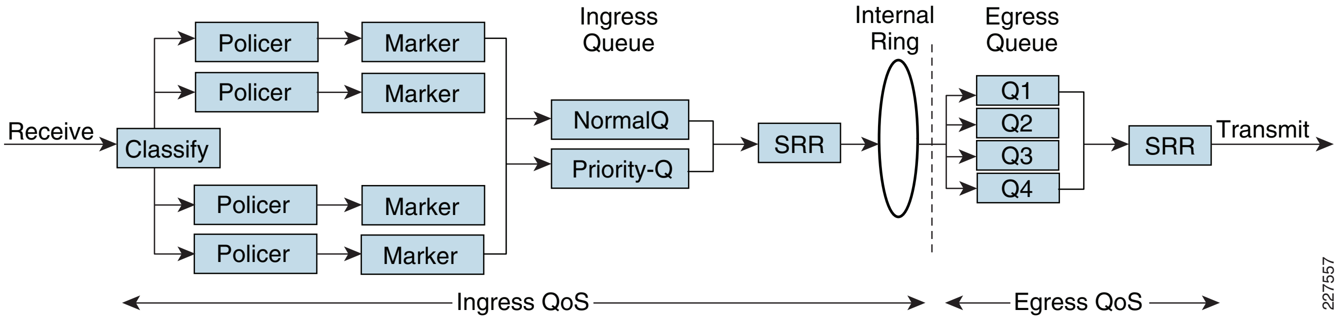
Schools QoS Deployment Guide

This document describes the Schools Service Ready Architecture network QoS design (see Figure 1).

IP networks forward traffic on a best-effort basis by default. The routing protocol forwards packets over the best path, but offers no guarantee of delivery. This model works well for TCP-based data applications that adapt gracefully to variations in latency, jitter, and loss. The Schools Service Ready Architecture is a multi service network design which supports voice and video as well as data traffic on a single network. Real-time applications (such as voice, video) require packets delivered with in specified loss, delay and jitter parameters. Quality-of-Service (QoS) is a collection of features which allows the network to dedicate network resources for higher priority real time applications, while reserving sufficient network resources to service lower priority traffic. QoS accomplishes this by providing differentiated services, depending on the traffic type. For a detailed discussion of QoS, refer to the Enterprise QoS SRND at the following URL:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book.html

Figure 1 Fixed Configuration Catalyst QoS Architecture



The main difference between these platforms is the switching capacity which ranges from 1G to 10G. The switching architecture and some of the internal QoS structure differs between these switches also. Following are some important differences to consider when selecting the access switch:

- The Catalyst 2960 and 2975 do not support multilayer switching and do not support per-VLAN or per-port/per-VLAN policies.
- The Catalyst 2960 and 2975 can police to a minimum rate of 1 Mbps; all other switches within this product family can police to a minimum rate of 8 kbps.
- Only the Catalyst 3650-E and 3750-E support IPv6 QoS.
- Only the Catalyst 3650-E and 3750-E support policing on 10 Gigabit Ethernet interfaces.
- Only the Catalyst 3650-E and 3750-E support SRR shaping weights on 10 Gigabit Ethernet interfaces

While design principles are common, QoS implementation varies between fixed-configuration switches and the modular switching platforms like the Cisco Catalyst 4500/6500. This section discusses the internal switching architecture and the differentiated QoS structure on a per-hop-basis.

QoS in Catalyst Fixed Configuration Switches

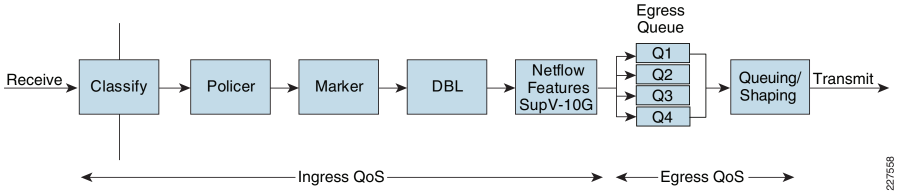
The QoS implementation in Cisco Catalyst 2960, 2975, 3560G, 3560-E, 3750G and 3750-E Series switches is similar. There is no difference in ingress or egress packet classification, marking, queuing and scheduling implementation among these Catalyst platforms. The Cisco Catalyst switches allow users to create a policy-map by classifying incoming traffic (Layer 2 to Layer 4). Catalyst switches allow attaching the policy-map to an individual physical port or to logical interfaces (SVI or port-channel). This creates a common QoS policy which may be used in multiple networks. To prevent switch fabric and egress physical port congestion, the ingress QoS policing structure can strictly filter excessive traffic at the network edge. All ingress traffic from edge ports passes through the switch fabric and congestion may occur at the egress ports. Congestion in access-layer switch can be prevented by tuning queuing scheduler and Weighted Tail Drop (WTD) drop parameters.

QoS in Cisco Modular Switches

Cisco Catalyst 4500 and 6500 are high density, resilient switches for large scale networks. The School Service Ready Architecture uses the Cisco Catalyst 4500 in the district office and larger school site designs; therefore, all the QoS recommendations in this section will be based on 4500 architecture. Cisco Catalyst 4500 Series platform are widely deployed with classic and next-generation supervisors.

The classification function in the classic supervisor module is based on incoming DSCP or CoS setting in the pack, which was assigned by the access-layer switches. Catalyst 4500 with classic supervisor performs ingress and egress QoS function based on internal mapping table that performs DSCP, ToS, or CoS interworking. Classic supervisor relies on trust model configuration; redirection of ingress traffic to an appropriate queue is based on the trust model defined on the edge port. See Figure 2.

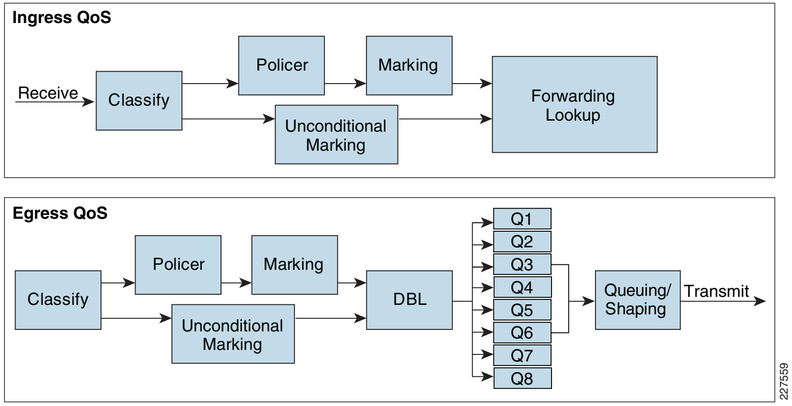
Figure 2 Catalyst 4500 - Classic Supervisor QoS Architecture



The Cisco Catalyst 4500 with next generation Sup-6E (see Figure 3) is designed to offer better differentiated and preferential QoS services for various class-of-service traffic. New QoS capabilities in the Sup-6E enable administrators to take advantage of hardware-based intelligent classification and take action to optimize application performance and network availability. The QoS implementation in Sup-6E supports Modular QoS CLI (MQC) as implemented in IOS-based routers that overall enhances QoS capabilities and eases implementation and operations. Following are some of the key QoS features which differentiate the Sup-6E versus classic supervisors:

- *Trust and Table-Map*—MQC-based QoS implementation offers a number of implementation and operational benefits over classic supervisors that rely on Trust model and internal Table-map as a tool to classify and *mark ingress traffic.*
- *Internal DSCP*—The queue placement in Sup-6E is simplified by leveraging the MQC capabilities to explicitly map DSCP or CoS traffic in hard-coded egress Queue structure,. For example, DSCP 46 can be classified with ACL and can be matched in PQ class-map of an MQC in Sup-6E.
- *Sequential vs Parallel Classification*—With MQC-based QoS classification, the Sup6-E provides sequential classification rather than parallel. Sequential classification method allows the network administrator to classify traffic at egress based on the ingress markings.

Figure 3 Catalyst 4500 - Supervisor 6-E QoS Architecture

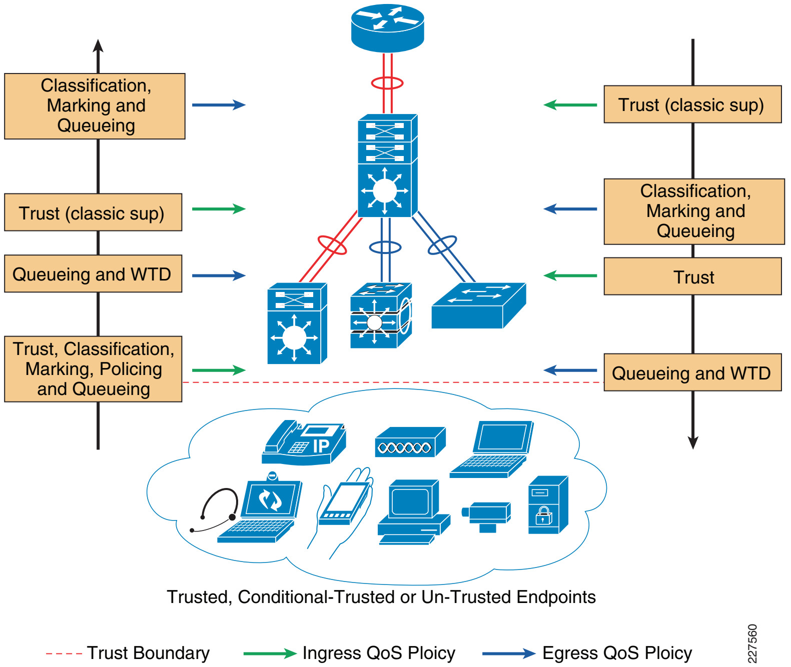


QoS Framework

QoS needs to be designed and implemented considering the entire network. This includes defining trust points, and determining which policies to enforce at each device within the network. Developing the trust model, guides policy implementations for each device.

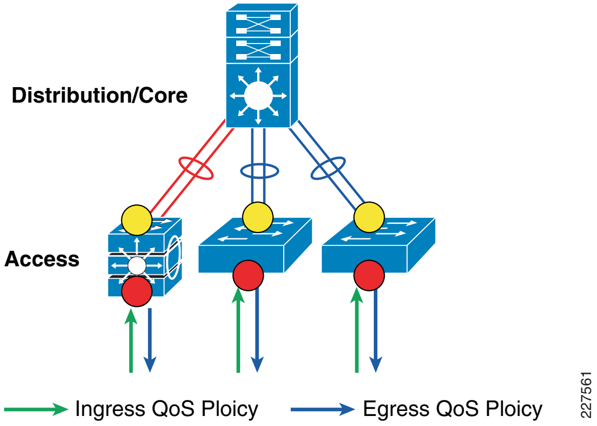
Figure 4 depicts QoS trust model that guides QoS policy implementation in the district office and school site networks.

Figure 4 School QoS Framework


Classification, Marking and Queueing
Trust (classic sup)
Queueing and WTD
Trust, Classification, Marking, Policing and Queueing
Trust (classic sup)
Classification, Marking and Queueing
Trust
Queueing and WTD
IP
Trusted, Conditional-Trusted or Un-Trusted Endpoints
Trust Boundary
Ingress QoS Ploicy
Egress QoS Ploicy
227560

The devices (routers, switches) within the internal network are managed by the system administrator, and hence are classified as trusted devices. Access-layer switches communicate with devices that are beyond the network boundary and within the internal network domain. QoS trust boundary at the access-layer communicates with various devices that could be deployed in different trust models (Trusted, Conditional-Trusted, or Un-Trusted). This section discusses the QoS policies for the traffic that traverses access-switch QoS trust boundary. The QoS function is unidirectional; it provides flexibility to set different QoS polices for traffic entering the network versus traffic that is exiting the network. See Figure 5.

Figure 5 School Network Edge QoS Boundary



QoS Trust Boundary

The access-switch provides the entry point to the network for end devices. The access-switch must decide whether to accept the QoS markings from each endpoint, or whether to change them. This is determined by the QoS policies, and the trust model with which the endpoint is deployed.

End devices are classified into one of three different trust models; each with it's own unique security and QoS policies to access the network:

- *Untrusted*—An unmanaged device that does not pass through the network security policies. For example, student-owned PC or network printer. Packets with 802.1p or DSCP marking set by untrusted endpoints are reset to default by the access-layer switch at the edge. Otherwise, it is possible for an unsecured user to take away network bandwidth that may impact network availability and security for other users.
- *Trusted*—Devices that passes through network access security policies and are managed by network administrator. For example, secure PC or IP endpoints (i.e., servers, cameras, DMP, wireless access points, VoIP/video conferencing gateways, etc). Even when these devices are network administrator maintained and secured, QoS policies must still be enforced to classify traffic and assign it to the appropriate queue to provide bandwidth assurance and proper treatment during network congestion.
- *Conditionally-Trusted*—A single physical connection with one trusted endpoint and a indirect untrusted endpoint must be deployed as conditionally-trusted model. The trusted endpoints are still managed by the network administrator, but it is possible that the untrusted user behind the endpoint may or may not be secure. For example, Cisco Unified IP Phone + PC. These deployment scenarios require hybrid QoS policy that intelligently distinguishes and applies different QoS policy to the trusted and untrusted endpoints that are connected to the same port.

Deploying Ingress QoS

The ingress QoS policy at the access-switches needs to be established, since this is the trust boundary, where traffic enters the network. The following ingress QoS techniques are applied to provide appropriate service treatment and prevent network congestion:

- *Trust*—After classifying the endpoint the trust settings must be explicitly set by a network administrator. By default, Catalyst switches set each port in untrusted mode when QoS is enabled.
- *Classification*—IETF standard has defined a set of application classes and provides recommended DSCP settings. This classification determines the priority the traffic will receive in the network. Using the IETF standard, simplifies the classification process and improves application and network performance.
- *Policing*—To prevent network congestion, the access-layer switch limits the amount of inbound traffic up to its maximum setting. Additional policing can be applied for known applications, to ensure the bandwidth of an egress queue is not completely consumed by one application.
- *Marking*—Based on trust model, classification, and policer settings the QoS marking is set at the edge before approved traffic enters through the access-layer switching fabric. Marking traffic with the appropriate DSCP value is important to ensure traffic is mapped to the appropriate internal queue, and treated with the appropriate priority.
- *Queueing*—To provide differentiated services internally in the Catalyst switching fabric, all approved traffic is queued into priority or non-priority ingress queue. Ingress queueing architecture assures real-time applications, like VoIP traffic, are given appropriate priority (eg transmitted before data traffic).

Implementing QoS Trust Mode

By default, QoS is disabled on all Catalyst switches and must be explicitly enabled in global configuration mode. The QoS configuration is the same for a multilayer or routed-access deployment. The following sample QoS configuration must be enabled on all the access-layer switches deployed in district office and school sites.

```
cr24-2960-DO(config)#mls qos
cr24-2960-DO#show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

Upon enabling QoS in the Catalyst switches, all physical ports are assigned untrusted mode. The network administrator must explicitly enable the trust settings on the physical port where trusted or conditionally trusted endpoints are connected. The Catalyst switches can trust the ingress packets based on 802.1P (CoS-based), ToS (ip-prec-based) or DSCP (DHCP-based) values. Best practice is to deploy DSCP-based trust mode on all the trusted and conditionally-trusted endpoints. This offers a higher level of classification and marking granularity than other methods. The following sample DSCP-based trust configuration must be enabled on the access-switch ports connecting to trusted or conditionally-trusted endpoints.

Access (Multilayer or Routed-Access)

Trusted Port

```
cr24-2960-DO(config)#interface FastEthernet0/5
cr24-2960-DO(config-if)# description CONNECTED TO IPVS 2500 - CAMERA
cr24-2960-DO(config-if)# mls qos trust dscp

cr24-2960-DO#show mls qos interface f0/5
FastEthernet0/5
trust state: trust dscp
trust mode: trust dscp
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

Conditionally-Trusted Port

```
cr24-2960-DO(config)#interface FastEthernet0/3
cr24-2960-DO(config-if)# description CONNECTED TO PHONE
cr24-2960-DO(config-if)# mls qos trust device cisco-phone
cr24-2960-DO(config-if)# mls qos trust dscp

cr24-2960-DO#show mls qos interface f0/3
FastEthernet0/3
trust state: trust dscp
trust mode: trust dscp
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: cisco-phone
qos mode: port-based
```

UnTrusted Port

As described earlier, the default trust mode is untrusted when globally enabling QoS function. Without explicit trust configuration on Fas0/1 port, the following show command verifies current trust state and mode:

```
cr24-2960-DO#show mls qos interface f0/1
FastEthernet0/1
trust state: not trusted
trust mode: not trusted
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

Implementing QoS Classification

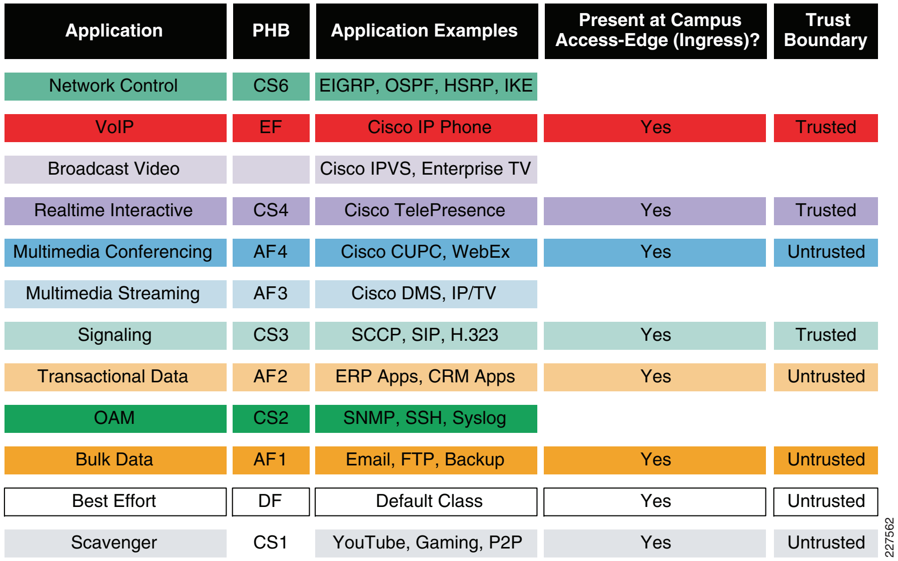
When creating QoS classification policies, the network administrator needs to consider what applications are present at the access edge (in the ingress direction) and whether these applications are sourced from trusted or untrusted endpoints. If PC endpoints are secured and centrally administered, then endpoint PCs may be considered trusted endpoints. In most deployments, this is not the case, thus PCs are considered untrusted endpoints for the remainder of this document.

Not every application class, as defined in the Cisco-modified RFC 4594-based model, is present in the ingress direction at the access edge; therefore, it is not necessary to provision the following application classes at the access-layer:

- *Network Control*—It is assumed that access-layer switch will not transmit or receive network control traffic from endpoints; hence this class is not implemented.
- *Broadcast Video*—Broadcast video and multimedia streaming server are centrally deployed at the district office and multicast traffic is originated from trusted data center servers and is unidirectional to school site endpoints (and should not be sourced from school endpoints).
- *Operation, Administration and Management*—Primarily generated by network devices (routers, switches) and collected by management stations which are typically deployed in the trusted data center network, or a network control center.

All applications present at the access edge need to be assigned a classification, as shown in Figure 6. Voice traffic is primarily sourced from Cisco IP telephony devices residing in the voice VLAN (VVLAN). These are trusted devices, or conditionally trusted, if users also attach PC's, etc to the same port. Voice communication may also be sourced from PC's with soft-phone applications, like Cisco Unified Personal Communicator (CUPC). Since such applications share the same UDP port range as multimedia conferencing traffic (UDP/RTP ports 16384-32767) this soft-phone VoIP traffic is indistinguishable, and should be classified with multimedia conferencing streams.

Figure 6 QoS Classes



Application	PHB	Application Examples	Present at Campus Access-Edge (Ingress)?	Trust Boundary
Network Control	CS6	EIGRP, OSPF, HSRP, IKE		
VoIP	EF	Cisco IP Phone	Yes	Trusted
Broadcast Video		Cisco IPVS, Enterprise TV		
Realtime Interactive	CS4	Cisco TelePresence	Yes	Trusted
Multimedia Conferencing	AF4	Cisco CUPC, WebEx	Yes	Untrusted
Multimedia Streaming	AF3	Cisco DMS, IP/TV		
Signaling	CS3	SCCP, SIP, H.323	Yes	Trusted
Transactional Data	AF2	ERP Apps, CRM Apps	Yes	Untrusted
OAM	CS2	SNMP, SSH, Syslog		
Bulk Data	AF1	Email, FTP, Backup	Yes	Untrusted
Best Effort	DF	Default Class	Yes	Untrusted
Scavenger	CS1	YouTube, Gaming, P2P	Yes	Untrusted

MQC offers scalability and flexibility in configuring QoS to classify all 8 application classes by using match statements or an extended access-list to match the exact value or range of Layer-4 known ports that each application uses to communicate on the network. The following sample configuration creates an extended access-list for each application and then applies it under class-map configuration mode.

```
cr24-3560r-DO(config)#ip access-list extended MULTIMEDIA-CONFERENCING
cr24-3560r-DO(config-ext-nacl)# remark RTP
cr24-3560r-DO(config-ext-nacl)# permit udp any any range 16384 32767
cr24-3560r-DO(config-ext-nacl)#!
cr24-3560r-DO(config-ext-nacl)#ip access-list extended SIGNALING
cr24-3560r-DO(config-ext-nacl)# remark SCCP
cr24-3560r-DO(config-ext-nacl)# permit tcp any any range 2000 2002
cr24-3560r-DO(config-ext-nacl)# remark SIP
cr24-3560r-DO(config-ext-nacl)# permit tcp any any range 5060 5061
cr24-3560r-DO(config-ext-nacl)# permit udp any any range 5060 5061
cr24-3560r-DO(config-ext-nacl)#
cr24-3560r-DO(config-ext-nacl)#ip access-list extended TRANSACTIONAL-DATA
cr24-3560r-DO(config-ext-nacl)# remark HTTPS
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 443
cr24-3560r-DO(config-ext-nacl)# remark ORACLE-SQL*NET
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 1521
cr24-3560r-DO(config-ext-nacl)# permit udp any any eq 1521
cr24-3560r-DO(config-ext-nacl)# remark ORACLE
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 1526
cr24-3560r-DO(config-ext-nacl)# permit udp any any eq 1526
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 1575
cr24-3560r-DO(config-ext-nacl)# permit udp any any eq 1575
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 1630
cr24-3560r-DO(config-ext-nacl)#
cr24-3560r-DO(config-ext-nacl)#ip access-list extended BULK-DATA
cr24-3560r-DO(config-ext-nacl)# remark FTP
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq ftp
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq ftp-data
cr24-3560r-DO(config-ext-nacl)# remark SSH/SFTP
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 22
cr24-3560r-DO(config-ext-nacl)# remark SMTP/SECURE SMTP
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq smtp
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 465
cr24-3560r-DO(config-ext-nacl)# remark IMAP/SECURE IMAP
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 143
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 993
cr24-3560r-DO(config-ext-nacl)# remark POP3/SECURE POP3
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq pop3
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 995
cr24-3560r-DO(config-ext-nacl)# remark CONNECTED PC BACKUP
cr24-3560r-DO(config-ext-nacl)# permit tcp any eq 1914 any
cr24-3560r-DO(config-ext-nacl)#
cr24-3560r-DO(config-ext-nacl)#ip access-list extended DEFAULT
cr24-3560r-DO(config-ext-nacl)# remark EXPLICIT CLASS-DEFAULT
cr24-3560r-DO(config-ext-nacl)# permit ip any any
cr24-3560r-DO(config-ext-nacl)#
cr24-3560r-DO(config-ext-nacl)#ip access-list extended SCAVENGER
cr24-3560r-DO(config-ext-nacl)# remark KAZAA
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 1214
cr24-3560r-DO(config-ext-nacl)# permit udp any any eq 1214
cr24-3560r-DO(config-ext-nacl)# remark MICROSOFT DIRECT X GAMING
cr24-3560r-DO(config-ext-nacl)# permit tcp any any range 2300 2400
cr24-3560r-DO(config-ext-nacl)# permit udp any any range 2300 2400
cr24-3560r-DO(config-ext-nacl)# remark APPLE ITUNES MUSIC SHARING
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 3689
cr24-3560r-DO(config-ext-nacl)# permit udp any any eq 3689
cr24-3560r-DO(config-ext-nacl)# remark BITTORRENT
cr24-3560r-DO(config-ext-nacl)# permit tcp any any range 6881 6999
cr24-3560r-DO(config-ext-nacl)# remark YAHOO GAMES
cr24-3560r-DO(config-ext-nacl)# permit tcp any any eq 11999
cr24-3560r-DO(config-ext-nacl)# remark MSN GAMING ZONE
cr24-3560r-DO(config-ext-nacl)# permit tcp any any range 28800 29100
cr24-3560r-DO(config-ext-nacl)#
```

Creating class-map for each application services and applying match statement:

```
cr24-3560r-DO(config)#class-map match-all VVLAN-SIGNALING
cr24-3560r-DO(config-cmap)# match ip dscp cs3
cr24-3560r-DO(config-cmap)#
cr24-3560r-DO(config-cmap)#class-map match-all VVLAN-VOIP
cr24-3560r-DO(config-cmap)# match ip dscp ef
cr24-3560r-DO(config-cmap)#
cr24-3560r-DO(config-cmap)#class-map match-all MULTIMEDIA-CONFERENCING
cr24-3560r-DO(config-cmap)# match access-group name
MULTIMEDIA-CONFERENCING
cr24-3560r-DO(config-cmap)#
cr24-3560r-DO(config-cmap)#class-map match-all SIGNALING
cr24-3560r-DO(config-cmap)# match access-group name SIGNALING
cr24-3560r-DO(config-cmap)#
cr24-3560r-DO(config-cmap)#class-map match-all TRANSACTIONAL-DATA
cr24-3560r-DO(config-cmap)# match access-group name TRANSACTIONAL-DATA
cr24-3560r-DO(config-cmap)#
cr24-3560r-DO(config-cmap)#class-map match-all BULK-DATA
cr24-3560r-DO(config-cmap)# match access-group name BULK-DATA
cr24-3560r-DO(config-cmap)#
cr24-3560r-DO(config-cmap)#class-map match-all DEFAULT
cr24-3560r-DO(config-cmap)# match access-group name DEFAULT
cr24-3560r-DO(config-cmap)#
cr24-3560r-DO(config-cmap)#class-map match-all SCAVENGER
cr24-3560r-DO(config-cmap)# match access-group name SCAVENGER
```

Implementing Ingress Policer

It is important to limit how much bandwidth each class may use at the ingress to the access-layer for two primary reasons:

- Bandwidth Bottleneck—To prevent network congestion, each physical port at trust boundary must be rate-limited. The rate-limit value may differ based on several factors—end-to-end network bandwidth capacity, end-station and application performance capacities, etc.
- Bandwidth Security—Well-known applications like Cisco IP telephony, use a fixed amount of bandwidth per device, based on codec. It is important to police high-priority application traffic which is assigned to the high-priority queue, otherwise it could consume too much overall network bandwidth and impact other application performance.

In addition to policing, the rate-limit function also provides the ability to take different actions on the excess incoming traffic which exceeds the established limits. The exceed-action for each class must be carefully designed based on the nature of application to provide best effort service based on network bandwidth availability. Table 10 provides best practice policing guidelines for different classes to be implemented for trusted and conditional-trusted endpoints at the network edge.

Table 1

Application	Policing Rate	Conform-Action	Exceed-Action
VoIP Signaling	<32 kbps	Pass	Drop
VoIP Bearer	<128 kbps	Pass	Drop
Multimedia Conferencing	<5Mbps[1]	Pass	Drop
Signaling	<32 kbps	Pass	Drop
Transactional Data	<10 Mbps [1]	Pass	Remark to CS1
Bulk Data	<10 Mbps [1]	Pass	Remark to CS1
Best Effort	<10 Mbps [1]	Pass	Remark to CS1
Scavenger	<10 Mbps [1]	Pass	Drop

[1] Rate varies based on several factors as defined earlier. This table depicts sample rate-limiting values.

As described in the “QoS in Catalyst Fixed Configuration Switches” section on page -1, the policer capabilities differ in Catalyst switching platforms. When deploying policer policies on the access-layer switches the following platform limitations must be taken into consideration:

- The Catalyst 2960 and 2975 can only police to a minimum rate of 1 Mbps; all other platforms within this switch-product family can police to a minimum rate of 8 kbps.
- Only the Cisco Catalyst 3650-E and 3750-E support policing on 10 Gigabit Ethernet interfaces.

The following sample configuration shows how to deploy policing for multiple classes on trusted and conditionally-trusted ingress ports in access-layer switches.

Trusted or Conditionally-Trusted Port

```
cr24-3560r-DO(config)#policy-map Phone+PC-Policy
cr24-3560r-DO(config-pmap)# class VVLAN-VOIP
cr24-3560r-DO(config-pmap-c)# police 128000 8000 exceed-action drop
cr24-3560r-DO(config-pmap-c)# class VVLAN-SIGNALING
cr24-3560r-DO(config-pmap-c)# police 32000 8000 exceed-action drop
cr24-3560r-DO(config-pmap-c)# class MULTIMEDIA-CONFERENCING
cr24-3560r-DO(config-pmap-c)# police 5000000 8000 exceed-action drop
cr24-3560r-DO(config-pmap-c)# class SIGNALING
cr24-3560r-DO(config-pmap-c)# police 32000 8000 exceed-action drop
cr24-3560r-DO(config-pmap-c)# class TRANSACTIONAL-DATA
cr24-3560r-DO(config-pmap-c)# police 10000000 8000 exceed-action
policed-dscp-transmit
cr24-3560r-DO(config-pmap-c)# class BULK-DATA
cr24-3560r-DO(config-pmap-c)# police 10000000 8000 exceed-action
policed-dscp-transmit
cr24-3560r-DO(config-pmap-c)# class SCAVENGER
cr24-3560r-DO(config-pmap-c)# police 10000000 8000 exceed-action drop
cr24-3560r-DO(config-pmap-c)# class DEFAULT
```

```
cr24-3560r-DO(config-pmap-c)# police 10000000 8000 exceed-action
policed-dscp-transmit
```

All ingress traffic (default class) from untrusted endpoint be must be policed without explicit classification that requires differentiated services. The following sample configuration shows how to deploy policing on untrusted ingress ports in access-layer switches:

UnTrusted Port

```
cr24-3560r-DO(config)#policy-map UnTrusted-PC-Policy
cr24-3560r-DO(config-pmap)# class class-default
cr24-3560r-DO(config-pmap-c)# police 10000000 8000 exceed-action drop
```

Implementing Ingress Marking

Accurate DSCP marking of ingress traffic at the access-layer switch is critical to ensure proper QoS service treatment as traffic traverses through the network. All classified and policed traffic must be explicitly marked using the policy-map configuration based on an 8-class QoS model as shown in Figure 6.

Best practice is to use a explicit marking command (set dscp) even for trusted application classes (like VVLAN-VOIP and VVLAN-SIGNALING), rather than a trust policy-map action. A trust statement in a policy map requires multiple hardware entries, while the use of an explicit (seemingly redundant) marking command, improves the hardware efficiency.

The following sample configuration shows how to implement explicit marking for multiple classes on trusted and conditionally-trusted ingress ports in access-layer switches:

Trusted or Conditionally-Trusted Port

```
cr24-3560r-DO(config)#policy-map Phone+PC-Policy
cr24-3560r-DO(config-pmap)# class VVLAN-VOIP
cr24-3560r-DO(config-pmap-c)# set dscp ef
cr24-3560r-DO(config-pmap-c)# class VVLAN-SIGNALING
cr24-3560r-DO(config-pmap-c)# set dscp cs3
cr24-3560r-DO(config-pmap-c)# class MULTIMEDIA-CONFERENCING
cr24-3560r-DO(config-pmap-c)# set dscp af41
cr24-3560r-DO(config-pmap-c)# class SIGNALING
cr24-3560r-DO(config-pmap-c)# set dscp cs3
cr24-3560r-DO(config-pmap-c)# class TRANSACTIONAL-DATA
cr24-3560r-DO(config-pmap-c)# set dscp af21
cr24-3560r-DO(config-pmap-c)# class BULK-DATA
cr24-3560r-DO(config-pmap-c)# set dscp af11
cr24-3560r-DO(config-pmap-c)# class SCAVENGER
cr24-3560r-DO(config-pmap-c)# set dscp cs1
cr24-3560r-DO(config-pmap-c)# class DEFAULT
cr24-3560r-DO(config-pmap-c)# set dscp default
```

All ingress traffic (default class) from an untrusted endpoint must be marked without a explicit classification. The following sample configuration shows how to implement explicit DSCP marking:

Untrusted Port

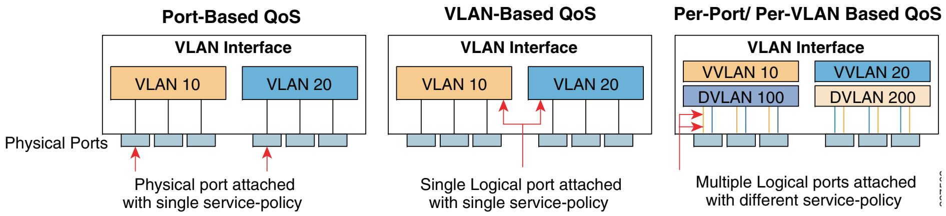
```
cr24-3560r-DO(config)#policy-map UnTrusted-PC-Policy
cr24-3560r-DO(config-pmap)# class class-default
cr24-3560r-DO(config-pmap-c)# set dscp default
```

Applying Ingress Policies

the access-layer to enforce the QoS configuration. Cisco Catalyst switches offer three simplified methods to apply service-policies. Depending on the deployment model, any of these methods may be used:

- *Port-based QoS*—Applying service-policy on a per physical port basis will force traffic to pass-through the QoS policies before entering the network. Port-based QoS functions on a per-physical port basis even if the port is associated with a logical VLAN.
- *VLAN-based QoS*—Applying service-policy on per VLAN basis requires the policy-map to be attached to a logical Layer-3 SVI interface. Every physical port associated with the VLAN will require an extra configuration to enforce the QoS policies defined on a logical interface.
- *Per-Port/Per-VLAN-based QoS*—Not supported on all the Catalyst platforms and the configuration commands are platform-specific. Per-port/per-VLAN-based QoS creates a nested hierarchical policy-map that operates on a trunk interface. A different policy-map can be applied on each logical SVI interface that is associated to a single physical port.

Figure 7 Depicts All Three QoS Implementation Method


Port-Based QoS
VLAN Interface
VLAN 10
VLAN 20
Physical Ports
Physical port attached with single service-policy
VLAN-Based QoS
VLAN Interface
VLAN 10
VLAN 20
Single Logical port attached with single service-policy
Per-Port/ Per-VLAN Based QoS
VLAN Interface
VVLAN 10
VVLAN 20
DVLAN 100
DVLAN 200
Multiple Logical ports attached with different service-policy

The following sample configuration shows how to deploy port-based QoS on the access-layer switches:

```
cr24-3560r-DO(config)#interface fastethernet0/4
cr24-3560r-DO(config-if)# description CONNECTED TO PHONE+PC
cr24-3560r-DO(config-if)# service-policy input Phone+PC-Policy

cr24-3560r-DO#show policy-map interface f0/4 | inc Service|Class
Service-policy input: Phone+PC-Policy
Class-map: VVLAN-VOIP (match-all)
Class-map: VVLAN-SIGNALING (match-all)
Class-map: MULTIMEDIA-CONFERENCING (match-all)
```

```
Class-map: SIGNALING (match-all)
Class-map: TRANSACTIONAL-DATA (match-all)
Class-map: BULK-DATA (match-all)
Class-map: SCAVENGER (match-all)
 Class-map: DEFAULT (match-all)
    Class-map: class-default (match-any)
```

Applying Ingress Queueing

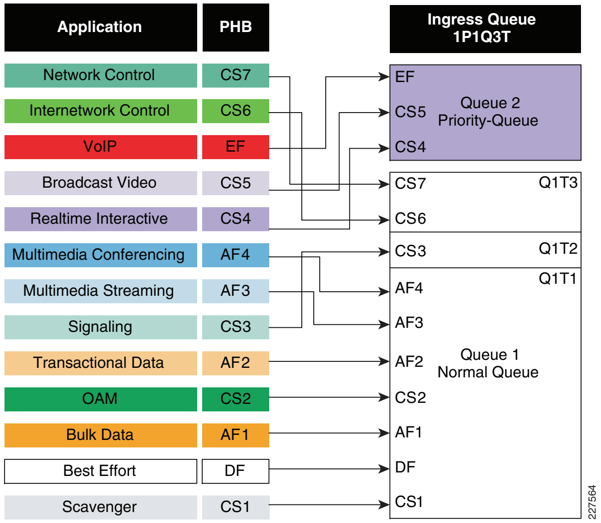
Fixed configuration Cisco Catalyst switches (29xx and 3xxx) not only offer differentiated services on the network ports but also internally on the switching fabric. After enabling QoS and attaching inbound policies on the physical ports, all the packets that meet the specified policy are forwarded to the switching fabric for egress switching. The aggregate bandwidth from all edge ports may exceed switching fabric bandwidth and cause internal congestion.

These platforms support two internal ingress queues: normal queue and priority queue. The ingress queue inspects the DSCP value on each incoming frame and assigns it to either the normal or priority queue. High priority traffic, like DSCP EF marked packets, are placed in the priority queue and switched before processing the normal queue.

The Catalyst 3750-E family of switches supports the weighted tail drop (WTD) congestion avoidance mechanism. WTD is implemented on queues to manage the queue length. WTD drops packets from the queue, based on dscp value, and the associated threshold. If the threshold is exceeded for a given internal DSCP value, the switch drops the packet. Each queue has three threshold values. The internal DSCP determines which of the three threshold values is applied to the frame. Two of the three thresholds are configurable (explicit) and one is not (implicit). This last threshold corresponds to the tail of the queue (100% limit).

Figure 8 depicts how different class-of-service applications are mapped to the Ingress Queue structure (1P1Q3T) and how each queue is assigned a different WTD threshold.

Figure 8 Ingress Queueing



The DSCP marked packets in the policy-map must be assigned to the appropriate queue and each queue must be configured with the recommended WTD threshold as defined in Figure 8. The following ingress queue configuration must be enabled in global configuration mode on every access-layer switch.

```
cr25-3750-DO(config)#mls qos srr-queue input priority-queue 2 bandwidth 30
 ! Q2 is enabled as a strict-priority ingress queue with 30% BW

cr25-3750-DO(config)#mls qos srr-queue input bandwidth 70 30
 ! Q1 is assigned 70% BW via SRR shared weights
 ! Q1 SRR shared weight is ignored (as it has been configured as a PQ)

cr25-3750-DO(config)#mls qos srr-queue input threshold 1 80 90
 ! Q1 thresholds are configured at 80% (Q1T1) and 90% (Q1T2)
 ! Q1T3 is implicitly set at 100% (the tail of the queue)
 ! Q2 thresholds are all set (by default) to 100% (the tail of Q2)

! This section configures ingress DSCP-to-Queue Mappings
cr25-3750-DO(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 8 10 12 14
 ! DSCP DF, CS1 and AF1 are mapped to ingress Q1T1
cr25-3750-DO(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 16 18 20 22
 ! DSCP CS2 and AF2 are mapped to ingress Q1T1
cr25-3750-DO(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 26 28 30 34 36
38
 ! DSCP AF3 and AF4 are mapped to ingress Q1T1
cr25-3750-DO(config)#mls qos srr-queue input dscp-map queue 1 threshold 2 24
 ! DSCP CS3 is mapped to ingress Q1T2
cr25-3750-DO(config)#mls qos srr-queue input dscp-map queue 1 threshold 3 48 56
 ! DSCP CS6 and CS7 are mapped to ingress Q1T3 (the tail of Q1)
cr25-3750-DO(config)#mls qos srr-queue input dscp-map queue 2 threshold 3 32 40 46
 ! DSCP CS4, CS5 and EF are mapped to ingress Q2T3 (the tail of the PQ)

cr25-3750-DO#show mls qos input-queue
Queue:       12
-----------------------------------
buffers     :9010
bandwidth :7030
priority   :030
threshold1:80100
threshold2:90100

cr25-3750-DO#show mls qos maps dscp-input-q
   Dscp-inputq-threshold map:
     d1 :d2    0        1         2        3          4         5        6          7
8          9

-----------------------------------------------------------------------------------------
      0 :     01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      1 :     01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      2 :     01-01 01-01 01-01 01-01 01-02 01-01 01-01 01-01 01-01 01-01
      3 :     01-01 01-01 02-03 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      4 :     02-03 02-01 02-01 02-01 02-01 02-01 02-03 02-01 01-03 01-01
      5 :     01-01 01-01 01-01 01-01 01-01 01-01 01-03 01-01 01-01 01-01
      6 :     01-01 01-01 01-01 01-01
```

Deploying Egress QoS

The QoS implementation for egress traffic toward the network edge on access-layer switches is much simpler than the ingress traffic QoS. The egress QoS implementation provides optimal queueing policies for each class and sets the drop thresholds to prevent network congestion and application performance impact. Cisco Catalyst switches support four hardware queues which are assigned the following policies:

- Real-time queue (to support a RFC 3246 EF PHB service)
- Guaranteed bandwidth queue (to support RFC 2597 AF PHB services)
- Default queue (to support a RFC 2474 DF service)

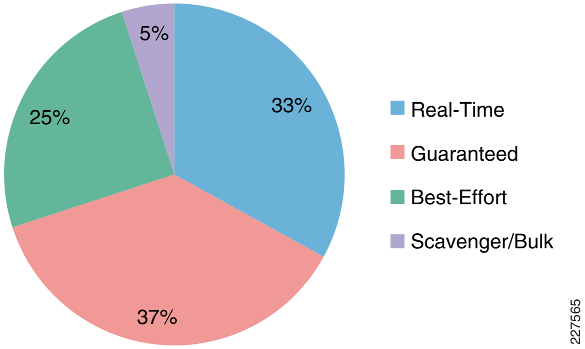
- Bandwidth constrained queue (to support a RFC 3662 scavenger service)

As a best practice, each physical or logical link must diversify bandwidth assignment to map with hardware queues:

- Real-time queue should not exceed 33% of the link's bandwidth.
- Default queue should be at least 25% of the link's bandwidth.
- Bulk/scavenger queue should not exceed 5% of the link's bandwidth.

Figure 9 shows the best practice egress queue bandwidth allocation for each class.

Figure 9 Engress QoS

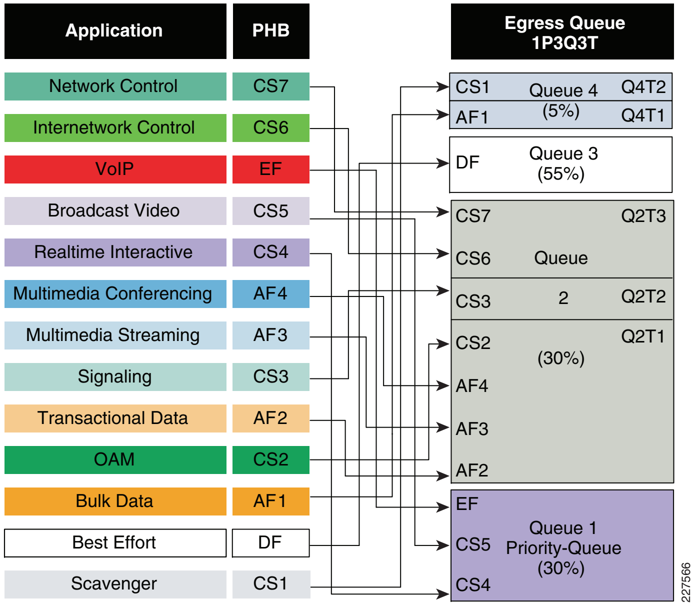


Given these minimum queuing requirements and bandwidth allocation recommendations, the following application classes can be mapped to the respective queues:

- *Realtime Queue*—Voice, broadcast video, and realtime interactive may be mapped to the realtime queue (per RFC 4594).
- *Guaranteed Queue*—Network/internetwork control, signaling, network management, multimedia conferencing, multimedia streaming, and transactional data can be mapped to the guaranteed bandwidth queue. Congestion avoidance mechanisms (i.e., selective dropping tools), such as WRED, can be enabled on this class. If configurable drop thresholds are supported on the platform, these may be enabled to provide intra-queue QoS to these application classes, in the respective order they are listed (such that control plane protocols receive the highest level of QoS within a given queue).
- *Scavenger/Bulk Queue*—Bulk data and scavenger traffic can be mapped to the bandwidth-constrained queue and congestion avoidance mechanisms can be enabled on this class. If configurable drop thresholds are supported on the platform, these may be enabled to provide inter-queue QoS to drop scavenger traffic ahead of bulk data.
- *Default Queue*—Best effort traffic can be mapped to the default queue; congestion avoidance mechanisms can be enabled on this class.

The egress queueing is designed to map traffic, based on DSCP value, to four egress queues. as shown above. The egress QoS model for a platform that supports DSCP-to-queue mapping with a 1P3Q8T queuing structure is depicted in Figure 10.

Figure 10 Access-Layer 1P3Q3T Egress Queue model



DSCP marked packets are assigned to the appropriate queue and each queue is configured with appropriate WTD threshold as defined in Figure 10. Egress queueing is the same on network edge port as well as on uplink connected to internal network, and it is independent of trust mode. The following egress queue configuration in global configuration mode, must be enabled on every access-layer switch in the network.

```
! This section configures explicit WTD thresholds on Q2 and Q4
cr25-3750-DO(config)#mls qos queue-set output 1 threshold 2 80 90 100 100
 ! Q2T1 is set to 80%; Q2T2 is set to 90%
cr25-3750-DO(config)#mls qos queue-set output 1 threshold 4 60 100 100 100
 ! Q4T1 is set to 60%; all other thresholds for Q4 remain at 100%


 ! This section configures egress DSCP-to-Queue mappings
cr25-3750-DO(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46
 ! DSCP CS4, CS5 and EF are mapped to egress Q1T3 (tail of the PQ)
cr25-3750-DO(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
 ! DSCP CS2 and AF2 are mapped to egress Q2T1

cr25-3750-DO(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36
38
 ! DSCP AF3 and AF4 are mapped to egress Q2T1
cr25-3750-DO(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 24
 ! DSCP CS3 is mapped to egress Q2T2
cr25-3750-DO(config)#mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
 ! DSCP CS6 and CS7 are mapped to egress Q2T3
cr25-3750-DO(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 0
 ! DSCP DF is mapped to egress Q3T3 (tail of the best effort queue)
cr25-3750-DO(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 8
 ! DSCP CS1 is mapped to egress Q4T1
cr25-3750-DO(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
 ! DSCP AF1 is mapped to Q4T2 (tail of the less-than-best-effort queue)

 ! This section configures interface egress queuing parameters
cr25-3750-DO(config)#interface range GigabitEthernet1/0/1-48
cr25-3750-DO(config-if-range)# queue-set 1
 ! The interface(s) is assigned to queue-set 1
```

```
cr25-3750-DO(config-if-range)# srr-queue bandwidth share 1 30 35 5
 ! The SRR sharing weights are set to allocate 30% BW to Q2
 ! 35% BW to Q3 and 5% BW to Q4
 ! Q1 SRR sharing weight is ignored, as it will be configured as a PQ
cr25-3750-DO(config-if-range)# priority-queue out
 ! Q1 is enabled as a strict priority queue

cr25-3750-DO#show mls qos interface GigabitEthernet1/0/27 queueing
GigabitEthernet1/0/27
Egress Priority Queue : enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  1 30 35 5
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
     The port is mapped to qset : 1
```

Table 2 and Table 3 summarize the ingress and egress QoS policies at the access-layer for several types of validated endpoints.

Table 2 Summarized Network Edge Ingress QoS Deployment Guidelines

End-Point	Trust Model	DSCP Trust	Classification	Marking	Policing	Ingress Queueing
Unmanaged devices, printers etc	UnTrusted	Don't Trust. Default.	None	None	Yes	Yes
Managed secured devices, Servers etc	Trusted	Trust	8 Class Model	Yes	Yes	Yes
Phone	Trusted	Trust	Yes	Yes	Yes	Yes
Phone + Mobile PC	Conditionally-Trusted	Trust	Yes	Yes	Yes	Yes
IP Video surveillance Camera	Trusted	Trust	No	No	No	Yes
Digital Media Player	Trusted	Trust	No	No	No	Yes
Core facing Uplinks	Trusted	Trust	No	No	No	Yes

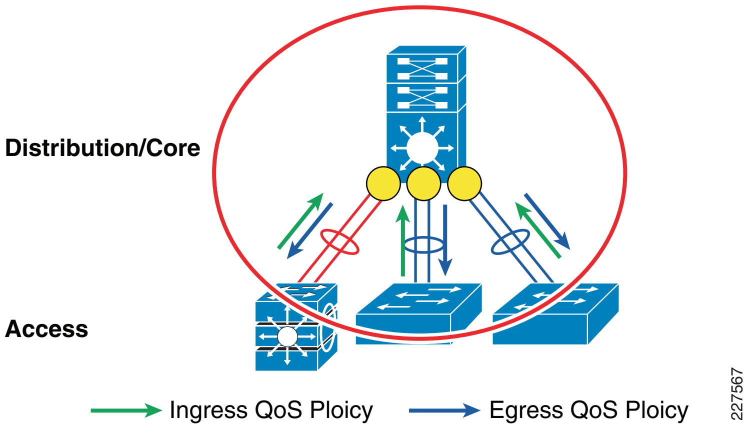
Table 3 Summarized Network Edge Egress QoS Deployment Guidelines

End-Point	Trust Model	Classification / Marking / Policing	Egress Queueing	Bandwidth Share
Unmanaged devices, printers etc	UnTrusted	None	Yes	Yes
Managed secured devices, Servers etc	Trusted	None	Yes	Yes
Phone	Trusted	None	Yes	Yes
Phone + Mobile PC	Conditionally-Trusted	None	Yes	Yes
IP Video surveillance Camera	Trusted	None	Yes	Yes
Digital Media Player	Trusted	None	Yes	Yes
Core facing Uplinks	Trusted	None	Yes	Yes

Deploying Network Core QoS

All connections between internal network devices that are deployed within the network domain boundary are classified as trusted devices and follow the same QoS best practices recommended in the previous section. Ingress and egress core QoS policies are simpler than those applied at the network edge, See Figure 11.

Figure 11 Core QoS



The core network devices are considered trusted and rely on the access-switch to properly mark DSCP values. The core network is deployed to ensure consistent differentiated QoS service across the network. This ensures there is no service quality degradation for high-priority traffic, such as IP telephony or video.

The QoS implementation at the District Office and Larger School Site differ from the Smaller School Site, due to different platforms used as the collapsed core router (Catalyst 4500 vs Catalyst 3750 StackWise).

Deploying District Office or Large School Site Ingress QoS

The District Office collapsed core is deployed with Cisco Catalyst 4500 with Supervisor-6E, whereas the Larger School Site collapsed core is deployed with Cisco Catalyst 4500 with either Supervisor-6E or Supervisor-V. The Supervisor-6E product has a redesigned QoS implementation which matches Cisco IOS routers. No ingress QoS configuration is required, since QoS is enabled by default, and all ports are considered trusted.

The Cisco Catalyst 4500 with Supervisor-V requires ingress QoS configuration similar to trusted endpoints in the access-layer.

Following is a sample configuration which enables QoS in the Catalyst 4500 with Supervisor-V

```
cr35-4507-SS1(config)#qos
! Enables QoS function in the switch

cr35-4507-SS1#show qos
QoS is enabled globally
IP header DSCP rewrite is enabled
```

After QoS is globally enabled, all interfaces are in the untrusted mode by default. QoS trust settings must be set on each Layer 2 or Layer 3 port that is physically connected to another device within the network trust boundary. When Cisco Catalyst 4500 is deployed in EtherChannel mode, the QoS trust settings must be applied to every physical member-link and logical port-channel interface. Best practice is to enable trust DSCP settings on each physical and logical interface that connects to another internal trusted device (e.g., access-layer switches in wiring closet or data-center, a router, wireless LAN controller (WLC)).

```
cr35-4507-SS1(config)#interface range Po11 , Gi1/2 , Gi2/2
cr35-4507-SS1(config-if-range)#description Connected to cr35-2960-SS1
cr35-4507-SS1(config-if-range)#qos trust dscp

cr35-4507-SS1#show qos interface Port-channel 11
QoS is enabled globally
Port QoS is enabled
Administrative Port Trust State: 'dscp'
Operational Port Trust State: 'dscp'
Trust device: none
Default DSCP: 0 Default CoS: 0
```

Additional ingress QoS techniques (such as classification, marking, and policing) are not required at the collapsed core layer since these functions are already performed by the access-layer switches. The architecture of Catalyst 4500 with classic or next-generation Supervisor do not need ingress queueing since all of the forwarding decisions are made centrally on the supervisor. There are no additional QoS configurations required at the collapsed core-layer system.

Deploying Small School Site Ingress QoS

The Smaller School Site is deployed using Cisco Catalyst 3750-E StackWise as the collapsed core switch. The QoS implementation remains the same whether deployed as 3750-E StackWise or as a standalone switch. By default, QoS is disabled on the 3750-E switch.   Following is a sample configuration to enable QoS in global configuration mode:

```
cr36-3750s-SS100(config)#mls qos
! Enables QoS function in the switch

cr36-3750s-SS100#show mls qos
QoS is enabled
QoS ip packet dscp rewrite is enabled
```

After QoS is globally enabled, all interfaces are in the untrusted mode by default. QoS trust settings must be set on each Layer 2 or Layer 3 port that is physically connected to another device within the network trust boundary. When Cisco Catalyst 3750-E StackWise Plus is deployed in EtherChannel mode, the QoS trust settings must be applied to every physical member-link. Best practice is to enable trust DSCP settings on each physical and logical interface that connects to another internal trusted device (e.g., access-layer switches in wiring closet or data-center, a router, wireless LAN controller (WLC)).

```
cr36-3750s-SS100(config)#int range gi1/0/49 , gi3/0/49
cr36-3750s-SS100(config-if-range)# description Connected to
cr36-2960-SS100
cr36-3750s-SS100(config-if-range)#mls qos trust dscp

cr36-3750s-SS100#show mls qos interface Gi1/0/49
GigabitEthernet1/0/49
trust state: trust dscp
trust mode: trust dscp
trust enabled flag: ena
COS override: dis
default COS: 0
DSCP Mutation Map: Default DSCP Mutation Map
Trust device: none
qos mode: port-based
```

Additional ingress QoS techniques (such as classification, marking, and policing) are not required at the collapsed core layer since these functions are already performed by the access-layer switches. The ingress queueing and DSCP-Ingress-Queue function in 3750-E StackWise Plus must be enabled to allow differentiation between normal versus high-priority traffic. The ingress queuing configuration is consistent with the implementation at the access-edge. Following is a sample configuration for the ingress queues of the Catalyst 3750-E StackWise collapsed core switch:

```
cr36-3750-SS100(config)#mls qos srr-queue input priority-queue 2 bandwidth 30
 ! Q2 is enabled as a strict-priority ingress queue with 30% BW

cr36-3750-SS100(config)#mls qos srr-queue input bandwidth 70 30
 ! Q1 is assigned 70% BW via SRR shared weights
 ! Q1 SRR shared weight is ignored (as it has been configured as a PQ)

cr36-3750-SS100(config)#mls qos srr-queue input threshold 1 80 90
 ! Q1 thresholds are configured at 80% (Q1T1) and 90% (Q1T2)
 ! Q1T3 is implicitly set at 100% (the tail of the queue)
 ! Q2 thresholds are all set (by default) to 100% (the tail of Q2)

! This section configures ingress DSCP-to-Queue Mappings
cr36-3750-SS100(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 0 8 10 12 14
 ! DSCP DF, CS1 and AF1 are mapped to ingress Q1T1cr36-3750-SS100(config)# mls qos
srr-queue input dscp-map queue 1 threshold 1 16 18 20 22
```

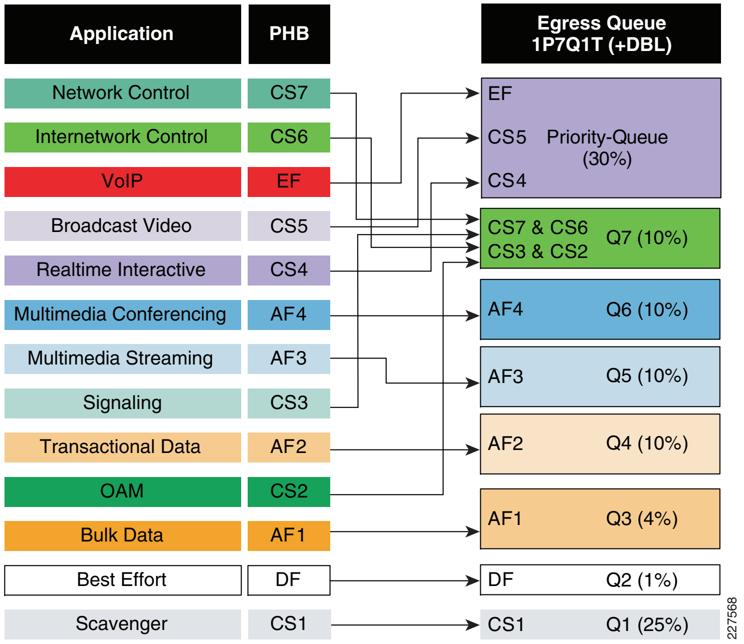
```
 ! DSCP CS2 and AF2 are mapped to ingress Q1T1
cr36-3750-SS100(config)# mls qos srr-queue input dscp-map queue 1 threshold 1 26 28 30 34
36 38
 ! DSCP AF3 and AF4 are mapped to ingress Q1T1
cr36-3750-SS100(config)#mls qos srr-queue input dscp-map queue 1 threshold 2 24
 ! DSCP CS3 is mapped to ingress Q1T2
cr36-3750-SS100(config)# mls qos srr-queue input dscp-map queue 1 threshold 3 48 56
 ! DSCP CS6 and CS7 are mapped to ingress Q1T3 (the tail of Q1)
cr36-3750-SS100(config)# mls qos srr-queue input dscp-map queue 2 threshold 3 32 40 46
 ! DSCP CS4, CS5 and EF are mapped to ingress Q2T3 (the tail of the PQ)

cr36-3750s-SS100#show mls qos input-queue
Queue     :       1       2
----------------------------------------
buffers   :      90      10
bandwidth :      70      30
priority  :       0      30
threshold1:      80     100
threshold2:      90     100

cr36-3750s-SS100#show mls qos maps dscp-input-q
   Dscp-inputq-threshold map:
     d1 :d2    0        1         2        3          4         5        6          7
8          9

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

      0 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      1 :    01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      2 :    01-01 01-01 01-01 01-01 01-02 01-01 01-01 01-01 01-01 01-01
      3 :    01-01 01-01 02-03 01-01 01-01 01-01 01-01 01-01 01-01 01-01
      4 :    02-03 02-01 02-01 02-01 02-01 02-01 02-03 02-01 01-03 01-01
      5 :    01-01 01-01 01-01 01-01 01-01 01-01 01-03 01-01 01-01 01-01
      6 :    01-01 01-01 01-01 01-01
```

Deploying District Office Egress QoS

The District Office is deployed with Cisco Catalyst 4500 with Supervisor-6E as the collapsed core router. Egress QoS from the collapsed core router provides optimized queueing and drop thresholds to drop excess low-priority traffic and protect high-priority traffic.

The Supervisor-6E supports up to 8 traffic classes for QoS mapping. It also supports a platform-specific congestion avoidance algorithm to provide Active Queue Management (AQM) with Dynamic Buffer Limiting (DBL). DBL tracks the queue length for each traffic flow in the switch. When the queue length of a flow exceeds its limit, DBL drops packets or sets the Explicit Congestion Notification (ECN) bit in the TCP packet header. With 8 egress (1P7Q1T) queues and DBL capability in the Sup-6E, the bandwidth distribution for each class changes, as shown in Figure 12

Figure 12 District Office School Network



Implementing QoS policies on Sup-6E-based Catalyst 4500 platform follows IOS (MQC)-model. The egress QoS implementation bundles the queueing and policing functions on EtherChannel based networks. To provide low-latency for high priority traffic, all lower priority traffic must wait until the priority-queue is empty. Best practice includes implementing a policer along with the priority-queue to provide more fair treatment for all traffic.

The following sample configuration shows how to create an 8-class egress queueing model and protect from high-priority traffic consuming more bandwidth than global policies allow. The egress QoS service-policy must be applied to all the physical EtherChannel member-links connected to different service-blocks (i.e., WAN edge, data center, access-layer switches, etc).

```
! Creating class-map for each classes using match dscp statement as marked by edge
systems
cr24-4507-DO(config)#class-map match-all PRIORITY-QUEUE
cr24-4507-DO(config-cmap)# match dscp ef
cr24-4507-DO(config-cmap)# match dscp cs5
cr24-4507-DO(config-cmap)# match dscp cs4
cr24-4507-DO(config-cmap)# class-map match-all CONTROL-MGMT-QUEUE
cr24-4507-DO(config-cmap)# match dscp cs7
cr24-4507-DO(config-cmap)# match dscp cs6
cr24-4507-DO(config-cmap)# match dscp cs3
cr24-4507-DO(config-cmap)# match dscp cs2
cr24-4507-DO(config-cmap)# class-map match-all MULTIMEDIA-CONFERENCING-QUEUE
cr24-4507-DO(config-cmap)# match dscp af41 af42 af43
cr24-4507-DO(config-cmap)# class-map match-all MULTIMEDIA-STREAMING-QUEUE
cr24-4507-DO(config-cmap)# match dscp af31 af32 af33
cr24-4507-DO(config-cmap)# class-map match-all TRANSACTIONAL-DATA-QUEUE
cr24-4507-DO(config-cmap)# match dscp af21 af22 af23
```

```
cr24-4507-DO(config-cmap)# class-map match-all BULK-DATA-QUEUE
cr24-4507-DO(config-cmap)# match dscp af11 af12 af13
cr24-4507-DO(config-cmap)# class-map match-all SCAVENGER-QUEUE
cr24-4507-DO(config-cmap)# match dscp cs1

! Creating policy-map and configure queueing for class-of-service
cr24-4507-DO(config)#policy-map EGRESS-POLICY
cr24-4507-DO(config-pmap)# class PRIORITY-QUEUE
cr24-4507-DO(config-pmap-c)# priority
cr24-4507-DO(config-pmap-c)# class CONTROL-MGMT-QUEUE
cr24-4507-DO(config-pmap-c)# bandwidth remaining percent 10
cr24-4507-DO(config-pmap-c)# class MULTIMEDIA-CONFERENCING-QUEUE
cr24-4507-DO(config-pmap-c)# bandwidth remaining percent 10
cr24-4507-DO(config-pmap-c)# class MULTIMEDIA-STREAMING-QUEUE
cr24-4507-DO(config-pmap-c)# bandwidth remaining percent 10
cr24-4507-DO(config-pmap-c)# class TRANSACTIONAL-DATA-QUEUE
cr24-4507-DO(config-pmap-c)# bandwidth remaining percent 10
cr24-4507-DO(config-pmap-c)# dbl
cr24-4507-DO(config-pmap-c)# class BULK-DATA-QUEUE
cr24-4507-DO(config-pmap-c)# bandwidth remaining percent 4
cr24-4507-DO(config-pmap-c)# dbl
cr24-4507-DO(config-pmap-c)# class SCAVENGER-QUEUE
cr24-4507-DO(config-pmap-c)# bandwidth remaining percent 1
cr24-4507-DO(config-pmap-c)# class class-default
cr24-4507-DO(config-pmap-c)# bandwidth remaining percent 25
cr24-4507-DO(config-pmap-c)# dbl

! Attaching egress service-policy on all physical member-link ports
cr24-4507-DO(config)#int range Gi1/1 - 6 , Gi2/1 - 6
cr24-4507-DO(config-if-range)# service-policy output EGRESS-POLICY
```

EtherChannel is an aggregated logical bundle interface that does not perform queueing and relies on individual member-links to queue egress traffic. The policer to rate-limit priority class traffic must be implemented on EtherChannel and not on individual member-links since it governs the aggregate egress traffic limits. The following additional policy-map must be created to classify priority-queue class traffic and rate-limit the traffic to 30% of egress link capacity:

```
cr24-4507-DO(config)#class-map match-any PRIORITY-QUEUE
cr24-4507-DO(config-cmap)# match dscp ef
cr24-4507-DO(config-cmap)# match dscp cs5
cr24-4507-DO(config-cmap)# match dscp cs4

cr24-4507-DO(config)#policy-map PQ-POLICER
cr24-4507-DO(config-pmap)# class PRIORITY-QUEUE
cr24-4507-DO(config-pmap-c)# police cir 300 m conform-action transmit
exceed-action drop

cr24-4507-DO(config)#interface range Port-Channel 1 , Port-channel 11 -
17
cr24-4507-DO(config-if-range)#service-policy output PQ-POLICER
```

Deploying Large School Site Egress QoS

The large school site is deployed with Cisco Catalyst 4500 and either Supervisor-6E or Supervisor-V as the collapsed core router. If the larger school site network is deployed with Sup-6E, then the configuration is the same as described in the previous section.

The QoS deployment and implementation guidelines differ when the Cisco Catalyst 4500 is deployed with the classic Supervisor-V module. The SupV supervisor can have up to four egress queues like the Cisco Catalyst 29xx and 35xx/37xx Series switches. Before forwarding egress traffic, each packet must be internally classified and placed in the appropriate egress-queue. Placing traffic into different class-of-service queues, will offer traffic prioritization and guaranteed bandwidth to the network. The following sample configuration shows how to implement egress QoS on the Catalyst 4500 with Supervisor-V:

```
cr35-4507-SS1(config)#qos dbl
 ! DBL is globally enabled
cr35-4507-SS1(config)#no qos dbl dscp-based 32
cr35-4507-SS1(config)#no qos dbl dscp-based 40
cr35-4507-SS1(config)#no qos dbl dscp-based 46
 ! DBL is explicitly disabled on DSCP CS4, CS5 and EF
 ! as these DSCP values are assigned to the PQ
 ! and as such should never experience congestion avoidance drops
cr35-4507-SS1(config)#qos dbl exceed-action ecn
 ! DBL will mark IP ECN bits in the event of congestion

! This section configures the DBL policy-map
cr35-4507-SS1(config)#policy-map DBL
cr35-4507-SS1(config-pmap)# class class-default
cr35-4507-SS1(config-pmap-c)# dbl
 ! DBL is enabled on all flows
 ! (with the exception of DSCP CS4, CS5 and EF)
 ! This section configures the DSCP-to-Queue mappings


cr35-4507-SS1(config)#qos map dscp 8 10 12 14 to tx-queue 1
 ! DSCP CS1 and AF1 are mapped to Q1 (the less than best effort queue)
cr35-4507-SS1(config)#qos map dscp 0 to tx-queue 2
 ! DSCP DF is mapped to Q2 (the best effort/default queue)
cr35-4507-SS1(config)#qos map dscp 32 40 46 to tx-queue 3
 ! DSCP CS4, CS5 and EF are mapped to Q3 (the PQ)
cr35-4507-SS1(config)#qos map dscp 16 18 20 22 to tx-queue 4
 ! DSCP CS2 and AF2 are mapped to Q4 (guaranteed BW queue)
cr35-4507-SS1(config)#qos map dscp 24 26 28 30 to tx-queue 4
 ! DSCP CS3 and AF3 are mapped to Q4 (guaranteed BW queue)
cr35-4507-SS1(config)#qos map dscp 34 36 38 to tx-queue 4
 ! DSCP AF4 is mapped to Q4 (guaranteed BW queue)
cr35-4507-SS1(config)#qos map dscp 48 56 to tx-queue 4
! DSCP CS6 and CS7 are mapped to Q4 (guaranteed BW queue)
! This section configures all the EtherChannel member-link for egress queuing
cr35-4507-SS1(config)#interface range Gig1/1 - 6 , Gig2/1 - 6
cr35-4507-SS1(config-if-range)# tx-queue 1
cr35-4507-SS1(config-if-tx-queue)#  bandwidth percent 5
 ! Q1 (less than best effort queue) is assigned 5% BW
cr35-4507-SS1(config-if-tx-queue)# tx-queue 2
cr35-4507-SS1(config-if-tx-queue)#  bandwidth percent 35
 ! Q2 (default/best effort queue) is assigned 35% BW
cr35-4507-SS1(config-if-tx-queue)# tx-queue 3
cr35-4507-SS1(config-if-tx-queue)# priority high
cr35-4507-SS1(config-if-tx-queue)# bandwidth percent 30
 ! Q3 is enabled as a PQ and assigned 30% BW
cr35-4507-SS1(config-if-tx-queue)# tx-queue 4
cr35-4507-SS1(config-if-tx-queue)# bandwidth percent 30
```

```
 ! Q4 (guaranteed BW queue) is assigned 30% BW
cr35-4507-SS1(config-if-range)# service-policy output DBL
 ! DBL policy-map is attached to the interface(s)

cr35-4507-SS1#show qos dbl
QOS is enabled globally
DBL is enabled globally on DSCP values:
     0-31,33-39,41-45,47-63
DBL flow includes vlan
DBL flow includes layer4-ports
DBL uses ecn to indicate congestion
DBL exceed-action probability: 15%
DBL max credits: 15
DBL aggressive credit limit: 10
DBL aggressive buffer limit: 2 packets



cr35-4507-SS1#show qos maps dscp tx-queue
DSCP-TxQueue Mapping Table (dscp = d1d2)
d1 : d2  0   1   2    3   4   5   6    7   8   9
------------------------------------------------
 0 :    02 01 01 01 01 01 01 01 01 01
 1 :    01 01 01 01 01 01 04 02 04 02
 2 :    04 02 04 02 04 02 04 02 04 02
 3 :    04 02 03 03 04 03 04 03 04 03
 4 :    03 03 03 03 03 03 03 03 04 04
 5 :    04 04 04 04 04 04 04 04 04 04
 6 :    04 04 04 04

cr35-4507-SS1#show qos interface Gig1/2
QoS is enabled globally
Port QoS is enabled
Administrative Port Trust State: 'dscp'
Operational Port Trust State: 'dscp'
Trust device: none
Default DSCP: 0 Default CoS: 0
Appliance trust: none
Tx-Queue   Bandwidth   ShapeRate   Priority   QueueSize
             (bps)       (bps)                (packets)
  1        50000000     disabled     N/A        2080
  2        350000000     disabled     N/A2080
  3        300000000disabled     high2080
  4        300000000disabledN/A2080
```

Deploying Small School Site Egress QoS

Collapsed Core—Catalyst 3750-E StackWise Plus

The small school site is deployed with Cisco Catalyst 3750-E StackWise as the collapsed core router.

The Catalyst 3750-E can have up to four egress queues. Before forwarding egress traffic, each packet is placed in the appropriate egress-queue as shown in Figure 10. The Catalyst 3750-E switch supports Shaped Round Robin (SRR) packet schedule service which can be deployed in two different modes:

- Shaped—To provide guaranteed bandwidth, the shaped egress queue reserves some of the bandwidth of the port for each queue. Traffic load exceeding the shape parameter gets dropped. The queue cannot take advantage of excess bandwidth capacity when other queues are not using their bandwidth allocations.
- Shared—Shared mode also provides guaranteed bandwidth for each queue; however, it allows the flexibility of using excess bandwidth when there is any available.

The following sample configuration shows how to implement egress QoS on the Catalyst 3750-E:

```
! This section configures explicit WTD thresholds on Q2 and Q4
cr36-3750s-SS100(config)#mls qos queue-set output 1 threshold 2 80 90 100 100
 ! Q2T1 is set to 80%; Q2T2 is set to 90%
cr36-3750s-SS100(config)#mls qos queue-set output 1 threshold 4 60 100 100 100
 ! Q4T1 is set to 60%; all other thresholds for Q4 remain at 100%

 ! This section configures egress DSCP-to-Queue mappings
cr36-3750s-SS100(config)# mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46
 ! DSCP CS4, CS5 and EF are mapped to egress Q1T3 (tail of the PQ)
cr36-3750s-SS100(config)# mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20
22
 ! DSCP CS2 and AF2 are mapped to egress Q2T1


cr36-3750s-SS100(config)#mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34
36 38
 ! DSCP AF3 and AF4 are mapped to egress Q2T1
cr36-3750s-SS100(config)#mls qos srr-queue output dscp-map queue 2 threshold 2 24
 ! DSCP CS3 is mapped to egress Q2T2
cr36-3750s-SS100(config)#mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
 ! DSCP CS6 and CS7 are mapped to egress Q2T3
cr36-3750s-SS100(config)#mls qos srr-queue output dscp-map queue 3 threshold 3 0
 ! DSCP DF is mapped to egress Q3T3 (tail of the best effort queue)
cr36-3750s-SS100(config)#mls qos srr-queue output dscp-map queue 4 threshold 1 8
 ! DSCP CS1 is mapped to egress Q4T1
cr36-3750s-SS100(config)# mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
 ! DSCP AF1 is mapped to Q4T2 (tail of the less-than-best-effort queue)

 ! This section configures interface egress queuing parameters
cr36-3750s-SS100(config)#interface range GigabitEthernet1/0/1-48
cr36-3750s-SS100(config-if-range)# queue-set 1
 ! The interface(s) is assigned to queue-set 1
cr36-3750s-SS100(config-if-range)# srr-queue bandwidth share 1 30 35 5
 ! The SRR sharing weights are set to allocate 30% BW to Q2
 ! 35% BW to Q3 and 5% BW to Q4
 ! Q1 SRR sharing weight is ignored, as it will be configured as a PQ
cr36-3750s-SS100(config-if-range)# priority-queue out
 ! Q1 is enabled as a strict priority queue

cr36-3750s-SS100#show mls qos interface GigabitEthernet1/0/49 queueing
GigabitEthernet1/0/49
Egress Priority Queue : enabled
Shaped queue weights (absolute) :  25 0 0 0
Shared queue weights  :  1 30 35 5
The port bandwidth limit : 100  (Operational Bandwidth:100.0)
     The port is mapped to qset : 1
```