7210 SAS D, E OS
Quality of Service Guide

Software Version: 7210 SAS OS 4.0 Rev. 01
October 2011
Document Part Number: 93-0374-01-01

TABLE OF CONTENTS

Table of Contents

LIST OF TABLES

LIST OF FIGURES

QoS Policies

Preface

About This Guide

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

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.

This guide provides information to configure QoS policies on both 7210 SAS E and 7210 SAS D devices. Unless otherwise noted, the QoS policies are applicable to both 7210 SAS E and 7210 SAS D devices.

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 D and E OS documentation set is composed of the following books:

- 7210-SAS D and E OS Basic System Configuration Guide

  This guide describes basic system configurations and operations.

- 7210-SAS D and E OS System Management Guide

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

- 7210-SAS D and E OS Interface Configuration Guide

  This guide describes card, Media Dependent Adapter (MDA), and port provisioning.

- 7210-SAS D and E 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 D and E OS Services Guide

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

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

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

- 7210-SAS D and E OSQuality of Service Guide

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

Technical Support

If you purchased a service agreement for your 7210 SAS 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.

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 63
	• Accounting Mode	Frame Based Accounting on page 69
	• Network	Network QoS Policies on page 85
	• Network queue	Network Queue QoS Policies on page 133
	• SAP ingress	Service Ingress QoS Policies on page 155
	• Access egress	Access Egress QoS Policies on page 219
	• Port scheduler	QoS Port Scheduler Policies on page 243
	• Slope	Slope QoS Policies on page 261
Reference	• List of IEEE, IETF, and other proprietary entities	Standards and Protocol Support on page 361

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 D, E are designed with QoS mechanisms on both ingress and egress to support multiple services per physical port. The 7210 SAS D, E have 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 58.

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 D, E QoS policies are applied on service ingress, access ports, egress and access uplink ports and define:

- 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 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.

Network QoS policies are applied to access uplink ports. On ingress, the policy applied to 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 access uplink ports . The policies define the forwarding class queue characteristics for these entities.

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 port. A network QoS policy defines both ingress and egress behavior. One network queue policy can be applied to the access uplink port.

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

A summary of the major functions performed by the QoS policies is listed in Table 2.

Table 2: QoS Policy Types and Descriptions

Policy Type	Applied at…	Description	Page
Service Ingress	SAP ingress	• Defines up to 32 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).	39
Access Egress	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.	39
Egress Rate	Port	Configures the maximum bandwidth available for egress-traffic.	
Accounting Mode	Device Level	Sets the accounting mode to packet-based or frame-based for ingress and egress QoS policies	
Network	Access uplink ports	• Used for classification/marking of IP packets. • At ingress, defines Dot1p to FC mapping and 12 meters. • At egress, defines FC to Dot1p marking.	
Network Queue	Access uplink ports	• Defines forwarding class mappings to network queues and queue characteristics for the queues.	26
Slope	Ports	• Enables or disables the high-slope, low-slope, and non-TCP parameters within the egress pool.	54
Port scheduler	Port	• Defines the parameters for the port scheduler.	111

Service and Network QoS Policies

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

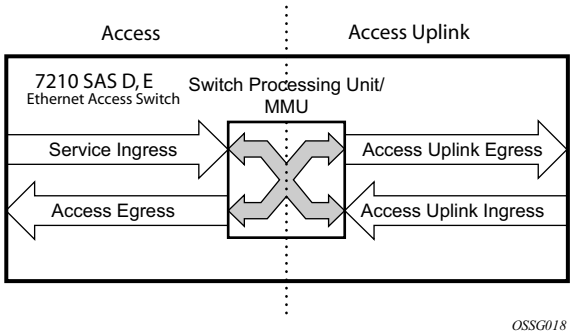

Figure 1: 7210 SAS D, E Traffic Types

The 7210 SAS uses QoS policies applied to a SAP for a service or to an access uplink portto define the queuing, queue attributes, 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

Network QoS policies 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 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 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.
  - → 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 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 28.
- 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. 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 for 7210 SAS E devices and can be enabled or disabled for 7210 SAS D devices. Table 5 lists the default mapping of forwarding class to Dot1p values.

Table 4: Default Network QoS Policy Egress Marking

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	001 - 1	001 - 1
0	Best Effort	be	BE	000 - 0	000 - 0

For network ingress, Table 5 lists the default mapping of Dot1p values to forwarding class and profile state for the default network QoS policy.

Table 5: Default Network QoS Policy Dot1p to FC Mapping

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

Table 5: Default Network QoS Policy Dot1p to FC Mapping

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 access uplink ports. The system allocates 8 queues for the network port and FCs are mapped to these 8 queues. All policies will use eight queues like the default network queue policy.

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 6 describes the default network queue policy definition.

Table 6: Default Network Queue Policy Definition.(For 7210 SAS E and 7210 SAS D devices)

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%
Low-1 (l1	Queue 4	• PIR = 100% • CIR = 25% • CBS = 7%

Table 6: Default Network Queue Policy Definition.(For 7210 SAS E and 7210 SAS D devices)

Forwarding Class	Queue	Definition (Continued)
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 access uplinkfor QoS.

The meter parameters are:

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 D, E have 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 29.

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 D, E have 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 29.

The PIR for meter is provisioned on service ingress and access uplink/network 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.

Adaptation Rule for Meters in 7210 SAS E Devices

Hardware supports rates to be in the multiple of 64 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 64 kbps that is equal to or higher than the specified rate.
- Maximum: Find the next multiple of 64 kbps that is equal to or less than the specified rate.
- Closest: Find the next multiple of 64 kbps that is closest to the specified rate.

Table 7 lists the rate values configured in the hardware when different PIR or CIR rates are specified in the CLI.

Table 7: Administrative Rate Example

Administrative Rate	Operation Rate (Min)	Operation Rate (Max)	Operation Rate (Closest)
64	64	64	64
65	128	64	64

Table 7: Administrative Rate Example (Continued)

Administrative Rate	Operation Rate (Min)	Operation Rate (Max)	Operation Rate (Closest)
127	128	64	128

If user has configured any value greater than 0 and less than 64 then operation rate configured on hardware would be 64 kbps irrespective of the constraint used.

Adaptation Rule for Meters in 7210 SAS D Devices

Hardware supports meter rates in the multiples of 8 kbps for the entire range of CIR or PIR rates supported on the device. The system identifies the best operational rate depending on the defined constraint. The supported constraints are listed below:

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

For 7210 SAS D devices, the maximum CIR and PIR rate is 4000000. The range of CBS and MBS is 4 up to 16384.

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.

Maximum Burst Size

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.

trtcm1 implements the policing algorithm defined in RFC2698 and trtcm2 implements the policing algorithm defined in RFC4115.

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

Meter Counters

The 7210 SAS D, E maintain the 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 E supports following meter modes:

- srtcm: Single Rate Three Color Marking
- trtcm1:Two Rate Three Color Marking1

The 7210 SAS D supports the following meter modes:

- srtcm: Single Rate Three Color Marking
- trtcm1:Two Rate Three Color Marking1
- 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 . trtcm1 implements the policing algorithm defined in RFC2698 and trtcm2 implements the policing algorithm defined in RFC4115.

Color Aware Policing

The 7210 SAS D, E support 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).

Queue Parameters

This section describes the queue parameters provisioned on access ports and access uplink port's queues for QoS.

The queue parameters are:

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 D, E, 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 20.

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 36

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 access uplink queues are defined within network queue policies based on the forwarding class. The CIR for the access uplink 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 access uplink queues are defined within network queue policies based on the forwarding class. The PIR for the access uplink 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 36

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 64to 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.

In 7210 SAS E devices, for the supported CIR/PIR range values 0 to 1Gb, the same hardware rate step of 64 kbps is used.

In 7210 SAS D devices, for the supported CIR/PIR range values 0 to 1Gb, the same hardware rate is shown in Table 8.

Table 8: Supported Hardware Rates and CIR/PIR Values

Hardware Rate Steps	Rate Range (kbps)
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 - 1000000 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 128 Kbps and 192 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 64 Kbps and 128 Kbps.

If the adaptation rule is **closest**, the operational CIR and PIR values will be 64 Kbps and 128 Kbps, respectively, as those are the closest matches for the administrative values that are even multiples of the 64 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 and access uplink 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.
- At least one default unicast forwarding class meter. The parameters that can be configured for a meter are discussed in Meter Parameters on page 28.
- At least one multipoint forwarding class meter.

Optional service ingress QoS policy elements for 7210 SAS E include:

- Additional unicast meters up to a total of 17.
- Additional multipoint meters up to 17.
- QoS policy match criteria to map packets to a forwarding class.

Optional service ingress QoS policy elements for 7210 SAS-D include:

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

Each meter can have unique meter parameters to allow individual policing of the flow mapped to the forwarding class. Figure 2 depicts service traffic being classified into three different forwarding classes.

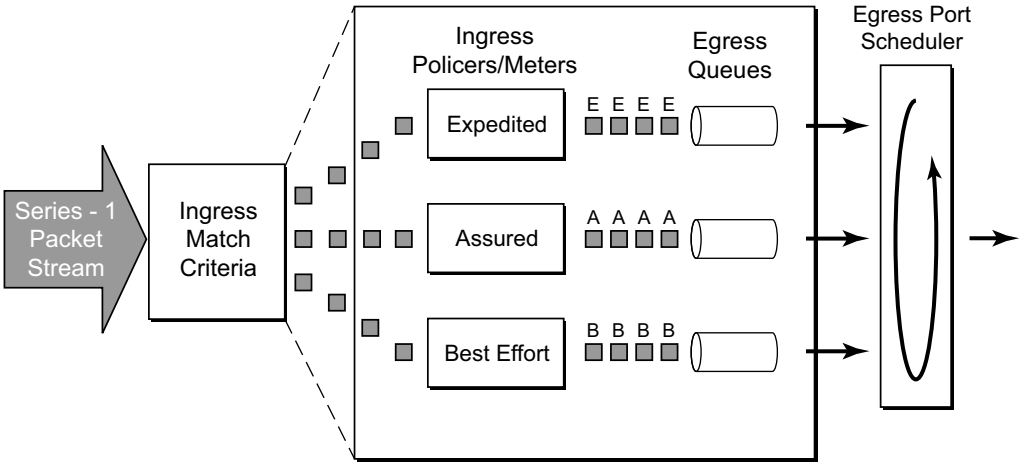

Figure 2: Traffic Queuing Model for Forwarding Classes

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 9 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 9 and Table 10 list the supported IP and MAC match criteria.

Table 9: Service Ingress QoS Policy IP Match Criteria

IP Criteria
• DSCP value

Table 10: Service Ingress QoS Policy MAC Match Criteria

MAC Criteria
• IEEE 802.1p value/mask • Source MAC address/mask • Destination MAC address/mask • EtherType value

The MAC match criteria that can be used for an Ethernet frame depends on the frame's format. Note that 7210 SAS D, E do not support configuring of the **frame-type** match criteria. See Table 11.

Table 11: MAC Match Ethernet Frame Types

Note: The default frame type configured is Ethernet - II

Frame Format	Description
802dot3	IEEE 802.3 Ethernet frame. Only the source MAC, destination MAC and IEEE 802.1p value are compared for match criteria.
802dot2-llc	IEEE 802.3 Ethernet frame with an 802.2 LLC header. Only the source MAC and destination MAC address are compared for match criteria.
802dot2-snap	IEEE 802.2 Ethernet frame with 802.2 SNAP header. Only the source MAC and destination MAC address 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 12 lists the criteria that can be matched for the various MAC frame types.

Table 12: MAC Match Criteria Frame Type Dependencies

Frame Format	Source MAC	Dest MAC	IEEE 802.1p Value	Etype Value
802dot3	Yes	Yes	Yes	No
802dot2-llc	Yes	Yes	Yes	No
802dot2-snap	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. The characteristics of the default policy are listed in Table 13.

Table 13: 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 (line rate) • MBS, CBS = default (values derived from applicable policy)
	Meter 11	1 (one) meter for all multipoint traffic: • CIR = 0 • PIR = max (line rate) • 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)

Hierarchical Ingress Policing

Note: Hierarchical Ingress Policing supported only on 7210 SAS-D devices.

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 disposition of the packet, refer to the command description of "aggregate-meter-rate" command in the 7210 SAS D, E 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.

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 20, Forwarding Class to Queue-ID Map, on page 59. 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 33.
- IEEE 802.1p priority value remarking based on forwarding class.

  All customer traffic containing IEEE 802.1p encapsulation will be marked according to the default FC-Dot1p marking map if Dot1p values are not explicitly configured.

Each queue in a policy is associated with one forwarding class. Each queue can have its individual queue parameters allowing individual rate shaping of the forwarding class mapped to the queue.

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. If the packet was received over a service transport tunnel on a network port, the forwarding class is markedin the outer tag of the QinQ encapsulation.

Access egress QoS policy ID 1 is reserved as the default access egress policy. The default policy cannot be deleted or changed. The default access egress policy is applied to all 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 14: 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 14: 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 destroyed in the 7210 SAS. The **default** pools created by the system are distributed among various ports.

The 7210 SAS D, E only support port egress buffer pools. The egress buffer pools are distributed as access uplink egress buffer pool and access egress buffer pools. During system initialization, based on the maximum number of ports to be supported for access and access uplink, the total buffer is distributed into the access egress buffer pool and the access uplink egress buffer pool. The distribution of the buffers into access and access uplink 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.

The access uplink port is allocated more buffer as compared to an access port. The 7210 SAS device is typically used with traffic received through the access ports being aggregated on the access uplink ports. Thus the access uplink ports will be mostly congested. By providing additional buffer capacity to access uplink ports as compared to the access ports more bursty traffic can be transported over the congested links with improved throughput.

Slope Policies

The available buffer space is partitioned into buffer pools. The buffers for a queue are allocated from a single buffer pool. Buffer pools are created for access port egress, and access uplink port egress.

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

Default buffer pools exist (logically) at the port levels. Each physical port has two pools objects associated:

- Access egress pool
- Access uplink egress pool

By default, each pool is associated with slope-policy **default** which disables the high-slope and low-slope for all the queues.

Access and access uplink pools are created at the port level; creation is dependent on the physical port mode (access uplink or access).

RED Slopes

Operation and Configuration (for 7210 SAS-E devices)

Each buffer pool supports a high-priority RED slope, a non-TCP 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.

By default, the high-slope and low-slope for all the 8 queues are disabled.

In the 7210 SAS E, SRED is supported. SRED 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.

Operation and Configuration (for 7210 SAS-D devices)

Each buffer pool supports a high-priority RED slope, a non-TCP 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.

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

In the 7210 SAS D, WRED is supported. 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 usersoftware (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 61.)
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.

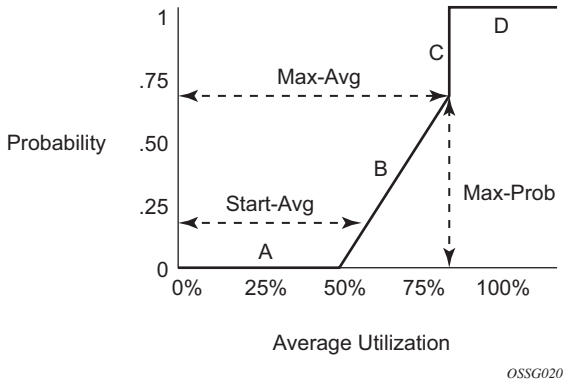

Figure 3: RED Slope Characteristics

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 3):

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 D allows 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 D 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 15 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 15: 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 15: 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 (for 7210 SAS-E devices)

The elements required to define a slope policy are:

- A unique policy ID
- The high and low RED slope shapes for the buffer pool: start-threshold, drop-rate per egress queue settings for the high-priority and low-priority RED slopes.

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

Each access egress buffer pool and access uplink egress pool can be associated with one only 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 access uplinkbuffer pools which do not have another slope policy explicitly assigned.

Table 16 lists the default values for the default slope policy.

Table 16: Default Slope Policy Definition

Parameter	Description	Setting
Policy ID	Slope policy ID	1 (Policy ID 1 reserved for default slope policy)
High (RED) slope	Administrative state	Shutdown
	start-avg	70% utilization
	max-avg	90% utilization
	max-prob	80% probability
Low (RED) slope	Administrative state	Shutdown
	start-avg	50% utilization
	max-avg	75% utilization
	max-prob	80% probability
TAF	Time average factor	7

Table 17 lists the mapping from drop-rate scalar value to percent value.

Table 17: Drop Rate Value to Percent Mapping Values

Drop Rate	% Drop Rate
0	100% cliff drop.
1	6.25%.
2	3.125%.
3	1.5625%.
4	0.78125%.
5	0.390625%.
6	0.1953125%.
7	0.09765625%.

Slope Policy Parameters (for 7210 SAS D devices)

The elements required to define a slope policy are:

- A unique policy ID
- The high and low RED slope shapes for the buffer pool: settings for the high-priority and low-priority RED slopes.
- The high-slope (for tcp in-profile packets), low-slope (for tcp out-of-profile packets) and non-tcp slope(for non-tcp packets). All three slopes are on a per port per queue basis. And configurable parameters on each slope are start-avg, max-avg,max-prob and timeaveraging-factor.

A slope policy is defined with generic parameters so that it is not inherently an access or an 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 one only 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 andnetworkbuffer pools which do not have another slope policy explicitly assigned.

Table 18 lists the default values for the default slope policy.

Table 18: Default Slope Policy Definition (for 7210 SAS D)

Parameter	Description	Setting
Policy ID	policy ID	default (for default policy)
High (RED) slope	Administrative state	Shutdown
	start-avg	70% utilization
	max-avg	90% utilization
	max-prob	75% probability
Low (RED) slope	Administrative state	Shutdown
	start-avg	50% utilization
	max-avg	75% utilization
	max-prob	75% probability
Non-TCP (RED) slope	Administrative State	Shutdown
	start-avg	50% utilization
	max-avg	75% utilization
	max-prob	75% probability

Egress Port Rate Limiting

The 7210 SAS D, E support 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 19).

Table 19: Forwarding Classes

FC-ID	FC Name	FC Designa-tion	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 19 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 on page 23. 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 D, E. Each of these FC is mapped to a specific queue while traffic is flowing on the egress port. By mapping FC to different queues the differential treatment is imparted to various classes of traffic.

In the7210 SAS D, E, 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 access uplink 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 access uplink 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 20.

Table 20: 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, one default network QoS policy and one default port scheduler policy. Only one ingress QoS policy and one egress QoS policy can be applied to a SAP or access/access-uplink port.

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.

QoS policies can be applied to the following entities:

- Access egress policies on access ports
- Network QoS policy on access uplinknetwork port
- Network queue policy (egress) on access uplinknetwork port .

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

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/access uplinkaccess 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 and access uplinksupport 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.

Affect of Port Level Rate-Limiting on Access Uplink Queue Functionality

- When an egress-rate sub-rate value is given, the /access-uplink queue 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 and 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.
- For 7210 SAS E devices, 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 32kb for a 1G port and 66kb for a 10G port. User cannot configure max-burst without configuring egress-rate. The value should be between 32 and 16384 or default. 7210 SAS-D devices do not support 10G port.
- By default there is no egress-rate command set on port. By default egress-rate for a port is maximum (equal to line-rate).

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 egress-rate command. The rate for egress-rate option and the 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. For more information on the CLI and description, see Port Level Egress-Rate Command Reference on page 73.

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.

Affects 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. Access uplink 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.

Affects of Enabling Egress Frame Based Accounting on Access Uplink 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, 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.

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 32 and 16384 or default.

Note: 7210 SAS-D devices do not support 10G port.

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. 7210 SAS-D devices do not support 10G port.

max-burst — Specifies an integer value, in kilo-bits, between 32 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>qos>network-queue# show port 1/1/1
===============================================================================
Ethernet Interface
===============================================================================
Description        : 10/100/Gig Ethernet SFP
Interface          : 1/1/1                       Oper Speed       : 1 Gbps
Link-level         : Ethernet                    Config Speed     : 1 Gbps
Admin State        : up                          Oper Duplex      : full
Oper State         : up                          Config Duplex    : full
Physical Link      : Yes                         MTU              : 1514
IfIndex            : 35684352                    Hold time up     : 0 seconds
Last State Change  : 01/17/2011 04:05:37         Hold time down   : 0 seconds
Last Cleared Time  : N/A

Configured Mode    : access                      Encap Type       : null
Dot1Q Ethertype    : 0x8100                      QinQ Ethertype   : 0x8100
Net. Egr. Queue Pol: default                     Access Egr. Qos *: 1
Egr. Sched. Pol    : default                     Network Qos Pol  : n/a
Auto-negotiate     : limited                     MDI/MDX          : MDI
Accounting Policy  : None                        Collect-stats    : Disabled
Egress Rate        : Default                     Max Burst        : Default
Uplink             : No

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

Configured Address : 00:78:76:45:54:02
Hardware Address   : 00:78:76:45:54:02
Cfg Alarm          :
Alarm Status       :

Transceiver Data

Transceiver Type   : SFP
Model Number       : 3HE00027AAAA02  ALA  IPUIAELDAB=
TX Laser Wavelength: 850 nm                      Diag Capable     : yes
```

```
Connector Code     : LC                          Vendor OUI       : 00:0a:1d
Manufacture date   : 2008/08/10                  Media            : Ethernet
Serial Number      : OPCPCH08052638
Part Number        : TRPAG1SXLAES-TM
Optical Compliance : GIGE-SX
Link Length support: 550m for 50u MMF; 280m for 62.5u MMF;
===============================================================================
Traffic Statistics
===============================================================================
                                                    Input                Output
-------------------------------------------------------------------------------
Octets                                                 0                     0
Packets                                                0                     0
Errors                                                 0                     0
===============================================================================
* indicates that the corresponding row element may have been truncated.
===============================================================================
Port Statistics
===============================================================================
                                                    Input                Output
-------------------------------------------------------------------------------
Unicast Packets                                        0                     0
Multicast Packets                                      0                     0
Broadcast Packets                                      0                     0
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:dut-1>config>qos>network-queue#
```

Frame Based Accounting Command Reference

Command Hierarchies

Configuration Commands

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

associations — Displays the associations of the sap-ingress policy.

match-criteria — Displays the match criteria of the sap-ingress policy.

detail — Displays the detailed information of the sap-ingress policy.

Sample Output

```
*A:Dut-1# show qos sap-ingress 1
===============================================================================
QoS Sap Ingress
===============================================================================
-------------------------------------------------------------------------------
Sap Ingress Policy (1)
-------------------------------------------------------------------------------
Policy-id          : 1                        Scope              : Template
Default FC         : be
Criteria-type      : None
Accounting         : frame-based
Classifiers Allowed: 16                       Meters Allowed     : 8
Classifiers Used   : 2                        Meters Used        : 2
Description    : Default SAP ingress QoS policy.

===============================================================================
*A:Dut-1#
```

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.

detail — Displays the detail policy information.

Sample Output

```
*A:Dut-1# show qos network 1
===============================================================================
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     : frame-based
Description    : Default network-port QoS policy.
-------------------------------------------------------------------------------
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.
-------------------------------------------------------------------------------
Port Attachments
-------------------------------------------------------------------------------
Port-id : 1/1/3
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:Dut-1#
```

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

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 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 portsIt 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 marking values associated with each forwarding class.

Each forwarding class defined within the system automatically creates a queue on each access uplink ports. This queue gets all the parameters defined within the default network QoS policy 1 until an explicit policy is defined for the access uplink ports.

For 7210 SAS-E, remarking is always enabled on the access uplink ports. For 7210 SAS-D devices, remarking can be enabled or disabled on access ports and access uplink ports. 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, 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 Dot1p-to-FC mapping and default meters for unicast and multipoint meters for the ingress. For the egress, it defines eight forwarding classes 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 access uplink ports 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 7210 SAS D, E OS Basic System Configuration Guide.

Normal QoS Operation

The following types of QoS mapping decisions are applicable on an access-uplink port.

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

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

DSCP Marking CPU Generated Traffic

DSCP marking for CPU generated traffic is not configurable by the user. The default values are given in Table 23:

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

Table 21: DSCP and Dot1p Marking

Protocol	IPv4	DSCP Marking	Dot1P Marking	Default FC	DSCP Values	DOT1P Values
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
SNMP trap/log	Yes	Yes	Yes	H2	34	4
ICMP ping	Yes	Yes	Yes	NC	0	7
Trace route	Yes	Yes	Yes	NC	0	7
TACPLUS	Yes	Yes	Yes	H2	34	4

Default DSCP Mapping Table

```
DSCP Name  DSCP Value   DSCP Value  DSCP Value   Label
           Decimal      Hexadecimal Binary
============================================================
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 appropriate typeis applied to each uplink port.

To create an network QoS policy , define the following:

- A network policy ID value. The system will not dynamically assign a value.
- Include a description. The description provides a brief overview of policy features.
- You can modify egress FC-Dot1p marking map. Otherwise, the default values are applied.
  - → Remarking — For 7210 SAS-E devices, remarking is always enabled, this command remarks ALL packets that egress on the specified access uplink port. The remarking is based on the forwarding class to Dot1p bit mapping defined under the egress node of the network QoS policy. For 7210 SAS-D devices remarking can be enabled or disabled.
  - → 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 the Dot1p to forwarding class mapping for all packets and defines Dot1p bits to forwarding class mapping for all packets.
  - → Default action — Defines the default action to be taken for packets that have an undefined 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 network 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:

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 {closest | 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: access uplink portsconfig>port
ethernet
access
uplink
qos *network-policy-id*

The following output displays the configuration for uplink port 1/1/1 with network policy 600 applied to the interface.

```
A:ALA-7>config# info
#------------------------------------------------
echo "Port Configuration"
#------------------------------------------------
    port 1/1/1
        shutdown
        description "port 1/1/1"
        ethernet
            mode access uplink
            access
                uplink
                    qos 600
                exit
            exit
        exit
    exit
...
#------------------------------------------------
A:ALA-7>config#
```

Default Network Policy Values

The default network policy access uplink ports is identified as policy-id **1**. Default policies cannot be modified or deleted. The following displays default network policy parameters:

Table 22: Network Policy Defaults

Field	Default
description	Default network QoS policy.
scope	template
ingress	
default-action	fc be profile out
egress	
remarking	yes (for 7210 SAS-E), no (for 7210 SAS-D)
fc af:	
dot1p-in-profile	3
dot1p-out-profile	2
fc be:	
dot1p-in-profile	0
dot1p-out-profile	0
fc ef:	
dot1p-in-profile	5
dot1p-out-profile	5
fc h1:	
dot1p-in-profile	6
dot1p-out-profile	6
fc h2:	
dot1p-in-profile	4
dot1p-out-profile	4

Table 22: Network Policy Defaults (Continued)

Field	Default
fc l1:	
dot1p-in-profile	3
dot1p-out-profile	2
fc l2:	
dot1p-in-profile	1
dot1p-out-profile	1
fc nc:	
dot1p-in-profile	7
dot1p-out-profile	7

Table 23: Default Network QoS Policy Dot1p to FC Mapping

Dot1p 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 following output displays the default configuration:

```
*A:ALU-7210>config>qos>network# info detail
----------------------------------------------
            description "Default network QoS policy."
            scope template
            ingress
                default-action fc be profile out
                meter 1 create
                    mode trtcm
```

```
                    adaptation-rule pir closest pir closest
                    rate 0 pir max
                    mbs default
                    cbs default
                exit
                meter 9 multipoint create
                    mode trtcm
                    adaptation-rule pir closest cir closest
                    rate 0 pir max
                    mbs default
                    cbs default
                exit
                dot1p 0 fc be profile out
                dot1p 1 fc l2 profile in
                dot1p 2 fc af profile out
                dot1p 3 fc af profile in
                dot1p 4 fc h2 profile in
                dot1p 5 fc ef profile in
                dot1p 6 fc h1 profile in
                dot1p 7 fc nc profile in
            exit
            egress
                no remarking
                fc af
                    dot1p-in-profile 3
                    dot1p-out-profile 2
                exit
                fc be
                    dot1p-in-profile 0
                    dot1p-out-profile 0
                exit
                fc ef
                    dot1p-in-profile 5
                    dot1p-out-profile 5
                exit
                fc h1
                    dot1p-in-profile 6
                    dot1p-out-profile 6
                exit
                fc h2
                    dot1p-in-profile 4
                    dot1p-out-profile 4
                exit
                fc l1
                    dot1p-in-profile 3
                    dot1p-out-profile 2
                exit
                fc l2
                    dot1p-in-profile 1
                    dot1p-out-profile 1
                exit
                fc nc
                    dot1p-in-profile 7
                    dot1p-out-profile 7
                exit
            exit
        ----------------------------------------------
        *A:ALU-7210>config>qos>network#
```

Service Management Tasks

Deleting QoS Policies

A network policy is associated by default with access uplink ports.

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 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.

Resource Allocation for Network QoS policy

This section describes the allocation of QoS resources for network QoS policy.

When the port mode is changed to access-uplink, a default network QoS policy is applied. For the default policy, two meters and eighteen classification entries in hardware are allocated.

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.

For computing the number of QoS resources used by an access uplink port:

- 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):

$$TC = \Sigma_{i=nc,h1,ef,h2,l1,af,l2,be} \; 2 * E(i)$$

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

Example 1

```
network 1 create
     description “default nowork QoS policy”
            ingress
                default-action fc be profile out
                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 = 18

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

Example 2

```
network 2 create
     description “network-policy-2”

            ingress
                default-action fc be profile out
                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
                dot1p 2 fc af profile out
            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 create
     description “network-policy-3”
            ingress
                default-action fc be profile out
                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
                dot1p 2 fc af profile out
            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 create
     description “network-policy-4”
            ingress
                default-action fc be profile out
                meter 1 create
                exit
                meter 9 multipoint create
                exit
                dot1p 1 fc l2 profile in
                dot1p 2 fc af profile out
                dot1p 3 fc af profile in
                dot1p 4 fc h2 profile in
                dot1p 5 fc ef profile in
                dot1p 6 fc h1 profile in
                dot1p 7 fc nc profile in
            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 create
     description “network-policy-5”
            ingress
                default-action fc be profile out
                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
            dot1p 1 fc l2 profile in
            dot1p 2 fc af profile out
            dot1p 3 fc af profile in
            dot1p 4 fc h2 profile in
            dot1p 5 fc ef profile in
            dot1p 6 fc h1 profile in
            dot1p 7 fc nc profile in
        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 create
     description “network-policy-6”

            ingress
                default-action fc be profile out
                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
                dot1p 1 fc l2 profile in
                dot1p 2 fc af profile out
                dot1p 3 fc af profile in
                dot1p 4 fc h2 profile in
                dot1p 5 fc ef profile in
                dot1p 6 fc h1 profile in
                dot1p 7 fc nc profile in
            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 create
            description "network-policy 2"
            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
                meter 9 multipoint create
                    mode trtcm
                    adaptation-rule cir closest pir closest
                    rate cir 0 pir max
                    mbs default
                    cbs default
                exit
                network-policy 2 0 fc be profile out
                network-policy 2 1 fc l2 profile in
                network-policy 2 2 fc af profile out
                network-policy 2 3 fc af profile in
                network-policy 2 4 fc h2 profile in
                network-policy 2 5 fc ef profile in
                network-policy 2 6 fc h1 profile in
                network-policy 2 7 fc nc profile in
            exit
            egress
                no remarking
```

The number of classification entries (TC) used is: 18.

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

Example 8

```
network 8 create
     description “network-policy-8”
            ingress
                default-action fc nc profile in
                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
                dot1p 1 fc l2 profile in
                dot1p 3 fc af profile in
                dot1p 5 fc ef profile in
                dot1p 7 fc nc profile in
            exit
            egress
```

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

$$(2 * 2)\text{nc} + (2 * 0)\text{h1} + (2 * 1)\text{ef} + (2 * 0)\text{h2} + (2 * 0)\text{l1} + (2 * 1)\text{af} + (2 * 1)\text{l2} + (0 * 0)\text{be} = 10$$

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

Network QoS Policy Command Reference

Command Hierarchies

Configuration Commands

```
config
    — qos
        — [no] network network-policy-id [create]
            — description description-string
            — no description
            — scope {exclusive | template}
            — no scope
            — egress
                — [no] fc fc-name
                    — no dot1p-in-profile dot1p-priority
                    — no dot1p-out-profile dot1p-priority
                — [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 {trtcm 1| srtcm}
                    — no mode
                    — rate cir-rate-in-kbps [pir pir-rate-in-kbps]
                    — no rate
```

Operational Commands

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

Show Commands

show
— **qos**
— **network** *policy-id* [**detail**]

Configuration Commands

Generic Commands

description

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

Context config>qos>network *policy-id*

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]
[**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. The default network policy can be copied (use the copy command) to create a new network policy that includes the default ingress Dot1p 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

ldp-local-fc-enableldp-local-fc-enable

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 Dot1p to forwarding class mappingfor all 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 Dot1pbits 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 Dot1por dot1p bits 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, the in-profile packets are preferentially queued over the out-of-profile packets.

Default None

Values in, out

dot1p

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

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 be assigned to the forwarding class and 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 ports 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 . 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 1 — 12

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 queue 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 For network policy : 1 — 12 (except 9, the default multipoint meter)

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.

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 2— 12

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 64 kbps (for 7210 SAS E) and 8 kbps (for 7210 SAS D) 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 64 kbps (for 7210 SAS E) and 8 kbps (for 7210 SAS D) 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 64 kbps (for 7210 SAS E) and 8 kbps (for 7210 SAS D) 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 32(for 7210 SAS E) — 16384, default

4(for 7210 SAS D)-- 16384, 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 32(for 7210 SAS E) — 16384, default

4(for 7210 SAS D) -- 16384, default

mode

Syntax **mode** {**trtcm1** | **srtcm**}
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 (trTCM1) 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 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.

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).

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 1 — 2000000(for 7210 SAS E), max

0 — 4000000(for 7210 SAS D), 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 0 — 2000000(for 7210 SAS E), max

0 — 4000000(for 7210 SAS D), 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 Dot1p marking map to be instantiated when this policy is applied to the network port.

The forwarding class and profile state mapping to Dot1p bits mapping for all packets are defined in this context.

All out-of-profile service packets are marked with the corresponding out-of-profile Dot1p bit value at network egress. All the in-profile service ingress packets are marked with the corresponding in-profile Dot1p bit 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.

The **no** form of this command removes the forwarding class Dot1p map associated with this queue, 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

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

remarking

Syntax **remarking**

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

Description Remarking is always enabled on the access uplink ports for 7250 SAS E devices. For 7210 SAS D devices remarking can be enabled or disabled. Since the 7210 SAS D, E are used to connect to a particular diffserv domain so it is very important that each and every packet ingressing on the 7210 SAS D, E is mapped and marked and thereby assigned to a particular diffserv class while going through the network. The downstream node, a 7x50 router, will be assigning the FC based on the Dot1P assigned in 7210 SAS D, E.

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 Dot1p bit mappings and network policy interface associations.

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

Table 24: Show QoS Network Output Fields

Label	Description
Policy-Id	The ID that uniquely identifies the policy.
Remark	True – For 7210 E devices, 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. For 7210 SAS D devices remarking can be enabled or disabled.
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 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:ALA-12# show qos network
===============================================================================
Network Policies
===============================================================================
Policy-Id            Remark    Description
-------------------------------------------------------------------------------
1                    True Default network QoS policy.
```

```
===============================================================================
A:ALA-12#

*A:SN12345678# show qos network 1
===============================================================================
QoS Network Policy
===============================================================================
-------------------------------------------------------------------------------
Network Policy (1)
-------------------------------------------------------------------------------
Policy-id      : 1                            Remark       : True
Forward Class  : be                           Profile      : Out
Attach Mode    : l2                           Config Mode  : l2
Scope          : Template
Description    : Default network QoS policy.
-------------------------------------------------------------------------------
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.
-------------------------------------------------------------------------------
Port Attachments
-------------------------------------------------------------------------------
Port-id : 1/1/24
===============================================================================
*A:SN12345678#



*A:dut-g# show qos network 1 detail
===============================================================================
QoS Network Policy
===============================================================================
-------------------------------------------------------------------------------
Network Policy (1)
-------------------------------------------------------------------------------
Policy-id      : 1                            Remark       : True
Forward Class  : be                           Profile      : Out
Attach Mode    : l2                           Config Mode  : l2
Scope          : Template
Description    : Default network QoS policy.
-------------------------------------------------------------------------------
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.
-------------------------------------------------------------------------------
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

-------------------------------------------------------------------------------
Egress Forwarding Class Queuing
-------------------------------------------------------------------------------
FC Value       : 0                          FC Name      : be
- Dot1p Mapping
Out-of-Profile : 0                          In-Profile   : 0

FC Value       : 1                          FC Name      : l2
- Dot1p Mapping
Out-of-Profile : 1                          In-Profile   : 1

FC Value       : 2                          FC Name      : af
- Dot1p Mapping
Out-of-Profile : 2                          In-Profile   : 3

FC Value       : 3                          FC Name      : l1
- Dot1p Mapping
Out-of-Profile : 2                          In-Profile   : 3

FC Value       : 4                          FC Name      : h2
- Dot1p Mapping
Out-of-Profile : 4                          In-Profile   : 4

FC Value       : 5                          FC Name      : ef
- Dot1p Mapping
Out-of-Profile : 5                          In-Profile   : 5

FC Value       : 6                          FC Name      : h1
- Dot1p Mapping
Out-of-Profile : 6                          In-Profile   : 6

FC Value       : 7                          FC Name      : nc
- Dot1p Mapping
Out-of-Profile : 7                          In-Profile   : 7
-------------------------------------------------------------------------------
Port Attachments
-------------------------------------------------------------------------------
Port-id : 1/1/24
===============================================================================
*A:dut-g#
```

Sample output for 7210 SAS D:

```
*A:SAS-D>show>qos# network
Policy-id  Remark     LerUseDscp     Description
-------------------------------------------------------------------------------
1          False  False      Default network QoS policy.
===============================================================================
```

```
*A:SAS-D>show>qos# network


*A:SAS-D>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 QoS policy.

-------------------------------------------------------------------------------
DSCP                                  Forwarding Class               Profile
-------------------------------------------------------------------------------
No Matching Entries


-------------------------------------------------------------------------------
Dot1p Bit Map                        Forwarding Class               Profile
*A:SAS-D>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 access uplink ports. 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 . 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 access uplink ports . 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 access uplink ports.

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 20, Forwarding Class to Queue-ID Map, on page 59.

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.

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:

Table 25: Network Queue Policy Defaults

Field	Default
description	Default network queue QoS policy.
queue 1	
rate	100
cir	0
cbs	7
queue 2	
rate	100
cir	25
cbs	7
queue 3	
rate	100
cir	25
cbs	21
queue 4	
rate	100
cir	25
cbs	7
queue 5	
rate	100
cir	100
cbs	21
queue 6	

Table 25: Network Queue Policy Defaults (Continued)

Field	Default
rate	100
cir	100
cbs	21
queue 7	
rate	100
cir	10
cbs	7
queue 8	
rate	100
cir	10
cbs	7

```
*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#
```

Service Management Tasks

This section discusses the following service management tasks:

Deleting QoS Policies

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

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

```
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
                — 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 —** 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.

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 20, Forwarding Class to Queue-ID Map, on page 59. 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 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.

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 percentage that the queue can transmit packets through the switch fabric. 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 percentage at which the system prioritizes the queue over other queues competing for the same bandwidth. For network egress, the CIR also defines the rate that the queue isconsidered in-profile by the system. The in-profile and out-profile of the queue influences the scheduler priority queue metric. The in-profile and out-profile of the queue based on CIR and PIR is never marked in the packets. The packets at egress are considered in-profile and out-profile based on the SAP ingress policy meter results.

The **rate** command can be executed at anytime, altering the PIR and CIR rates for all queues The 8 queues which are available at egress port are always associated with the network queue QoS policy by the queue-id.

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

Default 100

Show 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 26: Network Queue Labels and Descriptions

Label	Description
Policy	The policy name that uniquely identifies the policy.
Accounting	Displays whether the accounting mode is packet-based or frame-based.
Description	A text string that helps identify the policy's context in the configuration file.
Port-Id	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>config>qos# show qos network-queue nq1-cbs detail
===============================================================================
QoS Network Queue Policy
-------------------------------------------------------------------------------
Network Queue Policy (nq1-cbs)
-------------------------------------------------------------------------------
Policy        : nq1-cbs
Accounting    : packet-based
-------------------------------------------------------------------------------
Queue CIR        PIR       CBS
      CIR Rule   PIR Rule
-------------------------------------------------------------------------------
1      0         32        8.29
       max       closest
2      0         100       6.00
       closest   closest
3      0         100       10.00
       closest   closest
4      0         100       6.00
       closest   closest
5      0         100       10.00
       closest   closest
6      0         4         10.00
       closest   closest
7      3         93        1.00
       closest   closest
8      0         3         7.00
       closest   closest
-------------------------------------------------------------------------------
FC    UCastQ
-------------------------------------------------------------------------------
be     1
l2     2
af     3
l1     4
h2     5
ef     6
h1     7
nc     8
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Port-id : 1/1/1
Port-id : 1/1/22
===============================================================================
*A:card-1>config>qos#
```

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

There is one default service ingress policy.

Each policy can have up to 32 ingress meters. The default policies can be copied and modified but they 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 SR OS Basic System Configuration Guide.

Default SAP Ingress Policy

```
A:ALA-7>config>qos>sap-ingress$ info detail
----------------------------------------------
     description “Default SAP ingress QoS policy”
     scope template
     meter 1 create
          mode trtcm1
          adaptation-rule cir closest pir closest
          rate cir 0 pir max
          mbs default
          cbs default
     exit
     meter 11 multipoint create
          mode trtcm1
          adaptation-rule cir closest pir closest
          rate cir 0 pir max
          mbs default
          cbs default
     exit
     default-fc be

----------------------------------------------
A:ALA-7>config>qos>sap-ingress$
```

SAP Ingress Policy Defaults

Table 27: SAP Ingress Policy Defaults

Field	Default
description	"Default SAP ingress QoS policy."
scope	template
meter	1
mode	trtcm1
adaptation-rule	cir closest pir closest
rate	pir = max, cir= 0
cbs	32kb
mbs	128kb
meter	11 (Multipoint)
mode	trtcm
adaptation-rule	cir closest pir closest
rate	pir = max, cir= 0
cbs	32kb
mbs	128kb
default-fc	be

Service Ingress Meter Selection Rules

The following are rules for meter selection by different traffic types under various configurations for VPLS services:

- 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 unknownunicast).
- 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.

The following are rules for meter selection for Epipe 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 QoS 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) 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 depending on policy association with a Epipe service,VPLS service or both Epipe and VPLS service.

Allocation of QoS Resources for a 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: If the number of SAPs is greater than the system limit, then the system limit takes precedence.

The user is allowed to mix and match SAPs with different QoS resources (that is, using different values of TQ). The allowed values in the 7210 SAS E devices for the parameter **num-qos-classifiers** are 16, 36, and 72. The allowed values in 7210 SAS D devices for the parameter num-qos-classifiers are 4,8,16,32,64,128 and 256. For 7210 SAS E, when **num-qos-resources** is configured with a value of 16, the system internally uses a value of 18.

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.

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 default meter #11 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 #11 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 meter #11 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 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, then the default unicast meter and the default 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 binary number (power of 2).

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.
- 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 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 165

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.
- For 7210 SAS E, Specify *num-qos-classifiers* parameter. By default, it is set to 16. It can be set to 16, 36 or 72. The number of meters allowed is equal to half the number of classifiers specified. The maximum number of meters allowed is equal to 32.
- For 7210 SAS D ,specify the num-qos-classifiers parameter. By default, it is set to 4. It can be set to 4, 8, 16, 32, 64, 128 or 256. The number of meters allowed is equal to half the number of classifiers specified. The maximum number of meters allowed is equal to 32.
- 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 IP or MAC criteria. You can define IP 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 multipoint create
          cbs 256
          mbs 512
          rate cir 100 pir 36
     exit
     meter 8 multipoint create
          cbs 256
          mbs 512
          rate cir 11000
     exit
     meter 9 multipoint create
          rate cir 11000
     exit
     meter 10 multipoint create
          rate cir 1
```

```
        exit
        meter 12 multipoint create
            rate cir 1500 pir 1500
        exit
        meter 13 multipoint create
            rate cir 2500 pir 2500
        exit
        meter 14 multipoint create
            rate cir 36 pir 100
        exit
            meter 15 multipoint create
            rate cir 36 pir 100
        exit
        meter 16 multipoint 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 17
          unknown-meter 18
     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:

```
A:ALA-7>config>qos# info
...
#------------------------------------------
echo "QoS Policy Configuration"
#------------------------------------------
...
sap-ingress 100 create
...
     ip-criteria
          entry 10 create
               description "Entry 10-FC-AF"
               match dscp af12
               exit
               action fc af
          exit
          entry 20 create
               description "Entry 20-FC-BE"
               match dscp be
               exit
               no action
          exit
     exit
exit
..
#------------------------------------------
A:ALA-7>config>qos#
```

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:

```
A:ALA-7>config>qos# info
...
#------------------------------------------
echo "QoS Policy Configuration"
#------------------------------------------
...
        sap-ingress 101 create
...
            mac-criteria
                entry 10 create
                    description "Entry10"
                    match
                        dst-mac 04-67-ff-00-00-01 ff-ff-ff-ff-ff-ff
                        dot1p 7 7
                    exit
                    action fc be
                exit
            exit
        exit
#------------------------------------------
A:ALA-7>config>qos#
```

Service Ingress QoS Policies Resource Usage Examples

Example 1

```
sap-ingress 10 create
     description“example-policy-1”
           num-qos-classifiers 8
            meter 1 create
            exit
            meter 3 create
                rate cir 100 pir 100
            exit
            meter 11 multipoint create
            exit
            fc "af" create
                meter 1
            exit
            fc "be" create
                meter 3
            exit
            fc "h2" create
                meter 3
            exit
            fc "l1" create
                meter 3
            exit
            mac-criteria
                entry 1 create
                    match
                        dot1p 7 7
                    exit
                    action fc "af"
                exit
                entry 2 create
                    match
                        dot1p 5 7
                    exit
                    action fc "l1"
                exit
                entry 3 create
                    match
                        dot1p 6 7
                    exit
                    action fc "h2"
                exit
                default-fc "be"
```

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, 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.

```
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, the total classification entries used by this policy is calculated as:

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).

Meters used = 3 (since FCs use meter #1, meter #3 and meter #11).

Therefore, in this example, **num-qos-classifiers 16** is used (i.e. 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, the total classification entries used = 4 and total meters used = 2.

Example 2

```
sap-ingress 10 create
     description“example-policy-1”
     num-qos-classifiers16
              meter 1 create
               exit
             meter 2 multipoint create
                 rate cir 1 pir 20
             exit
             meter 3 create
                 rate cir 100 pir 100
             exit
             meter 11 multipoint create
             exit
             fc "af" create
                 meter 3
                 broadcast-meter 2
             exit
```

```
fc "be" create
    meter 3
    broadcast-meter 2
exit
fc "h2" create
    meter 3
    broadcast-meter 2
exit
fc "l1" create
    meter 3
    broadcast-meter 2
exit
mac-criteria
    entry 1 create
        match
            dot1p 7 7
        exit
        action fc "af"
    exit
    entry 2 create
        match
            dot1p 5 7
        exit
        action fc "l1"
    exit
    entry 3 create
        match
            dot1p 6 7
        exit
        action fc "h2"
    exit
exit
default-fc "be"
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, classification entries used per FC are as follows:

```
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 required to identify these traffic types explicitly. Another entry is required 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 = 2
```

Using the above equation, the total classification entries used = 11 (since three explicit match criteria entries map to each of FC H2, L1, and AF along with a default classification rule for BE).

Meters used = 3 (since FCs use only meter #2, meter #3 and meter #11).

Therefore, in this example, **num-qos-classifiers 16** is used (i.e. maximum of (12, (2*3))). Note that the system internally uses 18, instead of 16.

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 is used:

```
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 the total meters used = 1.

Example 3

```
sap-ingress 10 create
     description“example-policy-2”
     num-qos-classifiers16
              meter 1 create
                  rate cir 100 pir 100
             exit
             meter 2 multipoint create
                  rate cir 1 pir 20
             exit
             meter 3 create
                  rate cir 100 pir 100
             exit
             meter 4 multipoint create
                  rate cir 10 pir 100
             exit
             meter 5 create
                  rate cir 10 pir 10
             exit
             meter 11 multipoint create
                  rate cir 1 pir 20
             exit
             fc "af" create
                  meter 3
                  broadcast-meter 2
                  multicast-meter 4
             exit
             fc "h1" create
                  meter 5
                  broadcast-meter 4
                  multicast-meter 4
                  unknown-meter 4
             exit
             fc "h2" create
                  meter 3
                  broadcast-meter 2
             exit
```

```
fc "l1" create
    meter 3
    broadcast-meter 2
exit
mac-criteria
    entry 1 create
        match
            dot1p 7 7
        exit
        action fc "af"
    exit
    entry 2 create
        match
            dot1p 5 7
        exit
        action fc "l1"
    exit
    entry 3 create
        match
            dot1p 6 7
        exit
        action fc "h2"
    exit
    entry 4 create
        match
            dot1p 3 7
        exit
        action fc "h1"
    exit
exit
default-fc "be"
```

In the example above, assuming the policy is attached to a SAP in a VPLS service, the classification entries used per FC are as follows:

```
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 required 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 required to identify these traffic types explicitly. Another entry is required 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 required to identify this traffic type explicitly. Another entry is required 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 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.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the above equation, the total classification entries used = 15 and the total 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 are used:

```
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 the total meters used = 3 (since all FCs used only meter #1, meter #3 and meter #5).

Example 4

```
sap-ingress 10 create
     description“example-policy-3”
     num-qos-classifiers 36
            meter 1 create
                rate cir 100 pir 100
            exit
            meter 2 multipoint create
                rate cir 1 pir 20
            exit
            meter 3 create
                rate cir 100 pir 100
            exit
            meter 4 multipoint 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 multipoint create
                rate cir 20 pir 100
            exit
            meter 11 multipoint create
                rate cir 1 pir 20
            exit
            fc "af" create
```

```
        meter 3
        broadcast-meter 2
        multicast-meter 4
    exit
    fc "ef" create
        meter 6
        broadcast-meter 2
        multicast-meter 8
    exit
    fc "h1" create
        meter 5
        broadcast-meter 4
        multicast-meter 4
        unknown-meter 4
    exit
    fc "h2" create
        meter 3
        broadcast-meter 2
    exit
    fc "l1" create
        meter 3
        broadcast-meter 2
    exit
    fc "nc" create
        meter 6
        broadcast-meter 2
        multicast-meter 8
    exit
    mac-criteria
        entry 1 create
            match
                dot1p 4 7
            exit
            action fc "af"
        exit
        entry 2 create
            match
                dot1p 5 7
            exit
            action fc "l1"
        exit
        entry 3 create
            match
                dot1p 6 7
            exit
            action fc "h2"
        exit
        entry 4 create
            match
                dot1p 3 7
            exit
            action fc "h1"
        exit
        entry 5 create
            match
                dot1p 2 7
            exit
            action fc "ef"
        exit
```

```
            entry 6 create
                match
                    dot1p 7 7
                exit
                action fc "nc"
            exit
        exit
        default-fc "be"
```

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 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.

```
FCh1 = 1 + 1 + 1 + 1 = 4
```

Since this FC uses unicast, broadcast, multicast and unknown-unicast meter, four entries are required to identify these traffic types explicitly.

```
FCef = 1 + 1 + 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.

```
FCh2 = 1 + 1 + 1 + 0 = 3
```

Since this FC uses unicast meter and broadcast meter, two entries are required to identify these traffic types explicitly. Another entry is required 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 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.

```
FCl2 = 0 + 0 + 0 + 0 = 0
FCbe = 1 + 0 + 1 + 0 = 2
```

Using the above equation, the total classification entries used = 21 and the total 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 are used:

```
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 the total meters used = 4.

As illustrated in this example, 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** = 16)

Example 5

```
sap-ingress 10 create

          num-qos-classifiers 72
            meter 1 create
            exit
            meter 3 create
            exit
            meter 4 multipoint create
            exit
            meter 11 multipoint create
            exit
            fc "af" create
                meter 3
                broadcast-meter 11
                multicast-meter 4
            exit
            fc "be" create
                meter 1
                broadcast-meter 11
            exit
            ip-criteria
                entry 1 create
                    match
                        dscp be
                    exit
                    action fc "af"
                exit
                entry 2 create
                    match
                        dscp cp1
                    exit
                    action fc "af"
                exit
                entry 3 create
                    match
                        dscp cp3
                    exit
                    action fc "af"
                exit
                entry 4 create
                    match
```

```
            dscp cp4
        exit
        action fc "af"
    exit
    entry 5 create
        match
            dscp cp5
        exit
        action fc "af"
    exit
    entry 6 create
        match
            dscp cp6
        exit
        action fc "af"
    exit
    entry 7 create
        match
            dscp cp7
        exit
        action fc "af"
    exit
    entry 8 create
        match
            dscp cs1
        exit
        action fc "af"
    exit
    entry 9 create
        match
            dscp cp9
        exit
        action fc "af"
    exit
    entry 10 create
        match
            dscp af11
        exit
        action fc "af"
    exit
    entry 11 create
        match
            dscp cp11
        exit
        action fc "af"
    exit
    entry 12 create
        match
            dscp af12
        exit
        action fc "af"
    exit
    entry 13 create
        match
            dscp cp13
        exit
        action fc "af"
    exit
    entry 14 create
```

```
                match
                    dscp cp15
                exit
                action fc "af"
            exit
            entry 15 create
                match
                    dscp cp15
                exit
                action fc "af"
            exit
        exit
        default-fc "be"
```

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 required to identify these traffic types explicitly. Another entry is required 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 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.

Using the equation, the total classification entries used by this policy is calculated as follows:

TC = (0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (15 * 3)af + (0 * 0)l2 + (1 * 3)be = 48

The total meters used in this policy = 4.

Hence, in this example, **num-qos-classifiers 72** are used (i.e. maximum of (48, (2 * 4)) = 48, rounded off to the next available numQosClassifier range .

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 are used:

```
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, the total classification entries used by this policy is calculated as follows:

(0 * 0)nc + (0 * 0)h1 + (0 * 0)ef + (0 * 0)h2 + (0 * 0)l1 + (15 * 1)af + (0 * 0)l2 + (1 * 1)be = 16

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 16 is used (maximum of (16, (2 * 2)) = 16.

```
dscp-only
```

Applying Service Ingress Policies

Apply SAP ingress policies to the following service SAPs:

- Epipe
- VPLS

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#
```

Service Management Tasks

This section discusses the following service management tasks:

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 Commands

```
config
    — qos
        — [no] sap-ingress policy-id [create]
            — default-fc fc-name
            — 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
                — renum [<old-entry-id>< new-entry-id>]
            — [no] mac-criteria [dot1p-only]
                — [no] entry entry-id [create]
                    — action [fc fc-name]
                    — no action
                    — description description-string
                    — no description
```

— **match**
— **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** <*old-entry-id*> <*new-entry-id*>
— **num-qos-classifiers** [*num-resources*]
— **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}**(trtcm2 supported only on 7210 SAS-D)
— **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* [**detail | 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** <*old-entry-id*> <*new-entry-id*>

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 *old-entry-id* — Enter the entry number of an existing entry.

Default none

Values 1 — 64

new-entry-id — Enter the new entry-number to be assigned to the old entry.

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.

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

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-name*

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-name* **—** Specify the forwarding class name for the queue. The value given for *fc-name* must be one of the predefined forwarding classes in the system.

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)

ip-criteria

Syntax [**no**] **ip-criteria [any|dscp-only]**

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)

dscp-only — Specifies that entries can use only the DSCP field.

mac-criteria

Syntax [**no**] **mac-criteria [dot1p-only]**

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 dot1p-only

Parameters **dot1p-only —** Specifies that entries can use only the Dot1p field.

num-qos-classifiers

Syntax **num-qos-classifiers** [*num-resources*]

Context config>qos>sap-ingress>num-qos-classifiers

Description This command configures the number of classifiers the SAP ingress Qos policy can use. This parameter cannot be modified when it is associated with 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 (maximum of 32). 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).

Default 16 (for 7210 SAS-E), 4 (for 7210 SAS-D)

Parameters *num-resources* — Specifies the number of resources planned for use by this policy

Values 16, 6, 72 (for 7210 SAS E)

Values 4, 8, 16, 32, 64, 128, 256 (for 7210 SAS D)

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 (for 7210 SAS D, E)

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 (except 11)

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 2— 18 (for 7210 SAS E)

Values 2 to 32 (for 7210 SAS D)

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 2— 18 (for 7210 SAS E)

Values 2 to 32 (for 7210 SAS D)

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.

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.

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*.

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

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	DDDDDDDDDDDDD	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	DDDDDDDDDDDDD	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)

Values

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 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 32 — 16384, default (for 7210 SAS E)

Values 4 — 16384, default (for 7210 SAS D)

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 32 — 16384, default (for 7210 SAS E)

Values 4 — 16384, default (for 7210 SAS D)

mode

Syntax **mode** {**trtcm1** | **trtcm2 | srtcm**} (trtcm2 supported only on 7210 SAS D)
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 — Note: trtcm2 supported only on 7210 SAS-D. 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 system configures the policer's EIR rate, based on the value of the PIR rate configured by the user.

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.

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 — 2000000, max (for 7210 SAS E)

Values 0 — 4000000, max (for 7210 SAS D)

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.

Values 0 — 2000000, max (for 7210 SAS E)

Values 0 -- 4000000, max (for 7210 SAS D)

Show Commands

sap-ingress

Syntax **sap-ingress** [*policy-id*] [**detail | 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

detail — Displays detailed policy information including policy associations. .

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.

Label	Description (Continued)
Mode	For 7210 SAS E: Specifies the configured mode of the meter (trTcm1 or srTcm). For 7210 SAS-D: Specifies the configured mode of the meter (trTcm1,trTcm2 or srTcm).
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.

Label	Description (Continued)
UnknownM	Specifies the default unknown unicast forwarding type meters mapping.
Match Criteria	Specifies an IP or MAC criteria entry for the policy.
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.

Sample Output

```
*A:SAS-E>show>qos# sap-ingress 1 detail

===============================================================================
QoS Sap Ingress
===============================================================================
-------------------------------------------------------------------------------
Sap Ingress Policy (1)
-------------------------------------------------------------------------------
```

```
Policy-id                : 1                Scope               : Template
Default FC               : be
Criteria-type            : None
Accounting               : packet-based
Classifiers Allowed      : 16               Meters Allowed      : 8
Classifiers Reqrd (VPLS) : 2                Meters Reqrd (VPLS) : 2
Classifiers Reqrd (EPIPE) : 1               Meters Reqrd (EPIPE) : 1
Description    : Default SAP ingress QoS policy.

-------------------------------------------------------------------------------
Meter Mode  CIR Admin    CIR Rule   PIR Admin   PIR Rule   CBS Admin MBS Admin
-------------------------------------------------------------------------------
1     TrTcm1      0         closest       max       closest   def       def
11    TrTcm1      0         closest       max       closest   def       def

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

-------------------------------------------------------------------------------
Match Criteria
-------------------------------------------------------------------------------
No Matching Criteria.

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Service-Id               : 10 (Epipe)       Customer-Id         : 1
 - SAP : 1/1/2
Service-Id               : 50 (VPLS)        Customer-Id         : 1
 - SAP : 1/1/1
===============================================================================
*A:SAS-E>show>qos#

Sample output for 7210 SAS D:

*A:SAS-D>show>qos# sap-ingress 1 detail

===============================================================================
QoS Sap Ingress
===============================================================================
-------------------------------------------------------------------------------
Sap Ingress Policy (1)
-------------------------------------------------------------------------------
Policy-id                : 1                Scope               : Template
Default FC               : be
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.

-------------------------------------------------------------------------------
Meter Mode  CIR Admin    CIR Rule   PIR Admin   PIR Rule   CBS Admin MBS Admin
            CIR Oper               PIR Oper               CBS Oper  MBS Oper
-------------------------------------------------------------------------------
1     TrTcm1      0         closest       max       closest   def       def
```

```
                   0                       max                 def       def
11    TrTcm1       0          closest      max        closest  def       def
                   0                       max                 def       def

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

-------------------------------------------------------------------------------
Match Criteria
-------------------------------------------------------------------------------
No Matching Criteria.

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
No Associations Found.

===============================================================================
*A:SAS-D>show>qos#
```

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 20, Forwarding Class to Queue-ID Map, on page 59.
- Remark - For 7210 SAS E devices, by default, remarking is always enabled. The Dot1p values in the customer packets which are egressing on this access port are marked

according to the FC-Dot1p marking map Table 14, Default Access Egress Policy ID 1 Definition, on page 45. For 7210 SAS-D devices, remarking can be enabled or disabled.

- 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:

```
A:card-1>config>qos# info
#------------------------------------------------
echo "QoS Policy Configuration"
#------------------------------------------------
....
        access-egress 30 create
            remarking
            queue 1
                rate cir 100 pir 4500
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
            exit
            queue 5
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
        exit
...
------------------------------------------------
A:card-1>config>qos#
```

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 20, Forwarding Class to Queue-ID Map, on page 59.
- Queue parameters. Egress queues support configuration of CIR and PIR rates.

The following displays the access egress QoS policy configuration:

```
A:card-1>config>qos# info
#------------------------------------------------
echo "QoS Policy Configuration"
#------------------------------------------------
....
        access-egress 30 create
            remarking
            queue 1
                rate cir 100 pir 4500
            exit
            queue 2
            exit
            queue 3
            exit
            queue 4
            exit
            queue 5
            exit
            queue 6
            exit
            queue 7
            exit
            queue 8
            exit
        exit
------------------------------------------
A:card-1>config>qos#
```

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 28: 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 28: Access Egress Default Policy Details (Continued)

Field	Default
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	
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	

Table 28: Access Egress Default Policy Details (Continued)

Field	Default
adaptation-rule	adaptation-rule cir closest pir closest
rate	cir 0 pir max
cbs	default = 3200 bytes
remarking	yes (for 7210 SAS-E), no (for 7210 SAS-D)
fc af:	dot1p-in-profile 2
	dot1p-out-profile 2
fc be:	dot1p-in-profile 0
	dot1p-out-profile 0
fc ef:	dot1p-in-profile 5
	dot1p-out-profile 5
fc h1:	dot1p-in-profile 6
	dot1p-out-profile 6
fc h2:	dot1p-in-profile 4
	dot1p-out-profile 4
fc l1:	
	dot1p-in-profile 3
	dot1p-out-profile 3
fc l2:	dot1p-in-profile 1
	dot1p-out-profile 1
fc nc:	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
                —  queue queue-id
                        — adaptation-rule [cir adaptation-rule] [pir adaptation-rule]
                        — no adaptation-rule
                        — rate cir cir-rate [pir pir-rate]
                        — no rate
                — scope {exclusive | template}
                — no scope
```

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 14, Default Access Egress Policy ID 1 Definition, on page 45. 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 14, Default Access Egress Policy ID 1 Definition, on page 45.

Default Dot1p values are marked according to Access Egress Default Policy Details on page 224.

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 14, Default Access Egress Policy ID 1 Definition, on page 45. 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 14, Default Access Egress Policy ID 1 Definition, on page 45.

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

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 20, Forwarding Class to Queue-ID Map, on page 59.

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 20, Forwarding Class to Queue-ID Map, on page 59 .

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**

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**

Default max

remarking

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

Context config>qos>access-egress

Description This command enables the system to remark egress packets. Remarking cannot be disabled on the 7210 SAS E devices.For 7210 SAS D, remarking can be enabled or disabled.

The user can specify if either dot1p or dscp or both needs to be used for marking the packets egressing the port. If use-dot1p is configured, then for all the FCs only the configured dot1p values will be used. If use-dscp is configured, then for all the FCs only the configured dscp values are used. If all is configured, then for all the FCs both the dot1p and dscp values configured is used (if both have been provided).

If only dot1p-value is configured for a given FC, then use the configured value to mark the dot1p bits in the VLAN tag of the packet on the egress. If only dscp-value is configured for a given FC, then use the configured value to mark DSCP bits in the IP header the packet on the egress. If both of them are configured simultaneously, both dscp bits and dot1p bits are marked in the appropriate headers if its an IP packet and if its a non-IP packet then only dot1p is marked in the Ethernet header.

Note: This applies to all SAPs configured on the port, irrespective of the service they belong to. DSCP marking, if enabled, also marks the packets associated with SAPs configured in an L2 VPN service.

Default no remarking

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.

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 — For 7210 SAS E, 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 14, Default Access Egress Policy ID 1 Definition, on page 45. False — Remarking is disabled for the policy. For 7210 SAS D devices remarking can be enabled or disabled.
`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 14, Default Access Egress Policy ID 1 Definition, on page 45 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:Dut-B>config>qos>access-egress# show qos access-egress 2 association
===============================================================================
QoS Access Egress
===============================================================================
-------------------------------------------------------------------------------
Policy-id     : 2                             Scope        : Template
Remark        : True
Accounting    : packet-based
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Port-id : 1/1/2
===============================================================================
*A:Dut-B>config>qos>access-egress#
```

Sample Output for 7210 SAS D

```
*A:SAS-D>show>qos# access-egress 1 detail

===============================================================================
QoS Access Egress
===============================================================================
-------------------------------------------------------------------------------
Policy-id      : 1                              Scope        : Template
Remark         :
Accounting     : packet-based
Description    : Default Access egress QoS policy.

-------------------------------------------------------------------------------
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)

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
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
===============================================================================
*A:SAS-D>show>qos#


*A:SAS-D>show>qos# sap-ingress 1 association

===============================================================================
QoS Sap Ingress
===============================================================================
-------------------------------------------------------------------------------
Sap Ingress Policy (1)
-------------------------------------------------------------------------------
Policy-id                : 1                Scope               : Template
Default FC               : be
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.

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
No Associations Found.

===============================================================================
*A:SAS-D>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

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.

A port scheduler policy cannot be deleted unless it is removed from all ports where it is applied. The “default” port-scheduler policy cannot be deleted.

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 Port 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]`

Example: `config>qos# copy port-scheduler-policy psp psp1`

```
*A:card-1>config# qos port-scheduler-policy psp create
*A:card-1>config>qos>port-sched-plcy# mode WRR
*A:card-1>config>qos>port-sched-plcy# queue 1 weight 1
*A:card-1>config>qos>port-sched-plcy# queue 2 weight 3
*A:card-1>config>qos>port-sched-plcy# queue 3 weight 5
*A:card-1>config>qos>port-sched-plcy# exit
*A:card-1>config# qos copy port-scheduler-policy psp psp1
*A:card-1>config# qos copy port-scheduler-policy psp psp1
MINOR: CLI Destination "psp1" exists - use {overwrite}.
*A:card-1>config# qos copy port-scheduler-policy psp psp1 overwrite
*A:card-1>config# show qos port-scheduler-policy
===============================================================
Port Scheduler Policies
===============================================================
Policy-Id     Description                          Mode
---------------------------------------------------------------------------
default       Default Port Scheduler policy.       STRICT
psp                                                WRR
psp1                                               WRR
===============================================================
*A:card-1>config#

*A:card-1>config# show qos port-scheduler-policy psp
===============================================================
QoS Port Scheduler Policy
===============================================================
Policy-Name        : psp
Accounting         : packet-based
Mode               : WRR
Last changed       : 01/01/2000 22:13:01
Queue 1            Weight: 1
Queue 2            Weight: 3
Queue 3            Weight: 5
```

```
Queue 4            Weight: strict
Queue 5            Weight: strict
Queue 6            Weight: strict
Queue 7            Weight: strict
Queue 8            Weight: strict
===============================================================
*A:card-1>config#
*A:card-1>config# show qos port-scheduler-policy psp1
===============================================================
QoS Port Scheduler Policy
===============================================================
Policy-Name        : psp1
Accounting         : packet-based
Mode               : WRR
Last changed       : 01/01/2000 22:13:17
Queue 1            Weight: 1
Queue 2            Weight: 3
Queue 3            Weight: 5
Queue 4            Weight: strict
Queue 5            Weight: strict
Queue 6            Weight: strict
Queue 7            Weight: strict
Queue 8            Weight: strict
===============================================================================
*A:card-1>config#
```

Editing QoS Policies

You can edit a port-scheduler policy, the modifications are done and it affects the port where it is applied. The “default” port-scheduler policy cannot be modified.

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

```
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 — 5 (For 7210 SAS-E)

Values 1—15 (For 7210 SAS-D)

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-R#
*A:card-1>config# show qos port-scheduler-policy
===============================================================================
Port Scheduler Policies
===============================================================================
Policy-Id                Description                              Mode
default                  Default Port Scheduler Policy.           STRICT
psp                                                               WRR
test                     psp                                      WRR
===============================================================================
*A:card-1>config#

*A:card-1>config# show qos port-scheduler-policy psp association
===============================================================================
```

```
QoS Port Scheduler Policy
===============================================================================
Policy-Name        : psp
Mode               : WRR
Accounting         : packet-based
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
- Port : 1/1/1
===============================================================================
*A:card-1>config#

*A:card-1>config# show qos port-scheduler-policy psp
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name        : psp
Mode               : WRR
Accounting         : packet-based
Last changed       : 01/01/2000 05:14:06
Queue 1:          Weight: 1
Queue 2:          Weight: 3
Queue 3:          Weight: 5
Queue 4:          Weight: 0
Queue 5:          Weight: 5
Queue 6:          Weight: 5
Queue 7:          Weight: strict
Queue 8:          Weight: strict
===============================================================================
*A:card-1>config#

*A:SN12345678>config# show qos port-scheduler-policy default
===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : default
Accounting        : frame-based
Description       : Default Port Scheduler policy.
Mode              : STRICT
Last changed      : 08/04/2009 20:55:46
Number Of Queues  : 8
===============================================================================
*A:SN12345678>config#
```

Sample output for 7210 SAS D

```
*A:SAS-D>show>qos# port-scheduler-policy abc

===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : abc
Description       : (Not Specified)
Accounting        : packet-based
Mode              : STRICT
Last changed      : 01/01/1970 04:57:48
Number Of Queues  : 8
```

```
===============================================================================
*A:SAS-D>show>qos# port-scheduler-policy abc association

===============================================================================
QoS Port Scheduler Policy
===============================================================================
Policy-Name       : abc
Description       : (Not Specified)
Accounting        : packet-based
Mode              : STRICT

-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
No Association Found.

===============================================================================
*A:SAS-D>show>qos#
```

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

Default buffer pool exists (logically) at each port. Each physical port has two associated pool objects:

- Access egress pool
- Access uplink egress pool

By default, each pool is associated with slope-policy default which disables the high-slope and low-slope parameters within the pool.

For information about the tasks and commands necessary to access the command line interface and to configure and maintain your 7210 SAS D, E, refer to CLI Usage chapter in the 7210 SAS D, E OS Basic System Configuration Guide.

Basic Configurations

A basic slope QoS policy must conform to the following:

- Each slope policy must have a unique policy ID.
- High slope and low slope are shut down (default).
- Default values can be modified but parameters cannot be deleted.

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 for 7210 SAS-E devices, 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.

To create a new slope policy for 7210 SAS-D devices, 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.

For 7210 SAS E devices, Use the following CLI syntax to configure a slope policy:

CLI Syntax:
```
config>qos
 slope-policy name
    description description-string
    high slope
       start-threshold percent
       queue queue-id drop-rate rate
       no shutdown
    low-slope
       start-threshold percent
       queue queue-id drop-rate rate
       no shutdown
```

The following displays the slope policy configuration (for 7210 SAS E devices):

```
A:ALA-7>config>qo>slope-policy# info
----------------------------------------------
            description "slope policy SlopePolicy1"
            high-slope
                no shutdown
            exit
            low-slope
                no shutdown
            exit
----------------------------------------------
A:ALA-7>config>qos>slope-policy#
```

For 7210 SAS-D devices, 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:

```
A:7210 SAS-D>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:7210 SAS-D>config>qos>slope-policy#
```

Applying Slope Policies

- Ports

Apply slope policies to the egress buffer pool on the 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>accesss>uplink>egress>pool>slope-policy name
```

Default Slope Policy Values

The default access egress and access uplink egress policies are identified as policy-id “default”. The default policies cannot be edited or deleted. The following table displays default policy parameters:

Table 29: Slope Policy Defaults (for 7210 SAS E)

Description	Default Slope Policy
high (RED) slope	
Administrative state	shutdown
start-threshold	75% utilization
queue 1 — 8 drop-rate	1 (6.25% drop rate)
low (RED) slope	
Administrative state	shutdown
start-threshold	50% utilization
queue 1 — 8 drop-rate	0 (100% drop rate)

The following output displays the default configuration:

```
ALA7>config>qos>slope-policy# info detail
----------------------------------------------
            description "Default slope policy."
            high-slope
                shutdown
                start-threshold 75
                queue 1 drop-rate 1
                queue 2 drop-rate 1
                queue 3 drop-rate 1
                queue 4 drop-rate 1
                queue 5 drop-rate 1
                queue 6 drop-rate 1
                queue 7 drop-rate 1
                queue 8 drop-rate 1
            exit
            low-slope
                shutdown
                start-threshold 50
                queue 1 drop-rate 0
                queue 2 drop-rate 0
                queue 3 drop-rate 0
                queue 4 drop-rate 0
                queue 5 drop-rate 0
                queue 6 drop-rate 0
```

```
                queue 7 drop-rate 0
                queue 8 drop-rate 0
            exit
-------------------------------------------
ALA7>config>qos>slope-policy#
```

Default Slope Policy Values (for 7210 SAS-D devices)

Table 30: 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 access uplink 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>accesss>uplink>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 (7210 SAS E devices):

```
A:ALA-7>config>qos#slope-policy "default" create
----------------------------------------------
            description "Default slope policy."
            high-slope
                shutdown
                start-threshold 75
                queue 1 drop-rate 1
                queue 2 drop-rate 1
                queue 3 drop-rate 1
                queue 4 drop-rate 1
                queue 5 drop-rate 1
                queue 6 drop-rate 1
                queue 7 drop-rate 1
                queue 8 drop-rate 1
            exit
            low-slope
                shutdown
                start-threshold 50
                queue 1 drop-rate 0
                queue 2 drop-rate 0
                queue 3 drop-rate 0
                queue 4 drop-rate 0
                queue 5 drop-rate 0
                queue 6 drop-rate 0
                queue 7 drop-rate 0
                queue 8 drop-rate 0
            exit
----------------------------------------------
A:ALA-7>config>qos#


A:ALA-7>config>qos#slope-policy "slopePolicy1" create
----------------------------------------------
            description "Default slope policy."
            high-slope
                shutdown
                start-threshold 75
                queue 1 drop-rate 1
                queue 2 drop-rate 1
                queue 3 drop-rate 1
                queue 4 drop-rate 1
                queue 5 drop-rate 1
                queue 6 drop-rate 1
                queue 7 drop-rate 1
```

```
                queue 8 drop-rate 1
            exit
            low-slope
                shutdown
                start-threshold 50
                queue 1 drop-rate 0
                queue 2 drop-rate 0
                queue 3 drop-rate 0
                queue 4 drop-rate 0
                queue 5 drop-rate 0
                queue 6 drop-rate 0
                queue 7 drop-rate 0
                queue 8 drop-rate 0
            exit
-------------------------------------------
A:ALA-7>config>qos#
```

The following output displays the copied policies for (7210 SAS D devices):

```
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 E devices)

```
config
    — qos
        — [no] slope-policy name [create]
            — description description-string
            — no description
            — [no] high-slope
                — start-threshold <threshold>
                — no start-threshold
                — queue <queue> drop-rate <drop-rate>
                — no queue <queue>
                — [no] shutdown
            — [no] low-slope
                — start-threshold <threshold>
                — no start-threshold
                — queue <queue> drop-rate <drop-rate>
                — no queue <queue>
                — [no] shutdown
```

Configuration Commands (for 7210 SAS D devices)

```
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] shutdown
                — [no] non-tcp-slope
```

```
                        — 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]
```

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* [create]

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(for 7210 SAS-E devices)

high-slope

Syntax [**no**] **high-slope**

Context config>qos>slope-policy

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

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.

RED Slope Commands(for 7210 SAS-E devices)

shutdown

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

Context config>qos>slope-policy>high-slope
config>qos>slope-policy>low-slope

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-threshold

Syntax **start-threshold** <*threshold*>
no start-threshold

Context config>qos>slope-policy>high-slope
config>qos>slope-policy>low-slope

Description This command sets the low priority or high priority Random Early Detection (RED) slope position for the shared buffer instantaneous utilization value where the packet discard probability comes into affect. The percent parameter is expressed as a percentage of the shared buffer size.

The **no** form of this command restores the start-threshold value to the default setting.

Default start-threshold 75 — High slope default is 75% buffer utilization before discard probability comes into affect.

start-threshold 50 — Low slope default is 50% buffer utilization before discard probability comes into affect.

Parameters <*threshold*> — The percentage of the shared buffer space for the buffer pool at which point the drop probability comes into affect.

Values 0 — 100

queue

Syntax **queue** <*queue*> **drop-rate** <*drop-rate*>
no queue <*queue*>

Context config>qos>slope-policy>high-slope
config>qos>slope-policy>low-slope

Description The drop-rate num parameter is expressed as a scalar number, and mapping to the percent of packets dropped in congestion conditions is specified in Table 35, Drop Rate Value to Percent Mapping Values, on page 95. The **no** form of this command restores the drop-rate value to the default setting.

Default drop-rate 1 — High slope default is 1 (6.25 drop-rate) for all the queues, this implies that once the shared buffer utilization reaches the start-threshold level then packets egressing out from a particular queue would be dropped at 6.25% rate.

drop-rate 0 — Low slope default is 0 (100% drop-rate) for all the queues, this implies that once the shared buffer utilization reaches the start-threshold level then packets egressing out from a particular queue would be dropped at 100% rate.

Parameters *queue* — Specifies the ID of the queue for which the drop-rate is to be configured.

Values 1 — 8

drop-rate — Specifies the drop rate to be configured.

Values 0 — 7

Slope Policy QoS Policy Commands(for 7210 SAS-D devices)

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>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

Slope Policy QoS Policy Commands (for 7210 SAS D devices)

RED SLOPE COMMANDS

max-avg

Syntax **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.

Parameters *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 startavg. 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 75 represents 75% of 1, or a packet discard probability of 0.75.

The **no** form of this command restores the **max-prob** value to the default setting.

Default **max-prob 75 —** 75% 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

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.

Output **Slope QoS Policy Output Fields (for 7210 SAS E) —** The following table describes slope QoS policy output fields.

Table 31: 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 (for 7210 SAS E)

```
*A:>config# show qos slope-policy 1
===============================================================================
QoS Slope Policy
===============================================================================
Policy         : 1
-------------------------------------------------------------------------------
Utilization                   State       Start-Threshold
-------------------------------------------------------------------------------
High-Slope                    Down              75%
Low-Slope                     Down              50%
-------------------------------------------------------------------------------
Queue                    High Slope Drop Rate(%)       Low Slope Drop Rate(%)
-------------------------------------------------------------------------------
Queue 1                        6.250000              100.000000
Queue 2                        6.250000              100.000000
Queue 3                        6.250000              100.000000
Queue 4                        6.250000              100.000000
Queue 5                        6.250000              100.000000
Queue 6                        6.250000              100.000000
Queue 7                        6.250000              100.000000
Queue 8                        6.250000              100.000000
===============================================================================
*A:>config#


*A:>config# show qos slope-policy 1 detail
===============================================================================
QoS Slope Policy
===============================================================================
Policy         : 1
-------------------------------------------------------------------------------
Utilization                   State       Start-Threshold
-------------------------------------------------------------------------------
High-Slope                    Down              75%
Low-Slope                     Down              50%
-------------------------------------------------------------------------------
Queue                    High Slope Drop Rate(%)       Low Slope Drop Rate(%)
-------------------------------------------------------------------------------
Queue 1                        6.250000              100.000000
Queue 2                        6.250000              100.000000
Queue 3                        6.250000              100.000000
Queue 4                        6.250000              100.000000
Queue 5                        6.250000              100.000000
Queue 6                        6.250000              100.000000
Queue 7                        6.250000              100.000000
Queue 8                        6.250000              100.000000
-------------------------------------------------------------------------------
Associations
-------------------------------------------------------------------------------
Object Type Object Id     Application          Pool
-------------------------------------------------------------------------------
Port        1/1/1         Acc-Egr              default
===============================================================================
*A:>config#
```

Output **Slope QoS Policy Output Fields (for 7210 SAS D) —** The following table describes slope QoS policy output fields.

Table 32: 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 (for 7210 SAS-D)

```
*A:SAS-D>show>qos# slope-policy abc detail

===============================================================================
QoS Slope Policy
===============================================================================
Policy         : abc
Description    : (Not Specified)
-------------------------------------------------------------------------------
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
-------------------------------------------------------------------------------
No Matching Entries

*A:SAS-D>show>qos#
```

Standards and Protocol Support

Standards Compliance

IEEE 802.1ab-REV/D3 Station and Media Access Control Connectivity Discovery
IEEE 802.1d Bridging
IEEE 802.1p/Q VLAN Tagging
IEEE 802.1s Multiple Spanning Tree
IEEE 802.1w Rapid Spanning Tree Protocol
IEEE 802.1x Port Based Network Access Control
IEEE 802.1ad Provider Bridges
IEEE 802.1ag Service Layer OAM
IEEE 802.3ah Ethernet in the First Mile
IEEE 802.3 10BaseT
IEEE 802.3ad Link Aggregation
IEEE 802.3ah Ethernet OAM
IEEE 802.3u 100BaseTX
IEEE 802.3z 1000BaseSX/LX
ITU-T Y.1731 OAM functions and mechanisms for Ethernet based networks
IANA-IFType-MIB
IEEE8023-LAG-MIB
ITU-T G.8032 Ethernet Ring Protection Switching (version 2)

Protocol Support

DHCP

RFC 2131 Dynamic Host Configuration Protocol

DIFFERENTIATED SERVICES

RFC 2474 Definition of the DS Field the IPv4 and IPv6 Headers (Rev)
RFC 2597 Assured Forwarding PHB Group (rev3260)
RFC 2598 An Expedited Forwarding PHB
RFC 3140 Per-Hop Behavior Identification Codes
RFC 4115 A Differentiated Service Two-Rate, Three-Color Marker with Efficient Handling of in-Profile Traffic [Only for 7210 SAS-D]
IPv6 [Only for 7210 SAS-E]
RFC 2460 Internet Protocol, Version 6 (IPv6) Specification
RFC 2461 Neighbor Discovery for IPv6
RFC 2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 Specification
RFC 2464 Transmission of IPv6 Packets over Ethernet Networks

Multicast

RFC 1112 Host Extensions for IP Multicasting (Snooping)
RFC 2236 Internet Group Management Protocol, (Snooping)
RFC 3376 Internet Group Management Protocol, Version 3 (Snooping)

NETWORK MANAGEMENT

ITU-T X.721: Information technology-OSI-Structure of Management Information
ITU-T X.734: Information technology-OSI-Systems Management: Event Report Management Function
M.3100/3120 Equipment and Connection Models
TMF 509/613 Network Connectivity Model
RFC 1157 SNMPv1
RFC 1215 A Convention for Defining Traps for use with the SNMP
RFC 1907 SNMPv2-MIB
RFC 2011 IP-MIB
RFC 2012 TCP-MIB
RFC 2013 UDP-MIB
RFC 2096 IP-FORWARD-MIB
RFC 2138 RADIUS
RFC 2571 SNMP-FRAMEWORKMIB
RFC 2572 SNMP-MPD-MIB
RFC 2573 SNMP-TARGET-&-NOTIFICATION-MIB
RFC 2574 SNMP-USER-BASED-SMMIB
RFC 2575 SNMP-VIEW-BASEDACM-MIB
RFC 2576 SNMP-COMMUNITY-MIB
RFC 2665 EtherLike-MIB
RFC 2819 RMON-MIB
RFC 2863 IF-MIB
RFC 2864 INVERTED-STACK-MIB
RFC 3014 NOTIFICATION-LOGMIB
RFC 3164 Syslog
RFC 3273 HCRMON-MIB
RFC 3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 - Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 - Simple Network Management Protocol (SNMP) Applications
RFC 3414 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3418 - SNMP MIB
draft-ietf-disman-alarm-mib-04.txt

RADIUS

RFC 2865 Remote Authentication Dial In User Service
RFC 2866 RADIUS Accounting

SSH

draft-ietf-secsh-architecture.txt SSH Protocol Architecture
draft-ietf-secsh-userauth.txt SSH Authentication Protocol
draft-ietf-secsh-transport.txt SSH Transport Layer Protocol
draft-ietf-secsh-connection.txt SSH Connection Protocol
draft-ietf-secsh- newmodes.txt SSH Transport Layer Encryption Modes

TACACS+

draft-grant-tacacs-02.txt

TCP/IP

RFC 768 UDP

RFC 1350 The TFTP Protocol
RFC 791 IP
RFC 792 ICMP
RFC 793 TCP
RFC 826 ARP
RFC 854 Telnet
RFC 1519 CIDR
RFC 1812 Requirements for IPv4 Routers
RFC 2347 TFTP option Extension
RFC 2328 TFTP Blocksize Option
RFC 2349 TFTP Timeout Interval and Transfer Size option
Timing (Only on 7210 SAS-D ETR)
ITU-T G.781 Telecommunication Standardization Section of ITU, Synchronization layer functions, issued 09/2008
ITU-T G.813 Telecommunication Standardization Section of ITU, Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003.
GR-1244-CORE Clocks for the Synchronized Network: Common Generic Criteria, Issue 3,May 2005
ITU-T G.8261 Telecommunication Standardization Section of ITU, Timing and synchronization aspects in packet networks, issued 04/2008.
ITU-T G.8262 Telecommunication Standardization Section of ITU, Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007.
ITU-T G.8264 Telecommunication Standardization Section of ITU, Distribution of timing information through packet networks, issued 10/2008.

Proprietary MIBs

ALCATEL-IGMP-SNOOPING-MIB.mib
TIMETRA-CAPABILITY-7210-SAS-E-V1v0.mib (Only for 7210 SAS-E)
TIMETRA-CAPABILITY-7210-SAS-D-V1v0.mib (Only for 7210 SAS-D)
TIMETRA-CHASSIS-MIB.mib
TIMETRA-CLEAR-MIB.mib
TIMETRA-DOT3-OAM-MIB.mib
TIMETRA-FILTER-MIB.mib
TIMETRA-GLOBAL-MIB.mib
TIMETRA-IEEE8021-CFM-MIB.mib
TIMETRA-LAG-MIB.mib
TIMETRA-LOG-MIB.mib
TIMETRA-MIRROR-MIB.mib
TIMETRA-NTP-MIB.mib
TIMETRA-OAM-TEST-MIB.mib
TIMETRA-PORT-MIB.mib
TIMETRA-QOS-MIB.mib
TIMETRA-SAS-ALARM-INPUT-MIB.mib [Only for 7210 SAS-E]
TIMETRA-SAS-IEEE8021-CFM-MIB.mib
TIMETRA-SAS-GLOBAL-MIB.mib
TIMETRA-SAS-PORT-MIB.mib
TIMETRA-SAS-QOS-MIB.mib
TIMETRA-SAS-SYSTEM-MIB.mib
TIMETRA-SCHEDULER-MIB.mib
TIMETRA-SECURITY-MIB.mib
TIMETRA-SERV-MIB.mib
TIMETRA-SYSTEM-MIB.mib
TIMETRA-TC-MIB.mib
TIMETRA-VRTR-MIB.mib