



Configuring QoS

- [Prerequisites for Quality of Service, on page 1](#)
- [QoS Components, on page 2](#)
- [QoS Terminology, on page 2](#)
- [Information About QoS, on page 3](#)
- [QoS Implementation, on page 4](#)
- [QoS Wired Model, on page 8](#)
- [Classification, on page 9](#)
- [Policing, on page 13](#)
- [Marking, on page 13](#)
- [Traffic Conditioning, on page 15](#)
- [Queuing and Scheduling, on page 18](#)
- [Trust Behavior, on page 23](#)
- [Standard QoS Default Settings, on page 24](#)
- [Restrictions for QoS on Wired Targets, on page 26](#)
- [How to Configure QoS, on page 28](#)
- [Configuring QoS Features and Functionality, on page 49](#)
- [Configuring Queues and Shaping, on page 55](#)
- [Monitoring QoS, on page 62](#)
- [Configuration Examples for QoS, on page 62](#)
- [Where to Go Next, on page 71](#)
- [Additional References for QoS, on page 72](#)
- [Feature History for QoS, on page 73](#)

Prerequisites for Quality of Service

Before configuring standard QoS, you must have a thorough understanding of these items:

- Standard QoS concepts.
- Classic Cisco IOS QoS.
- Modular QoS CLI (MQC).
- Understanding of QoS implementation.
- The types of applications used and the traffic patterns on your network.

- Traffic characteristics and needs of your network. For example, is the traffic on your network bursty? Do you need to reserve bandwidth for voice and video streams?
- Bandwidth requirements and speed of the network.
- Location of congestion points in the network.

QoS Components

Quality of service (QoS) consists of the following key components:

- **Classification**— Classification is the process of distinguishing one type of traffic from another based upon access control lists (ACLs), Differentiated Services Code Point (DSCP), Class of Service (CoS), and other factors.
- **Marking and mutation**— Marking is used on traffic to convey specific information to a downstream device in the network, or to carry information from one interface in a device to another. When traffic is marked, QoS operations on that traffic can be applied. This can be accomplished directly using the `set` command or through a table map, which takes input values and translates them directly to values on output.
- **Shaping and policing**— Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that downstream devices are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface. Policing is used to impose a maximum rate on a traffic class. If the rate is exceeded, then a specific action is taken as soon as the event occurs.
- **Queuing** — Queuing is used to prevent traffic congestion. Traffic is sent to specific queues for servicing and scheduling based upon bandwidth allocation. Traffic is then scheduled or sent out through the port.
- **Bandwidth**—Bandwidth allocation determines the available capacity for traffic that is subject to QoS policies.
- **Trust**— Trust enables traffic to pass through the device, and the Differentiated Services Code Point (DSCP), precedence, or CoS values coming in from the end points are retained in the absence of any explicit policy configuration.

QoS Terminology

The following terms are used interchangeably in this QoS configuration guide:

- Upstream (direction towards the device) is the same as ingress.
- Downstream (direction from the device) is the same as egress.

Information About QoS

QoS Overview

By configuring the quality of service (QoS), you can provide preferential treatment to specific types of traffic at the expense of other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size. The device sends the packets without any assurance of reliability, delay bounds, or throughput.

The following are specific features provided by QoS:

- Low latency
- Bandwidth guarantee
- Buffering capabilities and dropping disciplines
- Traffic policing
- Enables the changing of the attribute of the frame or packet header
- Relative services

Modular QoS Command-Line Interface

With the device, QoS features are enabled through the Modular QoS command-line interface (MQC). The MQC is a command-line interface (CLI) structure that allows you to create traffic policies and attach these policies to interfaces. A traffic policy contains a traffic class and one or more QoS features. A traffic class is used to classify traffic, while the QoS features in the traffic policy determine how to treat the classified traffic. One of the main goals of MQC is to provide a platform-independent interface for configuring QoS across Cisco platforms.

Supported QoS Features for Wired Access

The following table describes the supported QoS features for wired access.

Table 1: Supported QoS Features for Wired Access

| Feature | Description |
|--|--|
| Supported targets | <ul style="list-style-type: none"> • Gigabit Ethernet • 10-Gigabit Ethernet • 40-Gigabit Ethernet • VLAN |
| Configuration sequence | QoS policy installed using the service-policy command. |
| Supported number of queues at port level | Up to 8 queues supported on a port. |

| Feature | Description |
|------------------------------------|--|
| Supported classification mechanism | <ul style="list-style-type: none"> • DSCP • IP precedence • CoS • QoS-group • ACL membership including: <ul style="list-style-type: none"> • IPv4 ACLs • IPv6 ACLS • MAC ACLs • VLAN |

Hierarchical QoS

The device supports hierarchical QoS (HQoS). HQoS allows you to perform:

- Hierarchical classification— Traffic classification is based upon other classes.
- Hierarchical policing—The process of having the policing configuration at multiple levels in a hierarchical policy.
- Hierarchical shaping—Shaping can also be configured at multiple levels in the hierarchy.



Note Hierarchical shaping is only supported for the port shaper, where for the parent you only have a configuration for the class default, and the only action for the class default is shaping.

QoS Implementation

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure the QoS feature, you can select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your network makes network performance more predictable and bandwidth utilization more effective.

The QoS implementation is based on the Differentiated Services (Diff-Serv) architecture, a standard from the Internet Engineering Task Force (IETF). This architecture specifies that each packet is classified upon entry into the network.

The classification is carried in the IP packet header, using 6 bits from the deprecated IP type of service (ToS) field to carry the classification (*class*) information. Classification can also be carried in the Layer 2 frame.

Figure 1: QoS Classification Layers in Frames and Packets

The special bits in the Layer 2 frame or a Layer 3 packet are shown in the following

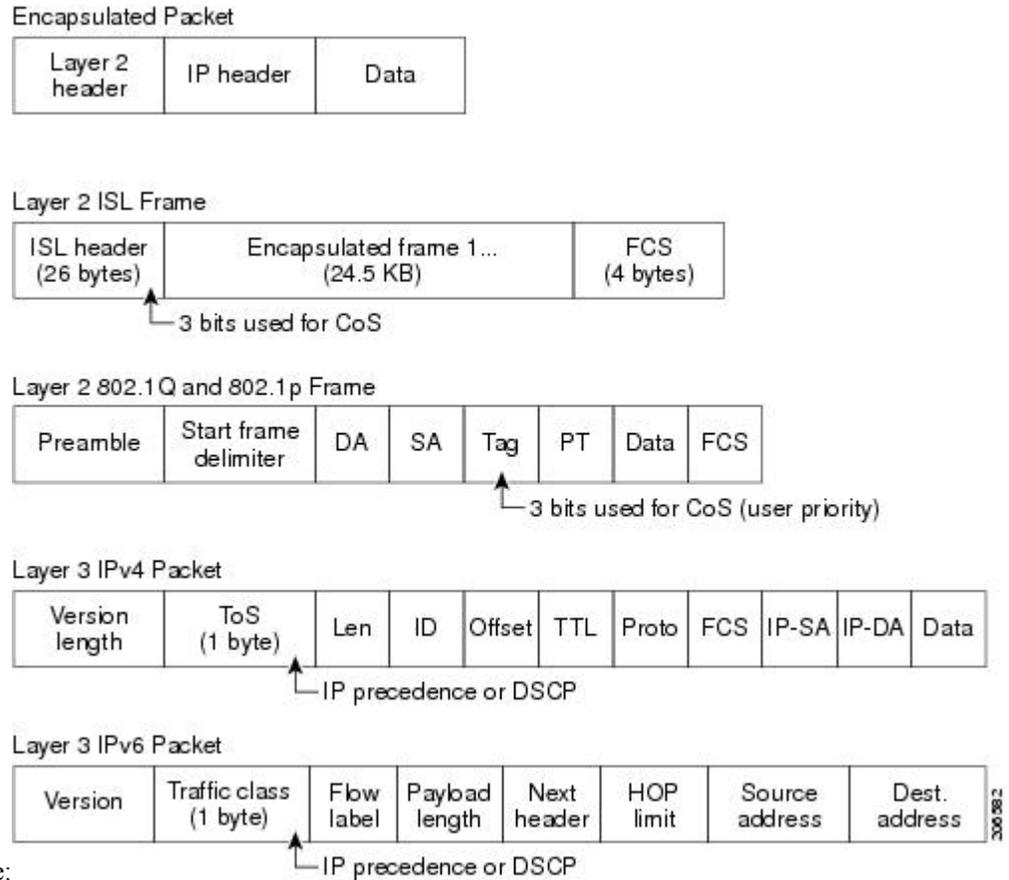


figure:

Layer 2 Frame Prioritization Bits

Layer 2 Inter-Switch Link (ISL) frame headers have a 1-byte User field that carries an IEEE 802.1p class of service (CoS) value in the three least-significant bits. On ports configured as Layer 2 ISL trunks, all traffic is in ISL frames.

Layer 2 802.1Q frame headers have a 2-byte Tag Control Information field that carries the CoS value in the three most-significant bits, which are called the User Priority bits. On ports configured as Layer 2 802.1Q trunks, all traffic is in 802.1Q frames except for traffic in the native VLAN.

Other frame types cannot carry Layer 2 CoS values.

Layer 2 CoS values range from 0 for low priority to 7 for high priority.

Layer 3 Packet Prioritization Bits

Layer 3 IP packets can carry either an IP precedence value or a Differentiated Services Code Point (DSCP) value. QoS supports the use of either value because DSCP values are backward-compatible with IP precedence values.

IP precedence values range from 0 to 7. DSCP values range from 0 to 63.

End-to-End QoS Solution Using Classification

All switches and routers that access the Internet rely on the class information to provide the same forwarding treatment to packets with the same class information and different treatment to packets with different class information. The class information in the packet can be assigned by end hosts or by switches or routers along the way, based on a configured policy, detailed examination of the packet, or both. Detailed examination of the packet is expected to occur closer to the edge of the network, so that the core switches and routers are not overloaded with this task.

Switches and routers along the path can use the class information to limit the amount of resources allocated per traffic class. The behavior of an individual device when handling traffic in the Diff-Serv architecture is called per-hop behavior. If all devices along a path provide a consistent per-hop behavior, you can construct an end-to-end QoS solution.

Implementing QoS in your network can be a simple task or complex task and depends on the QoS features offered by your internetworking devices, the traffic types and patterns in your network, and the granularity of control that you need over incoming and outgoing traffic.

Packet Classification

Packet classification is the process of identifying a packet as belonging to one of several classes in a defined policy, based on certain criteria. The Modular QoS CLI (MQC) is a policy-class based language. The policy class language is used to define the following:

- Class-map template with one or several match criteria
- Policy-map template with one or several classes associated to the policy map

The policy map template is then associated to one or several interfaces on the device.

Packet classification is the process of identifying a packet as belonging to one of the classes defined in the policy map. The process of classification will exit when the packet being processed matches a specific filter in a class. This is referred to as first-match exit. If a packet matches multiple classes in a policy, irrespective of the order of classes in the policy map, it would still exit the classification process after matching the first class.

If a packet does not match any of the classes in the policy, it would be classified into the default class in the policy. Every policy map has a default class, which is a system-defined class to match packets that do not match any of the user-defined classes.

Packet classification can be categorized into the following types:

- Classification based on information that is propagated with the packet
- Classification based on information that is device specific
- Hierarchical classification

Classification Based on Information That is Propagated with the Packet

Classification that is based on information that is part of the packet and propagated either end-to-end or between hops, typically includes the following:

- Classification based on Layer 3 or 4 headers
- Classification based on Layer 2 information

Classification Based on Layer 3 or Layer 4 Header

This is the most common deployment scenario. Numerous fields in the Layer 3 and Layer 4 headers can be used for packet classification.

At the most granular level, this classification methodology can be used to match an entire flow. For this deployment type, an access control list (ACLs) can be used. ACLs can also be used to match based on various subsets of the flow (for example, source IP address only, or destination IP address only, or a combination of both).

Classification can also be done based on the precedence or DSCP values in the IP header. The IP precedence field is used to indicate the relative priority with which a particular packet needs to be handled. It is made up of three bits in the IP header's type of service (ToS) byte.

The following table shows the different IP precedence bit values and their names.

Table 2: IP Precedence Values and Names

| IP Precedence Value | IP Precedence Bits | IP Precedence Names |
|---------------------|--------------------|----------------------|
| 0 | 000 | Routine |
| 1 | 001 | Priority |
| 2 | 010 | Immediate |
| 3 | 011 | Flash |
| 4 | 100 | Flash Override |
| 5 | 101 | Critical |
| 6 | 110 | Internetwork control |
| 7 | 111 | Network control |



Note All routing control traffic in the network uses IP precedence value 6 by default. IP precedence value 7 also is reserved for network control traffic. Therefore, the use of IP precedence values 6 and 7 is not recommended for user traffic.

The DSCP field is made up of 6 bits in the IP header and is being standardized by the Internet Engineering Task Force (IETF) Differentiated Services Working Group. The original ToS byte contained the DSCP bits has been renamed the DSCP byte. The DSCP field is part of the IP header, similar to IP precedence. The

DSCP field is a super set of the IP precedence field. Therefore, the DSCP field is used and is set in ways similar to what was described with respect to IP precedence.



Note The DSCP field definition is backward-compatible with the IP precedence values. Some fields in Layer 2 header can also be set using a policy.

Classification Based on Layer 2 Header

A variety of methods can be used to perform classification based on the Layer 2 header information. The most common methods include the following:

- MAC address-based classification (only for access groups)—Classification is based upon the source MAC address (for policies in the input direction) and destination MAC address (for policies in the output direction).
- Class-of-Service—Classification is based on the 3 bits in the Layer 2 header based on the IEEE 802.1p standard. This usually maps to the ToS byte in the IP header.
- VLAN ID—Classification is based on the VLAN ID of the packet.



Note Some of these fields in the Layer 2 header can also be set using a policy.

Classification Based on Information that is Device Specific

The device also provides classification mechanisms that are available where classification is not based on information in the packet header or payload.

At times you might be required to aggregate traffic coming from multiple input interfaces into a specific class in the output interface. For example, multiple customer edge routers might be going into the same access device on different interfaces. The service provider might want to police all the aggregate voice traffic going into the core to a specific rate. However, the voice traffic coming in from the different customers could have a different ToS settings. QoS group-based classification is a feature that is useful in these scenarios.

Policies configured on the input interfaces set the QoS group to a specific value, which can then be used to classify packets in the policy enabled on output interface.

The QoS group is a field in the packet data structure internal to the device. It is important to note that a QoS group is an internal label to the device and is not part of the packet header.

Hierarchical Classification

The device permits you to perform a classification based on other classes. Typically, this action may be required when there is a need to combine the classification mechanisms (that is, filters) from two or more classes into a single class map.

QoS Wired Model

To implement QoS, the device must perform the following tasks:

- Traffic classification—Distinguishes packets or flows from one another.
- Traffic marking and policing—Assigns a label to indicate the given quality of service as the packets move through the device, and then make the packets comply with the configured resource usage limits.
- Queuing and scheduling—Provides different treatment in all situations where resource contention exists.
- Shaping—Ensures that traffic sent from the device meets a specific traffic profile.

Ingress Port Activity

The following activities occur at the ingress port of the device:

- Classification—Classifying a distinct path for a packet by associating it with a QoS label. For example, the device maps the CoS or DSCP in the packet to a QoS label to distinguish one type of traffic from another. The QoS label that is generated identifies all future QoS actions to be performed on this packet.
- Policing—Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.
- Marking—Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).

Egress Port Activity

The following activities occur at the egress port of the device:

- Policing—Policing determines whether a packet is in or out of profile by comparing the rate of the incoming traffic to the configured policer. The policer limits the bandwidth consumed by a flow of traffic. The result is passed to the marker.
- Marking—Marking evaluates the policer and configuration information for the action to be taken when a packet is out of profile and determines what to do with the packet (pass through a packet without modification, mark down the QoS label in the packet, or drop the packet).
- Queuing—Queuing evaluates the QoS packet label and the corresponding DSCP or CoS value before selecting which of the egress queues to use. Because congestion can occur when multiple ingress ports simultaneously send data to an egress port, Weighted Tail Drop (WTD) differentiates traffic classes and subjects the packets to different thresholds based on the QoS label. If the threshold is exceeded, the packet is dropped.

Classification

Classification is the process of distinguishing one kind of traffic from another by examining the fields in the packet. Classification is enabled only if QoS is enabled on the device. By default, QoS is enabled on the device.

During classification, the device performs a lookup and assigns a QoS label to the packet. The QoS label identifies all QoS actions to be performed on the packet and from which queue the packet is sent.

Access Control Lists

You can use IP standard, IP extended, or Layer 2 MAC ACLs to define a group of packets with the same characteristics (class). You can also classify IP traffic based on IPv6 ACLs.

In the QoS context, the permit and deny actions in the access control entries (ACEs) have different meanings from security ACLs:

- If a match with a permit action is encountered (first-match principle), the specified QoS-related action is taken.
- If a match with a deny action is encountered, the ACL being processed is skipped, and the next ACL is processed.



Note Deny action is supported in Cisco IOS XE Release 3.7.4E and later releases.

- If no match with a permit action is encountered and all the ACEs have been examined, no QoS processing occurs on the packet, and the device offers best-effort service to the packet.
- If multiple ACLs are configured on a port, the lookup stops after the packet matches the first ACL with a permit action, and QoS processing begins.



Note When creating an access list, note that by default the end of the access list contains an implicit deny statement for everything if it did not find a match before reaching the end.

After a traffic class has been defined with the ACL, you can attach a policy to it. A policy might contain multiple classes with actions specified for each one of them. A policy might include commands to classify the class as a particular aggregate (for example, assign a DSCP) or rate-limit the class. This policy is then attached to a particular port on which it becomes effective.

You implement IP ACLs to classify IP traffic by using the **access-list** global configuration command; you implement Layer 2 MAC ACLs to classify non-IP traffic by using the **mac access-list extended** global configuration command.

Class Maps

A class map is a mechanism that you use to name a specific traffic flow (or class) and isolate it from all other traffic. The class map defines the criteria used to match against a specific traffic flow to further classify it. The criteria can include matching the access group defined by the ACL or matching a specific list of DSCP or IP precedence values or CoS values. If you have more than one type of traffic that you want to classify, you can create another class map and use a different name. After a packet is matched against the class-map criteria, you further classify it through the use of a policy map.



Note You cannot configure IPv4 and IPv6 classification criteria simultaneously in the same class-map. However, they can be configured in different class-maps in the same policy.

You create a class map by using the **class-map** global configuration command or the **class** policy-map configuration command. You should use the **class-map** command when the map is shared among multiple policies. When you enter the **class-map** command, the device enters the class-map configuration mode.

You can create a default class by using the **class class-default** policy-map configuration command. The default class is system-defined and cannot be configured. Unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as default traffic.

Policy Maps

A policy map specifies which traffic class to act on. Actions can include the following:

- Setting a specific DSCP or IP precedence value in the traffic class
- Setting a CoS value in the traffic class
- Setting a QoS group
- Specifying the traffic bandwidth limitations and the action to take when the traffic is out of profile

Before a policy map can be effective, you must attach it to a port.

You create and name a policy map using the **policy-map** global configuration command. When you enter this command, the device enters the policy-map configuration mode. In this mode, you specify the actions to take on a specific traffic class by using the **class** or **set** policy-map configuration and policy-map class configuration commands.

The policy map can also be configured using the **police** and **bandwidth** policy-map class configuration commands, which define the policer, the bandwidth limitations of the traffic, and the action to take if the limits are exceeded. In addition, the policy-map can further be configured using the **priority** policy-map class configuration command, to schedule priority for the class or the queuing policy-map class configuration commands, **queue-buffers** and **queue-limit**.

To enable the policy map, you attach it to a port by using the **service-policy** interface configuration command.



Note You cannot configure both **priority** and **set** for a policy map. If both these commands are configured for a policy map, and when the policy map is applied to an interface, error messages are displayed. The following example shows this restriction:

```
Switch# configure terminal
Switch(config)# class-map cmap
Switch(config-cmap)# exit
Switch(config)# class-map classmap1
Switch(config-cmap)# exit
Switch(config)# policy-map pmap
Switch(config-pmap)# class cmap
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classmap1
Switch(config-pmap-c)# set
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1/1
Switch(config-if)# service-policy output pmap

Non-queuing action only is unsupported in a queuing policy!!!
%QOS-6-POLICY_INST_FAILED:
Service policy installation failed
```

Policy Map on Physical Port

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions can include setting a specific DSCP or IP precedence or CoS values in the traffic class, specifying the traffic bandwidth limitations for each matched traffic class (policer), and taking action when the traffic is out of profile (marking).

A policy map also has these characteristics:

- A policy map can contain multiple class statements, each with different match criteria and policers.
- A policy map can contain a predefined default traffic class explicitly placed at the end of the map.

When you configure a default traffic class by using the **class class-default** policy-map configuration command, unclassified traffic (traffic that does not meet the match criteria specified in the traffic classes) is treated as the default traffic class (**class-default**).

- A separate policy-map class can exist for each type of traffic received through a port.

Policy Map on VLANs

The device supports a VLAN QoS feature that allows the user to perform QoS treatment at the VLAN level (classification and QoS actions) using the incoming frame's VLAN information. In VLAN-based QoS, a service policy is applied to an SVI interface. All physical interfaces belonging to a VLAN policy map then need to be programmed to refer to the VLAN-based policy maps instead of the port-based policy map.

Although the policy map is applied to the VLAN SVI, any policing (rate-limiting) action can only be performed on a per-port basis. You cannot configure the policer to take account of the sum of traffic from a number of physical ports. Each port needs to have a separate policer governing the traffic coming into that port.

Policing

After a packet is classified and has a DSCP-based, CoS-based, or QoS-group label assigned to it, the policing and marking process can begin.

Policing involves creating a policer that specifies the bandwidth limits for the traffic. Packets that exceed the limits are *out of profile* or *nonconforming*. Each policer decides on a packet-by-packet basis whether the packet is in or out of profile and specifies the actions on the packet. These actions, carried out by the marker, include passing through the packet without modification, dropping the packet, or modifying (marking down) the assigned DSCP or CoS value of the packet and allowing the packet to pass through.

To avoid out-of-order packets, both conform and nonconforming traffic typically exit the same queue.



Note All traffic, regardless of whether it is bridged or routed, is subjected to a policer, if one is configured. As a result, bridged packets might be dropped or might have their DSCP or CoS fields modified when they are policed and marked.

You can only configure policing on a physical port.

After you configure the policy map and policing actions, attach the policy-map to an ingress or egress port by using the **service-policy** interface configuration command.

Token-Bucket Algorithm

Policing uses a token-bucket algorithm. As each frame is received by the device, a token is added to the bucket. The bucket has a hole in it and leaks at a rate that you specify as the average traffic rate in bits per second. Each time a token is added to the bucket, the device verifies that there is enough room in the bucket. If there is not enough room, the packet is marked as nonconforming, and the specified policer action is taken (dropped or marked down).

How quickly the bucket fills is a function of the bucket depth (burst-byte), the rate at which the tokens are removed (rate-bps), and the duration of the burst above the average rate. The size of the bucket imposes an upper limit on the burst length and limits the number of frames that can be transmitted back-to-back. If the burst is short, the bucket does not overflow, and no action is taken against the traffic flow. However, if a burst is long and at a higher rate, the bucket overflows, and the policing actions are taken against the frames in that burst.

You configure the bucket depth (the maximum burst that is tolerated before the bucket overflows) by using the burst-byte option of the **police** policy-map class configuration command. You configure how fast (the average rate) that the tokens are removed from the bucket by using the rate option of the **police** policy-map class configuration command.

Marking

Marking is used to convey specific information to a downstream device in the network, or to carry information from one interface in a device to another.

Marking can be used to set certain field/bits in the packet headers, or marking can also be used to set certain fields in the packet structure that is internal to the device. Additionally, the marking feature can be used to define mapping between fields. The following marking methods are available for QoS:

- Packet header
- Device specific information
- Table maps

Packet Header Marking

Marking on fields in the packet header can be classified into two general categories:

- IPv4/v6 header bit marking
- Layer 2 header bit marking

The marking feature at the IP level is used to set the precedence or the DSCP in the IP header to a specific value to get a specific per-hop behavior at the downstream device (switch or router), or it can also be used to aggregate traffic from different input interfaces into a single class in the output interface. The functionality is currently supported on both the IPv4 and IPv6 headers.

Marking in the Layer 2 headers is typically used to influence dropping behavior in the downstream devices (switch or router). It works in tandem with the match on the Layer 2 headers. The bits in the Layer 2 header that can be set using a policy map are class of service.

Switch Specific Information Marking

This form of marking includes marking of fields in the packet data structure that are not part of the packets header, so that the marking can be used later in the data path. This is not propagated between the switches. Marking of QoS-group falls into this category. This form of marking is only supported in policies that are enabled on the input interfaces. The corresponding matching mechanism can be enabled on the output interfaces on the same switch and an appropriate QoS action can be applied.

Table Map Marking

Table map marking enables the mapping and conversion from one field to another using a conversion table. This conversion table is called a table map.

Depending upon the table map attached to an interface, CoS, DSCP, and Precedence values of the packet are rewritten. The device allows configuring both ingress table map policies and egress table map policies.

As an example, a table map can be used to map the Layer 2 CoS setting to a precedence value in Layer 3. This feature enables combining multiple `set` commands into a single table, which indicates the method to perform the mapping. This table can be referenced in multiple policies, or multiple times in the same policy.

The following table shows the currently supported forms of mapping:

Table 3: Packet-Marking Types Used for Establishing a To-From Relationship

| The To Packet-Marking Type | The From Packet-Marking Type |
|----------------------------|------------------------------|
| Precedence | CoS |

| The To Packet-Marking Type | The From Packet-Marking Type |
|----------------------------|------------------------------|
| Precedence | QoS Group |
| DSCP | CoS |
| DSCP | QoS Group |
| CoS | Precedence |
| CoS | DSCP |
| QoS Group | Precedence |
| QoS Group | DSCP |

A table map-based policy supports the following capabilities:

- Mutation—You can have a table map that maps from one DSCP value set to another DSCP value set, and this can be attached to an egress port.
- Rewrite—Packets coming in are rewritten depending upon the configured table map.
- Mapping—Table map based policies can be used instead of set policies.

The following steps are required for table map marking:

1. Define the table map—Use the **table-map** global configuration command to map the values. The table does not know of the policies or classes within which it will be used. The default command in the table map is used to indicate the value to be copied into the to field when there is no matching from field.
2. Define the policy map—You must define the policy map where the table map will be used.
3. Associate the policy to an interface.



Note A table map policy on an input port changes the trust setting of that port to the from type of qos-marking.

Traffic Conditioning

To support QoS in a network, traffic entering the service provider network needs to be policed on the network boundary routers to ensure that the traffic rate stays within the service limit. Even if a few routers at the network boundary start sending more traffic than what the network core is provisioned to handle, the increased traffic load leads to network congestion. The degraded performance in the network makes it difficult to deliver QoS for all the network traffic.

Traffic policing functions (using the police feature) and shaping functions (using the traffic shaping feature) manage the traffic rate, but differ in how they treat traffic when tokens are exhausted. The concept of tokens comes from the token bucket scheme, a traffic metering function.



Note When running QoS tests on network traffic, you may see different results for the shaper and policing data. Network traffic data from shaping provides more accurate results.

This table compares the policing and shaping functions.

Table 4: Comparison Between Policing and Shaping Functions

| Policing Function | Shaping Function |
|---|--|
| Sends conforming traffic up to the line rate and allows bursts. | Smooths traffic and sends it out at a constant rate. |
| When tokens are exhausted, action is taken immediately. | When tokens are exhausted, it buffers packets and sends them out later, when tokens are available. A class with shaping has a queue associated with it which will be used to buffer the packets. |
| Policing has multiple units of configuration – in bits per second, packets per second and cells per second. | Shaping has only one unit of configuration - in bits per second. |
| Policing has multiple possible actions associated with an event, marking and dropping being example of such actions. | Shaping does not have the provision to mark packets that do not meet the profile. |
| Works for both input and output traffic. | Implemented for output traffic only. |
| Transmission Control Protocol (TCP) detects the line at line speed but adapts to the configured rate when a packet drop occurs by lowering its window size. | TCP can detect that it has a lower speed line and adapt its retransmission timer accordingly. This results in less scope of retransmissions and is TCP-friendly. |

Policing

The QoS policing feature is used to impose a maximum rate on a traffic class. The QoS policing feature can also be used with the priority feature to restrict priority traffic. If the rate is exceeded, then a specific action is taken as soon as the event occurs. The rate (committed information rate [CIR] and peak information rate [PIR]) and the burst parameters (conformed burst size [B_c] and extended burst size [B_e]) are all configured in bytes per second.

The following policing forms or policers are supported for QoS:

- Single-rate two-color policing
- Dual-rate three-color policing



Note Single-rate three-color policing is not supported.

Single-Rate Two-Color Policing

Single-rate two-color policer is the mode in which you configure only a CIR and a B_c .

The B_c is an optional parameter, and if it is not specified it is computed by default. In this mode, when an incoming packet has enough tokens available, the packet is considered to be conforming. If at the time of packet arrival, enough tokens are not available within the bounds of B_c , the packet is considered to have exceeded the configured rate.



Note For information about the token-bucket algorithm, see [Token-Bucket Algorithm, on page 13](#).

Dual-Rate Three-Color Policing

With the dual rate policer, the device supports only color-blind mode. In this mode, you configure a committed information rate (CIR) and a peak information rate (PIR). As the name suggests, there are two token buckets in this case, one for the peak rate, and one for the conformed rate.



Note For information about the token-bucket algorithm, see [Token-Bucket Algorithm, on page 13](#).

In the color-blind mode, the incoming packet is first checked against the peak rate bucket. If there are not enough tokens available, the packet is said to violate the rate. If there are enough tokens available, then the tokens in the conformed rate buckets are checked to determine if there are enough tokens available. The tokens in the peak rate bucket are decremented by the size of the packet. If it does not have enough tokens available, the packet is said to have exceeded the configured rate. If there are enough tokens available, then the packet is said to conform, and the tokens in both the buckets are decremented by the size of the packet.

The rate at which tokens are replenished depends on the packet arrival. Assume that a packet comes in at time T_1 and the next one comes in at time T_2 . The time interval between T_1 and T_2 determines the number of tokens that need to be added to the token bucket. This is calculated as:

Time interval between packets $(T_2 - T_1) * CIR / 8$ bytes

Shaping

Shaping is the process of imposing a maximum rate of traffic, while regulating the traffic rate in such a way that the downstream switches and routers are not subjected to congestion. Shaping in the most common form is used to limit the traffic sent from a physical or logical interface.

Shaping has a buffer associated with it that ensures that packets which do not have enough tokens are buffered as opposed to being immediately dropped. The number of buffers available to the subset of traffic being shaped is limited and is computed based on a variety of factors. The number of buffers available can also be tuned using specific QoS commands. Packets are buffered as buffers are available, beyond which they are dropped.

Class-Based Traffic Shaping

The device uses class-based traffic shaping. This shaping feature is enabled on a class in a policy that is associated to an interface. A class that has shaping configured is allocated a number of buffers to hold the packets that do not have tokens. The buffered packets are sent out from the class using FIFO. In the most

common form of usage, class-based shaping is used to impose a maximum rate for an physical interface or logical interface as a whole. The following shaping forms are supported in a class:

- Average rate shaping
- Hierarchical shaping

Shaping is implemented using a token bucket. The values of CIR, B_c and B_e determine the rate at which the packets are sent out and the rate at which the tokens are replenished.



Note For information about the token-bucket algorithm, see [Token-Bucket Algorithm, on page 13](#).

Average Rate Shaping

You use the **shape average** policy-map class command to configure average rate shaping.

This command configures a maximum bandwidth for a particular class. The queue bandwidth is restricted to this value even though the port has more bandwidth available. The supports configuring shape average by either a percentage or by a target bit rate value.

Hierarchical Shaping

Shaping can also be configured at multiple levels in a hierarchy. This is accomplished by creating a parent policy with shaping configured, and then attaching child policies with additional shaping configurations to the parent policy.

There are two supported types of hierarchical shaping:

- Port shaper
- User-configured shaping

The port shaper uses the class default and the only action permitted in the parent is shaping. The queuing action is in the child with the port shaper. With the user configured shaping, you cannot have queuing action in the child.

Queuing and Scheduling

The device uses both queuing and scheduling to help prevent traffic congestion. The device supports the following queuing and scheduling features:

- Bandwidth
- Weighted Tail Drop
- Priority queues
- Queue buffers
- Weighted Random Early Detection

When you define a queuing policy on a port, control packets are mapped to the best priority queue with the highest threshold. Control packets queue mapping works differently in the following scenarios:

- Without a quality of service (QoS) policy—If no QoS policy is configured, control packets with DSCP values 16, 24, 48, and 56 are mapped to queue 0 with the highest threshold of threshold2.
- With an user-defined policy—An user-defined queuing policy configured on egress ports can affect the default priority queue setting on control packets.



Note Queuing policy in egress direction does not support **match access-group** classification.

Control traffic is redirected to the best queue based on the following rules:

1. If defined in a user policy, the highest-level priority queue is always chosen as the best queue.
2. In the absence of a priority queue, Cisco IOS software selects queue 0 as the best queue. When the software selects queue 0 as the best queue, you must define the highest bandwidth to this queue to get the best QoS treatment to the control plane traffic.
3. If thresholds are not configured on the best queue, Cisco IOS software assigns control packets with Differentiated Services Code Point (DSCP) values 16, 24, 48, and 56 are mapped to threshold2 and reassigns the rest of the control traffic in the best queue to threshold1.

If a policy is not configured explicitly for control traffic, the Cisco IOS software maps all unmatched control traffic to the best queue with threshold2, and the matched control traffic is mapped to the queue as configured in the policy.



Note To provide proper QoS for Layer 3 packets, you must ensure that packets are explicitly classified into appropriate queues. When the software detects DSCP values in the default queue, then it automatically reassigns this queue as the best queue.

Bandwidth

The supports the following bandwidth configurations:

- Bandwidth percent
- Bandwidth remaining ratio

Bandwidth Percent

You can use the **bandwidth percent** policy-map class command to allocate a minimum bandwidth to a particular class. The total sum cannot exceed 100 percent and in case the total sum is less than 100 percent, then the rest of the bandwidth is divided equally among all bandwidth queues.



Note A queue can oversubscribe bandwidth in case the other queues do not utilize the entire port bandwidth.

You cannot mix bandwidth types on a policy map. For example, you cannot configure bandwidth in a single policy map using both a bandwidth percent and in kilobits per second.

Bandwidth Remaining Ratio

You use the **bandwidth remaining ratio** policy-map class command to create a ratio for sharing unused bandwidth in specified queues. Any unused bandwidth will be used by these specific queues in the ratio that is specified by the configuration. Use this command when the **priority** command is also used for certain queues in the policy.

When you assign ratios, the queues will be assigned certain weights which are inline with these ratios.

You can specify ratios using a range from 0 to 100. For example, you can configure a bandwidth remaining ratio of 2 on one class, and another queue with a bandwidth remaining ratio of 4 on another class. The bandwidth remaining ratio of 4 will be scheduled twice as often as the bandwidth remaining ratio of 2.

The total bandwidth ratio allocation for the policy can exceed 100. For example, you can configure a queue with a bandwidth remaining ratio of 50, and another queue with a bandwidth remaining ratio of 100.

Weighted Tail Drop

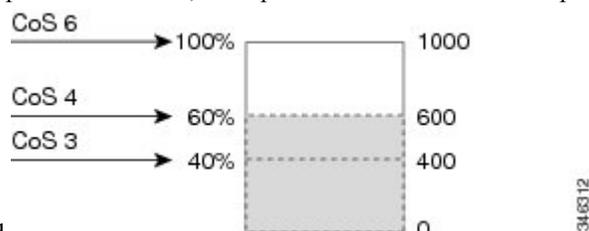
The egress queues use an enhanced version of the tail-drop congestion-avoidance mechanism called weighted tail drop (WTD). WTD is implemented on queues to manage the queue lengths and to provide drop precedences for different traffic classifications.

As a frame is enqueued to a particular queue, WTD uses the frame's assigned QoS label to subject it to different thresholds. If the threshold is exceeded for that QoS label (the space available in the destination queue is less than the size of the frame), the drops the frame.

Each queue has three configurable threshold values. The QoS label determines which of the three threshold values is subjected to the frame.

Figure 2: WTD and Queue Operation

The following figure shows an example of WTD operating on a queue whose size is 1000 frames. Three drop percentages are configured: 40 percent (400 frames), 60 percent (600 frames), and 100 percent (1000 frames). These percentages indicate that up to 400 frames can be queued at the 40-percent threshold, up to 600 frames at the 60-percent threshold, and up to 1000 frames at the 100-percent



threshold.

In the example, CoS value 6 has a greater importance than the other CoS values, and is assigned to the 100-percent drop threshold (queue-full state). CoS values 4 is assigned to the 60-percent threshold, and CoS values 3 is assigned to the 40-percent threshold. All of these threshold values are assigned using the **queue-limit cos** command.

Assuming the queue is already filled with 600 frames, and a new frame arrives. It contains CoS value 4 and is subjected to the 60-percent threshold. If this frame is added to the queue, the threshold will be exceeded, so the drops it.

Weighted Tail Drop Default Values

The following are the Weighted Tail Drop (WTD) default values and the rules for configuring WTD threshold values.

- If you configure less than three queue-limit percentages for WTD, then WTD default values are assigned to these thresholds.

The following are the WTD threshold default values:

Table 5: WTD Threshold Default Values

| Threshold | Default Value Percentage |
|-----------|--------------------------|
| 0 | 80 |
| 1 | 90 |
| 2 | 400 |

- If 3 different WTD thresholds are configured, then the queues are programmed as configured.
- If 2 WTD thresholds are configured, then the maximum value percentage will be 400.
- If a WTD single threshold is configured as x, then the maximum value percentage will be 400.
 - If the value of x is less than 90, then threshold1=90 and threshold 0=x.
 - If the value of x equals 90, then threshold1=90, threshold 0=80.
 - If the value x is greater than 90, then threshold1=x, threshold 0=80.

Priority Queues

Each port supports eight egress queues, of which two can be given a priority.

You use the **priority level** policy class-map command to configure the priority for two classes. One of the classes has to be configured with a priority queue level 1, and the other class has to be configured with a priority queue level 2. Packets on these two queues are subjected to less latency with respect to other queues.



Note You can configure a priority only with a level.

Only one strict priority or a priority with levels is allowed in one policy map. Multiple priorities with the same priority levels without kbps/percent are allowed in a policy map only if all of them are configured with police.

Queue Buffer

At boot time, when there is no policy map enabled on the wired port, there are two queues created by default. Wired ports can have a maximum of 8 queues configured using MQC-based policies. The following table shows which packets go into which one of the queues:

Table 6: DSCP, Precedence, and CoS - Queue Threshold Mapping Table

| DSCP, Precedence or CoS | Queue | Threshold |
|-------------------------|-------|-----------|
| Control Packets | 0 | 2 |
| Rest of Packets | 1 | 2 |



Note You can guarantee the availability of buffers, set drop thresholds, and configure the maximum memory allocation for a queue. You use the **queue-buffers** policy-map class command to configure the queue buffers. You use the **queue-limit** policy-map class command to configure the maximum thresholds.

There are two types of buffer allocations: hard buffers, which are explicitly reserved for the queue, and soft buffers, which are available for other ports when unused by a given port.



Note By default, Queue 0 is not a priority queue. A policy-map can enable Queue 0 to be a priority queue by using the **priority level** command. If Queue 0 is assigned a priority level of 1, the soft maximum limit for this queue is automatically set to the same value as the hard maximum limit.

Queue Buffer Allocation

The buffer allocation to any queue can be tuned using the **queue-buffers ratio** policy-map class configuration command.

Dynamic Threshold and Scaling

Traditionally, reserved buffers are statically allocated for each queue. No matter whether the queue is active or not, its buffers are held up by the queue. In addition, as the number of queues increases, the portion of the reserved buffers allocated for each queue can become smaller and smaller. Eventually, a situation may occur where there are not enough reserved buffers to support a jumbo frame for all queues.

The device supports Dynamic Thresholding and Scaling (DTS), which is a feature that provides a fair and efficient allocation of buffer resources. When congestion occurs, this DTS mechanism provides an elastic buffer allocation for the incoming data based on the occupancy of the global/port resources. Conceptually, DTS scales down the queue buffer allocation gradually as the resources are used up to leave room for other queues, and vice versa. This flexible method allows the buffers to be more efficiently and fairly utilized.

As mentioned in the previous sections, there are two limits configured on a queue—a hard limit and a soft limit.

Hard limits are not part of DTS. These buffers are available only for that queue. The sum of the hard limits should be less than the globally set up hard maximum limit. The global hard limit configured for egress queuing is currently set to 12672. In the default scenario, when there are no MQC policies configured, each port takes up 176 buffers, allowing room for more hard buffers to be allocated based upon the configuration.

Soft limit buffers participate in the DTS process. Additionally, some of the soft buffer allocations can exceed the global soft limit allocation. The global soft limit allocation for egress queuing is currently set to 27024. The sum of the hard and soft limits add up to 39696, which in turn translates to 10.1 MB. Because the sum of the soft buffer allocations can exceed the global limit, it allows a specific queue to use a large number of

buffers when the system is lightly loaded. The DTS process dynamically adjusts the per-queue allocation as the system becomes more heavily loaded.

Trust Behavior

Port Security on a Trusted Boundary for Cisco IP Phones

In a typical network, you connect a Cisco IP Phone to a device port and cascade devices that generate data packets from the back of the telephone. The Cisco IP Phone guarantees the voice quality through a shared data link by marking the CoS level of the voice packets as high priority (CoS = 5) and by marking the data packets as low priority (CoS = 0). Traffic sent from the telephone to the device is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the class of service (CoS) 3-bit field, which is the priority of the packet.

For most Cisco IP Phone configurations, the traffic sent from the telephone to the device should be trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network. By using the **trust device** interface configuration command, you configure the device port to which the telephone is connected to trust the traffic received on that port.



Note The **trust device** *device_type* command available in interface configuration mode is a stand-alone command on the device. When using this command in an AutoQoS configuration, if the connected peer device is not a corresponding device (defined as a device matching your trust policy), both CoS and DSCP values are set to "0" and any input policy will not take effect. If the connected peer device is a corresponding device, input policy will take effect.

With the trusted setting, you also can use the trusted boundary feature to prevent misuse of a high-priority queue if a user bypasses the telephone and connects the PC directly to the device. Without trusted boundary, the CoS labels generated by the PC are trusted by the device (because of the trusted CoS setting). By contrast, trusted boundary uses CDP to detect the presence of a Cisco IP Phone (such as the Cisco IP Phone 7910, 7935, 7940, and 7960) on a device port. If the telephone is not detected, the trusted boundary feature disables the trusted setting on the device port and prevents misuse of a high-priority queue. Note that the trusted boundary feature is not effective if the PC and Cisco IP Phone are connected to a hub that is connected to the device.

Trust Behavior for Wired Ports

For wired ports that are connected to the device (end points such as IP phones, laptops, cameras, telepresence units, or other devices), their DSCP, precedence, or CoS values coming in from these end points are trusted by the device and therefore are retained in the absence of any explicit policy configuration.

The packets are enqueued to the appropriate queue per the default initial configuration. No priority queuing at the device is done by default. This is true for unicast and multicast packets.

In scenarios where the incoming packet type differs from the outgoing packet type, the trust behavior and the queuing behavior are explained in the following table. Note that the default trust mode for a port is DSCP based. The trust mode 'falls back' to CoS if the incoming packet is a pure Layer 2 packet. You can also change the trust setting from DSCP to CoS. This setting change is accomplished by using an MQC policy that has a

class default with a 'set cos cos table default default-cos' action, where default-cos is the name of the table map created (which only performs a default copy).

Table 7: Trust and Queuing Behavior

| Incoming Packet | Outgoing Packet | Trust Behavior | Queuing Behavior |
|-----------------|-----------------|--------------------------------|---|
| Layer 3 | Layer 3 | Preserve DSCP/Precedence | Based on DSCP |
| Layer 2 | Layer 2 | Not applicable | Based on CoS |
| Tagged | Tagged | Preserve DSCP and CoS | Based on DSCP (trust DSCP takes precedence) |
| Layer 3 | Tagged | Preserve DSCP, CoS is set to 0 | Based on DSCP |

Standard QoS Default Settings

Default Wired QoS Configuration

There are two queues configured by default on each wired interface on the device. All control traffic traverses and is processed through queue 0. All other traffic traverses and is processed through queue 1.

DSCP Maps

Default CoS-to-DSCP Map

When DSCP transparency mode is disabled, the DSCP values are derived from CoS as per the following table. If these values are not appropriate for your network, you need to modify them.

Note When the DSCP transparency mode is disabled by default. If it is enabled (`mls qos rewrite ip dscp` interface configuration command), DSCP rewrite will not happen.

Table 8: Default CoS-to-DSCP Map

| CoS Value | DSCP Value |
|-----------|------------|
| 0 | 0 |
| 1 | 8 |
| 2 | 16 |
| 3 | 24 |
| 4 | 32 |
| 5 | 40 |
| 6 | 48 |

| CoS Value | DSCP Value |
|-----------|------------|
| 7 | 56 |

Default IP-Precedence-to-DSCP Map

You use the IP-precedence-to-DSCP map to map IP precedence values in incoming packets to a DSCP value that QoS uses internally to represent the priority of the traffic. The following table shows the default IP-precedence-to-DSCP map. If these values are not appropriate for your network, you need to modify them.

Table 9: Default IP-Precedence-to-DSCP Map

| IP Precedence Value | DSCP Value |
|---------------------|------------|
| 0 | 0 |
| 1 | 8 |
| 2 | 16 |
| 3 | 24 |
| 4 | 32 |
| 5 | 40 |
| 6 | 48 |
| 7 | 56 |

Default DSCP-to-CoS Map

You use the DSCP-to-CoS map to generate a CoS value, which is used to select one of the four egress queues. The following table shows the default DSCP-to-CoS map. If these values are not appropriate for your network, you need to modify them.

Table 10: Default DSCP-to-CoS Map

| DSCP Value | CoS Value |
|------------|-----------|
| 0–7 | 0 |
| 8–15 | 1 |
| 16–23 | 2 |
| 24–31 | 3 |
| 32–39 | 4 |
| 40–47 | 5 |
| 48–55 | 6 |
| 56–63 | 7 |

Restrictions for QoS on Wired Targets

A target is an entity where a policy is applied. A wired target can be either a port or VLAN.

The following are restrictions for applying QoS features on the device for the wired target:

- A maximum of 8 queuing classes are supported on the device port for the wired target.
- A maximum of 63 policers are supported per policy on the wired port for the wired target, in the ingress or egress directions.
- A maximum of 1599 policy-maps can be created.
- No more than two levels are supported in a QoS hierarchy.
- In a hierarchical policy, overlapping actions between parent and child are not allowed, except when a policy has the port shaper in the parent and queuing features in the child policy.
- A QoS policy cannot be attached to any EtherChannel interface.
- Policing in both the parent and child is not supported in a QoS hierarchy.
- Marking in both the parent and child is not supported in a QoS hierarchy.
- With shaping, there is an IPG overhead of 20Bytes for every packet that is accounted internally in the hardware. Shaping accuracy will be effected by this, specially for packets of small size.
- Class-maps with empty actions are not supported. If there are two policies with the same order of class-maps and if there are class-maps with no action in one of the policies, there may be traffic drops. As a workaround, allocate minimal bandwidth for all the classes in `PRIORITY_QUEUE`.
- A maximum of 256 classes are supported per policy on the wired port for the wired target.
- Based on the Cisco UADP architecture, traffic is subjected to QoS lookup and the corresponding configured actions even if this traffic is later dropped in the Egress Global Resolution block and is never transmitted out of the actual interface.
- The actions under a policer within a policy map have the following restrictions:
 - The conform action must be transmit.
 - The exceed/violate action for markdown type can only be `cos2cos`, `prec2prec`, `dscp2dscp`.
 - The markdown types must be the same within a policy.
- Only marking policy is supported on SVI.
- A port-level input marking policy takes precedence over an SVI policy; however, if no port policy is configured, the SVI policy takes precedence. For a port policy to take precedence, define a port-level policy; so that the SVI policy is overwritten.
- Classification counters have the following specific restrictions:
 - Classification counters count packets instead of bytes.
 - Filter-based classification counters are not supported
 - Only QoS configurations with marking or policing trigger the classification counter.

- As long as there is policing or marking action in the policy, the class will have classification counters.
 - Classification counters are not supported on pure queuing policies under any class-map.
 - When there are multiple match statements in a class, the traffic counter is cumulative for all the match statements in the class.
- The device supports a total of eight table maps for policer exceed markdown and eight table maps for policer violate markdown.
 - Hierarchical policies are required for the following:
 - Port-shapers
 - Aggregate policers
 - PV policy
 - Parent shaping and child marking/policing
 - In a HQoS policy with parent shaping and child policy having priority level queuing and priority level policing, the statistics for policing are not updated. Only QoS shaper statistics are updated. To view the QoS shaper statistics, use the **show policy-map interface** command in global configuration mode.
 - For ports with wired targets, these are the only supported hierarchical policies:
 - Police chaining in the same policy is unsupported.
 - Hierarchical queuing is unsupported in the same policy (port shaper is the exception).
 - In a parent class, all filters must have the same type. The child filter type must match the parent filter type with the following exceptions:
 - If the parent class is configured to match IP, then the child class can be configured to match the ACL.
 - If the parent class is configured to match CoS, then the child class can be configured to match the ACL.
 - The **trust device device_type** command available in interface configuration mode is a stand-alone command on the device. When using this command in an AutoQoS configuration, if the connected peer device is not a corresponding device (defined as a device matching your trust policy), both CoS and DSCP values are set to "0" and any input policy will not take effect. If the connected peer device is a corresponding device, input policy will take effect.

The following are restrictions for applying QoS features on the VLAN to the wired target:

- For a flat or nonhierarchical policy, only marking or a table map is supported.

The following are restrictions and considerations for applying QoS features on EtherChannel and channel member interfaces:

- QoS is not supported on an EtherChannel interface.
- QoS is supported on EtherChannel member interfaces in both ingress and egression directions. All EtherChannel members must have the same QoS policy applied. If the QoS policy is not the same, each individual policy on the different link acts independently.

- On attaching a service policy to channel members, the following warning message appears to remind the user to make sure the same policy is attached to all ports in the EtherChannel: ' Warning: add service policy will cause inconsistency with port xxx in ether channel xxx. '.
- Auto QoS is not supported on EtherChannel members.



Note On attaching a service policy to an EtherChannel, the following message appears on the console: ' Warning: add service policy will cause inconsistency with port xxx in ether channel xxx. '. This warning message should be expected. This warning message is a reminder to attach the same policy to other ports in the same EtherChannel. The same message will be seen during boot up. This message does not mean there is a discrepancy between the EtherChannel member ports.

How to Configure QoS

Configuring Class, Policy, and Maps

Creating a Traffic Class

To create a traffic class containing match criteria, use the **class-map** command to specify the traffic class name, and then use the following **match** commands in class-map configuration mode, as needed.

Before you begin

All match commands specified in this configuration task are considered optional, but you must configure at least one match criterion for a class.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | class-map <i>class-map name</i> { match-any match-all } Example: <pre>(config)# class-map test_1000 (config-cmap)#</pre> | Enters class map configuration mode. <ul style="list-style-type: none"> • Creates a class map to be used for matching packets to the class whose name you specify. • match-any: Any one of the match criteria must be met for traffic entering the traffic class to be classified as part of it. |

| | Command or Action | Purpose |
|----------------------|---|---|
| | | <ul style="list-style-type: none"> • match-all: All of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. <p>Note This is the default. If match-any or match-all is not explicitly defined, match-all is chosen by default.</p> |
| <p>Step 3</p> | <p>match access-group { <i>index number</i> <i>name</i> }</p> <p>Example:</p> <pre>(config-cmap) # match access-group 100 (config-cmap) #</pre> | <p>The following parameters are available for this command:</p> <ul style="list-style-type: none"> • access-group • cos • dscp • group-object • ip • mpls • non-client-nrt • precedence • protocol • qos-group • vlan • wlan <p>(Optional) For this example, enter the access-group ID:</p> <ul style="list-style-type: none"> • Access list index (value from 1 to 2799) • Named access list |
| <p>Step 4</p> | <p>match cos <i>cos value</i></p> <p>Example:</p> <pre>(config-cmap) # match cos 2 3 4 5 (config-cmap) #</pre> | <p>(Optional) Matches IEEE 802.1Q or ISL class of service (user) priority values.</p> <ul style="list-style-type: none"> • Enters up to 4 CoS values separated by spaces (0 to 7). |
| <p>Step 5</p> | <p>match dscp <i>dscp value</i></p> <p>Example:</p> <pre>(config-cmap) # match dscp af11 af12</pre> | <p>(Optional) Matches the DSCP values in IPv4 and IPv6 packets.</p> |

| | Command or Action | Purpose |
|---------------|--|---|
| | <code>(config-cmap) #</code> | |
| Step 6 | <p>match ip { dscp <i>dscp value</i> precedence <i>precedence value</i> }</p> <p>Example:</p> <pre>(config-cmap) # match ip dscp af11 af12 (config-cmap) #</pre> | <p>(Optional) Matches IP values including the following:</p> <ul style="list-style-type: none"> • dscp—Matches IP DSCP (DiffServ codepoints). • precedence—Matches IP precedence (0 to 7). <p>Note Since CPU generated packets are not marked at egress, the packet will not match the configured class-map.</p> |
| Step 7 | <p>match qos-group <i>qos group value</i></p> <p>Example:</p> <pre>(config-cmap) # match qos-group 10 (config-cmap) #</pre> | (Optional) Matches QoS group value (from 0 to 31). |
| Step 8 | <p>match vlan <i>vlan value</i></p> <p>Example:</p> <pre>(config-cmap) # match vlan 210 (config-cmap) #</pre> | (Optional) Matches a VLAN ID (from 1 to 4095). |
| Step 9 | <p>end</p> <p>Example:</p> <pre>(config-cmap) # end</pre> | Saves the configuration changes. |

What to do next

Configure the policy map.

Creating a Traffic Policy

To create a traffic policy, use the **policy-map** global configuration command to specify the traffic policy name.

The traffic class is associated with the traffic policy when the **class** command is used. The **class** command must be entered after you enter the policy map configuration mode. After entering the **class** command, the device is automatically in policy map class configuration mode, which is where the QoS policies for the traffic policy are defined.

The following policy map class-actions are supported:

- bandwidth—Bandwidth configuration options.
- exit—Exits from the QoS class action configuration mode.
- no—Negates or sets default values for the command.
- police—Policer configuration options.
- priority—Strict scheduling priority configuration options for this class.
- queue-buffers—Queue buffer configuration options.
- queue-limit—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options.
- service-policy—Configures the QoS service policy.
- set—Sets QoS values using the following options:
 - CoS values
 - DSCP values
 - Precedence values
 - QoS group values
- shape—Traffic-shaping configuration options.

Before you begin

You should have first created a class map.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | policy-map <i>policy-map name</i> Example: <pre>(config)# policy-map test_2000 (config-pmap)#</pre> | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| Step 3 | class { <i>class-name</i> class-default } Example: <pre>(config-pmap)# class test_1000 (config-pmap-c)#</pre> | Specifies the name of the class whose policy you want to create or change. You can also create a system default class for unclassified packets. |

| | Command or Action | Purpose |
|--------|---|--|
| Step 4 | <p>bandwidth { <i>kb/s kb/s value</i> percent <i>percentage</i> remaining { <i>percent</i> <i>ratio</i> } }</p> <p>Example:</p> <pre>(config-pmap-c) # bandwidth 50 (config-pmap-c) #</pre> | <p>(Optional) Sets the bandwidth using one of the following:</p> <ul style="list-style-type: none"> • kb/s—Kilobits per second, enter a value between 20000 and 10000000 for Kb/s. • percent—Enter the percentage of the total bandwidth to be used for this policy map. • remaining—Enter the percentage ratio of the remaining bandwidth. <p>For a more detailed example of this command and its usage, see Configuring Bandwidth, on page 49.</p> |
| Step 5 | <p>exit</p> <p>Example:</p> <pre>(config-pmap-c) # exit (config-pmap-c) #</pre> | <p>(Optional) Exits from QoS class action configuration mode.</p> |
| Step 6 | <p>no</p> <p>Example:</p> <pre>(config-pmap-c) # no (config-pmap-c) #</pre> | <p>(Optional) Negates the command.</p> |
| Step 7 | <p>police { <i>target_bit_rate</i> cir rate }</p> <p>Example:</p> <pre>(config-pmap-c) # police 100000 (config-pmap-c) #</pre> | <p>(Optional) Configures the policer:</p> <ul style="list-style-type: none"> • target_bit_rate—Enter the bit rate per second, enter a value between 8000 and 10000000000. • cir—Committed Information Rate • rate—Specify police rate, PCR for hierarchical policies or SCR for single-level ATM 4.0 policer policies. <p>For a more detailed example of this command and its usage, see Configuring Police, on page 51.</p> |
| Step 8 | <p>priority level <i>level value</i></p> <p>Example:</p> <pre>(config-pmap-c) # priority level 1 (config-pmap-c) #</pre> | <p>(Optional) Sets the strict scheduling priority for this class. Command options include:</p> <ul style="list-style-type: none"> • level—Establishes a multi-level priority queue. Enter a value (1 or 2). |

| | Command or Action | Purpose |
|----------------|---|--|
| | | For a more detailed example of this command and its usage, see Configuring Priority, on page 53 . |
| Step 9 | queue-buffers ratio <i>ratio limit</i> Example: <pre>(config-pmap-c) # queue-buffers ratio 10 (config-pmap-c) #</pre> | (Optional) Configures the queue buffer for the class. Enter the queue buffers ratio limit (0 to 100). For a more detailed example of this command and its usage, see Configuring Queue Buffers, on page 55 . |
| Step 10 | queue-limit { <i>packets</i> cos dscp percent } Example: <pre>(config-pmap-c) # queue-limit cos 7 percent 50 (config-pmap-c) #</pre> | (Optional) Specifies the queue maximum threshold for the tail drop: <ul style="list-style-type: none"> • packets—Packets by default, enter a value between 1 to 2000000. • cos—Enter the parameters for each COS value. • dscp—Enter the parameters for each DSCP value. • percent—Enter the percentage for the threshold. For a more detailed example of this command and its usage, see Configuring Queue Limits, on page 58 . |
| Step 11 | service-policy <i>policy-map name</i> Example: <pre>(config-pmap-c) # service-policy test_2000 (config-pmap-c) #</pre> | (Optional) Configures the QoS service policy. |
| Step 12 | set { cos dscp ip precedence qos-group wlan } Example: <pre>(config-pmap-c) # set cos 7 (config-pmap-c) #</pre> | (Optional) Sets the QoS values. Possible QoS configuration values include: <ul style="list-style-type: none"> • cos—Sets the IEEE 802.1Q/ISL class of service/user priority. • dscp—Sets DSCP in IP(v4) and IPv6 packets. • ip—Sets IP specific values. • precedence—Sets precedence in IP(v4) and IPv6 packet. • qos-group—Sets the QoS Group. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 13 | shape average { <i>target_bit_rate</i> percent } Example: <pre>(config-pmap-c) #shape average percent 50 (config-pmap-c) #</pre> | (Optional) Sets the traffic shaping. Command parameters include: <ul style="list-style-type: none"> • <i>target_bit_rate</i>—Target bit rate. • percent—Percentage of interface bandwidth for Committed Information Rate. For a more detailed example of this command and its usage, see Configuring Shaping, on page 60 . |
| Step 14 | end Example: <pre>(config-pmap-c) #end (config-pmap-c) #</pre> | Saves the configuration changes. |

What to do next

Configure the interface.

Configuring Class-Based Packet Marking

This procedure explains how to configure the following class-based packet marking features on your device:

- CoS value
- DSCP value
- IP value
- Precedence value
- QoS group value

Before you begin

You should have created a class map and a policy map before beginning this procedure.

Procedure

| | Command or Action | Purpose |
|---------------|---|---------------------------------------|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | <p>policy-map <i>policy name</i></p> <p>Example:</p> <pre>(config)# policy-map policy1 (config-pmap)#</pre> | <p>Enters policy map configuration mode.</p> <p>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</p> |
| Step 3 | <p>class <i>class name</i></p> <p>Example:</p> <pre>(config-pmap)# class class1 (config-pmap-c)#</pre> | <p>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change.</p> <p>Command options for policy class map configuration mode include the following:</p> <ul style="list-style-type: none"> • bandwidth—Bandwidth configuration options. • exit—Exits from the QoS class action configuration mode. • no—Negates or sets default values for the command. • police—Policer configuration options. • priority—Strict scheduling priority configuration options for this class. • queue-buffers—Queue buffer configuration options. • queue-limit—Queue maximum threshold for Weighted Tail Drop (WTD) configuration options. • service-policy—Configures the QoS service policy. • set—Sets QoS values using the following options: <ul style="list-style-type: none"> • CoS values • DSCP values • Precedence values • QoS group values • shape—Traffic-shaping configuration options. |

| | Command or Action | Purpose |
|---------------|---|---|
| | | <p>Note This procedure describes the available configurations using set command options. The other command options (admit, bandwidth, etc.) are described in other sections of this guide. Although this task lists all of the possible set commands, only one set command is supported per class.</p> |
| Step 4 | <p>set cos {<i>cos value</i> cos table <i>table-map name</i> dscp table <i>table-map name</i> precedence table <i>table-map name</i> qos-group table <i>table-map name</i> }</p> <p>Example:</p> <pre>(config-pmap) # set cos 5 (config-pmap) #</pre> | <p>(Optional) Sets the specific IEEE 802.1Q Layer 2 CoS value of an outgoing packet. Values are from 0 to 7.</p> <p>You can also set the following values using the set cos command:</p> <ul style="list-style-type: none"> • cos table—Sets the CoS value based on a table map. • dscp table—Sets the code point value based on a table map. • precedence table—Sets the code point value based on a table map. • qos-group table—Sets the CoS value from QoS group based on a table map. |
| Step 5 | <p>set dscp {<i>dscp value</i> default dscp table <i>table-map name</i> ef precedence table <i>table-map name</i> qos-group table <i>table-map name</i> wlan user-priority table <i>table-map name</i> }</p> <p>Example:</p> <pre>(config-pmap) # set dscp af11 (config-pmap) #</pre> | <p>(Optional) Sets the DSCP value.</p> <p>In addition to setting specific DSCP values, you can also set the following using the set dscp command:</p> <ul style="list-style-type: none"> • default—Matches packets with default DSCP value (000000). • dscp table—Sets the packet DSCP value from DSCP based on a table map. • ef—Matches packets with EF DSCP value (101110). • precedence table—Sets the packet DSCP value from precedence based on a table map. • qos-group table—Sets the packet DSCP value from a QoS group based upon a table map. |

| | Command or Action | Purpose |
|---------------|--|--|
| Step 6 | <p>set ip {dscp precedence}</p> <p>Example:</p> <pre>(config-pmap) # set ip dscp c3 (config-pmap) #</pre> | <p>(Optional) Sets IP specific values. These values are either IP DSCP or IP precedence values.</p> <p>You can set the following values using the set ip dscp command:</p> <ul style="list-style-type: none"> • <i>dscp value</i>—Sets a specific DSCP value. • default—Matches packets with default DSCP value (000000). • dscp table—Sets the packet DSCP value from DSCP based on a table map. • ef—Matches packets with EF DSCP value (101110). • precedence table—Sets the packet DSCP value from precedence based on a table map. • qos-group table—Sets the packet DSCP value from a QoS group based upon a table map. <p>You can set the following values using the set ip precedence command:</p> <ul style="list-style-type: none"> • <i>precedence value</i>—Sets the precedence value (from 0 to 7) . • cos table—Sets the packet precedence value from Layer 2 CoS based on a table map. • dscp table—Sets the packet precedence from DSCP value based on a table map. • precedence table—Sets the precedence value from precedence based on a table map • qos-group table—Sets the precedence value from a QoS group based upon a table map. |
| Step 7 | <p>set precedence {precedence value cos table table-map name dscp table table-map name precedence table table-map name qos-group table table-map name}</p> <p>Example:</p> <pre>(config-pmap) # set precedence 5</pre> | <p>(Optional) Sets precedence values in IPv4 and IPv6 packets.</p> <p>You can set the following values using the set precedence command:</p> <ul style="list-style-type: none"> • <i>precedence value</i>—Sets the precedence value (from 0 to 7) . |

| | Command or Action | Purpose |
|----------------|---|--|
| | <code>(config-pmap) #</code> | <ul style="list-style-type: none"> • cos table—Sets the packet precedence value from Layer 2 CoS on a table map. • dscp table—Sets the packet precedence from DSCP value on a table map. • precedence table—Sets the precedence value from precedence based on a table map. • qos-group table—Sets the precedence value from a QoS group based upon a table map. |
| Step 8 | <p>set qos-group {<i>qos-group value</i> dscp table <i>table-map name</i> precedence table <i>table-map name</i>}</p> <p>Example:</p> <pre>(config-pmap) # set qos-group 10 (config-pmap) #</pre> | <p>(Optional) Sets QoS group values. You can set the following values using this command:</p> <ul style="list-style-type: none"> • <i>qos-group value</i>—A number from 1 to 31. • dscp table—Sets the code point value from DSCP based on a table map. • precedence table—Sets the code point value from precedence based on a table map. |
| Step 9 | <p>end</p> <p>Example:</p> <pre>(config-pmap) # end #</pre> | Saves configuration changes. |
| Step 10 | <p>show policy-map</p> <p>Example:</p> <pre># show policy-map</pre> | (Optional) Displays policy configuration information for all classes configured for all service policies. |

What to do next

Attach the traffic policy to an interface using the **service-policy** command.

Attaching a Traffic Policy to an Interface

After the traffic class and traffic policy are created, you must use the **service-policy** interface configuration command to attach a traffic policy to an interface, and to specify the direction in which the policy should be applied (either on packets coming into the interface or packets leaving the interface).

Before you begin

A traffic class and traffic policy must be created before attaching a traffic policy to an interface.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | interface <i>type</i> Example: <pre>(config)# interface GigabitEthernet1/0/1 (config-if)#</pre> | Enters interface configuration mode and configures an interface. Command parameters for the interface configuration include: <ul style="list-style-type: none"> • ANI— Autonomic-Networking virtual interface • AccessTunnel — Access Tunnel interface • Auto Template— Auto-template interface • CEM-PG— Circuit Emulation interface with Protection group • FortyGigabitEthernet— Forty Gigabit Ethernet • GigabitEthernet—Gigabit Ethernet IEEE 802.3z • Internal Interface— Internal interface • LISP— Locator ID Separation Protocol Virtual Interface • Loopback—Loopback interface • Null—Null interface • PROTECTION_GROUP—Protection-group controller • Port-channel—Ethernet Channel of interface • SDH_ACR —Virtual SDH-ACR controller • TLS-VIF —TLS Virtual Interface • TenGigabitEthernet—10-Gigabit Ethernet |

| | Command or Action | Purpose |
|---------------|--|--|
| | | <ul style="list-style-type: none"> • Tunnel—Tunnel interface • Vlan—Catalyst VLANs • Range—Interface range |
| Step 3 | service-policy {input <i>policy-map</i> output <i>policy-map</i> } Example: <pre>(config-if) # service-policy output policy_map_01 (config-if) #</pre> | Attaches a policy map to an input or output interface. This policy map is then used as the service policy for that interface. In this example, the traffic policy evaluates all traffic leaving that interface. |
| Step 4 | end Example: <pre>(config-if) # end #</pre> | Saves configuration changes. |
| Step 5 | show policy map Example: <pre># show policy map</pre> | (Optional) Displays statistics for the policy on the specified interface. |

What to do next

Proceed to attach any other traffic policy to an interface, and to specify the direction in which the policy should be applied.

Classifying, Policing, and Marking Traffic on Physical Ports by Using Policy Maps

You can configure a nonhierarchical policy map on a physical port that specifies which traffic class to act on. Actions supported are remarking and policing.

Before you begin

You should have already decided upon the classification, policing, and marking of your network traffic by policy maps prior to beginning this procedure.

Procedure

| | Command or Action | Purpose |
|---------------|--|---------------------------------------|
| Step 1 | configure terminal Example: | Enters the global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | <code># configure terminal</code> | |
| Step 2 | <p>class-map { <i>class-map name</i> match-any }</p> <p>Example:</p> <pre>(config)# class-map ipclass1 (config-cmap)# exit (config)#</pre> | <p>Enters class map configuration mode.</p> <ul style="list-style-type: none"> Creates a class map to be used for matching packets to the class whose name you specify. If you specify match-any, one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default. |
| Step 3 | <p>match access-group { <i>access list index</i> <i>access list name</i> }</p> <p>Example:</p> <pre>(config-cmap)# match access-group 1000 (config-cmap)# exit (config)#</pre> | <p>The following parameters are available for this command:</p> <ul style="list-style-type: none"> access-group cos dscp group-object ip mpls non-client-nrt precedence protocol qos-group vlan wlan <p>(Optional) For this example, enter the access-group ID:</p> <ul style="list-style-type: none"> Access list index (value from 1 to 2799) Named access list |
| Step 4 | <p>policy-map <i>policy-map-name</i></p> <p>Example:</p> <pre>(config)# policy-map flowit (config-pmap)#</pre> | <p>Creates a policy map by entering the policy map name, and enters policy-map configuration mode.</p> <p>By default, no policy maps are defined.</p> |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 5 | <p>class {<i>class-map-name</i> class-default}</p> <p>Example:</p> <pre>(config-pmap) # class ipclass1 (config-pmap-c) #</pre> | <p>Defines a traffic classification, and enter policy-map class configuration mode.</p> <p>By default, no policy map class-maps are defined.</p> <p>If a traffic class has already been defined by using the class-map global configuration command, specify its name for <i>class-map-name</i> in this command.</p> <p>A class-default traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied match any included in the class-default class, all packets that have not already matched the other traffic classes will match class-default.</p> |
| Step 6 | <p>set {cos dscp ip precedence qos-group wlan user-priority}</p> <p>Example:</p> <pre>(config-pmap-c) # set dscp 45 (config-pmap-c) #</pre> | <p>(Optional) Sets the QoS values. Possible QoS configuration values include:</p> <ul style="list-style-type: none"> • cos—Sets the IEEE 802.1Q/ISL class of service/user priority. • dscp—Sets DSCP in IP(v4) and IPv6 packets. • ip—Sets IP specific values. • precedence—Sets precedence in IP(v4) and IPv6 packet. • qos-group—Sets QoS group. <p>In this example, the set dscp command classifies the IP traffic by setting a new DSCP value in the packet.</p> |
| Step 7 | <p>police {<i>target_bit_rate</i> cir rate}</p> <p>Example:</p> <pre>(config-pmap-c) # police 100000 conform-action transmit exceed-action drop (config-pmap-c) #</pre> | <p>(Optional) Configures the policer:</p> <ul style="list-style-type: none"> • <i>target_bit_rate</i>—Specifies the bit rate per second, enter a value between 8000 and 10000000000. • cir—Committed Information Rate. • rate—Specifies the police rate PCR for hierarchical policies. <p>In this example, the police command adds a policer to the class where any traffic beyond the 100000 set target bit rate is dropped.</p> |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 8 | exit Example: <code>(config-pmap-c) # exit</code> | Returns to policy map configuration mode. |
| Step 9 | exit Example: <code>(config-pmap) # exit</code> | Returns to global configuration mode. |
| Step 10 | interface <i>interface-id</i> Example: <code>(config) # interface HundredGigabitEthernet 1/0/2</code> | Specifies the port to attach to the policy map, and enters interface configuration mode. Valid interfaces include physical ports. |
| Step 11 | service-policy input <i>policy-map-name</i> Example: <code>(config-if) # service-policy input flowit</code> | Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported. |
| Step 12 | end Example: <code>(config-if) # end</code> | Returns to privileged EXEC mode. |
| Step 13 | show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]] Example: <code># show policy-map</code> | (Optional) Verifies your entries. |
| Step 14 | copy running-config startup-config Example: <code># copy-running-config startup-config</code> | (Optional) Saves your entries in the configuration file. |

What to do next

If applicable to your QoS configuration, configure classification, policing, and marking of traffic on SVIs by using policy maps.

Classifying, Policing, and Marking Traffic on SVIs by Using Policy Maps**Before you begin**

You should have already decided upon the classification, policing, and marking of your network traffic by using policy maps prior to beginning this procedure.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | class-map { <i>class-map name</i> match-any } Example: <pre>(config)# class-map class_vlan100</pre> | Enters class map configuration mode. <ul style="list-style-type: none"> • Creates a class map to be used for matching packets to the class whose name you specify. • If you specify match-any, one of the match criteria must be met for traffic entering the traffic class to be classified as part of the traffic class. This is the default. |
| Step 3 | match vlan <i>vlan number</i> Example: <pre>(config-cmap)# match vlan 100 (config-cmap)# exit (config)#</pre> | Specifies the VLAN to match to the class map. |
| Step 4 | policy-map <i>policy-map-name</i> Example: <pre>(config)# policy-map policy_vlan100 (config-pmap)#</pre> | Creates a policy map by entering the policy map name, and enters policy-map configuration mode. By default, no policy maps are defined. |
| Step 5 | description <i>description</i> Example: | (Optional) Enters a description of the policy map. |

| | Command or Action | Purpose |
|---------------|---|--|
| | <pre>(config-pmap) # description vlan 100</pre> | |
| Step 6 | <p>class {<i>class-map-name</i> class-default}</p> <p>Example:</p> <pre>(config-pmap) # class class_vlan100 (config-pmap-c) #</pre> | <p>Defines a traffic classification, and enters the policy-map class configuration mode.</p> <p>By default, no policy map class-maps are defined.</p> <p>If a traffic class has already been defined by using the class-map global configuration command, specify its name for <i>class-map-name</i> in this command.</p> <p>A class-default traffic class is predefined and can be added to any policy. It is always placed at the end of a policy map. With an implied match any included in the class-default class, all packets that have not already matched the other traffic classes will match class-default.</p> |
| Step 7 | <p>set {cos dscp ip precedence qos-group wlan user-priority}</p> <p>Example:</p> <pre>(config-pmap-c) # set dscp af23 (config-pmap-c) #</pre> | <p>(Optional) Sets the QoS values. Possible QoS configuration values include:</p> <ul style="list-style-type: none"> • cos—Sets the IEEE 802.1Q/ISL class of service/user priority. • dscp—Sets DSCP in IP(v4) and IPv6 packets. • ip—Sets IP specific values. • precedence—Sets precedence in IP(v4) and IPv6 packet. • qos-group—Sets QoS group. <p>In this example, the set dscp command classifies the IP traffic by matching the packets with a DSCP value of AF23 (010010).</p> |
| Step 8 | <p>police {<i>target_bit_rate</i> cir rate}</p> <p>Example:</p> <pre>(config-pmap-c) # police 200000 conform-action transmit exceed-action drop (config-pmap-c) #</pre> | <p>(Optional) Configures the policer:</p> <ul style="list-style-type: none"> • <i>target_bit_rate</i>—Specifies the bit rate per second. Enter a value between 8000 and 10000000000. • cir—Committed Information Rate. • rate—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies. |

| | Command or Action | Purpose |
|----------------|--|--|
| | | In this example, the police command adds a policer to the class where any traffic beyond the 200000 set target bit rate is dropped. |
| Step 9 | exit Example: <code>(config-pmap-c) # exit</code> | Returns to policy map configuration mode. |
| Step 10 | exit Example: <code>(config-pmap) # exit</code> | Returns to global configuration mode. |
| Step 11 | interface <i>interface-id</i> Example: <code>(config) # interface gigabitethernet 1/0/3</code> | Specifies the port to attach to the policy map, and enters interface configuration mode. Valid interfaces include physical ports. |
| Step 12 | service-policy input <i>policy-map-name</i> Example: <code>(config-if) # service-policy input policy_vlan100</code> | Specifies the policy-map name, and applies it to an ingress port. Only one policy map per ingress port is supported. |
| Step 13 | end Example: <code>(config-if) # end</code> | Returns to privileged EXEC mode. |
| Step 14 | show policy-map [<i>policy-map-name</i> [class <i>class-map-name</i>]] Example: <code># show policy-map</code> | (Optional) Verifies your entries. |
| Step 15 | copy running-config startup-config Example: <code># copy-running-config startup-config</code> | (Optional) Saves your entries in the configuration file. |

Configuring Table Maps

Table maps are a form of marking, and also enable the mapping and conversion of one field to another using a table. For example, a table map can be used to map and convert a Layer 2 CoS setting to a precedence value in Layer 3.



Note

- A table map can be referenced in multiple policies or multiple times in the same policy.
- A table map configured for a custom output policy under the default class-map, takes affect for all DSCP traffic regardless of which class map the traffic is classified for. The workaround is to remove the table map and configure the **set dscp** command under the default class to change the DSCP marking for classified traffic. If there is any non-queuing action (policer or marking) on a user-defined class, then the packet retains its value or remarks in the user-defined class itself.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 2 | table-map name {default {default value copy ignore} exit map {from from value to to value } no} Example: Device(config)# table-map table01 Device(config-tablemap)# | Creates a table map and enters the table map configuration mode. In table map configuration mode, you can perform the following tasks: <ul style="list-style-type: none"> • default: Configures the table map default value, or sets the default behavior for a value not found in the table map to copy or ignore. • exit: Exits from the table map configuration mode. • map: Maps a <i>from</i> to a <i>to</i> value in the table map. • no: Negates or sets the default values of the command. |
| Step 3 | map from value to value Example: Device(config-tablemap)# map from 0 to 2 Device(config-tablemap)# map from 1 to | In this step, packets with DSCP values 0 are marked to the CoS value 2, DSCP value 1 to the CoS value 4, DSCP value 24 to the CoS value 3, DSCP value 40 to the CoS value 6 and all others to the CoS value 0. |

| | Command or Action | Purpose |
|---------------|---|--|
| | <pre> 4 Device(config-tablemap) # map from 24 to 3 Device(config-tablemap) # map from 40 to 6 Device(config-tablemap) # default 0 Device(config-tablemap) # </pre> | <p>Note The mapping from CoS values to DSCP values in this example is configured by using the set policy map class configuration command as described in a later step in this procedure.</p> |
| Step 4 | <p>exit</p> <p>Example:</p> <pre> Device(config-tablemap) # exit Device(config) # </pre> | Returns to global configuration mode. |
| Step 5 | <p>exit</p> <p>Example:</p> <pre> Device(config) exit Device# </pre> | Returns to privileged EXEC mode. |
| Step 6 | <p>show table-map</p> <p>Example:</p> <pre> Device# show table-map Table Map table01 from 0 to 2 from 1 to 4 from 24 to 3 from 40 to 6 default 0 </pre> | Displays the table map configuration. |
| Step 7 | <p>configure terminal</p> <p>Example:</p> <pre> Device# configure terminal Device(config) # </pre> | Enters global configuration mode. |
| Step 8 | <p>policy-map</p> <p>Example:</p> <pre> Device(config) # policy-map table-policy Device(config-pmap) # </pre> | Configures the policy map for the table map. |
| Step 9 | <p>class class-default</p> <p>Example:</p> <pre> Device(config-pmap) # class </pre> | Matches the class to the system default. |

| | Command or Action | Purpose |
|----------------|--|--|
| | <code>class-default</code> Device(config-pmap-c) # | |
| Step 10 | set cos dscp table <i>table map name</i> Example: Device(config-pmap-c) # set cos dscp table table01 Device(config-pmap-c) # | If this policy is applied on input port, that port will have trust DSCP enabled on that port and marking will take place depending upon the specified table map. |
| Step 11 | end Example: Device(config-pmap-c) # end Device# | Returns to privileged EXEC mode. |

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or policies to an interface using the **service-policy** command.

Configuring QoS Features and Functionality

Configuring Bandwidth

This procedure explains how to configure bandwidth on your .

Before you begin

You should have created a class map for bandwidth before beginning this procedure.

Procedure

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | configure terminal Example: # configure terminal | Enters the global configuration mode. |
| Step 2 | policy-map <i>policy name</i> Example: (config) # policy-map policy_bandwidth01 | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

| | Command or Action | Purpose |
|---------------|--|--|
| | (config-pmap) # | |
| Step 3 | <p>class <i>class name</i></p> <p>Example:</p> <pre>(config-pmap) # class class_bandwidth01 (config-pmap-c) #</pre> | <p>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</p> <ul style="list-style-type: none"> • <i>word</i>—Class map name. • class-default—System default class matching any otherwise unclassified packets. |
| Step 4 | <p>bandwidth {<i>Kb/s</i> percent <i>percentage</i> remaining { <i>ratio ratio</i> } }</p> <p>Example:</p> <pre>(config-pmap-c) # bandwidth 200000 (config-pmap-c) #</pre> | <p>Configures the bandwidth for the policy map. The parameters include:</p> <ul style="list-style-type: none"> • <i>Kb/s</i>—Configures a specific value in kilobits per second (from 20000 to 10000000). • percent—Allocates minimum bandwidth to a particular class based on a percentage. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues. • remaining— Allocates minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the priority command is used for certain queues in the policy. You can also assign ratios rather than percentages to each queue; the queues will be assigned certain weights which are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100. <p>Note You cannot mix bandwidth types on a policy map. For example, you cannot configure bandwidth in a single policy map using both a bandwidth percent and in kilobits per second.</p> |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 5 | end Example: <pre>(config-pmap-c) # end #</pre> | Saves configuration changes. |
| Step 6 | show policy-map Example: <pre># show policy-map</pre> | (Optional) Displays policy configuration information for all classes configured for all service policies. |

What to do next

Configure any additional policy maps for QoS for your network. After creating the policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Configuring Police

This procedure explains how to configure policing on your .

Before you begin

You should have created a class map for policing before beginning this procedure.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | policy-map <i>policy name</i> Example: <pre>(config) # policy-map policy_police01 (config-pmap) #</pre> | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| Step 3 | class <i>class name</i> Example: <pre>(config-pmap) # class class_police01 (config-pmap-c) #</pre> | Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following: <ul style="list-style-type: none"> • <i>word</i>—Class map name. |

| | Command or Action | Purpose |
|---------------|---|--|
| | | <ul style="list-style-type: none"> • class-default—System default class matching any otherwise unclassified packets. |
| Step 4 | <p>police {<i>target_bit_rate</i> [<i>burst bytes</i> bc conform-action pir] cir {<i>target_bit_rate</i> percent <i>percentage</i>} rate {<i>target_bit_rate</i> percent <i>percentage</i>} conform-action transmit exceed-action {drop [<i>violate action</i>] set-cos-transmit set-dscp-transmit set-prec-transmit transmit [<i>violate action</i>] } }</p> <p>Example:</p> <pre>(config-pmap-c)# police 8000 conform-action transmit exceed-action drop (config-pmap-c)#</pre> | <p>The following police subcommand options are available:</p> <ul style="list-style-type: none"> • target_bit_rate—Bits per second (from 8000 to 10000000000). <ul style="list-style-type: none"> • burst bytes—Enter a value from 1000 to 512000000. • bc—Conform burst. • conform-action—Action taken when rate is less than conform burst. • pir—Peak Information Rate. • cir—Committed Information Rate. <ul style="list-style-type: none"> • target_bit_rate—Target bit rate (8000 to 100000000000). • percent—Percentage of interface bandwidth for CIR. • rate—Specifies the police rate, PCR for hierarchical policies, or SCR for single-level ATM 4.0 policer policies. <ul style="list-style-type: none"> • target_bit_rate—Target Bit Rate (8000 to 100000000000). • percent—Percentage of interface bandwidth for rate. <p>The following police conform-action transmit exceed-action subcommand options are available:</p> <ul style="list-style-type: none"> • drop—Drops the packet. • set-cos-transmit—Sets the CoS value and sends it. • set-dscp-transmit—Sets the DSCP value and sends it. • set-prec-transmit—Rewrites the packet precedence and sends it. • transmit—Transmits the packet. |

| | Command or Action | Purpose |
|---------------|---|--|
| | | <p>Note Policer-based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the .</p> |
| Step 5 | <p>end</p> <p>Example:</p> <pre>(config-pmap-c) # end #</pre> | Saves configuration changes. |
| Step 6 | <p>show policy-map</p> <p>Example:</p> <pre># show policy-map</pre> | <p>(Optional) Displays policy configuration information for all classes configured for all service policies.</p> <p>Note The show policy-map command output does not display counters for conformed bytes and exceeded bytes</p> |

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Configuring Priority

This procedure explains how to configure priority on your device.

The device supports giving priority to specified queues. There are two priority levels available (1 and 2).



Note Queues supporting voice and video should be assigned a priority level of 1.

Before you begin

You should have created a class map for priority before beginning this procedure.

Procedure

| | Command or Action | Purpose |
|---------------|---|---------------------------------------|
| Step 1 | <p>configure terminal</p> <p>Example:</p> <pre># configure terminal</pre> | Enters the global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 2 | <p>policy-map <i>policy name</i></p> <p>Example:</p> <pre>(config)# policy-map policy_priority01 (config-pmap)#</pre> | <p>Enters policy map configuration mode.</p> <p>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.</p> |
| Step 3 | <p>class <i>class name</i></p> <p>Example:</p> <pre>(config-pmap)# class class_priority01 (config-pmap-c)#</pre> | <p>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</p> <ul style="list-style-type: none"> • <i>word</i>—Class map name. • class-default—System default class matching any otherwise unclassified packets. |
| Step 4 | <p>priority level<i>level_value</i></p> <p>Example:</p> <pre>(config-pmap-c)# priority level 1 (config-pmap-c)#</pre> | <p>(Optional) The priority command assigns a strict scheduling priority for the class.</p> <p>The command options include:</p> <ul style="list-style-type: none"> • level <i>level_value</i>—Specifies the multilevel (1-2) priority queue. <p>Note Priority level 1 is more important than priority level 2. Priority level 1 reserves bandwidth that is processed first for QoS, so its latency is very low. Both priority level 1 and 2 reserve bandwidth.</p> |
| Step 5 | <p>end</p> <p>Example:</p> <pre>(config-pmap-c)# end #</pre> | <p>Saves configuration changes.</p> |
| Step 6 | <p>show policy-map</p> <p>Example:</p> <pre># show policy-map</pre> | <p>(Optional) Displays policy configuration information for all classes configured for all service policies.</p> |

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Configuring Queues and Shaping

Configuring Egress Queue Characteristics

Depending on the complexity of your network and your QoS solution, you may need to perform all of the procedures in this section. You need to make decisions about these characteristics:

- Which packets are mapped by DSCP, CoS, or QoS group value to each queue and threshold ID?
- What drop percentage thresholds apply to the queues, and how much reserved and maximum memory is needed for the traffic type?
- How much of the fixed buffer space is allocated to the queues?
- Does the bandwidth of the port need to be rate limited?
- How often should the egress queues be serviced and which technique (shaped, shared, or both) should be used?



Note You can only configure the egress queues on the device.

Configuring Queue Buffers

The `queue-limit` command allows you to allocate buffers to queues. If there is no allocation made to buffers, then they are divided equally for all queues. You can use the `queue-buffer` ratio to divide it in a particular ratio. Since by default DTS (Dynamic Threshold and Scaling) is active on all queues, these are soft buffers.



Note Queue-buffer ratio cannot be configured with a queue-limit.

Before you begin

The following are prerequisites for this procedure:

- You should have created a class map for the queue buffer before beginning this procedure.
- You must have configured either bandwidth, shape, or priority on the policy map prior to configuring the queue buffers.

Procedure

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | policy-map <i>policy name</i> Example: <pre>(config)# policy-map policy_queuebuffer01 (config-pmap)#</pre> | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| Step 3 | class <i>class name</i> Example: <pre>(config-pmap)# class class_queuebuffer01 (config-pmap-c)#</pre> | Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following: <ul style="list-style-type: none"> • <i>word</i>—Class map name. • class-default—System default class matching any otherwise unclassified packets. |
| Step 4 | bandwidth {<i>Kb/s</i> <i>percent percentage</i> <i>remaining { ratio ratio value }</i>} Example: <pre>(config-pmap-c)# bandwidth percent 80 (config-pmap-c)#</pre> | Configures the bandwidth for the policy map. The command parameters include: <ul style="list-style-type: none"> • <i>Kb/s</i>—Use this command to configure a specific value. The range is 20000 to 10000000. • percent—Allocates a minimum bandwidth to a particular class using a percentage. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues. • remaining—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the priority command is used for certain queues in the policy. You can also assign |

| | Command or Action | Purpose |
|---------------|--|--|
| | | <p>ratios rather than a percentage to each queue; the queues will be assigned certain weights that are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100.</p> <p>Note You cannot mix bandwidth types on a policy map.</p> |
| Step 5 | <p>queue-buffers {ratio <i>ratio value</i>}</p> <p>Example:</p> <pre>(config-pmap-c) # queue-buffers ratio 10 (config-pmap-c) #</pre> | <p>Configures the relative buffer size for the queue.</p> <p>Note The sum of all configured buffers in a policy must be less than or equal to 100 percent. Unallocated buffers are evenly distributed to all the remaining queues. Ensure sufficient buffers are allocated to all queues including the priority queues.</p> <p>Note Protocol Data Units(PDUs) for network control protocols such as spanning-tree and LACP utilize the priority queue or queue 0 (when a priority queue is not configured). Ensure sufficient buffers are allocated to these queues for the protocols to function.</p> |
| Step 6 | <p>end</p> <p>Example:</p> <pre>(config-pmap-c) # end #</pre> | Saves configuration changes. |
| Step 7 | <p>show policy-map</p> <p>Example:</p> <pre># show policy-map</pre> | (Optional) Displays policy configuration information for all classes configured for all service policies. |

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or policies to an interface using the **service-policy** command.

Configuring Queue Limits

You use queue limits to configure Weighted Tail Drop (WTD). WTD ensures the configuration of more than one threshold per queue. Each class of service is dropped at a different threshold value to provide for QoS differentiation. With the , each queue has 3 explicit programmable threshold classes—0, 1, 2. Therefore, the enqueue/drop decision of each packet per queue is determined by the packet's threshold class assignment, which is determined by the DSCP, CoS, or QoS group field of the frame header.

WTD also uses a soft limit, and therefore you are allowed to configure the queue limit to up to 400 percent (maximum four times the reserved buffer from common pool). This soft limit prevents overrunning the common pool without impacting other features.



Note You can only configure queue limits on the egress queues on wired ports.

Before you begin

The following are prerequisites for this procedure:

- You should have created a class map for the queue limits before beginning this procedure.
- You must have configured either bandwidth, shape, or priority on the policy map prior to configuring the queue limits.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | policy-map <i>policy name</i> Example: <pre>(config)# policy-map policy_queuelimit01 (config-pmap)#</pre> | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| Step 3 | class <i>class name</i> Example: <pre>(config-pmap)# class class_queuelimit01 (config-pmap-c)#</pre> | Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following: <ul style="list-style-type: none"> • <i>word</i>—Class map name. • class-default—System default class matching any otherwise unclassified packets. |

| | Command or Action | Purpose |
|--------|--|--|
| Step 4 | <p>bandwidth {<i>Kb/s</i> percent <i>percentage</i> remaining { <i>ratio</i> <i>ratio value</i> } }</p> <p>Example:</p> <pre>(config-pmap-c) # bandwidth 500000 (config-pmap-c) #</pre> | <p>Configures the bandwidth for the policy map. The parameters include:</p> <ul style="list-style-type: none"> • Kb/s—Use this command to configure a specific value. The range is 20000 to 10000000. • percent—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize the entire port bandwidth. The total sum cannot exceed 100 percent, and in case it is less than 100 percent, the rest of the bandwidth is equally divided along all bandwidth queues. • remaining—Allocates a minimum bandwidth to a particular class. The queue can oversubscribe bandwidth in case other queues do not utilize entire port bandwidth. The total sum cannot exceed 100 percent. It is preferred to use this command when the priority command is used for certain queues in the policy. You can also assign ratios rather than a percentage to each queue; the queues will be assigned certain weights that are inline with these ratios. Ratios can range from 0 to 100. Total bandwidth ratio allocation for the policy in this case can exceed 100. <p>Note You cannot mix bandwidth types on a policy map.</p> |
| Step 5 | <p>queue-limit {<i>packets</i> packets cos {<i>cos value</i> percent <i>percentage</i> } values {<i>cos value</i> percent <i>percentage</i> } } dscp {<i>dscp value</i> maximum <i>threshold value</i> percent <i>percentage</i> } match <i>packet</i> {<i>maximum threshold value</i> percent <i>percentage</i> } default {<i>maximum threshold value</i> percent <i>percentage</i> } ef {<i>maximum threshold value</i> percent <i>percentage</i> } dscp <i>values</i> <i>dscp value</i> } percent <i>percentage</i> } }</p> <p>Example:</p> <pre>(config-pmap-c) # queue-limit dscp 3</pre> | <p>Sets the queue limit threshold percentage values.</p> <p>With every queue, there are three thresholds (0,1,2), and there are default values for each of these thresholds. Use this command to change the default or any other queue limit threshold setting. For example, if DSCP 3, 4, and 5 packets are being sent into a specific queue in a configuration, then you can use this command to set the threshold percentages for these three DSCP values. For additional information about queue limit threshold values, see Weighted Tail Drop, on page 20.</p> |

| | Command or Action | Purpose |
|---------------|---|---|
| | <pre>percent 20 (config-pmap-c) # queue-limit dscp 4 percent 30 (config-pmap-c) # queue-limit dscp 5 percent 40</pre> | Note The does not support absolute queue-limit percentages. The only supports DSCP or CoS queue-limit percentages. |
| Step 6 | end Example: <pre>(config-pmap-c) # end #</pre> | Saves configuration changes. |
| Step 7 | show policy-map Example: <pre># show policy-map</pre> | (Optional) Displays policy configuration information for all classes configured for all service policies. |

What to do next

Proceed to configure any additional policy maps for QoS for your network. After creating your policy maps, proceed to attach the traffic policy or policies to an interface using the **service-policy** command.

Configuring Shaping

You use the **shape** command to configure shaping (maximum bandwidth) for a particular class. The queue's bandwidth is restricted to this value even though the port has additional bandwidth left. You can configure shaping as an average percent, as well as a shape average value in bits per second.

Before you begin

You should have created a class map for shaping before beginning this procedure.

Procedure

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | configure terminal Example: <pre># configure terminal</pre> | Enters the global configuration mode. |
| Step 2 | policy-map <i>policy name</i> Example: <pre>(config)# policy-map policy_shaping01</pre> | Enters policy map configuration mode. Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

| | Command or Action | Purpose |
|---------------|---|--|
| | <code>(config-pmap) #</code> | |
| Step 3 | <p>class <i>class name</i></p> <p>Example:</p> <pre>(config-pmap) # class class_shaping01 (config-pmap-c) #</pre> | <p>Enters policy class map configuration mode. Specifies the name of the class whose policy you want to create or change. Command options for policy class map configuration mode include the following:</p> <ul style="list-style-type: none"> • <i>word</i>—Class map name. • class-default—System default class matching any otherwise unclassified packets. |
| Step 4 | <p>shape average {<i>target bit rate</i> percent percentage}</p> <p>Example:</p> <pre>(config-pmap-c) # shape average percent 50 (config-pmap-c) #</pre> | <p>Configures the average shape rate. You can configure the average shape rate by target bit rates (bits per second) or by percentage of interface bandwidth for the Committed Information Rate (CIR).</p> |
| Step 5 | <p>end</p> <p>Example:</p> <pre>(config-pmap-c) # end #</pre> | <p>Saves configuration changes.</p> |
| Step 6 | <p>show policy-map</p> <p>Example:</p> <pre># show policy-map</pre> | <p>(Optional) Displays policy configuration information for all classes configured for all service policies.</p> |

What to do next

Configure any additional policy maps for QoS for your network. After creating your policy maps, attach the traffic policy or polices to an interface using the **service-policy** command.

Monitoring QoS

The following commands can be used to monitor QoS on the .

Table 11: Monitoring QoS

| Command | Description |
|--|--|
| <code>show class-map [class_map_name]</code> | Displays a list of all class maps configured. |
| <code>show class-map type control subscriber {all name }</code> | Displays control class map and statistics. <ul style="list-style-type: none"> • all—Displays information for all class maps. • name—Displays configured class maps. |
| <code>show policy-map [policy_map_name]</code> | Displays a list of all policy maps configured. Command parameters include: <ul style="list-style-type: none"> • policy map name • interface • session |
| <code>show policy-map session [input output uid UUID]</code> | Displays the session QoS policy. Command parameters include: <ul style="list-style-type: none"> • input—Input policy • output—Output policy • uid—Policy based on SSS unique identification. |
| <code>show table-map</code> | Displays all the table maps and their configurations. |

Configuration Examples for QoS

Examples: Classification by Access Control Lists

This example shows how to classify packets for QoS by using access control lists (ACLs):

```
# configure terminal
```

```
(config)# access-list 101 permit ip host 12.4.1.1 host 15.2.1.1
(config)# class-map acl-101
(config-cmap)# description match on access-list 101
(config-cmap)# match access-group 101
(config-cmap)#
```

After creating a class map by using an ACL, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Class of Service Layer 2 Classification

This example shows how to classify packets for QoS using a class of service Layer 2 classification:

```
# configure terminal
(config)# class-map cos
(config-cmap)# match cos ?
    <0-7> Enter up to 4 class-of-service values separated by white-spaces
(config-cmap)# match cos 3 4 5
(config-cmap)#
```

After creating a class map by using a CoS Layer 2 classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Class of Service DSCP Classification

This example shows how to classify packets for QoS using a class of service DSCP classification:

```
# configure terminal
(config)# class-map dscp
(config-cmap)# match dscp af21 af22 af23
(config-cmap)#
```

After creating a class map by using a DSCP classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: VLAN ID Layer 2 Classification

This example shows how to classify for QoS using a VLAN ID Layer 2 classification:

```
# configure terminal
(config)# class-map vlan-120
(config-cmap)# match vlan ?
    <1-4095> VLAN id
(config-cmap)# match vlan 120
(config-cmap)#
```

After creating a class map by using a VLAN Layer 2 classification, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Classification by DSCP or Precedence Values

This example shows how to classify packets by using DSCP or precedence values:

```
# configure terminal
(config)# class-map prec2
(config-cmap)# description matching precedence 2 packets
(config-cmap)# match ip precedence 2
(config-cmap)# exit
(config)# class-map ef
(config-cmap)# description EF traffic
(config-cmap)# match ip dscp ef
(config-cmap)#
```

After creating a class map by using a DSCP or precedence values, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Hierarchical Classification

The following is an example of a hierarchical classification, where a class named parent is created, which matches another class named child. The class named child matches based on the IP precedence being set to 2.

```
# configure terminal
(config)# class-map child
(config-cmap)# match ip precedence 2
(config-cmap)# exit
(config)# class-map parent
(config-cmap)# match class child
(config-cmap)#
```

After creating the parent class map, you then create a policy map for the class, and apply the policy map to an interface for QoS.

Examples: Hierarchical Policy Configuration

The following is an example of a configuration using hierarchical policies:

```
# configure terminal
(config)# class-map c1
(config-cmap)# match dscp 30
(config-cmap)# exit

(config)# class-map c2
(config-cmap)# match precedence 4
(config-cmap)# exit

(config)# class-map c3
(config-cmap)# exit

(config)# policy-map child
(config-pmap)# class c1
(config-pmap-c)# priority level 1
(config-pmap-c)# police rate percent 20 conform-action transmit exceed action drop
```

```
(config-pmap-c-police)# exit
(config-pmap-c)# exit

(config-pmap)# class c2
(config-pmap-c)# bandwidth 20000
(config-pmap-c)# exit
(config-pmap)# class class-default
(config-pmap-c)# bandwidth 20000
(config-pmap-c)# exit
(config-pmap)# exit

(config)# policy-map parent
(config-pmap)# class class-default
(config-pmap-c)# shape average 1000000
(config-pmap-c)# service-policy child
(config-pmap-c)# end
```

The following example shows a hierarchical policy using table maps:

```
(config)# table-map dscp2dscp
  (config-tablemap)# default copy
(config)# table-map dscp2up
(config-tablemap)# map from 46 to 6
(config-tablemap)# map from 34 to 5
(config-tablemap)# default copy
(config)# policy-map ssid_child_policy
(config-pmap)# class voice
(config-pmap-c)# priority level 1
(config-pmap-c)# police 15000000
(config-pmap)# class video
(config-pmap-c)# priority level 2
(config-pmap-c)# police 10000000
(config)# policy-map ssid_policy
(config-pmap)# class class-default
(config-pmap-c)# shape average 30000000
(config-pmap-c)# queue-buffer ratio 0
(config-pmap-c)# set dscp dscp table dscp2dscp
(config-pmap-c)# service-policy ssid_child_policy
```

Examples: Classification for Voice and Video

This example describes how to classify packet streams for voice and video using device specific information.

In this example, voice and video are coming in from end-point A into GigabitEthernet1/0/1 on the device and have precedence values of 5 and 6, respectively. Additionally, voice and video are also coming from end-point B into GigabitEthernet1/0/2 on the device with DSCP values of EF and AF11, respectively.

Assume that all the packets from the both the interfaces are sent on the uplink interface, and there is a requirement to police voice to 100 Mbps and video to 150 Mbps.

To classify per the above requirements, a class to match voice packets coming in on GigabitEthernet1/0/1 is created, named voice-interface-1, which matches precedence 5. Similarly another class for voice is created, named voice-interface-2, which will match voice packets in GigabitEthernet1/0/2. These classes are associated to two separate policies named input-interface-1, which is attached to GigabitEthernet1/0/1, and input-interface-2, which is attached to GigabitEthernet1/0/2. The action for this class is to mark the qos-group to 10. To match packets with QoS-group 10 on the output interface, a class named voice is created which matches on QoS-group 10. This is then associated to another policy named output-interface, which is associated to the uplink interface. Video is handled in the same way, but matches on QoS-group 20.

The following example shows how classify using the above device specific information:

```
(config)#
(config)# class-map voice-interface-1
(config-cmap)# match ip precedence 5
(config-cmap)# exit

(config)# class-map video-interface-1
(config-cmap)# match ip precedence 6
(config-cmap)# exit

(config)# class-map voice-interface-2
(config-cmap)# match ip dscp ef
(config-cmap)# exit

(config)# class-map video-interface-2
(config-cmap)# match ip dscp af11
(config-cmap)# exit

(config)# policy-map input-interface-1
(config-pmap)# class voice-interface-1
(config-pmap-c)# set qos-group 10
(config-pmap-c)# exit

(config-pmap)# class video-interface-1
(config-pmap-c)# set qos-group 20

(config-pmap-c)# policy-map input-interface-2
(config-pmap)# class voice-interface-2
(config-pmap-c)# set qos-group 10
(config-pmap-c)# class video-interface-2
(config-pmap-c)# set qos-group 20
(config-pmap-c)# exit
(config-pmap-c)# exit

(config)# class-map voice
(config-cmap)# match qos-group 10
(config-cmap)# exit

(config)# class-map video
(config-cmap)# match qos-group 20

(config)# policy-map output-interface
(config-pmap)# class voice
(config-pmap-c)# police 256000 conform-action transmit exceed-action drop
(config-pmap-c-police)# exit
(config-pmap-c)# exit

(config-pmap)# class video
(config-pmap-c)# police 1024000 conform-action transmit exceed-action drop
(config-pmap-c-police)# exit
(config-pmap-c)# exit
```

Examples: Average Rate Shaping Configuration

The following example shows how to configure average rate shaping:

```
# configure terminal
(config)# class-map prec1
```

```

(config-cmap)# description matching precedence 1 packets
(config-cmap)# match ip precedence 1
(config-cmap)# end

# configure terminal
(config)# class-map prec2
(config-cmap)# description matching precedence 2 packets
(config-cmap)# match ip precedence 2
(config-cmap)# exit

(config)# policy-map shaper
(config-pmap)# class prec1
(config-pmap-c)# shape average 512000
(config-pmap-c)# exit

(config-pmap)# policy-map shaper
(config-pmap)# class prec2
(config-pmap-c)# shape average 512000
(config-pmap-c)# exit

(config-pmap)# class class-default
(config-pmap-c)# shape average 1024000

```

After configuring the class maps, policy map, and shape averages for your configuration, proceed to then apply the policy map to the interface for QoS.

Examples: Queue-limit Configuration

The following example shows how to configure a queue-limit policy based upon DSCP values and percentages:

```

# configure terminal
#(config)# policy-map port-queue
#(config-pmap)# class dscp-1-2-3
#(config-pmap-c)# bandwidth percent 20
#(config-pmap-c)# queue-limit dscp 1 percent 80
#(config-pmap-c)# queue-limit dscp 2 percent 90
#(config-pmap-c)# queue-limit dscp 3 percent 100
#(config-pmap-c)# exit

#(config-pmap)# class dscp-4-5-6
#(config-pmap-c)# bandwidth percent 20
#(config-pmap-c)# queue-limit dscp 4 percent 20
#(config-pmap-c)# queue-limit dscp 5 percent 30
#(config-pmap-c)# queue-limit dscp 6 percent 20
#(config-pmap-c)# exit

#(config-pmap)# class dscp-7-8-9
#(config-pmap-c)# bandwidth percent 20
#(config-pmap-c)# queue-limit dscp 7 percent 20
#(config-pmap-c)# queue-limit dscp 8 percent 30
#(config-pmap-c)# queue-limit dscp 9 percent 20
#(config-pmap-c)# exit

#(config-pmap)# class dscp-10-11-12
#(config-pmap-c)# bandwidth percent 20
#(config-pmap-c)# queue-limit dscp 10 percent 20
#(config-pmap-c)# queue-limit dscp 11 percent 30
#(config-pmap-c)# queue-limit dscp 12 percent 20
#(config-pmap-c)# exit

```

```
#(config-pmap)# class dscp-13-14-15
#(config-pmap-c)# bandwidth percent 10
#(config-pmap-c)# queue-limit dscp 13 percent 20
#(config-pmap-c)# queue-limit dscp 14 percent 30
#(config-pmap-c)# queue-limit dscp 15 percent 20
#(config-pmap-c)# end
#
```

After finishing with the above policy map queue-limit configuration, you can then proceed to apply the policy map to an interface for QoS.

Examples: Queue Buffers Configuration

The following example shows how configure a queue buffer policy and then apply it to an interface for QoS:

```
# configure terminal
(config)# policy-map policy1001
(config-pmap)# class class1001
(config-pmap-c)# bandwidth remaining ratio 10
(config-pmap-c)# queue-buffer ratio ?
<0-100> Queue-buffers ratio limit
(config-pmap-c)# queue-buffer ratio 20
(config-pmap-c)# end

# configure terminal
(config)# interface gigabitEthernet2/0/3
(config-if)# service-policy output policy1001
(config-if)# end
```

Examples: Policing Action Configuration

The following example displays the various policing actions that can be associated to the policer. These actions are accomplished using the conforming, exceeding, or violating packet configurations. You have the flexibility to drop, mark and transmit, or transmit packets that have exceeded or violated a traffic profile.

For example, a common deployment scenario is one where the enterprise customer polices traffic exiting the network towards the service provider and marks the conforming, exceeding and violating packets with different DSCP values. The service provider could then choose to drop the packets marked with the exceeded and violated DSCP values under cases of congestion, but may choose to transmit them when bandwidth is available.



Note The Layer 2 fields can be marked to include the CoS fields, and the Layer 3 fields can be marked to include the precedence and the DSCP fields.

One useful feature is the ability to associate multiple actions with an event. For example, you could set the precedence bit and the CoS for all conforming packets. A submode for an action configuration could then be provided by the policing feature.

This is an example of a policing action configuration:

```
# configure terminal
```

```
(config)# policy-map police
(config-pmap)# class class-default
(config-pmap-c)# police cir 1000000 pir 2000000
(config-pmap-c-police)# conform-action transmit
(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table exceed-markdown-table
(config-pmap-c-police)# violate-action set-dscp-transmit dscp table violate-markdown-table

(config-pmap-c-police)# end
```

In this example, the exceed-markdown-table and violate-mark-down-table are table maps.



Note Policer-based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the device.

Examples: Policer VLAN Configuration

The following example displays a VLAN policer configuration. At the end of this configuration, the VLAN policy map is applied to an interface for QoS.

```
# configure terminal
(config)# class-map vlan100
(config-cmap)# match vlan 100
(config-cmap)# exit
(config)# policy-map vlan100
(config-pmap)# policy-map class vlan100
(config-pmap-c)# police 100000 bc conform-action transmit exceed-action drop
(config-pmap-c-police)# end
# configure terminal
(config)# interface gigabitEthernet1/0/5
(config-if)# service-policy input vlan100
```

Examples: Policing Units

The policing unit is the basis on which the token bucket works. CIR and PIR are specified in bits per second. The burst parameters are specified in bytes. This is the default mode; it is the unit that is assumed when no units are specified. The CIR and PIR can also be configured in percent, in which case the burst parameters have to be configured in milliseconds.

The following is an example of a policer configuration in bits per second. In this configuration, a dual-rate three-color policer is configured where the units of measurement is bits. The burst and peak burst are all specified in bits.

```
Device(config)# policy-map bps-policer
Device(config-pmap)# class class-default
Device(config-pmap-c)# police rate 100000 peak-rate 1000000
conform-action transmit exceed-action set-dscp-transmit dscp table
DSCP_EXCE violate-action drop
```

Examples: Single-Rate Two-Color Policing Configuration

The following example shows how to configure a single-rate two-color policer:

```
(config)# class-map match-any prec1
(config-cmap)# match ip precedence 1
(config-cmap)# exit
(config)# policy-map policer
(config-pmap)# class prec1
(config-pmap-c)# police cir 256000 conform-action transmit exceed-action drop
(config-pmap-c-police)# exit
(config-pmap-c)#
```

Examples: Dual-Rate Three-Color Policing Configuration

The following example shows how to configure a dual-rate three-color policer:

```
# configure terminal
(config)# policy-map dual-rate-3color-policer
(config-pmap)# class class-default
(config-pmap-c)# police cir 64000 bc 2000 pir 128000 be 2000
(config-pmap-c-police)# conform-action transmit
(config-pmap-c-police)# exceed-action set-dscp-transmit dscp table exceed-markdown-table
(config-pmap-c-police)# violate-action set-dscp-transmit dscp table violate-markdown-table
(config-pmap-c-police)# exit
(config-pmap-c)#
```

In this example, the exceed-markdown-table and violate-mark-down-table are table maps.



Note Policer based markdown actions are only supported using table maps. Only one markdown table map is allowed for each marking field in the device.

Examples: Table Map Marking Configuration

The following steps and examples show how to use table map marking for your QoS configuration:

1. Define the table map.

Define the table-map using the **table-map** command and indicate the mapping of the values. This table does not know of the policies or classes within which it will be used. The default command in the table map indicates the value to be copied into the 'to' field when there is no matching 'from' field. In the example, a table map named table-map1 is created. The mapping defined is to convert the value from 0 to 1 and from 2 to 3, while setting the default value to 4.

```
(config)# table-map table-map1
(config-tablemap)# map from 0 to 1
(config-tablemap)# map from 2 to 3
(config-tablemap)# default 4
(config-tablemap)# exit
```

2. Define the policy map where the table map will be used.

In the example, the incoming CoS is mapped to the DSCP based on the mapping specified in the table `table-map1`. For this example, if the incoming packet has a DSCP of 0, the CoS in the packet is set 1. If no table map name is specified the command assumes a default behavior where the value is copied as is from the 'from' field (DSCP in this case) to the 'to' field (CoS in this case). Note however, that while the CoS is a 3-bit field, the DSCP is a 6-bit field, which implies that the CoS is copied to the first three bits in the DSCP.

```
(config)# policy map policy1
(config-pmap)# class class-default
(config-pmap-c)# set cos dscp table table-map1
(config-pmap-c)# exit
```

3. Associate the policy to an interface.

```
(config)# interface GigabitEthernet1/0/1
(config-if)# service-policy output policy1
(config-if)# exit
```

Example: Table Map Configuration to Retain CoS Markings

The following example shows how to use table maps to retain CoS markings on an interface for your QoS configuration.

The `cos-trust-policy` policy (configured in the example) is enabled in the ingress direction to retain the CoS marking coming into the interface. If the policy is not enabled, only the DSCP is trusted by default. If a pure Layer 2 packet arrives at the interface, then the CoS value will be rewritten to 0 when there is no such policy in the ingress port for CoS.

```
# configure terminal
(config)# table-map cos2cos
(config-tablemap)# default copy
(config-tablemap)# exit

(config)# policy map cos-trust-policy
(config-pmap)# class class-default
(config-pmap-c)# set cos cos table cos2cos
(config-pmap-c)# exit

(config)# interface GigabitEthernet1/0/2
(config-if)# service-policy input cos-trust-policy
(config-if)# exit
```

Where to Go Next

Review the auto-QoS documentation to see if you can use these automated capabilities for your QoS configuration.

Additional References for QoS

Related Documents

| Related Topic | Document Title |
|--|---|
| For complete syntax and usage information for the commands used in this chapter. | <i>Cisco IOS Quality of Service Solutions Command Reference</i> |

Error Message Decoder

| Description | Link |
|---|---|
| To help you research and resolve system error messages in this release, use the Error Message Decoder tool. | https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi |

Standards and RFCs

| Standard/RFC | Title |
|--------------|-------|
| — | |

MIBs

| MIB | MIBs Link |
|--|--|
| All the supported MIBs for this release. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| <p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p> | http://www.cisco.com/support |

Feature History for QoS

This table provides release and related information for features explained in this module.

These features are available on all releases subsequent to the one they were introduced in, unless noted otherwise.

| Release | Feature | Feature Information |
|-----------------------------|-------------------|--|
| Cisco IOS XE Everest 16.6.1 | QoS Functionality | <p>QoS provides preferential treatment to specific types of traffic at the expense of other traffic types. Without QoS, the device offers best-effort service for each packet, regardless of the packet contents or size.</p> <p>Note This release does not support converged access.</p> |

Use Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>.

