPLS - RSVP-TE

RFC 2430 A Provider Architecture DiffServ & TE

RFC 2702 Requirements for Traffic Engineering over MPLS

RFC2747 RSVP Cryptographic Authentication

RFC3097 RSVP Cryptographic Authentication

RFC 3209 Extensions to RSVP for Tunnels

RFC 4090 Fast reroute Extensions to RSVP-TE for LSP Tunnels

RFC 5817 Graceful Shutdown in MPLS and GMPLS Traffic Engineering Networks

PSEUDO-WIRE

RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3)

RFC 4385 Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN

RFC 3916 Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)

RFC 4448 Encapsulation Methods for Transport of Ethernet over MPLS Networks (draft-ietf-pwe3-ethernet-encap-11.txt)

RFC 4446 IANA Allocations for PWE3

RFC 4447 Pseudowire Setup and Maintenance Using LDP (draft-ietf-pwe3-control-protocol-17.txt)

RFC 5085, Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires

RFC 5880 Bidirectional Forwarding Detection

RFC 5881 BFD IPv4 and IPv6 (Single Hop)

RFC 5659 An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge

RFC6073, Segmented Pseudowire (draft-ietf-pwe3-segmented-pw-18.txt)

draft-ietf-l2vpn-vpws-iw-oam-02.txt

OAM Procedures for VPWS Interworking

draft-ietf-pwe3-oam-msg-map-14-txt, Pseudowire (PW) OAM Message Mapping

Pseudowire Preferential Forwarding Status bit definition

draft-pwe3-redundancy-02.txt

Pseudowire (PW) Redundancy

RADIUS

RFC 2865 Remote Authentication Dial In User Service

RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture

draft-ietf-secsh-userauth.txt SSH Authentication Protocol

draft-ietf-secsh-transport.txt SSH Transport Layer Protocol

draft-ietf-secsh-connection.txt SSH Connection Protocol

draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

TCP/IP

RFC 768 UDP

RFC 1350 The TFTP Protocol

RFC 791 IP

RFC 792 ICMP

RFC 793 TCP

RFC 826 ARP

RFC 854 Telnet

RFC 1519 CIDR

RFC 1812 Requirements for IPv4 Routers

RFC 2347 TFTP option Extension

RFC 2328 TFTP Blocksize Option

RFC 2349 TFTP Timeout Interval and Transfer Size option

draft-ietf-bfd-mib-00.txt Bidirectional Forwarding Detection Management Information Base

Timing

ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008

ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.

GR-1244-CORE Clocks for the Synchronized Network: Common Generic Criteria, Issue 3,May 2005

ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.

ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.

ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.

IEEE Std 1588™-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

VPLS

RFC 4762 Virtual Private LAN Services Using LDP (previously draft-ietf-l2vpn-vpls-ldp-08.txt)

VRRP

RFC 2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol

RFC 3768 Virtual Router Redundancy Protocol

Proprietary MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib

TIMETRA-CAPABILITY-7210-SAS-M-V5v0.mib

(7210 SAS-M Only)

TIMETRA-CAPABILITY-7210-SAS-X-V5v0.mib (7210 SAS-X Only)

TIMETRA-CHASSIS-MIB.mib

TIMETRA-CLEAR-MIB.mib

TIMETRA-DOT3-OAM-MIB.mib

TIMETRA-FILTER-MIB.mib

TIMETRA-GLOBAL-MIB.mib

TIMETRA-IEEE8021-CFM-MIB.mib

TIMETRA-LAG-MIB.mib

TIMETRA-LOG-MIB.mib

TIMETRA-MIRROR-MIB.mib

TIMETRA-NTP-MIB.mib

TIMETRA-OAM-TEST-MIB.mib

TIMETRA-PORT-MIB.mib

TIMETRA-QOS-MIB.mib

TIMETRA-SAS-ALARM-INPUT-MIB.mib

TIMETRA-SAS-FILTER-MIB.mib

TIMETRA-SAS-IEEE8021-CFM-MIB.mib

TIMETRA-SAS-IEEE8021-PAE-MIB.mib

TIMETRA-SAS-GLOBAL-MIB.mib

TIMETRA-SAS-LOG-MIB.mib.mib

TIMETRA-SAS-MIRROR-MIB.mib

TIMETRA-SAS-MPOINT-MGMT-MIB.mib (Only for 7210 SAS-X)

TIMETRA-SAS-PORT-MIB.mib

TIMETRA-SAS-QOS-MIB.mib

TIMETRA-SAS-SDP-MIB.mib

TIMETRA-SAS-SYSTEM-MIB.mib

TIMETRA-SAS-SERV-MIB.mib

TIMETRA-SAS-VRTR-MIB.mib

TIMETRA-SCHEDULER-MIB.mib

TIMETRA-SECURITY-MIB.mib

TIMETRA-SERV-MIB.mib

TIMETRA-SYSTEM-MIB.mib

TIMETRA-TC-MIB.mib

TIMETRA-ISIS-MIB.mib

TIMETRA-ROUTE-POLICY-MIB.mib

TIMETRA-MPLS-MIB.mib

TIMETRA-RSVP-MIB.mib

TIMETRA-LDP-MIB.mib

TIMETRA-VRRP-MIB.mib

TIMETRA-VRTR-MIB.mib

INDEX