Quality of Service

Cisco network devices have QoS disabled as a default setting. There are only hardware queues on network interfaces that forward ingress and egress traffic on a first-come first-served basis. When network congestion occurs and the queue is full, packets are dropped and performance is degraded. QoS policies are only active when there is network congestion detected. The following are primary reasons for deploying QoS.

- Guarantee SLAs for defined traffic classes
- Avoid and manage network congestion
- Prioritize traffic classes and assign bandwidth
- Minimize packet loss and network latency

Classification

The purpose of classification per-hop behavior is to examine and select (differentiate) traffic based on some matching criteria. It is a method for identifying and grouping traffic to apply some QoS action. Some common examples of classification include access control lists (ACL), marking, and NBAR (application header).

For example, you could create an ACL that selects all traffic within a subnet range or have a particular DSCP marking. In fact, classification is available on frames, packets, segments and up to application header. Once traffic is identified, then you can apply some action such as remark, drop, queue or forward with no action.

Marking

Traffic marking is a technique used to prioritize network traffic. The primary types include Class of Service (CoS), DSCP and IP precedence.

Class of Service (CoS)

Class of Service is found only with Layer 2 frames that are assigned to a trunk interface. There is a VLAN membership tag added that has an 802.1p field in the header for CoS marking. You can select from eight different levels or service or prioritization where the default on unmarked frames is zero (0). It is recommended to assign voice traffic CoS 5 marking since it is delay sensitive. There is a trunk created from Cisco IP phone to switch when the voice VLAN is configured on switch. That is for the purpose of tagging voice traffic with a CoS value. The trunk tags voice traffic from the phone and data from the host.

The upstream network switch would either trust the CoS value or rewrite the CoS marking. Cisco switches are configured with a trust state that determine frame handling. Cisco IP phones mark all voice traffic to the switch with default CoS 5.

Differentiated Services Code Point (DSCP)

There is a QoS marking as well within an IP header packet DS field (previously ToS). The purpose is to mark each packet with a specific DSCP value. Only routers and Layer 3 switches can examine an IP header. There are 6-bits allocated that enable 64 different DSCP values. For example, you could prioritize video traffic higher than data and signaling traffic. That would require to assign a higher marking than what is currently assigned. The default DSCP value on unmarked packets is zero (0) so any higher value would prioritize it. IP precedence is an older implementation standard that has been replaced with DSCP.

Policing

The primary purpose of policing is to provide multiple options for packet handling based on allowed data rate and burst rate. The conditions include conforming, exceeding and violating. The actions include forward, remark or drop. Traffic policing allows you to control maximum rate of traffic transmitted or received on an interface. Traffic policing is often configured on interfaces at the edge of a network to limit ingress and/or egress traffic. The standard configuration is to transmit packets less than or equal to CIR and drop or remark packets that exceed CIR.

Policing does not queue packets and that is preferred for delay sensitive traffic to minimizes latency. Policing can be applied to ingress and/or egress interfaces. The following describe each condition and the policing action that is available.

- Conforming = packet is forwarded or remarked
- Exceeding = packet has exceeded limits and is dropped or remarked
- Violating = data rate faster than CIR and allowed, dropped or remarked

Note that remark can refer to either marking up or down of a packet. The network administrator could decide for instance to remark packet to a higher (preferred) DSCP marking. Policing does allow access control lists as a classification method as well.

Shaping

The primary purpose of traffic shaping is to limit the maximum data rate on an egress network interface. The queuing of packets is used to prevent packet forwarding from exceeding CIR (data rate) and bandwidth. There is support for applying traffic shaping to single user or application. That minimizes the effect of any internet traffic and bandwidth hogging for instance. The queuing of packets from traffic shaping can affect delay sensitive traffic such as voice and video with higher latency. There is no guaranteed minimum bandwidth configurable with traffic shaping or policing. Queuing techniques are available for that purpose.

The following is a list of the correct features and operation of shaping.

- Minimize the effect of any single user traffic on network performance.
- Prevent ISP from dropping packets that exceed maximum data rate.
- Shape traffic to lower rate than what is available with customer physical interface. There is no support for traffic shaping on ingress interfaces (egress only).

Shaping vs Policing

The following statements describe the supported features for shaping and policing. In addition the differences are noted as well.

- Policing does not queue packets
- Shaping does support packet queueing
- Policing is applied to ingress and egress interfaces
- Policing drops or remarks traffic that exceed CIR

There is no support for traffic shaping on ingress interfaces (egress only). In addition policing does allow access lists as a classification method.

Queuing

After classification, policing and shaping, there is traffic queuing for congestion management. Cisco network interfaces have software and hardware queues. The software queues are created and used to prioritize different traffic classes defined from classification policies.

From there, traffic is forwarded to interface hardware queues where it is First In First Out (FIFO) scheduling. Software queues are only active when there is network congestion to prevent packet drops.

There are a variety of techniques for queuing that are summarized with Table 1. Each method assigns traffic to different queues based on some classification. In addition, queues can be assigned different weights to assign bandwidth. The bandwidth assigned to the priority queue (PQ) is allocated whether the interface is congested or not. It works as a minimum bandwidth guaranteed to the assigned traffic class at all times.

Packets assigned to the priority queue are discarded when the bandwidth is exceeded. The bandwidth assigned to Class Based Weighted Fair Queues (CBWFQ) are used only when there is congestion. That allocated bandwidth is available to all traffic classes until then. In addition they are serviced (dequeued) only after the priority queue is emptied.

Table 1 Queuing Methods

Queue Type	Description
Priority	traffic assigned to queue is serviced and emptied first
FIFO	default hardware queuing (QoS disabled)
WFQ	assigns bandwidth based on weights to traffic flow
WRED	congestion avoidance to avoid queue tail drops
CBWFQ	assigns specific bandwidth to traffic classes

Congestion Avoidance

During periods of higher network congestion, software queues can overflow and performance is degraded. There is a technique called tail drop that manages back of the software queue for arriving traffic. When any software queue is full, arriving packets at the back of queue are dropped first. There is WRED however that can select to drop packets based on marking for example when a threshold of 70% full is reached.

QoS is applied to packets (and frames) based on a specific order when configured. It starts with selecting traffic to apply QoS using classification. The most popular classification is accomplished with ACLs. The selected traffic is then marked and assigned to a queue. Any traffic shaping is applied before testing conditions for policing. Congestion avoidance drops queued packets based on configured settings. The flow management for applying QoS is described with the following techniques:

Figure 1 Cisco Per-Hop Behavior (PHB) Techniques

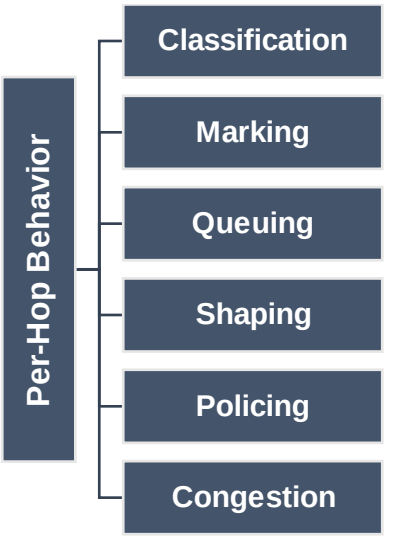


Table 1 Standard QoS Per Hop Behavior

Per Hop Behavior	QoS Technique
classification	CoS, DSCP, NBAR, ACL
congestion avoidance	WRED, tail drop, thresholds
service-policy	attach policy to interface
bandwidth management	shaping, policing, CAR
congestion management	FIFO, WFQ, PQ, CBWFQ (queuing)

Service Policy

QoS is based on per-hop behavior policies that are configured on each Cisco network device. There is a policy map created that is attached to a network interface and direction. That activates PHB and applies QoS to ingress (inbound) or egress (outbound) traffic. Where a service policy is applied is a key consideration when configuring QoS to network traffic.

```
router(config)# interface Gi0/1
router(config-if)# service-policy output voice-traffic
```

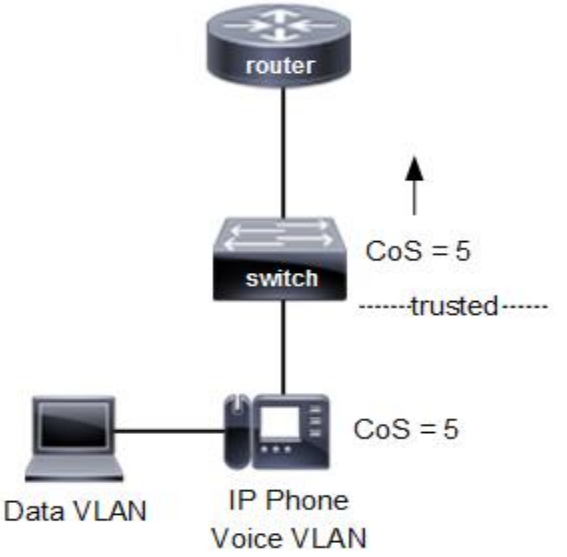
Trust State

Cisco network devices are configured with a trust state. All network interfaces are untrusted by default. Switches will remark all frames arriving at untrusted interfaces to CoS 0. Enabling QoS globally on a device and configuring trust state per interface is required to trust markings. 802.1q protocol used for trunking has CoS priority field. The CoS marking can only be applied to frames traversing trunk interfaces. Untagged packets (native VLAN) are assigned the default Class of Service (CoS) priority of the ingress switch port.

The trust state of a switch for example, determines how the marking is interpreted for inbound traffic. The default trust setting for a Cisco switch is untrusted. The switch will remark the CoS or DSCP value to zero (0) for all inbound packets on an untrusted interface. The switch will examine inbound marking and forward unaltered when trust state is enabled. For example, voice packets marked as Cos 5 from an IP phone are forwarded with that value. Ethernet frames from a host traffic in a data VLAN are remarked from a default zero (0) to a configured value on a trusted interface. The switch will trust Cisco IP phone connected and trust the CoS marking with the following IOS interface commands. CDP must be enabled at the switch for phone detection to work.

mls qos trust device cisco-phone
mls qos trust cos

Figure 2 QoS Trust Boundary



Refer to Figure 2 where the switch is configured as a trusted device. CoS frames arriving at switch-1 are forwarded with the same marking. Defining trust boundaries across the network affects how packets markings are processed. All network devices within a trust boundary won't remark packets as they traverse. The following describe the key points concerning QoS trust boundary configuration.

- Packets from a trusted device are not remarked on upstream device
- Trust boundary defines the point where trusted packets start
- Trust boundary is configured with **mls qos trust cos | dscp** command