

Modular QoS Overview

Quality of Service (QoS) is the technique of prioritizing traffic flows and providing preferential forwarding for higher-priority packets. The fundamental reason for implementing QoS in your network is to provide better service for certain traffic flows. A traffic flow can be defined as a combination of source and destination addresses, source and destination socket numbers, and the session identifier. A traffic flow can more broadly be described as a packet moving from an incoming interface that is destined for transmission to an outgoing interface. The traffic flow must be identified, classified, and prioritized on all routers and passed along the data forwarding path throughout the network to achieve end-to-end QoS delivery. The terms *traffic flow* and *packet* are used interchangeably throughout this module.

To implement QoS on a network requires the configuration of QoS features that provide better and more predictable network service by supporting bandwidth allocation, improving loss characteristics, avoiding and managing network congestion, metering network traffic, or setting traffic flow priorities across the network.

This module contains overview information about modular QoS features within a service provider network.

- Information About Modular Quality of Service Overview, on page 1
- Where to Go Next, on page 5
- Additional References, on page 6

Information About Modular Quality of Service Overview

Before configuring modular QoS on your network, you must understand these concepts:

Benefits of Cisco IOS XR QoS Features

The Cisco IOS XR QoS features enable networks to control and predictably service a variety of networked applications and traffic types. Implementing Cisco IOS XR QoS in your network promotes these benefits:

- Control over resources. You have control over which resources (bandwidth, equipment, wide-area facilities, and so on) are being used. For example, you can limit bandwidth consumed over a backbone link by FTP transfers or give priority to an important database access.
- Tailored services. If you are an Internet Service Provider (ISP), the control and visibility provided by QoS enables you to offer carefully tailored grades of service differentiation to your customers.
- Coexistence of mission-critical applications. Cisco IOS XR QoS features ensure:
  - That bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available.

- That your WAN is used efficiently by mission-critical applications that are most important to your business.
- That bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available.
- That other applications using the link get their fair service without interfering with mission-critical traffic.

QoS Techniques

QoS on Cisco IOS XR software relies on these techniques to provide for end-to-end QoS delivery across a heterogeneous network:

- Packet classification and marking
- Congestion management
- Congestion avoidance

Before implementing the QoS features for these techniques, you should identify and evaluate the traffic characteristics of your network because not all techniques are appropriate for your network environment.

Packet Classification and Marking

Packet classification and marking techniques identify the traffic flow, and provide the capability to partition network traffic into multiple priority levels or classes of service. After classification is complete, any other QoS actions can be performed.

Identification of a traffic flow can be performed by using several methods within a single router, such as access control lists (ACLs), protocol match, IP precedence, IP differentiated service code point (DSCP), MPLS EXP bit, or Class of Service (CoS).

Marking of a traffic flow is performed by:

- Setting IP Precedence or DSCP bits in the IP Type of Service (ToS) byte.
- Setting (CoS, DEI) bits in the Layer 2 headers.
- Setting EXP bits within the imposed or the topmost Multiprotocol Label Switching (MPLS) label.
- Setting qos-group and discard-class bits.

Marking can be carried out:

- Unconditionally—As part of the class-action.
- Conditionally—As part of a policer-action.
- Combination of conditionally and unconditionally.

You can set a maximum of two fields per class-map. For example:

```
class c1
set cos 2
set dscp 21
```

You can place these two fields in any of the following combinations:

- Two sets per policer (conform/exceed/violate)
- Two sets without policing

For example:

```
Policy-map p1
class c1
     set dscp af11
     set cos 5
     police rate 10 mbps peak-rate 20 mbps
          conform-action set dscp af12
          conform-action set cos 6
          exceed-action set dscp af13
          exceed-action set cos 4
```

For detailed conceptual and configuration information about packet marking, see the “Configuring Modular Quality of Service Packet Classification on Cisco ASR 9000 Series Routers” module in this guide for unconditional marking, and the “Configuring Modular Quality of Service Congestion Management on Cisco ASR 9000 Series Routers” module in this guide for conditional marking.

Default Marking Behavior

When an ingress or egress interface adds VLAN tags or MPLS labels, it requires a default value for the CoS and EXP values that go into those tags and labels. The default value can be then overridden based on the policy map. The default value for CoS and EXP is based on a trusted field in the packet upon ingress to the system. The router implements an implicit trust of certain fields based on the packet type and ingress interface forwarding type (Layer 2 or Layer 3).

By default, the router does not modify the IP precedence or DSCP without a policy-map being configured. The default behavior is described below.

On an ingress or egress Layer 2 interface, such as xconnect or bridge-domain, the outermost CoS value is used for any field that gets added in the ingress interface. If there is a VLAN tag that gets added due to a Layer 2 rewrite, the incoming outermost CoS value is used for the new VLAN tag. If an MPLS label is added, the CoS value would be used for the EXP bits in the MPLS tag.

On an ingress or egress Layer 3 interface (routed or label weighted for IPv4 or IPv6 packets), the three DSCP and precedence bits are identified in the incoming packet. For MPLS packets, the outermost label’s EXP bit is identified, and this value is used for any new field that gets added at the ingress interface. If an MPLS label is added, then the identified precedence, DSCP, or MPLS EXP value is used for the EXP bits in the newly added MPLS tag.

Provider Backbone Bridge (PBB) Configuration

In a PBB configuration, when a packet goes from a customer network to a service provider network using PBB encapsulation, the class of service (CoS) and discard eligibility indicator (DEI) used in the backbone VLAN tag (B-tag) and service instance tag (I-tag) of the PBB header is by default the CoS and DEI in the topmost tag of the incoming packet.

When a packet goes from a service provider to a customer network, the PBB header is removed and the I-tag CoS and DEI is used by default on any tags that are imposed on the customer interface. The default marking occurs only on imposed tags, and not on existing or translated tags.

Congestion Management

Congestion management techniques control congestion after it has occurred. One way that network elements handle an overflow of arriving traffic is to use a queuing algorithm to sort the traffic, then determine some servicing method of prioritizing it onto an output link.

Cisco IOS XR software implements the low-latency Queuing (LLQ) feature, which brings strict priority queuing (PQ) to the Modified Deficit Round Robin (MDRR) scheduling mechanism. LLQ with strict PQ allows delay-sensitive data such as voice, to be dequeued and sent before packets in other queues are dequeued.

Cisco IOS XR software includes traffic policing capabilities available on a per-class basis as well as class-based shaping.

The traffic policing feature limits the input or output transmission rate of a class of traffic based on user-defined criteria, and can mark packets by setting values such as IP Precedence, QoS group, or DSCP value.

Traffic shaping allows control over the traffic that leaves an interface to match its flow to the speed of the remote target interface and ensure that the traffic conforms to the policies contracted for it. Thus, traffic adhering to a particular profile can be shaped to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Cisco IOS XR software supports a class-based traffic shaping method through a CLI mechanism in which parameters are applied per class.

For detailed conceptual and configuration information about congestion management, see the “Configuring Modular Quality of Service Congestion Management on Cisco ASR 9000 Series Routers” module.

Congestion Avoidance

Congestion avoidance techniques monitor network traffic flows in an effort to anticipate and avoid congestion at common network and internetwork bottlenecks before problems occur. These techniques are designed to provide preferential treatment for traffic (such as a video stream) that has been classified as real-time critical under congestion situations while concurrently maximizing network throughput and capacity utilization and minimizing packet loss and delay. Cisco IOS XR software supports the Random Early Detection (RED), Weighted RED (WRED), and tail drop QoS congestion avoidance features.

For detailed conceptual and configuration information about congestion avoidance techniques, see the “Configuring Modular Quality of Service Congestion Management on Cisco ASR 9000 Series Routers” module in this guide.

Differentiated Service Model for Cisco IOS XR Software

Cisco IOS XR software supports a differentiated service that is a multiple-service model that can satisfy different QoS requirements. However, unlike in the integrated service model, an application using differentiated service does not explicitly signal the router before sending data.

For differentiated service, the network tries to deliver a particular kind of service based on the QoS specified by each packet. This specification can occur in different ways, for example, using the IP Precedence bit settings in IP packets or source and destination addresses. The network uses the QoS specification to classify, mark, shape, and police traffic, and to perform intelligent queuing.

The differentiated service model is used for several mission-critical applications and for providing end-to-end QoS. Typically, this service model is appropriate for aggregate flows because it performs a relatively coarse level of traffic classification.

Access Node Control Protocol

Access Node Control Protocol (ANCP) creates a control plane between a service-oriented aggregation device and an access node (AN) (for example, a DSLAM) in order to perform QoS-related, service-related, and subscriber-related operations. An ANCP Network Access Server (NAS) accepts and maintains ANCP adjacencies (sessions with an ANCP neighbor), and sending and receiving ANCP messages.

ANCP allows static mapping between AN ports and VLAN subinterfaces so that DSL rate updates for a specific subscriber received by the ANCP server are applied to the QoS configuration corresponding to that subscriber. DSL train rates received via ANCP are used to alter shaping rates on subscriber-facing interfaces and subinterfaces on the router.

Additional Cisco IOS XR QoS Supported Features

These sections describe the additional features that play an important role in the implementation of QoS on Cisco IOS XR software.

Modular QoS Command-Line Interface

In Cisco IOS XR software, QoS features are enabled through the Modular QoS command-line interface (MQC) feature. The *MQC* is a command-line interface (CLI) structure that allows you to create 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, whereas 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.

For detailed conceptual and configuration information about the MQC feature, see the “Configuring Modular Quality of Service Packet Classification on Cisco ASR 9000 Series Routers” module in this guide.

Fabric QoS

There is no separate configuration for fabric QoS. The fabric priority is derived from the priority action in the ingress service policy.

Where to Go Next

To configure the packet classification features that involve identification and marking of traffic flows, see the Configuring Modular Quality of Service Packet Classification module in this guide.

To configure the queuing, scheduling, policing, and shaping features, see the Configuring Modular Quality of Service Congestion Management module in this guide.

To configure the WRED and RED features, see the Configuring Modular QoS Congestion Avoidance module in this guide.

To configure Access Node Control Protocol (ANCP) features, see the “Configuring Access Node Control Protocol on Cisco ASR 9000 Series Routers” module in this guide.

Additional References

The following sections provide references related to implementing QoS.

Related Documents

Related Topic	Document Title
Initial system bootup and configuration	*Cisco ASR 9000 Series Aggregation Services Router Getting Guide*
QoS commands	*Cisco ASR 9000 Series Aggregation Services Router Modular of Service Command Reference*
User groups and task IDs	"Configuring AAA Services on Cisco ASR 9000 Series Route of Cisco Cisco ASR 9000 Series Aggregation Services Route Security Configuration Guide

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
CISCO-CLASS-BASED-QOS-MIB	To locate and download MIBs using Cisco IOS XR software, Cisco MIB Locator found at the following URL and choose a under the Cisco Access Products menu: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/cisco/web/support/index.html