CHAPTER 2

Campus QoS Design

This chapter includes the following topics:

- QoS Design Overview
- Catalyst 2950—QoS Considerations and Design
- Catalyst 3550—QoS Considerations and Design
- Catalyst 2970/3560/3750—QoS Considerations and Design
- Catalyst 4500 Supervisor II+/III/IV/V—QoS Considerations and Design
- Catalyst 6500 PFC2/PFC3—QoS Considerations and Design
- WAN Aggregator/Branch Router Handoff Considerations

QoS Design Overview

This section includes the following topics:

- Where is QoS Needed in a Campus?
- DoS/Worm Mitigation
- Call Signaling Ports
- Access Edge Trust Models
- Cisco IP Phones
- WAN Aggregator/Branch Router Connections

Where is QoS Needed in a Campus?

The case for Quality of Service (QoS) in WANs/VPNs is largely self-evident because of its low-bandwidth links compared to the high-bandwidth requirements of most applications. However, the need for QoS is sometimes overlooked or even challenged in high-bandwidth Gigabit/TenGigabit campus LAN environments.

Although network administrators sometimes equate QoS only with queuing, the QoS toolset extends considerably beyond just queuing tools. Classification, marking and policing are all important QoS functions that are optimally performed within the campus network, particularly at the access layer ingress edge (access edge).

Three important QoS design principles are important when deploying campus QoS policies:

- Classify and mark applications as close to their sources as technically and administratively feasible.

  This principle promotes end-to-end Differentiated Services/Per-Hop Behaviors. Sometimes endpoints can be trusted to set Class of Service (CoS)/Differentiated Services Code Point (DSCP) markings correctly, but this is not recommended because users can easily abuse provisioned QoS policies if permitted to mark their own traffic.

  For example, if DSCP Expedited Forwarding (EF) received priority services throughout the enterprise, a user could easily configure the NIC on a PC to mark *all* traffic to DSCP EF, thus hijacking network priority queues to service their non-real time traffic. Such abuse could easily ruin the service quality of real time applications (like VoIP) throughout the enterprise. For this reason, the clause "as close as… *administratively* feasible" is included in the design principle.

- *Police unwanted traffic flows as close to their sources as possible*.

  There is little sense in forwarding unwanted traffic only to police and drop it at a subsequent node. This is especially the case when the unwanted traffic is the result of Denial of Service (DoS) or worm attacks. Such attacks can cause network outages by overwhelming network device processors with traffic.

- Always perform QoS in hardware rather than software when a choice exists.

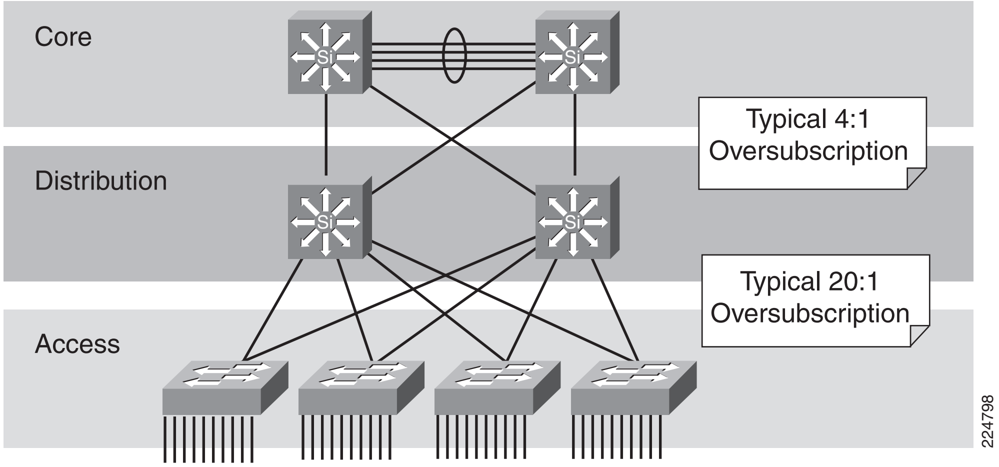
  Cisco IOS routers perform QoS in software. This places additional demands on the CPU, depending on the complexity and functionality of the policy. Cisco Catalyst switches, on the other hand, perform QoS in dedicated hardware ASICS and as such do not tax their main CPUs to administer QoS policies. You can therefore apply complex QoS policies at Gigabit/TenGigabitEthernet line speeds in these switches.

For these reasons, you should enable QoS policies such as classification and marking policies to establish and enforce trust boundaries as well as policers to protect against undesired flows at the access edge of the LAN.

Most campus links are underutilized. Some studies have shown that 95 percent of campus access layer links are utilized at less than 5 percent of their capacity. This means that you can design campus networks to accommodate oversubscription between access, distribution and core layers. Oversubscription allows for uplinks to be utilized more efficiently and more importantly, reduces the overall cost of building the campus network.

Common campus oversubscription values are 20:1 for the access-to-distribution layers and 4:1 for the distribution-to-core layers, as shown in Figure 2-1.

Figure 2-1 Typical Campus Oversubscription Ratios



It is quite rare under normal operating conditions for campus networks to suffer congestion. And if congestion does occur, it is usually momentary and not sustained, as at a WAN edge. However, critical applications like VoIP still require service guarantees regardless of network conditions.

The only way to provide service guarantees is to enable queuing at any node that has the potential for congestion—regardless of how rarely, in fact, this may occur. The potential for congestion exists in campus uplinks because of oversubscription ratios and speed mismatches in campus downlinks (for example, GigabitEthernet to FastEthernet links). The only way to provision service guarantees in these cases is to enable queuing at these points.

Queuing helps to meet network requirements under normal operating conditions, but enabling QoS within the campus is even more critical under abnormal network conditions such as DoS/worm attacks. During such conditions, network traffic may increase exponentially until links are fully utilized. Without QoS, the worm-generated traffic drowns out applications and causes denial of service through unavailability. Enabling QoS policies within the campus, as detailed later in this chapter, maintains network availability by protecting and servicing critical applications such as VoIP and even Best Effort traffic.

The intrinsic interdependencies of network QoS, High Availability and security are clearly manifest in such worse-case scenarios.

So where is QoS required in campus?

Access switches require the following QoS policies:

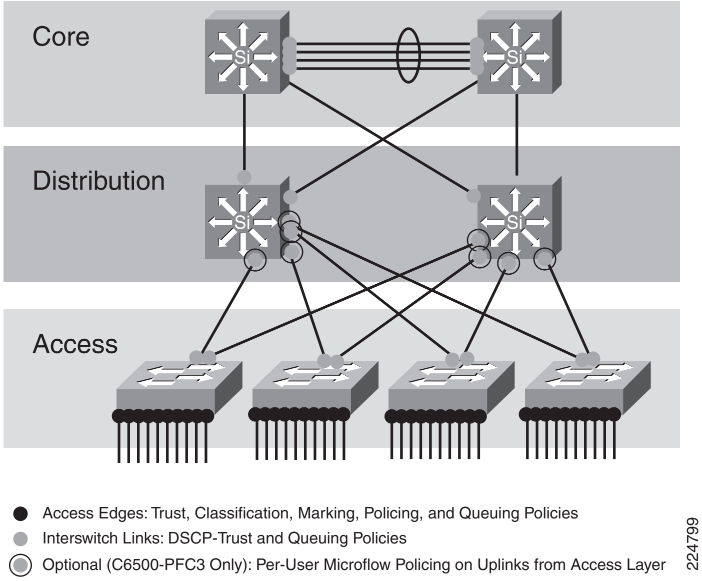
- Appropriate (endpoint-dependant) trust policies, and/or classification and marking policies
- Policing and markdown policies
- Queuing policies.

Distribution and core switches require the following QoS policies:

- DSCP trust policies
- Queuing policies
- Optional per-user microflow policing policies (only on supported platforms)

These recommendations are summarized in Figure 2-2.

Figure 2-2 Where is QoS Required within the Campus?


Core
Si
Si
Distribution
Si
Si
Access
● Access Edges: Trust, Classification, Marking, Policing, and Queuing Policies
● Interswitch Links: DSCP-Trust and Queuing Policies
◎ Optional (C6500-PFC3 Only): Per-User Microflow Policing on Uplinks from Access Layer
224799

DoS/Worm Mitigation Strategies

A proactive approach to mitigating DoS/worm flooding attacks within campus environments is to immediately respond to out-of-profile network behavior indicative of a DoS or worm attack through access layer policers. Such policers meter traffic rates received from endpoint devices and markdown excess traffic when these exceed specified watermarks (at which point they are no longer considered normal flows).

These policers are relatively “dumb” because they do not match specific network characteristics of specific types of attacks. Instead, they simply meter traffic volumes and respond to abnormally high volumes as close to the source as possible. The simplicity of this approach negates the need for the policers to be programmed with knowledge of the specific details of *how* the attack is being generated or propagated.

It is precisely this “dumbness” of such access layer policers that allow them to stay effective as worms mutate and become more complex. The policers do not care *how* the traffic was generated or *what* it looks like, they only care *how much* traffic is being put onto the wire. Therefore, they continue to police even advanced worms that continually change the tactics of how traffic is being generated.

For example, in most enterprises it is quite abnormal (within a 95 percent statistical confidence interval) for PCs to generate sustained traffic in excess of 5 percent of their link capacity. In the case of a FastEthernet switch port, this means that it is unusual in most organizations for an end-user PC to generate more than 5 Mbps of uplink traffic on a sustained basis.

Note It is important to recognize that this value for normal access edge utilization by endpoints of 5 percent is just an *example* value used for simplicity in this chapter. This value would likely vary from industry vertical to vertical, and from enterprise to enterprise.

Cisco does not recommend policing all traffic to 5 Mbps and automatically dropping the excess. If that was the case, there would be no need to deploy FastEthernet or GigabitEthernet switch ports to endpoint devices because even 10-BaseT Ethernet switch ports have more uplink capacity than a 5 Mbps policer-enforced limit. Such an approach would also penalize legitimate traffic that *did* exceed 5 Mbps on a FastEthernet switch port.

A less severe approach is to couple access layer policers with hardware/software (campus/WAN/VPN) queuing polices, with both sets of policies provisioning for a less-than Best-Effort Scavenger class.

With this method, access layer policers mark down out-of-profile traffic to DSCP CS1 (Scavenger) and then all congestion management policies (whether in Catalyst hardware or in IOS software) provision a less-than Best-Effort service for any traffic marked to CS1 during periods of congestion.

This method works for both legitimate traffic exceeding the access layer policer's watermark and also for illegitimate excess traffic as a result of a DoS or worm attack.

In the former case, for example, assume that the PC generates over 5 Mbps of traffic, perhaps because of a large file transfer or backup. Congestion under normal operating conditions is rarely if ever experienced because there is generally abundant capacity to carry the traffic within the campus. This is usually true because the uplinks to the distribution and core layers of the campus network are typically GigabitEthernet and require 1000 Mbps of traffic from the access layer switch to congest. If the traffic is destined to the far side of a WAN/VPN link, which is rarely over 5 Mbps in speed, dropping occurs even without the access layer policer, because of the campus/WAN speed mismatch and resulting bottleneck. TCP's sliding windows mechanism eventually finds an optimal speed (under 5 Mbps) for the file transfer. Thus, access layer policers that mark down out-of-profile traffic to Scavenger (CS1) *do not affect legitimate traffic*, aside from the obvious remarking. No reordering or dropping occurs on such flows as a result of these policers that would not have occurred in any event.

In the case of illegitimate excess traffic, the effect of access layer policers on traffic caused by DoS or worm attacks is quite different. As many hosts become infected and traffic volumes multiply, congestion may be experienced in the campus up-links due to the aggregate traffic volume. For example, if just 11 end-user PCs on a single access-layer switch begin spawning worm flows to their maximum FastEthernet link capacities, the GigabitEthernet up-link to the distribution layer switch will congest, and queuing/reordering will engage. At such a point, VoIP and critical data applications, and even Best Effort applications, gain priority over worm-generated traffic. Scavenger traffic is dropped the most aggressively, while network devices remain accessible for the administration of patches/plugs/ACLs required to fully neutralize the specific attack.

WAN links are also protected. VoIP, critical data and even Best Effort flows continue to receive priority over any traffic marked down to Scavenger/CS1. This is a huge advantage, because WAN links are generally the first to be overwhelmed by DoS/worm attacks. Access layer policers thus *significantly mitigate* network traffic generated by DoS or worm attacks.

You should recognize the distinction between mitigating an attack and preventing it entirely. The strategy presented here *does not guarantee that no Denial of Service or worm attacks will ever happen, but serves only to reduce the risk and impact* that such attacks have on the campus network infrastructure and then, by extension, the WAN/VPN network infrastructure. Furthermore, while this strategy reduces the collateral damage to the network infrastructure caused by DoS/worm attacks, it may not mitigate other specific objectives of such worms, such as reconnaissance and vulnerability exploitation. Hence, a comprehensive approach much be used to address DoS/worm attacks, involving a holistic integration of security technologies with Quality of Service technologies.

Call Signaling Ports

In this design chapter, only Skinny Call Control Protocol (SCCP) ports (TCP Ports 2000–2002) are used to identify call signaling protocols to keep the examples relatively simple.

However, SCCP is by no means the only call signaling protocol used in IP telephony environments. Cisco recommends including all relevant call signaling ports required for a given IPT environment in the access lists that identify call signaling protocols. Firewalls protecting CallManagers should also allow additional ports to provide the supplementary services that CallManagers provide or require.

Access Edge Trust Models

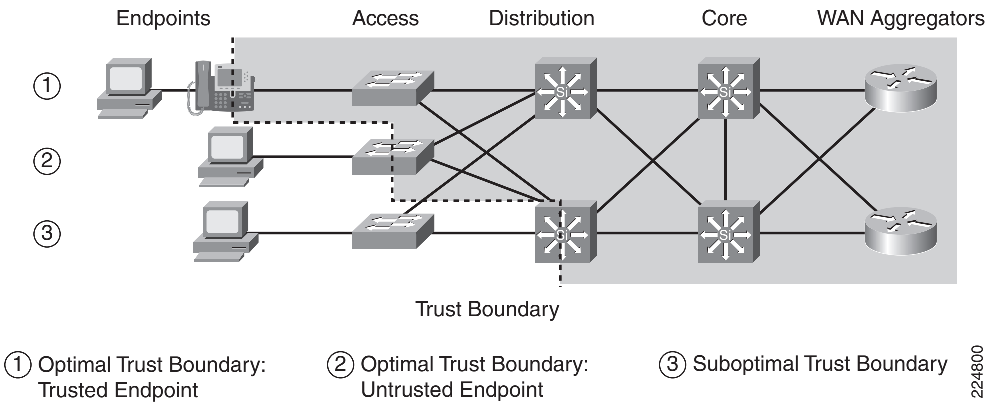
This section includes the following topics:

- Trusted Endpoints
- Untrusted Endpoints
- Conditionally-Trusted Endpoints

The primary function of access edge policies is to establish and enforce trust boundaries. A trust boundary is the point within the network where markings such as CoS or DSCP begin to be accepted. Previously-set markings are overridden as required at the trust boundary.

You should enforce trust boundaries as close to the endpoints as technically and administratively possible as shown in Figure 2-3.

Figure 2-3 Establishing Trust Boundaries


Endpoints
Access
Distribution
Core
WAN Aggregators
1
2
3
Trust Boundary
1 Optimal Trust Boundary: Trusted Endpoint
2 Optimal Trust Boundary: Untrusted Endpoint
3 Suboptimal Trust Boundary
224800

Legend for Figure 2-3:

1. Optimal trust boundary: trusted endpoint
2. Optimal trust boundary: untrusted endpoint
3. Sub-optimal trust boundary

The definition of the trust boundary depends on the capabilities of the endpoints that are being connected to the access edge of the LAN. The following are the three main categories of endpoints as they relate to trust boundaries:

- Trusted endpoints
- Untrusted endpoints
- Conditionally-trusted endpoints

Trusted Endpoints

Trusted endpoints have the capabilities and intelligence to mark application traffic to the appropriate CoS and/or DSCP values. Trusted endpoints also have the ability to remark traffic that may have been previously marked by an untrusted device. Trusted endpoints are not typically mobile devices, which means that the switch port into which they are plugged does not usually change.

Note Cisco IP Phones, which often change switch ports as users move, are more appropriately classified as conditionally-trusted endpoints.

Examples of trusted endpoints include the following:

- Analog gateways—These devices connect analog devices such as fax machines, modems, TDD/TTYs, and analog phones to the VoIP network, such that the analog signals can be packetized and transmitted over the IP network.

  Examples of analog gateways include the following:

  - Analog network modules (NM-1V and NM2-V, which support either high- or low-density Voice/Fax Interface Cards (VICs)
  - Cisco Communication Media Module (CMM) linecard
  - Catalyst 6500 Analog Interface Module (WS-X6624-FXS).
  - Cisco VG224 and VG248 IOS-based voice gateways
- IP conferencing stations—These devices are specialized IP Phones with 360 degree microphones and advanced speakerphones designed for meeting room VoIP conferencing. Examples of such devices include the Cisco 7935 and 7936.
- Videoconferencing gateways and systems—These devices transmit interactive video across the IP network. Examples of such devices capable of setting DSCP markings include the Cisco IP/VC 3511, 3521, 3526 and 3540 videoconferencing gateways and systems. If, on the other hand, video-conferencing devices do not have the ability to set DSCP markings correctly, they should be treated as untrusted devices.
- Video surveillance units—These third-party devices are used for security and remote monitoring purposes over an IP (as opposed to a closed-circuit) network. These may support DSCP marking, in which case they may be considered trusted endpoints.
- Servers—Certain servers, within the data center or otherwise, might be capable of correctly marking their traffic on their NICs. In such cases, the network administrator can choose to trust such markings. However, enforcing such a trust boundary requires cooperation between network administrators and system or server administrators, an alliance that is often fragile, at best, and usually involves considerable finger pointing. Additionally, network administrators should bear in mind that the majority of DoS/ worm attacks target servers. Infected servers not only might spew profuse amounts of traffic onto the network, but, in such cases, they might do so with trusted markings. There’s no hard-and-fast rule that will apply to every situation. Some administrators prefer to trust certain servers, like Cisco CallManagers, due to the large number of ports that may be in use to provide services rather than administer complex access lists. In either case, consider the tradeoffs involved when deciding whether or not to trust a server.
- Wireless access points—Some wireless access points (APs) have the ability to mark or remark 802.1p CoS and/or DSCP values and therefore qualify as trusted endpoints. Examples include Cisco Aironet 350, 1100 and 1200 series APs.

- Wireless IP Phones—Mobile wireless IP Phones can mark DSCP values for VoIP and call signaling and pass these on to the wireless AP with which they are associated. Examples include the Cisco 7920G wireless IP Phone.

When trusted endpoints are connected to a switch port, all that is typically required is enabling the following interface command: **mls qos trust dscp**.

Optionally, if the traffic rate of the trusted application is known, the network administrator could apply an access layer policer to protect against out-of-profile rates, in case the trusted endpoint is somehow compromised.

For example, consider the case of an IP videoconferencing (IP/VC) station that transmits 384 kbps of video (not including Layer 2–4 overhead) and correctly marks this traffic to DSCP AF41. An access edge ingress policer could be applied to the switch port to which this IP/VC station is connected and be configured to trust up to 500 kbps, allowing for Layer 2–4 overhead and policer granularity of interactive video traffic marked AF41. Excess traffic could be marked to CS1. Such a policy prevents network abuse if another device is inserted, perhaps via a hub, into the path, or if the trusted endpoint itself becomes compromised.

Untrusted Endpoints

This section includes the following topics:

- Untrusted PC + SoftPhone with Scavenger-Class QoS
- Untrusted Server with Scavenger-Class QoS

As previously mentioned, trusting end users and their PCs is generally a bad idea because newer operating systems like Windows XP and Linux make it relatively easy to set CoS or DSCP markings on PC NICs. Such markings may be set deliberately or even inadvertently. In either case, improperly set QoS markings can affect the service levels of multiple users within the enterprise and make troubleshooting a nightmare. Also, marking application traffic on server NICs has disadvantages as discussed in the previous section that may make it preferable to treat these as untrusted devices.

While client PCs and data center servers are related and complimentary, they also have unique considerations that affect their classification and marking policies, and so will be examined individually.

Untrusted PC + SoftPhone with Scavenger-Class QoS

Cisco generally recommends not trusting end user PC traffic. However, some PCs may be running applications that critically require QoS treatment. A classic example is a PC running Cisco IP Softphone. In such a case, the critical application needs to be identified using access lists and marked/remarked at the access edge. Remarking can be done with either an MLS QoS **set ip dscp** command or with a policer.

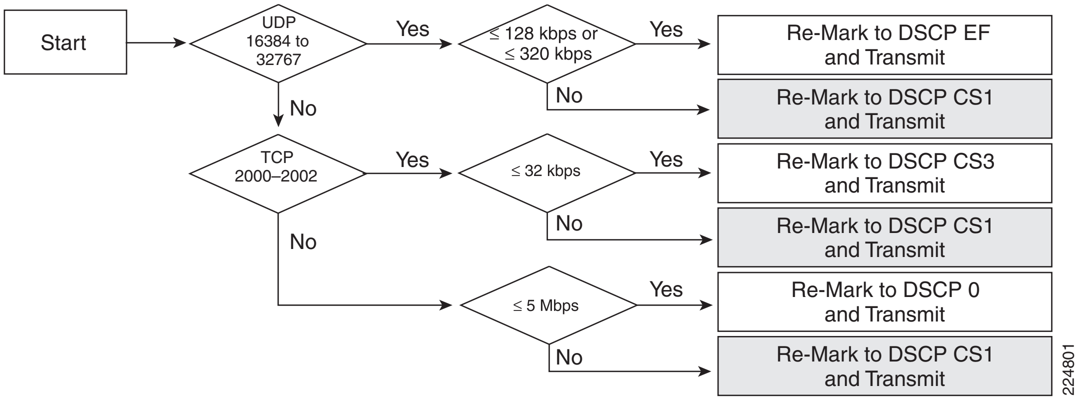
A policer is recommended in this case because limits on the amount of traffic being marked can then be imposed to prevent abuse. Cisco SoftPhones can use regular G.711 codecs, in which case 128 kbps is adequate, or they can be configured use a G.722 (wide codec), in which case 320 kbps is required. The tighter the policer the better, provided that adequate bandwidth has been allocated for application requirements.

Additionally, you can explicitly define the UDP ports used by Cisco SoftPhone within the application as opposed to simply picking random ports within the UDP range of 16383–32767. This is recommended because this allows for a more granular access list to match legitimate Cisco SoftPhone traffic, thereby tightening the overall security of the policy.

Note In this context, "Softphone" can be used to refer to any PC-Based IP Telephony application, including Cisco IP Communicator and similar products.

The logic of such an access edge policer marking Cisco Softphone traffic from an untrusted PC endpoint is shown in Figure 2-4.

Figure 2-4 Untrusted Endpoint Policing —PC + SoftPhone + Scavenger Model


Start
UDP 16384 to 32767
Yes
≤ 128 kbps or ≤ 320 kbps
Yes
Re-Mark to DSCP EF and Transmit
No
Re-Mark to DSCP CS1 and Transmit
No
TCP 2000–2002
Yes
≤ 32 kbps
Yes
Re-Mark to DSCP CS3 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
No
≤ 5 Mbps
Yes
Re-Mark to DSCP 0 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
224801

The syntax for implementing such a policer may vary slightly from platform to platform, as is detailed in the subsequent platform-specific sections.

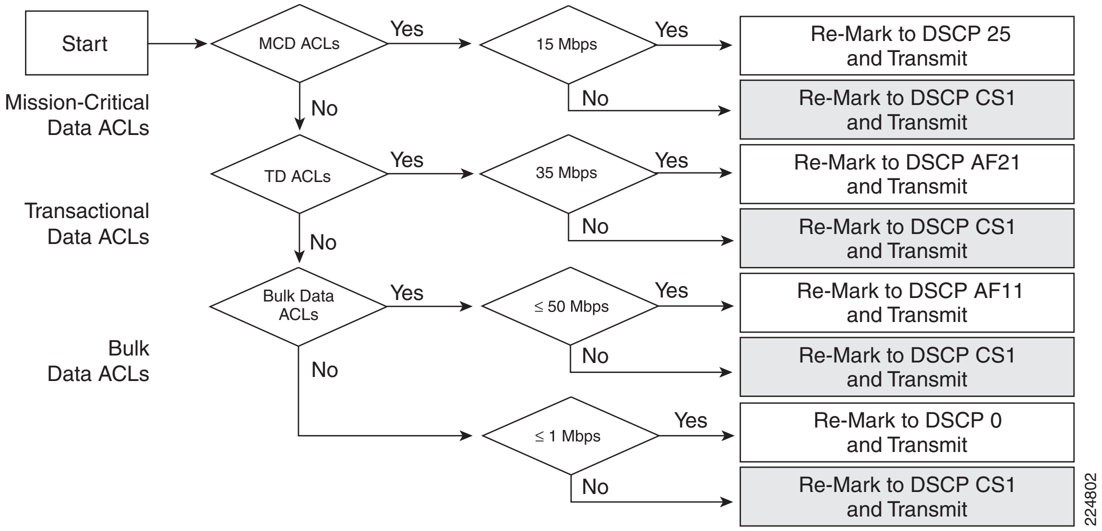
Untrusted Server with Scavenger-Class QoS

Servers as well as PCs are subject to attack and infection by worms and viruses, so these should also be policed as to the amounts of traffic they admit onto the network. The values are greater than PC endpoints and so network administrators should profile traffic patterns from servers to establish a baseline of normal and abnormal behavior.

For an example, assume a single server is running multiple applications, in this case SAP (TCP ports 3200–3203 and also 3600), Lotus Notes (TCP port 1352), and IMAP (TCP ports 143 and 220). SAP is considered a mission-critical application and until call signaling marking on IP telephony equipment fully migrates from DSCP AF31 to CS3 it should be marked to DSCP 25. Lotus Notes is classed as a Transactional Data application and should be marked to DSCP AF21. IMAP is considered a Bulk application and should be marked to DSCP AF11.

Application baselining has shown that 95 percent of the traffic rates for SAP, Lotus Notes and IMAP are less than 15 Mbps, 35 Mbps and 50 Mbps, respectively. To ensure that no other traffic comes from the server, a final policer to catch any other type traffic is included. In the event of legitimate traffic that temporarily exceeds these values, no dropping or re-ordering of packets occurs. However, should this server become infected and begin sending sustained traffic in excess of these normal rates, the excess is subject to aggressive dropping in the event of link congestion. The logic of such a policer is shown in Figure 2-5.

Figure 2-5 Untrusted Endpoint Policing—Multi-Application Server + Scavenger Model


Start
Mission-Critical Data ACLs
MCD ACLs
Yes
No
15 Mbps
Yes
No
Re-Mark to DSCP 25 and Transmit
Re-Mark to DSCP CS1 and Transmit
Transactional Data ACLs
TD ACLs
Yes
No
35 Mbps
Yes
No
Re-Mark to DSCP AF21 and Transmit
Re-Mark to DSCP CS1 and Transmit
Bulk Data ACLs
Bulk Data ACLs
Yes
No
≤ 50 Mbps
Yes
No
Re-Mark to DSCP AF11 and Transmit
Re-Mark to DSCP CS1 and Transmit
≤ 1 Mbps
Yes
No
Re-Mark to DSCP 0 and Transmit
Re-Mark to DSCP CS1 and Transmit
224802

Remember that when deploying QoS designs for untrusted servers, the applications are usually identified by source ports, and not destination ports (as is the case with client-to-server access lists). Thus the access list becomes:

```
permit [tcp | udp] any [eq | range] any
```

as opposed to:

```
permit [tcp | udp] any any [eq | range]
```

This is a subtle but critical difference.

Conditionally-Trusted Endpoints

This section includes the following topics:

- Cisco IP Phones
- Cisco AutoQoS—VoIP
- Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model
- Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model

One of the main business advantages of IP telephony is the simplicity and related cost savings of user adds/moves/changes. To move, a user simply picks up their IP phone, plugs it in at his or her new location and carries on business as usual. If their infrastructure supports inline power, it is literally a matter of unplugging a single RJ-45 cable and plugging it in at the new location.

IP phones are trusted devices, while PCs are not. This can be a problem when provisioning trust in a mobile environment. Consider the following example: Port A is configured to trust the endpoint connected to it, which initially is an IP phone. Port B is configured not to trust the endpoint connected to it, which initially is a PC. Because of a move, these endpoints get plugged into the opposite ports. This breaks the VoIP quality of calls made from the IP phone (now plugged into untrusted Port B) and opens the network up for unintentional or deliberate abuse of provisioned QoS by the PC (now plugged into the trusted Port A).

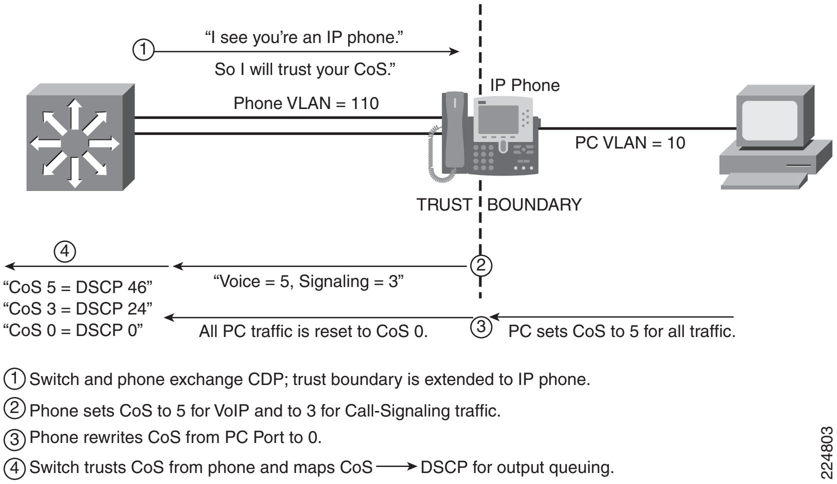
One solution is to place a call to the networking help desk when the move is scheduled, so that the switch ports can be reconfigured to trust/untrust the endpoints as required. However, this approach dampens the mobility business advantage of IP telephony, since manual network administration is then be required to complete the move.

Another solution is to have an intelligent exchange of information between the switch and the devices plugged into their ports. If the switch discovers a device that is trustworthy, then it can extend trust to it dynamically; if not, then not.

Cisco IP Phones use the latter solution. In the current Cisco implementation, the intelligent exchange of information is performed using Cisco Discovery Protocol (CDP).

Figure 2-6 shows a conditional trust boundary extension granted to an IP Phone that has passed a CDP exchange.

Figure 2-6 Conditionally-Trusted Endpoint—Trust Boundary Extension and Operation


1
"I see you're an IP phone."
So I will trust your CoS."
Phone VLAN = 110
IP Phone
PC VLAN = 10
TRUST BOUNDARY
4
"CoS 5 = DSCP 46"
"CoS 3 = DSCP 24"
"CoS 0 = DSCP 0"
2
"Voice = 5, Signaling = 3"
All PC traffic is reset to CoS 0.
3
PC sets CoS to 5 for all traffic.
1 Switch and phone exchange CDP; trust boundary is extended to IP phone.
2 Phone sets CoS to 5 for VoIP and to 3 for Call-Signaling traffic.
3 Phone rewrites CoS from PC Port to 0.
4 Switch trusts CoS from phone and maps CoS ⟶ DSCP for output queuing.
224803

The sequence shown in Figure 2-6 is the following:

1. Switch and phone exchange CDP; trust boundary is extended to IP Phone.
2. Phone sets CoS to 5 for VoIP and to 3 for call signaling traffic.
3. Phone rewrites CoS from PC to 0.
4. Switch trusts CoS from phone and maps CoS to DSCP for output queuing.

CDP is a lightweight, proprietary protocol engineered to perform neighbor discovery. It was never intended as a security or authentication protocol. Therefore, to improve the security of conditional trust extension, the next generation of Cisco IP Telephony products will incorporate the use of advanced protocols to perform authentication.

Cisco IP Phones

The following overview of some of the main IP Phones helps to explain their impact on access edge QoS design.

- Cisco 7902G— The 7902G is an entry-level IP phone that addresses the voice¬communication needs of areas where only a minimal amount of features is required, such as lobbies, hallways, and break rooms. These phones probably would not be moved. The 7902G has only a single 10BASE-T Ethernet port on the back of the phone; therefore, there is no hardware support to connect a PC to it.

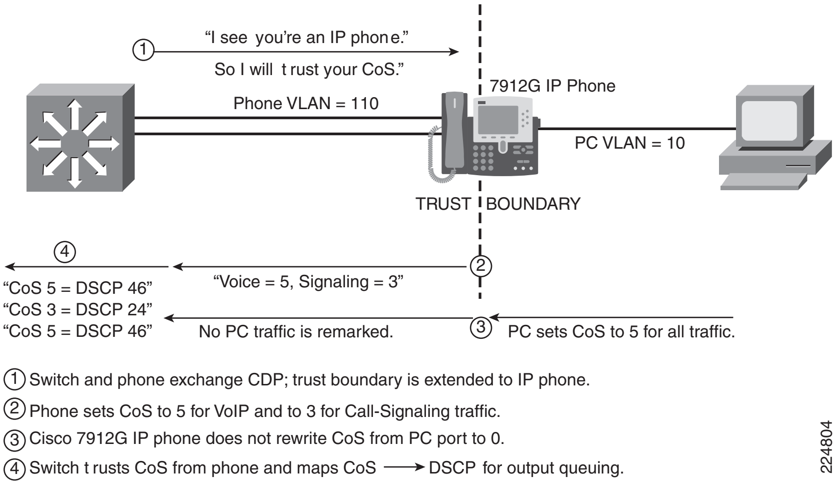
- Cisco 7905G—The 7905G is a basic IP phone that addresses the voice communication needs of a cubicle worker who conducts low to medium telephone traffic. The Cisco 7905G has only a single 10BASE-T Ethernet port on the back of the phone; therefore, there is no hardware support to connect a PC to it.
- Cisco 7910G and 7910G+SW—The 7910G and 7910G+SW IP phones address the voice-communication needs associated with a reception area, lab, manufacturing floor, or employee with a minimal amount of telephone traffic. The only difference between the Cisco 7910G and the Cisco 7910G+SW is that the former has a single 10BASE-T Ethernet port (therefore, there is no hardware support to connect a PC to it), and the latter has two 10/100BASE-T Ethernet ports, which allow a PC to be connected to the IP phone.
- Cisco 7912G—The 7912G is a basic IP phone that addresses the voice-communication needs of a cubicle worker who conducts low to medium telephone traffic. The 7912G supports inline power and an integrated 10/100 Ethernet switch for connecting a PC. The switch used in the 7912G has the capability to mark CoS and DSCP of Voice and Call Signaling traffic that originates from the IP phone, but ***the Cisco 7912G does not have the capability to re-mark CoS values of PC-generated traffic***.
- Cisco 7940G—The 7940G IP phone is suited best for an employee in a basic office cubicle environment—a transaction-type worker, for example—who conducts a medium amount of business by telephone. The 7940G supports inline power and has an integrated 10/100 Ethernet switch for connecting a PC.
- Cisco 7960G—The 7960G is designed to meet the communication needs of a profes¬sional worker in an enclosed office environment—an employee who experiences a high amount of phone traffic in the course of a business day. The 7960G supports inline power and has an integrated 10/100 Ethernet switch for connecting a PC.
- Cisco 7970G—The 7970G not only addresses the needs of the executive or major decision maker, but also brings network data and applications to users without PCs. This IP phone includes a backlit, high-resolution color touch-screen display. Cur¬rently, Cisco 7970G is the only Cisco IP phone that supports both Cisco prestandard Power over Ethernet (PoE) and the IEEE 802.3af PoE. The 7970G has an integrated 10/100 Ethernet switch for connecting a PC.

All of the IP Phones listed above have the ability to mark 802.1Q/p CoS values for both VoIP and call signaling (default values are 5 and 3, respectively). Furthermore, they also have the ability to mark DSCP values for both VoIP and call signaling (current defaults are EF and AF31, respectively; future software releases will change these values to EF and CS3, respectively).

IP Phone models 7902G, 7905G and 7910G lack the hardware to connecting a PC behind the Cisco IP Phone. All other IP Phone models listed above (except the 7912G) have the hardware support to connect a PC behind the IP Phone and also support 802.1Q/p CoS remarking of tagged packets that may originate from such PCs.

The 10/100 Ethernet switch built into the 7912G does not have the support to re-mark CoS values that might have been set by a PC, as illustrated in Figure 2-7. This re-marking limitation represents a potential security hole for enterprises deploying these IP phones. However, this hole can be plugged, for the most part, with access-edge policers, as will be detailed in this chapter. It is important to note that if 7912G IP phones are deployed to users that move locations, all user switch ports within the enterprise should have access-edge policers set on them to ensure mobility and security if a 7912G user moves the phones to another port.

Figure 2-7 Conditionally-Trusted Endpoint—Cisco 7912G Trust Boundary Extension and Operation


1
"I see you're an IP phone."
So I will trust your CoS."
Phone VLAN = 110
7912G IP Phone
PC VLAN = 10
TRUST BOUNDARY
4
"CoS 5 = DSCP 46"
"CoS 3 = DSCP 24"
"CoS 5 = DSCP 46"
"Voice = 5, Signaling = 3"
2
No PC traffic is remarked.
3
PC sets CoS to 5 for all traffic.
1 Switch and phone exchange CDP; trust boundary is extended to IP phone.
2 Phone sets CoS to 5 for VoIP and to 3 for Call-Signaling traffic.
3 Cisco 7912G IP phone does not rewrite CoS from PC port to 0.
4 Switch trusts CoS from phone and maps CoS → DSCP for output queuing.
224804

The sequence as shown in Figure 2-7 is as follows:

1. Switch and phone exchange CDP; trust boundary is extended to IP Phone
2. Phone sets CoS to 5 for VoIP and to 3 for call signaling traffic.
3. Cisco 7912G IP Phone does not rewrite CoS from PC port to 0
4. Switch trusts CoS from phone and maps CoS to DSCP for output queuing

AutoQoS—VoIP

When the main business objective of the QoS deployment is to enable QoS for IP Telephony only (i.e., without Scavenger-class QoS), then the network administrator may choose to take advantage of the Cisco AutoQoS VoIP feature.

AutoQoS VoIP is essentially an intelligent macro that enables an administrator to enter one or two simple AutoQoS commands to enable all the appropriate features for the recommended QoS settings for an VoIP and IP Telephony for a specific platform and/or a specific interface.

AutoQoS VoIP automatically configures the best-practice QoS configurations (based on previous Cisco Enterprise QoS SRNDs) for VoIP on Cisco Catalyst switches and IOS routers. By entering one global and/or one interface command (depending on the platform), the AutoQoS VoIP macro then would expand these commands into the recommended VoIP QoS configurations (complete with all the calculated parameters and settings) for the platform and interface on which the Auto-QoS VoIP macro is applied.

For example, on Cisco Catalyst switches, AutoQoS performs the following automatically:

- Enforces a conditional-trust boundary with any attached Cisco IP phones
- Enforces a trust boundary on Catalyst switch access ports and uplinks/downlinks
- Modifies CoS-to-DSCP (and IP Precedence-to-DSCP) mappings, as required
- Enables Catalyst strict priority queuing for voice (CoS 5/DSCP EF) and preferential queuing for Call-Signaling traffic (CoS 3/DSCP CS3)
- Enables best-effort queuing for all other data (CoS 0/DSCP 0) traffic
- Modifies queue admission criteria (such as CoS-to-queue mapping)

- Modifies queue sizes and queue weights, where required

The standard (interface) configuration commands to enable AutoQoS are: **auto qos voip**. Depending on the platform, AutoQoS VoIP can support the following additional keyword commands:

- **cisco-phone**—When you enter the **auto qos voip cisco-phone** interface configuration command on a port at the edge of a network that is connected to a Cisco IP Phone, the switch enables the conditional-trusted boundary feature. The switch uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP Phone. When a Cisco IP Phone is detected, the ingress classification on the interface is set to trust the CoS marking of the received packet. When a Cisco IP Phone is absent, the ingress classification is set to not trust the CoS (or DSCP) value of any packet.
- **cisco-softphone**—When you enter the **auto qos voip cisco-softphone** interface configuration command on a port at the edge of the network that is connected to a device running the Cisco SoftPhone, the switch uses policing to decide whether a packet is in or out of profile and to specify the action on the packet. If the packet does not have a DSCP value of 24, 26, or 46 or is out of profile, the switch changes the DSCP value to 0.
- **trust** —When you enter the **auto qos voip trust** interface configuration command on a port connected to the interior of the network, the switch trusts the CoS value in ingress packets (the assumption is that traffic has already been classified by other edge devices).

The AutoQoS commands and optional keywords are shown on a per-platform basis in the platform-specific design sections of this chapter.

Additionally, it should be pointed out that AutoQoS VoIP can also be viewed as a template which may be modified and expanded on to support additional classes of applications. In this manner, the AutoQoS VoIP feature can be used to quickly and accurately deploy 80% (or more) of the desired solution, which then can be manually customized further to tailor to the specific customer requirements.

Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model

In this model, trust of CoS markings is extended to CDP-verified IP Phones. An additional layer of protection can be offered by access edge policers. As stated previously, the tighter the policers the better, provided that adequate bandwidth is permitted for legitimate applications. The most granular policing can be achieved by the use of per-port/per-VLAN policers.

Note Currently, only the Catalyst 3550 family supports per-port/per-VLAN policing as a feature. Other platforms have already committed to supporting this feature in the near future. For platforms that do not yet support this feature, equivalent logic can be achieved by including subnet information within the access lists being referenced by the class maps. Such examples are provided later in this chapter.

For example, the peak amounts of legitimate traffic originating from the voice VLAN (VVLAN) on a per-port basis are:

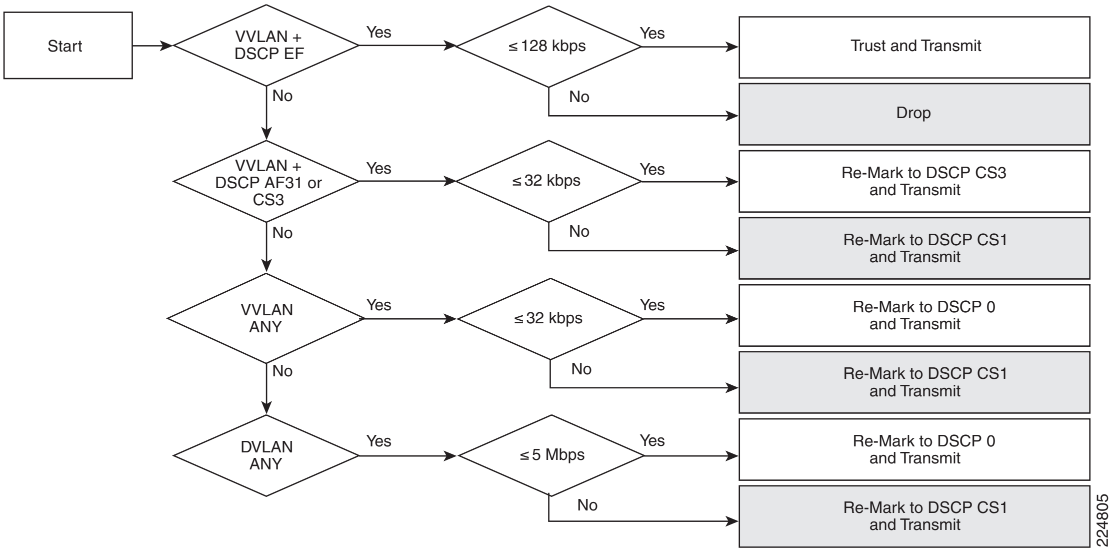
- 128 kbps for Voice traffic, marked CoS 5/DSCP EF (320 kbps in the case of G.722 codecs)
- 32 kbps for call signaling traffic (marked CoS 3/DSCP AF31 or CS3)
- 32 kbps of Best Effort services traffic (marked CoS 0)

There should not be any other traffic originating from the VVLAN, so the policer can be configured to remark anything else from the VVLAN because such traffic is considered illegitimate and indicative of an attack.

These policers can then be combined with a policer to meter traffic from the data VLAN (DVLAN), marking down traffic in excess of 5 percent (5 Mbps for FE ports) to Scavenger/CS1.

The logic of these policers is shown in Figure 2-8.

Figure 2-8 Conditionally-Trusted Endpoint Policing—IP Phone + PC + Scavenger (Basic) Model


Start
VVLAN + DSCP EF
Yes
≤ 128 kbps
Yes
Trust and Transmit
No
No
Drop
VVLAN + DSCP AF31 or CS3
Yes
≤ 32 kbps
Yes
Re-Mark to DSCP CS3 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
VVLAN ANY
Yes
≤ 32 kbps
Yes
Re-Mark to DSCP 0 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
DVLAN ANY
Yes
≤ 5 Mbps
Yes
Re-Mark to DSCP 0 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
224805

Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model

Building on the previous model, you can add additional marking and policing for PC-based video-conferencing and multiple levels of data applications.

Desktop videoconferencing applications use the same UDP port range by default as does Cisco SoftPhone. If the UDP ports used by the desktop videoconferencing application can be explicitly defined within the application, as with SoftPhone, then you can use two policers: one for IP/VC and another for SoftPhone. Otherwise, a single policer covering the UDP port range of 16384–32767 is required, which would be provisioned for the worst-case scenario of legitimate traffic. In this case, this is the videoconferencing application's requirement of 500 kbps (for a 384 kbps desktop IP/VC application), as compared to the SoftPhone requirement of 128 kbps (or 320 kbps for G.722 codecs).

Note Policer thresholds should be set according to the video application's requirements. Some interactive-video applications may have higher bandwidth requirements for their codecs; for example Cisco Video Telephony (VT) Advantage includes a proprietary codec that requires 7 Mbps of bandwidth.

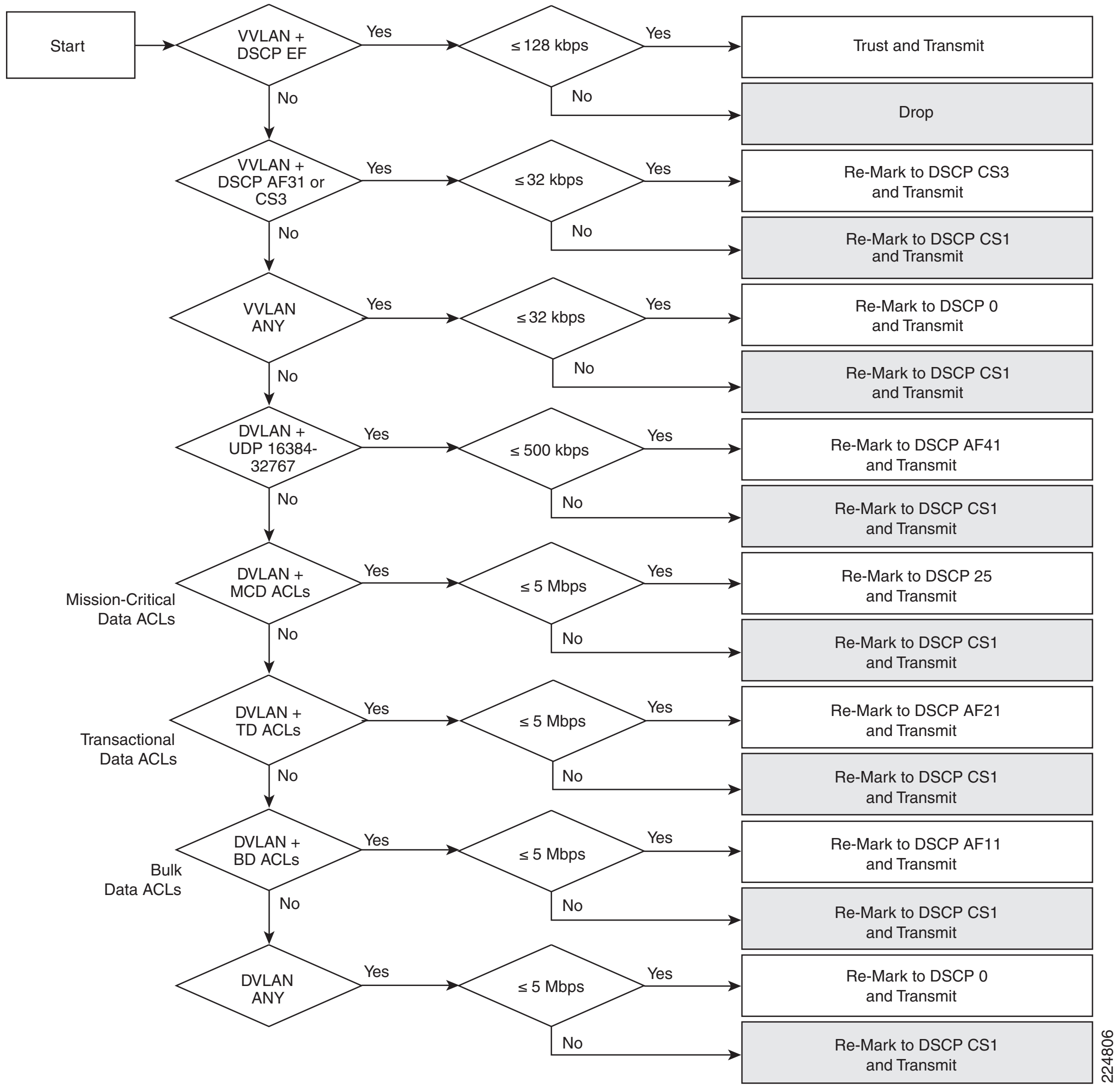
You can add additional data VLAN policers to meter Mission-Critical Data, Transactional Data and Bulk Data flows. Each of these classes can be policed on ingress to the switch port to an in-profile amount, such as 5 percent each.

Note Since Mission-Critical and Transactional Data applications are interactive foreground applications requiring user input, it is highly unlikely that both of these types of applications will be simultaneously generating 5 Mbps each from a client PC. However, in the rare case that they are, these flows will be policed further by any per-user microflow policing policies that may be deployed on distribution layer Catalyst 6500 Supervisor 720s (PFC3s), as is detailed later in this chapter.

Another factor to keep in mind is that certain Catalyst platforms allow only up to 8 policers per FastEthernet port. Therefore, the model presented here is made to conform to this constraint to make it more generic and modular. For this reason, a separate policer has not been defined for call signaling traffic from Softphone. An access list to identify such traffic could be included within the Mission-Critical Data access lists, which is detailed in the configuration examples presented later in this chapter.

The logic of these advanced policers is shown in Figure 2-9.

Figure 2-9 Conditionally-Trusted Endpoint Policing—IP Phone + PC + Scavenger (Advanced) Model


Start
VVLAN + DSCP EF
Yes
≤ 128 kbps
Yes
Trust and Transmit
No
No
Drop
VVLAN + DSCP AF31 or CS3
Yes
≤ 32 kbps
Yes
Re-Mark to DSCP CS3 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
VVLAN ANY
Yes
≤ 32 kbps
Yes
Re-Mark to DSCP 0 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
DVLAN + UDP 16384-32767
Yes
≤ 500 kbps
Yes
Re-Mark to DSCP AF41 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
Mission-Critical Data ACLs
DVLAN + MCD ACLs
Yes
≤ 5 Mbps
Yes
Re-Mark to DSCP 25 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
Transactional Data ACLs
DVLAN + TD ACLs
Yes
≤ 5 Mbps
Yes
Re-Mark to DSCP AF21 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
Bulk Data ACLs
DVLAN + BD ACLs
Yes
≤ 5 Mbps
Yes
Re-Mark to DSCP AF11 and Transmit
No
No
Re-Mark to DSCP CS1 and Transmit
DVLAN ANY
Yes
≤ 5 Mbps
Yes
Re-Mark to DSCP 0 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
224806

Legend for Figure 2-9:

- MCD = Mission Critical Data
- TD = Transactional Data
- BD = Bulk Data

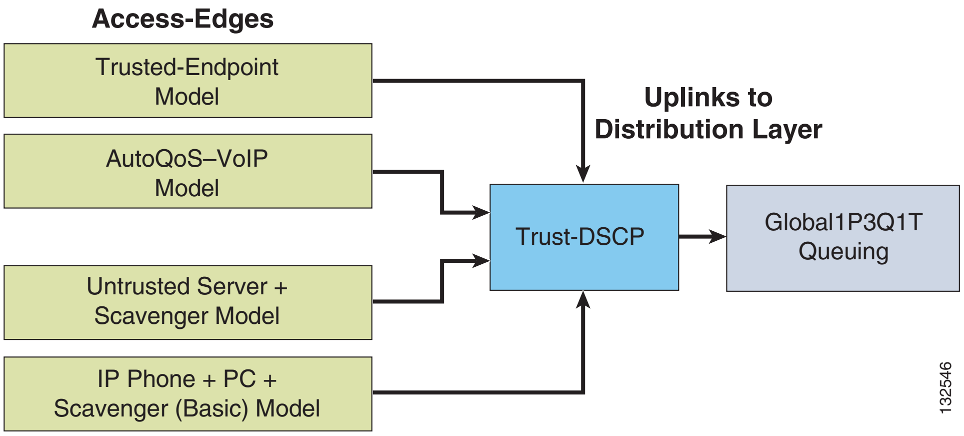
Catalyst 2950—QoS Considerations and Design

This section includes the following topics:

- Catalyst 2950—Trusted Endpoint Model
- Catalyst 2950—AutoQoS VoIP Model
- Catalyst 2950—Untrusted PC + SoftPhone with Scavenger-Class QoS Model
- Catalyst 2950—Untrusted Server with Scavenger-Class QoS Model
- Catalyst 2950—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model
- Catalyst 2950—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model
- Catalyst 2950—Queuing

The Catalyst 2950 does not support Layer 3 forwarding, and as such is only applicable as a low-end access layer switch. The QoS design options for a Catalyst 2950 are shown in Figure 2-10.

Figure 2-10 Access Layer Catalyst 2950 QoS Design Options


Access-Edges
Trusted-Endpoint Model
AutoQoS–VoIP Model
Untrusted Server + Scavenger Model
IP Phone + PC + Scavenger (Basic) Model
Uplinks to Distribution Layer
Trust-DSCP
Global1P3Q1T Queuing
132546

Cisco recommends using the Enhanced Image (EI) versions of IOS software on these platforms because these offer additional QoS features such as MQC/ACL classification options, policing and markdown functions, mapping tables and AutoQoS.

Catalyst 2950—Trusted Endpoint Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Command

Configuration

Configuring a Catalyst 2950 to trust an endpoint is fairly straightforward, as shown below. The trusted endpoint should be assigned either the voice VLAN (VVLAN) or the data VLAN (DVLAN) with the appropriate switchport commands.

Example 2-1 Catalyst 2950—Trusted Endpoint Model Configuration

```
CAT2950(config)#interface FastEthernet0/1
CAT2950(config-if)#mls qos trust dscp
```

Catalyst MLS QoS Verification Command

The **show mls qos interface** verification command reports the configured trust state and the current operating trust mode of a switchport interface.

In this example, the command verifies that interface FastEthernet 0/1 correctly trusts the DSCP values of the endpoint to which it is connected.

Example 2-2 Show MLS QoS Interface Verification of a Switchport Connected to a Trusted Endpoint

```
CAT2950#show mls qos interface FastEthernet0/1
FastEthernet0/1
trust state: trust dscp              ! Configured trust state is to trust DSCP
trust mode: trust dscp               ! Current operating mode is to trust DSCP
COS override: dis
default COS: 0
pass-through: none
trust device: none
CAT2950#
```

Catalyst 2950—AutoQoS VoIP Model

The Catalyst 2950 supports AutoQoS VoIP with the following keyword options:

- **auto qos voip cisco-phone**
- **auto qos voip cisco-softphone**
- **auto qos voip trust**

When you enable AutoQoS VoIP on the Catalyst 2950 by using the **auto qos voip cisco-phone**, the **auto qos voip cisco-softphone**, or the **auto qos voip trust** interface configuration command, the switch automatically generates a QoS configuration based on the traffic type and ingress packet label and applies the commands listed in Table 2-1 to the interface.

Table 2-1 Catalyst 2950 Auto-QoS Generated Configuration

Description	Automatically Generated QoS Command Equivalent
The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value).	CAT2950(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**
If you entered the **auto qos voip trust** command, the switch automatically sets the ingress classification on the interface to trust the CoS value received in the packet.	CAT2950(config-if)# **mls qos trust cos**

Table 2-1 Catalyst 2950 Auto-QoS Generated Configuration

If you entered the **auto qos voip cisco-phone** command, the switch automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP Phone.	CAT2950(config-if)# **mls qos trust device cisco-phone**
If you entered the **auto qos voip cisco-softphone** command, the switch automatically creates class maps and policy maps.	CAT2950(config)# **class-map match-all AutoQoS-VoIP-RTP-Trust** CAT2950(config-cmap)# **match ip dscp 46** CAT2950(config)# **class-map match-all AutoQoS-VoIP-Control-Trust** CAT2950(config-cmap)# **match ip dscp 24 26** CAT2950(config)# **policy-map AutoQoS-Police-SoftPhone** CAT2950(config-pmap)# **class AutoQoS-VoIP-RTP-Trust** CAT2950(config-pmap-c)# **set ip dscp 46** CAT2950(config-pmap-c)# **police 1000000 4096 exceed-action drop** CAT2950(config-pmap)# **class AutoQoS-VoIP-Control-Trust** CAT2950(config-pmap-c)# **set ip dscp 24** CAT2950(config-pmap-c)# **police 1000000 4096 exceed-action drop**
After creating the class maps and policy maps, the switch automatically applies the policy map called *AutoQoS-Police-SoftPhone* to an ingress interface on which auto-QoS with the Cisco SoftPhone feature is enabled.	CAT2950(config-if)# **service-policy input AutoQoS-Police-SoftPhone**
The switch automatically assigns egress queue usage on this interface. The switch enables the egress expedite queue and assigns WRR weights to queues 1, 2, and 3. (The lowest value for a WRR queue is 1. When the WRR weight of a queue is set to 0, this queue becomes an expedite queue.) The switch configures the CoS-to-egress-queue map: • CoS values 0 and 1 select queue 1. • CoS values 2 and 4 select queue 2. • CoS values 3, 6, and 7 select queue 3. • CoS value 5 selects queue 4.	CAT2950(config)# **wrr-queue bandwidth 10 20 70 1** CAT2950(config)# **no wrr-queue cos-map** CAT2950(config)# **wrr-queue cos-map 1 0 1** CAT2950(config)# **wrr-queue cos-map 2 2 4** CAT2950(config)# **wrr-queue cos-map 3 3 6 7** CAT2950(config)# **wrr-queue cos-map 4 5**

Catalyst 2950—Untrusted PC + SoftPhone with Scavenger-Class QoS Model

The Catalyst 2950 does not support the **range** keyword within an ACL when the ACL is being referenced by a MQC class-map. Therefore, a policy to mark UDP flows in the port range of 16384 through 32767 cannot be configured on the Catalyst 2950.

A possible workaround to this limitation would be to pre-set the port(s) to be used by SoftPhone within the application itself. In such a case, these ports would have to be discretely matched by ACL entries on the Catalyst 2950. Furthermore, each port being used for call signaling would also require a discrete ACL entry.

However, even in the case where all these ports are buttoned down and discrete ACLs are configured on the Catalyst 2950 to match them, another limitation of the switch would come into play. Specifically, the Catalyst 2950 can only support policing in 1 Mbps increments on FastEthernet ports. Such lax policing would leave a fairly large hole to allow unauthorized traffic that may be mimicking Voice or call signaling to be admitted onto the network.

Due to these limitations, it is not recommended to use a Catalyst 2950 to support an untrusted PC running SoftPhone.

Catalyst 2950—Untrusted Server with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

For the most part, the Catalyst 2950 can support the Untrusted Multi-Application Server + Scavenger Model as illustrated in Figure 2-5. Only the final element of the logical model, namely the policing of all other traffic to 1 Mbps (remarking traffic in excess of this limit to CS1) is not supported on the Catalyst 2950.

The main platform-specific caveats that should be kept in mind when deploying this model on the Catalyst 2950 are the following:

- Non-standard DSCP values are not supported; therefore, Mission-Critical Data traffic cannot be marked to DSCP 25 on Catalyst 2950s (a temporary recommendation during the interim of Cisco’s call signaling marking migration from AF31 to CS3); such application traffic can alternatively be marked to the more general class of Transactional Data (AF21), of which they are a subset.
- The **mls qos cos override** interface command must be used to ensure that untrusted CoS values are explicitly set 0 (default).
- The **range** keyword cannot be used in the ACLs being referenced by the class-maps; server-ports should be explicitly defined with a separate access list entry (ACE) per TCP/UDP port.
- User-defined masks must be consistent for all ACLs being referenced by class maps (if filtering is being done against TCP/UDP ports, then all Access Control Entries (ACEs) should be set to filter by TCP/UDP ports, as opposed to some ACEs filtering by ports and others by subnet or host addresses).
- System-defined masks (such as **permit ip any any**) cannot be used in conjunction with user-defined masks (such as **permit tcp any any eq 3200**) within the same policy map; therefore, if some traffic is being matched against TCP/UDP ports, then a final ACL cannot be used to match all other traffic via a **permit ip any any** statement).
- The Catalyst 2950 IOS implementation of MQC’s class-default does not (at the time of writing) function compatibly with mainline IOS; class-default should apply a policy to all other traffic not explicitly defined, but testing has shown that this is not the case.

Example 2-3 Catalyst 2950—Untrusted Multi-Application Server with Scavenger-Class QoS Model Configuration

```
CAT2950(config)#class-map SAP
CAT2950(config-cmap)# match access-group name SAP
CAT2950(config-cmap)#class-map LOTUS
CAT2950(config-cmap)# match access-group name LOTUS
CAT2950(config-cmap)#class-map IMAP
CAT2950(config-cmap)# match access-group name IMAP
CAT2950(config-cmap)#exit
CAT2950(config)#
CAT2950(config)#policy-map UNTRUSTED-SERVER
CAT2950(config-pmap)#  class SAP
CAT2950(config-pmap-c)#    set ip dscp 18                   ! DSCP 25 is not supported
CAT2950(config-pmap-c)#    police 15000000 8192 exceed-action dscp 8
     ! Out-of-profile Mission-Critical is marked down to Scavenger (CS1)
CAT2950(config-pmap-c)#  class LOTUS
CAT2950(config-pmap-c)#    set ip dscp 18                   ! Transactional is marked AF21
CAT2950(config-pmap-c)#    police 35000000 8192 exceed-action dscp 8
     ! Out-of-profile Transactional Data is marked down to Scavenger (CS1)
CAT2950(config-pmap-c)#  class IMAP
CAT2950(config-pmap-c)#    set ip dscp 10                   ! Bulk Data is marked AF11
CAT2950(config-pmap-c)#    police 50000000 8192 exceed-action dscp 8
     ! Out-of-profile Bulk Data is marked down to Scavenger (CS1)
CAT2950(config-pmap-c)#exit
CAT2950(config-pmap)#exit
CAT2950(config)#
CAT2950(config)#interface FastEthernet0/1
CAT2950(config-if)# mls qos cos override                ! Untrusted CoS is remarked to 0
CAT2950(config-if)# service-policy input UNTRUSTED-SERVER
CAT2950(config-if)#exit
CAT2950(config)#
CAT2950(config)#ip access list  extended SAP
CAT2950(config-ext-nacl)# permit tcp any eq 3200 any
CAT2950(config-ext-nacl)# permit tcp any eq 3201 any
CAT2950(config-ext-nacl)# permit tcp any eq 3202 any
CAT2950(config-ext-nacl)# permit tcp any eq 3203 any
CAT2950(config-ext-nacl)# permit tcp any eq 3600 any
CAT2950(config-ext-nacl)#
CAT2950(config-ext-nacl)#ip access list  extended LOTUS
CAT2950(config-ext-nacl)# permit tcp any eq 1352 any
CAT2950(config-ext-nacl)#
CAT2950(config-ext-nacl)#ip access list  extended IMAP
CAT2950(config-ext-nacl)# permit tcp any eq 143 any
CAT2950(config-ext-nacl)# permit tcp any eq 220 any
CAT2950(config-ext-nacl)#end
CAT2950#
```

Catalyst MLS QoS Verification Commands

This section includes the following Catalyst MLS verification commands:

- show mls qos interface policers
- show class-map and show policy-map
- show mls masks qos

show mls qos interface policers

The **show mls qos interface policers** verification command reports all configured policers attached to the specified interface.

In the following example, the policers defined for Mission-Critical data, Transactional Data and Bulk data which are applied to FastEthernet 0/1 are confirmed.

Example 2-4 Show MLS QoS Interface Policers Verification of a Switchport Connected to an Untrusted Multi-Application Server

```
CAT2950#show mls qos interface FastEthernet0/1 policers
FastEthernet0/1
policymap=UNTRUSTED-SERVER
type=Single rate=15000000, burst=8192                ! Mission-Critical Data Policer
type=Single rate=35000000, burst=8192                ! Transactional Data Policer
type=Single rate=50000000, burst=8192                ! Bulk Data Policer
CAT2950#
```

show class-map and show policy-map

The **show class-map** and **show policy-map** verification commands will report the class-map and policy-maps that have been globally configured (regardless of whether or not they've been applied to an interface).

In the following example, the class-maps for SAP, LOTUS and IMAP are displayed, as is the policy-map UNTRUSTED-SERVER that is referencing these.

Example 2-5 Show Class-Map and Show Policy-Map Verification of a Switch Connected to an Untrusted Multi-Application Server

```
CAT2950#show class-map
 Class Map match-all IMAP (id 3)
   Match access-group name IMAP

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all SAP (id 1)
   Match access-group name SAP

 Class Map match-all LOTUS (id 2)
   Match access-group name LOTUS

CAT2950#show policy-map
 Policy Map UNTRUSTED-SERVER
  class  SAP
   set ip dscp 18
   police 15000000 8192 exceed-action dscp 8
  class  LOTUS
   set ip dscp 18
   police 35000000 8192 exceed-action dscp 8
  class  IMAP
   set ip dscp 10
   police 50000000 8192 exceed-action dscp 8
CAT2950#
```

show mls masks qos

The **show mls masks qos** verification command is helpful in keeping track of the number of user-defined or system-defined masks that are being applied by access list entries that are referenced by MQC class-maps.

In the example below, the ACEs being referenced by QoS policies are using IP protocol masks, including (TCP/UDP) source ports.

Example 2-6 Show MLS Masks QoS Verification of an Untrusted Multi-Application Server Model

```
CAT2950#show mls masks qos
Mask1
    Type : qos
    Fields : ip-proto, src-port
    Policymap : UNTRUSTED-SERVER
        Interfaces : Fa0/1
CAT2950#
```

Catalyst 2950—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

When configuring an access-switch to trust/conditionally-trust CoS, then the default mapping for CoS 5 should be adjusted to point to DSCP EF (46), instead of DSCP CS5 (40). This modification is shown below.

Example 2-7 Catalyst 2950—CoS-to-DSCP Marking Modification for Voice

```
CAT2950(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56           ! Maps CoS 5 to EF
CAT2950(config)#
```

Note Adjusting the default CoS-to-DSCP mapping for call signaling (which formerly was mapped from CoS 3 to DSCP AF31/26) is no longer required. This is because the default mapping of CoS 3 points to DSCP CS3 (24), which is the call signaling marking that all Cisco IP Telephony devices markings will migrate to.

Catalyst MLS QoS Verification Commands

The **show mls qos map [cos-dscp | dscp-cos]** verification command returns the DSCP-to-CoS and CoS-to-DSCP mappings. These mappings may be either the default mappings or manually configured overrides.

In the example below, the default mapping for CoS 5 (DSCP CS5) has been modified to point to DSCP EF instead.

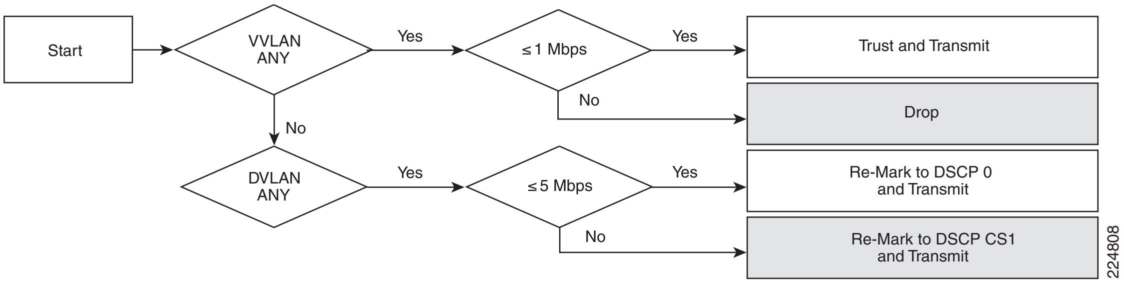
Example 2-8 Show MLS QoS Map Verification for a Catalyst 2950 Switch

```
CAT2950#show mls qos map
   Dscp-cos map:
       dscp:   0  8 10 16 18 24 26 32 34 40 46 48 56
     -----------------------------------------------
```

```
        cos:   0  1  1  2  2  3  3  4  4  5  5  6  7
   Cos-dscp map:
        cos:   0  1  2  3  4  5  6  7
     --------------------------------
       dscp:   0  8 16 24 32 46 48 56                  ! CoS 5 is now mapped to DSCP EF
CAT2950#
```

The Catalyst 2950's hardware policers lack the granularity to implement the Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model, as illustrated in Figure 2-8. However, they can implement a simplified version of this model, as shown in Figure 2-11.

Figure 2-11 Catalyst 2950—Conditionally-Trusted Endpoint Policing: IP Phone + PC with Scavenger-Class QoS (Basic) Model



It should be kept in mind that the coarse granularity of the Catalyst 2950's policers (which are configured in 1 Mbps minimum increments on FastEthernet interfaces) could potentially allow up to 1 Mbps of traffic mimicking legitimate voice traffic per conditionally-trusted switchport.

The configuration for configuring a switchport to conditionally trust an IP Phone that has a PC connected to it, with Scavenger-class QoS, is shown below.

Example 2-9 Catalyst 2950—Conditionally Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model

```
CAT2950(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56          ! Maps CoS 5 to EF
CAT2950(config)#
CAT2950(config)#class-map VVLAN-ANY
CAT2950(config-cmap)# match access-group name VVLAN-ANY
CAT2950(config-cmap)#class-map DVLAN-ANY
CAT2950(config-cmap)# match access-group name DVLAN-ANY
CAT2950(config-cmap)#exit
CAT2950(config)#
CAT2950(config)#policy-map IPPHONE+PC
CAT2950(config-pmap)#  class VVLAN-ANY
CAT2950(config-pmap-c)#    police 1000000 8192 exceed-action drop
    ! Out-of-profile traffic from the VVLAN is dropped
CAT2950(config-pmap-c)#  class DVLAN-ANY
CAT2950(config-pmap-c)#    set ip dscp 0
    ! Optional remarking in case the trust boundary is compromised
CAT2950(config-pmap-c)#    police 5000000 8192 exceed-action dscp 8
    ! Out-of-profile data traffic is marked down to Scavenger
CAT2950(config-pmap-c)#exit
CAT2950(config-pmap)#exit
CAT2950(config)#
CAT2950(config)#
CAT2950(config)#interface FastEthernet0/1
CAT2950(config-if)# switchport access vlan 10
CAT2950(config-if)# switchport voice vlan 110
CAT2950(config-if)# mls qos trust device cisco-phone              ! Conditional trust
CAT2950(config-if)# mls qos trust cos                         ! Trust CoS from IP Phone
```

```
CAT2950(config-if)# service-policy input IPPHONE+PC                ! Policing policy
CAT2950(config-if)#exit
CAT2950(config)#
CAT2950(config)#ip access list  standard VVLAN-ANY
CAT2950(config-std-nacl)# permit 10.1.110.0 0.0.0.255              ! VVLAN subnet
CAT2950(config-std-nacl)#
CAT2950(config-std-nacl)#ip access list  standard DVLAN-ANY
CAT2950(config-std-nacl)# permit 10.1.10.0 0.0.0.255               ! DVLAN subnet
CAT2950(config-std-nacl)#end
CAT2950#
```

Other Catalyst MLS QoS verification commands include the following:

- show mls qos interface
- show mls qos interface policers
- show mls qos map
- show class-map
- show policy-map
- show mls masks qos

Catalyst 2950—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model

The advanced model of the Conditionally-Trusted IP Phone + PC with Scavenger-class QoS, as shown in Figure 2-9 and Figure 2-10, cannot be supported on the Catalyst 2950 because of the previously discussed caveats and limitations of the Catalyst 2950, including the maximum number of policers supported per FE interface, the overly coarse policer granularity, the inability to mix user-defined masks with system-defined masks and other constraints.

Catalyst 2950—Queuing

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

The Catalyst 2950 can be configured to operate in a 4Q1T mode or in a 1P3Q1T mode (with Queue 4 being configured as a strict-priority queue); the 1P3Q1T mode is recommended for converged networks.

The strict priority queue is enabled by configuring the fourth queue's weight parameter, as defined in the **wrr-queue bandwidth** command, to be 0 (as shown in the example below).

The remaining bandwidth is allocated the other queues according to their defined weights. To allocate remaining bandwidths of 5%, 25% and 70% to Queues 1, 2 and 3, weights of 5, 25, 70 can be assigned these queues, respectively. The logic of these bandwidth allocations recommendations will be discussed in more detail momentarily.

Note Alternatively, as these weights are relative, they can be reduced by dividing each weight by the lowest common denominator (in this case 5) to arrive at queue weights of 1, 5 and 14 for Queues 1, 2 and 3 (respectively). Reduction is strictly optional and makes no difference to the servicing of the queues. Many network administrators tend to prefer defining bandwidth allocation ratios as percentages, and so bandwidth weight ratios aren't reduced in this design chapter.

So far, Campus QoS designs have been presented for the first half of the DoS/worm mitigation strategy discussed at the beginning of this chapter, namely, designs for access layer policers to mark down out-of-profile traffic to the Scavenger class PHB of CS1.

The second vital component of this strategy is to map Scavenger class traffic into a "less-than Best-Effort" queuing structure, ensuring that all other traffic will be serviced ahead of it in the event of congestion.

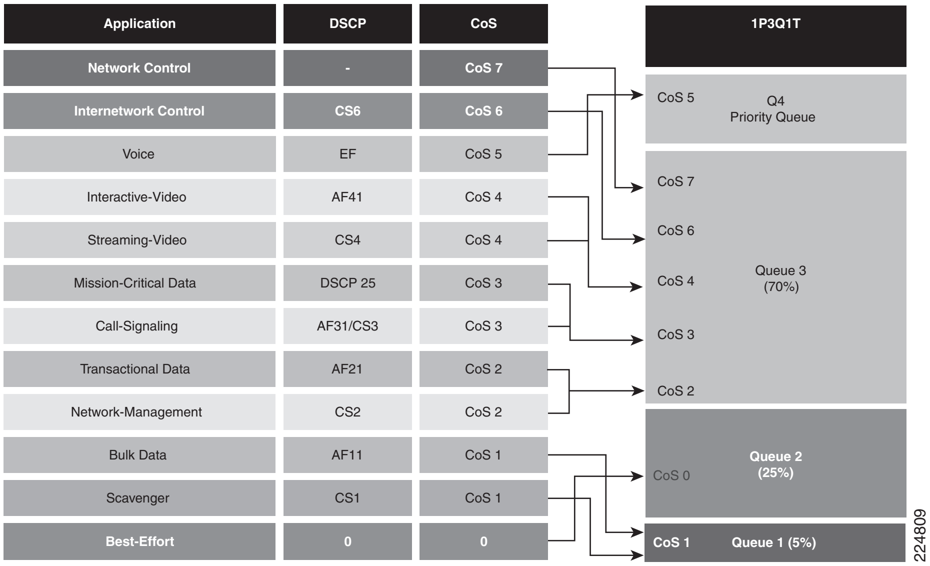
The Catalyst 2950, like most Catalyst platforms, supports the mapping of CoS values into queues. The CoS value that corresponds to Scavenger (DSCP CS1) is CoS 1; this CoS value is shared with Bulk data (DSCP AF11). Therefore, a small amount of bandwidth (5%) is allocated to the "less-than Best-Effort" queue: Q1. Q1 will thus service legitimate Bulk traffic but will constrain out-of-profile Scavenger traffic—which may be the result of a DoS/worm attack—to a small amount (<5%), in the event of congestion.

The next queue, Q2, is then assigned to service Best Effort traffic. A previously discussed design principle regarding Best Effort bandwidth allocation is to allocate approximately 25% of a link's bandwidth to service Best Effort traffic. In this manner the sheer volume of traffic that defaults to Best Effort will continue getting adequate bandwidth, both in the event of momentary campus congestion (due to bursts in the amount of legitimate traffic) and even in the case of a DoS/worm attack.

Preferential applications, such as Transactional Data, Mission-Critical Data, Call-Signaling, Network/Internetwork Control and Management, as well as both Interactive and Streaming Video will be serviced by Q3. Q3 is allocated 70% of the remaining bandwidth (after the PQ has serviced its voice traffic).

The recommended 1P3Q1T queuing model for the Catalyst 2950, along with CoS-to-Queue assignments is illustrated in Figure 2-12.

Figure 2-12 Catalyst 2950 1P3Q1T Queuing Model



Application	DSCP	CoS
Network Control	-	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive-Video	AF41	CoS 4
Streaming-Video	CS4	CoS 4
Mission-Critical Data	DSCP 25	CoS 3
Call-Signaling	AF31/CS3	CoS 3
Transactional Data	AF21	CoS 2
Network-Management	CS2	CoS 2
Bulk Data	AF11	CoS 1
Scavenger	CS1	CoS 1
Best-Effort	0	0

The configuration of the priority queue (Q4) and the bandwidth allocations for the remaining queues (Q1, Q2 & Q3) are shown below.

Example 2-10 Catalyst 2950 Scheduling Configuration—1P3Q1T Example

```
CAT2950(config)#wrr-queue bandwidth 5 25 70 0              ! Q1-5%, Q2-25%, Q3-70%, Q4=PQ
CAT2950(config)#
```

Catalyst MLS QoS Verification Commands

This section includes the following commands:

- show wrr-queue bandwidth
- show wrr-queue cos-map

show wrr-queue bandwidth

The **show wrr-queue bandwidth** verification command displays the weights that have been assigned to the queues. If the command returns a value of 0 for the weight of the fourth queue, this indicates that the scheduler is operating in 1P3Q1T mode, with Q4 being the strict-priority queue.

In the following example, the scheduler has been configured for 1P3Q1T queuing: Q1 gets 5% of the remaining bandwidth (after the priority queue has been fully-serviced), Q2 gets 25% and Q3 gets 70%.

Example 2-11 Show WRR-Queue Bandwidth Verification for a Catalyst 2950 Switch

```
CAT2950#show wrr-queue bandwidth
WRR Queue  :   1   2   3   4
Bandwidth  :   5  25  70   0             ! Q1 gets 5%, Q2 gets 25%, Q3 gets 70%, Q4 is PQ
CAT2950#
```

The CoS-to-Queue mapping configuration for the Catalyst 2950 is shown below.

Example 2-12 Catalyst 2950 CoS-to-Queue Mapping Example

```
CAT2950(config)#wrr-queue cos-map 1 1                ! Scavenger/Bulk is assigned to Q1
CAT2950(config)#wrr-queue cos-map 2 0                ! Best Effort is assigned to Q2
CAT2950(config)#wrr-queue cos-map 3 2 3 4 6 7        ! CoS 2,3,4,6,7 are assigned to Q3
CAT2950(config)#wrr-queue cos-map 4 5                ! VoIP is assigned to Q4 (PQ)
CAT2950(config)#
```

show wrr-queue cos-map

The **show wrr-queue cos-map** verification command displayst he queue that each CoS value has been assigned to.

In the example below, CoS 0 (Best Effort) is assigned to Q2 and CoS 1 (Scavenger) has been assigned to Q1. CoS values 2, 3, 4, 6 and 7 have all been assigned to Q3 and CoS 5 (Voice) has been assigned to the priority-queue, Q4.

Example 2-13 Show WRR-Queue CoS Map Verification for a Catalyst 2950 Switch

```
CAT2950#show wrr-queue cos-map
CoS Value      :  0  1  2  3  4  5  6  7
Priority Queue :  2  1  3  3  3  4  3  3

CAT2950#
```

Catalyst 3550—QoS Considerations and Design

This section includes the following topics:

- Catalyst 3550—Trusted Endpoint Model
- Catalyst 3550—AutoQoS VoIP Model
- Catalyst 3550—Untrusted PC + SoftPhone with Scavenger-Class QoS Model
- Catalyst 3550—Untrusted Server with Scavenger-Class QoS Model
- Catalyst 3500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model
- Catalyst 3550—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model
- Catalyst 3550—Queuing and Dropping

The Catalyst 3550 supports IP routing and so may be found in either the access or distribution layer of the campus.

Regarding QoS, the Catalyst 3550 supports a richer feature set than the Catalyst 2950, including an advanced policing feature that is ideal for out-of-profile policing, namely, per-port/per-VLAN policing. The access layer design options and distribution layer design recommendations for a Catalyst 3550 are shown in Figure 2-13 and Figure 2-14, respectively.

Figure 2-13 Access Layer Catalyst 3550 QoS Design Options

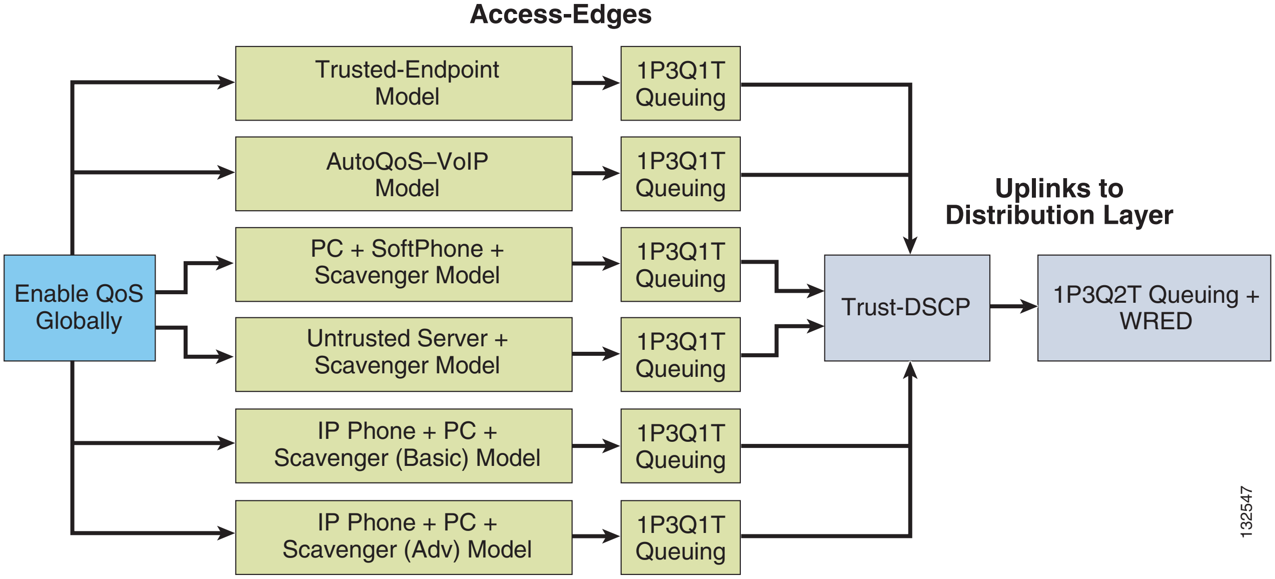
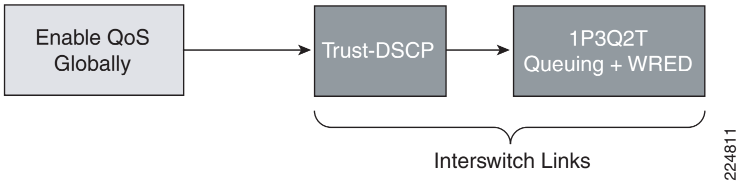


Figure 2-14 Distribution Layer Catalyst 3550 QoS Design



An important point to remember about the Catalyst 3550 is that QoS is disabled by default and must be enabled globally for configured policies to become effective. While QoS is disabled, all frames/packets are passed through the switch unaltered (which is equivalent to a trust CoS and trust DSCP state on all ports). When QoS is globally enabled however, all DSCP and CoS values are (by default) set to 0 (which is equivalent to an untrusted state on all ports). The example below shows how to verify if QoS has been enabled or not and also how it can be globally enabled.

Example 2-14 Enabling QoS Globally on the Catalyst 3550

```
CAT3550#show mls qos
QoS is disabled                                         ! By default QoS is disabled

CAT3550#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CAT3550(config)#mls qos                         ! Enables QoS globally for the Cat3550
CAT3550(config)#exit
CAT3550#

CAT3550#show mls qos
QoS is enabled                                  ! Verifies that QoS is enabled globally

CAT3550#
```

Note Enabling QoS in the Catalyst 3550 may (depending on the software version) require the disabling of IEEE 802.3X flow control on all interfaces (if enabled). Flowcontrol can be disabled on an interface by using the interface commands: **flowcontrol receive off** and **flowcontrol send off**.

Catalyst 3550—Trusted Endpoint Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

Configuring a Catalyst 3550 switchport to trust an endpoint is identical to the configuration required on a Catalyst 2950, provided that QoS has been globally enabled on the Catalyst 3550. Configuration is shown below.

Example 2-15 Catalyst 3550—Trusted Endpoint

```
CAT3550(config)#interface FastEthernet0/1
CAT3550(config-if)#mls qos trust dscp
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for the trusted endpoint model include the following:

- show mls qos
- show mls qos interface

Catalyst 3550—AutoQoS VoIP Model

The Catalyst 3550 supports AutoQoS VoIP with the following keyword options:

- **auto qos voip cisco-phone**
- **auto qos voip cisco-softphone**
- **auto qos voip trust**

When you enable AutoQoS VoIP on the Catalyst 3550 by using the **auto qos voip cisco-phone**, the **auto qos voip cisco-softphone**, or the **auto qos voip trust interface** configuration command, the switch automatically generates a QoS configuration based on the traffic type and ingress packet label and applies the commands listed in Table 2-2 to the interface.

Table 2-2 Catalyst 3550 Auto-QoS Generated Configuration

Description	Automatically Generated Command
The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value).	C3550(config)# **mls qos** C3550(config)# **mls qos map cos-dscp 0 8 16 26 32 46 48 56**
If 10/100 Ethernet ports are present, the switch automatically configures the buffer size of the minimum-reserve levels 5, 6, 7, and 8: • Level 5 can hold 170 packets. • Level 6 can hold 85 packets. • Level 7 can hold 51 packets. • Level 8 can hold 34 packets.	C3550(config)# **mls qos min-reserve 5 170** C3550(config)# **mls qos min-reserve 6 85** C3550(config)# **mls qos min-reserve 7 51** C3550(config)# **mls qos min-reserve 8 34**
If you entered the **auto qos voip trust** command, the switch automatically sets the ingress classification to trust the CoS value received in the packet on a nonrouted port or to trust the DSCP value received in the packet on a routed port.	C3550(config-if)# **mls qos trust cos** C3550(config-if)# **mls qos trust dscp**
If you entered the **auto qos voip cisco-phone** command, the switch automatically enables the trusted boundary feature which uses the CDP to detect the presence or absence of a Cisco IP Phone.	C3550(config-if)# **mls qos trust device cisco-phone**
If you entered the **auto qos voip cisco-softphone** command, the switch automatically creates class maps and policy maps.	C3550(config)# **mls qos map policed-dscp 24 26 46 to 0** C3550(config)# **class-map match-all AutoQoS-VoIP-RTP-Trust** C3550(config-cmap)# **match ip dscp 46** C3550(config)# **class-map match-all AutoQoS-VoIP-Control-Trust** C3550(config-cmap)# **match ip dscp 24 26** C3550(config)# **policy-map AutoQoS-Police-SoftPhone** C3550(config-pmap)# **class AutoQoS-VoIP-RTP-Trust** C3550(config-pmap-c)# **set dscp 46** C3550(config-pmap-c)# **police 320000 8000 exceed-action policed-dscp-transmit** C3550(config-pmap)# **class** AutoQoS-VoIP-Control-Trust C3550(config-pmap-c)# **set dscp 24** C3550(config-pmap-c)# **police 32000 8000 exceed-action policed-dscp-transmit**
After creating the class maps and policy maps, the switch automatically applies the policy map called *AutoQoS-Police-SoftPhone* to an ingress interface on which auto-QoS with the Cisco SoftPhone feature is enabled.	C3550(config-if)# **service-policy input AutoQoS-Police-SoftPhone**

Table 2-2 Catalyst 3550 Auto-QoS Generated Configuration

The switch automatically assigns egress queue usage on this interface.
The switch enables the egress expedite queue and assigns WRR weights to queues 1, 2, and 3. (The lowest value for a WRR queue is 1and is the recommended setting for Q4 when it is operating as an expedite queue.)
The switch configures the CoS-to-egress-queue map:
• CoS values 0 and 1 select queue 1.
• CoS values 2 and 4 select queue 2.
• CoS values 3, 6, and 7 select queue 3.
• CoS value 5 selects queue 4 (expedite queue).
Because the expedite queue (queue 4) contains the VoIP data traffic, the queue is serviced until empty.
	`C3550(config-if)# wrr-queue bandwidth 10 20 70 1`
	`C3550(config-if)# no wrr-queue cos-map`
	`C3550(config-if)# wrr-queue cos-map 1 0 1`
	`C3550(config-if)# wrr-queue cos-map 2 2 4`
	`C3550(config-if)# wrr-queue cos-map 3 3 6 7`
	`C3550(config-if)# wrr-queue cos-map 4 5`
	`C3550(config-if)# priority-queue out`

On Gigabit-capable Ethernet ports only, the switch automatically configures the ratio of the sizes of the WRR egress queues: • Queue 1 is 50 percent. • Queue 2 is 25 percent. • Queue 3 is 15 percent. • Queue 4 is 10 percent.	`C3550(config-if)# wrr-queue queue-limit 50 25 15 10`

On 10/100 Ethernet ports only, the switch automatically configures minimum-reserve levels for the egress queues:
• Queue 1 selects the minimum-reserve level 5.
• Queue 2 selects the minimum-reserve level 6.
• Queue 3 selects the minimum-reserve level 7.
• Queue 4 selects the minimum-reserve level 8.
	`C3550(config-if)# wrr-queue min-reserve 1 5`
	`C3550(config-if)# wrr-queue min-reserve 2 6`
	`C3550(config-if)# wrr-queue min-reserve 3 7`
	`C3550(config-if)# wrr-queue min-reserve 4 8`

Catalyst 3550—Untrusted PC + SoftPhone with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

Unlike the Catalyst 2950, the Catalyst 3550 has all the necessary QoS features to support and enforce the Untrusted PC + SoftPhone + Scavenger model, as illustrated in Figure 2-4. The Catalyst 3550 configuration for this access edge model is shown below.

Example 2-16 Catalyst 3550—Untrusted PC + SoftPhone + Scavenger Model Configuration

```
CAT3550(config)#mls qos map policed-dscp  0 24 46 to 8
    ! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT3550(config)#
CAT3550(config)#class-map match-all SOFTPHONE-VOICE
CAT3550(config-cmap)#  match access-group name SOFTPHONE-VOICE
CAT3550(config-cmap)#class-map match-all SOFTPHONE-SIGNALING
CAT3550(config-cmap)#  match access-group name SOFTPHONE-SIGNALING
CAT3550(config-cmap)#exit
CAT3550(config)#
CAT3550(config)#policy-map SOFTPHONE-PC
CAT3550(config-pmap)#class SOFTPHONE-VOICE
CAT3550(config-pmap-c)# set ip dscp 46              ! Softphone VoIP is marked to DSCP EF
CAT3550(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile SoftPhone voice traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class SOFTPHONE-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24                  ! Signaling is marked to DSCP CS3
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Signaling traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)# exit
CAT3550(config-pmap)#exit
CAT3550(config)#
CAT3550(config)#interface FastEthernet0/1
CAT3550(config-if)# service-policy input SOFTPHONE-PC           ! Applies policy to int
CAT3550(config-if)#exit
CAT3550(config)#
CAT3550(config)#ip access list  extended SOFTPHONE-VOICE
CAT3550(config-ext-nacl)# permit udp any any range 16384 32767             ! VoIP ports
CAT3550(config-ext-nacl)#
CAT3550(config-ext-nacl)#ip access list  extended SOFTPHONE-SIGNALING
CAT3550(config-ext-nacl)# permit tcp any any range 2000 2002               ! SCCP ports
CAT3550(config-ext-nacl)#end
CAT3550#
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for untrusted PC + SoftPhone +Scavenger model include the following:

- show mls qos

- show mls qos map
- show mls qos interface
- show mls qos interface policers
- show mls qos statistics
- show class-map
- show policy-map
- show policy interface

show mls qos interface statistics

The **show mls qos interface statistics** verification command reports dynamic counters for a given policy, including how many packets were classified and policed by the policy.

In the example below, untrusted packets from the PC are classified and policed according to the limits shown in Figure 2-4 for the Untrusted PC + SoftPhone + Scavenger access edge endpoint policing model.

Example 2-17 Show MLS QoS Interface Statistics Verification of a Catalyst 3550 Switchport Connected to an Untrusted PC + SoftPhone with Scavenger-Class QoS

```
CAT3550#show mls qos interface FastEthernet0/1 statistics
FastEthernet0/1
Ingress
  dscp: incoming   no_change  classified policed    dropped (in bytes)
Others: 1275410698 31426318   1243984380 1674978822 0
Egress
  dscp: incoming   no_change  classified policed    dropped (in bytes)
Others: 7271494       n/a       n/a      0          0
CAT3550#
```

show policy interface

The **show policy interface** verification command displays the policy maps (and related classes) that are attached to a given interface.

In this example, a summary of the Untrusted PC + SoftPhone + Scavenger policing policy is shown as applied to FastEthernet0/1.

Example 2-18 Show Policy Interface Verification of a of a Catalyst 3550 Switchport Connected to an Untrusted PC + SoftPhone with Scavenger-Class QoS

```
CAT3550#show policy interface FastEthernet0/1
 FastEthernet0/1
  service-policy input: SOFTPHONE-PC

    class-map: SOFTPHONE-VOICE (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      match: access-group name SOFTPHONE-VOICEqm_police_inform_feature:
 CLASS_SHOW

    class-map: SOFTPHONE-SIGNALING (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      match: access-group name SOFTPHONE-SIGNALINGqm_police_inform_feature:
 CLASS_SHOW
```

```
    class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      match: any
        0 packets, 0 bytes
        5 minute rate 0 bpsqm_police_inform_feature: CLASS_SHOW

CAT3550#
```

Note Currently, the counters reported via the **show policy interface** command on the Catalyst 3550 are not being incremented (i.e., all counters are currently frozen at zero), as is the case with the mainline IOS version of this command. A bug has been reported which, when fixed, should result in the counters incrementing dynamically. Catalyst 3550 IOS versions tested and affected with this bug include 12.1(19)EA1 a through c and 12.1(20)EA1.

Catalyst 3550—Untrusted Server with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

The Catalyst 3550 fully supports the Untrusted Multi-Application Server with Scavenger-Class QoS model, as depicted in Figure 2-5. The configuration for this model is shown below.

Example 2-19 Catalyst 3550—Untrusted Multi-Application Server with Scavenger-Class QoS Configuration

```
CAT3550(config)#mls qos map policed-dscp  0 10 18 25 to 8
  ! Excess traffic marked 0 or AF11 or AF21 or DSCP 25 will be remarked to CS1
CAT3550(config)#
CAT3550(config)#class-map SAP
CAT3550(config-cmap)# match access-group name SAP
CAT3550(config-cmap)#class-map LOTUS
CAT3550(config-cmap)# match access-group name LOTUS
CAT3550(config-cmap)#class-map IMAP
CAT3550(config-cmap)# match access-group name IMAP
CAT3550(config-cmap)#exit
CAT3550(config)#
CAT3550(config)#policy-map UNTRUSTED-SERVER
CAT3550(config-pmap)#class SAP
CAT3550(config-pmap-c)# set ip dscp 25               ! SAP is marked as Mission-Critical
CAT3550(config-pmap-c)# police 15000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile SAP is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class LOTUS
CAT3550(config-pmap-c)# set ip dscp 18               ! Lotus is marked as Transactional
CAT3550(config-pmap-c)# police 35000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile LOTUS is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class IMAP
CAT3550(config-pmap-c)# set ip dscp 10                   ! IMAP is marked as Bulk Data
CAT3550(config-pmap-c)# police 50000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile IMAP is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class class-default
```

```
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile excess data traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)# exit
CAT3550(config-pmap)#exit
CAT3550(config)#
CAT3550(config)#interface FastEthernet0/1
CAT3550(config-if)# service-policy input UNTRUSTED-SERVER
CAT3550(config-if)#exit
CAT3550(config)#
CAT3550(config)#ip access list  extended SAP
CAT3550(config-ext-nacl)# permit tcp any range 3200 3203 any
CAT3550(config-ext-nacl)# permit tcp any eq 3600 any
CAT3550(config-ext-nacl)#
CAT3550(config-ext-nacl)#ip access list  extended LOTUS
CAT3550(config-ext-nacl)# permit tcp any eq 1352 any
CAT3550(config-ext-nacl)#
CAT3550(config-ext-nacl)#ip access list  extended IMAP
CAT3550(config-ext-nacl)# permit tcp any eq 143 any
CAT3550(config-ext-nacl)# permit tcp any eq 220 any
CAT3550(config-ext-nacl)#end
CAT3550#
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for the Multi-Application Server+ Scavenger model include the following:

- show mls qos
- show mls qos map
- show mls qos interface
- show mls qos interface policers
- show mls qos statistics
- show class-map
- show policy-map
- show policy interface

Catalyst 3500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

The Catalyst 3550's support of Per-Port/Per-VLAN policing makes for a distinct advantage over other platforms when provisioning a (Basic or Advanced) Conditionally-Trusted Endpoint Model. This is because Per-Port/Per-VLAN policies can be provisioned without having to enter subnet-specific information for each switch. This makes such policies more modular and portable.

In the following example, the VLAN 10 is the DVLAN and VLAN 110 is the VVLAN.

Note Since the time of writing, newer versions of Catalyst 3550 switch software do **not** allow the configuration of a trust-statement in conjunction with a service-policy statement on a switch interface.

Example 2-20 Catalyst 3550—Conditionally-Trusted IP Phone + PC + Scavenger (Basic) Model Configuration

```
CAT3550(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
    ! Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF
CAT3550(config)#mls qos map policed-dscp 0 24 to 8
    ! Excess DVLAN & VVLAN traffic will be remarked to Scavenger (CS1)
CAT3550(config)#
CAT3550(config)#
CAT3550(config)#class-map match-all VOICE
CAT3550(config-cmap)#  match ip dscp 46                                ! DSCP EF (voice)
CAT3550(config-cmap)#class-map match-any CALL SIGNALING         ! Need ‘match-any’ here
CAT3550(config-cmap)#  match ip dscp 26                 ! DSCP AF31 (old Call-Signaling)
CAT3550(config-cmap)#  match ip dscp 24                 ! DSCP CS3 (new Call-Signaling)
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-VOICE
CAT3550(config-cmap)#  match vlan  110                             ! VLAN 110 is VVLAN
CAT3550(config-cmap)#  match class-map VOICE                    ! Matches VVLAN DSCP EF
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT3550(config-cmap)#  match vlan  110                             ! VLAN 110 is VVLAN
CAT3550(config-cmap)#  match class-map CALL SIGNALING           !Matches VVLAN AF31/CS3
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all ANY
CAT3550(config-cmap)#  match access-group name ANY                     ! Workaround ACL
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-ANY
CAT3550(config-cmap)#  match vlan  110                             ! VLAN 110 is VVLAN
CAT3550(config-cmap)#  match class-map ANY              ! Matches any other VVLAN traffic
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-ANY
CAT3550(config-cmap)#  match vlan  10                                  ! VLAN 10 is DVLAN
CAT3550(config-cmap)#  match class-map ANY                  ! Matches all DVLAN traffic
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map IPPHONE+PC-BASIC
CAT3550(config-pmap)#class VVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 46                                 ! DSCP EF (Voice)
CAT3550(config-pmap-c)# police 128000 8000 exceed-action drop
    ! Only one voice call is permitted per switchport VVLAN
CAT3550(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24                      ! DSCP CS3 (Call-Signaling)
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile call signaling is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class VVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Unauthorized VVLAN traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class DVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)# exit
CAT3550(config-pmap)#exit
CAT3550(config)#
CAT3550(config)#interface FastEthernet0/1
CAT3550(config-if)# switchport access vlan 10                                  ! DVLAN
```

```
CAT3550(config-if)# switchport voice vlan 110                                  ! VVLAN
CAT3550(config-if)# mls qos trust device cisco-phone                ! Conditional Trust
CAT3550(config-if)# service-policy input IPPHONE+PC-BASIC              ! Attaches policy
CAT3550(config-if)#exit
CAT3550(config)#
CAT3550(config)#
CAT3550(config)#ip access list  standard ANY                            ! Workaround ACL
CAT3550(config-std-nacl)# permit any
CAT3550(config-std-nacl)#end
CAT3550#
```

Catalyst MLS QoS Verification Commands

The Catalyst MLS QoS verification commands for the Conditionally-Trusted IP Phone + PC + Scavenger (Basic) Model Configuration include the following:

- show mls qos
- show mls qos map
- show mls qos interface
- show mls qos interface policers
- show mls qos statistics
- show class-map
- show policy-map
- show policy interface

Note While Catalyst 3550 IOS syntax supports the **match any** criteria within a class-map (which the parser allows to be configured in conjunction with a per-VLAN policy), testing with some versions of Catalyst 3500 IOS have revealed a limitation with this function, since it does not match any other traffic on a per-VLAN basis. Hence an explicit access list named ANY has been used in the example above as a workaround.

Catalyst 3550—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

The Conditionally-Trusted IP Phone + PC + Scavenger Advanced model builds on the Basic model by including policers for PC-based video-conferencing (and/or PC SoftPhone), Mission-Critical Data applications, Transactional Data applications, and Bulk Data applications. This model is graphically depicted in Figure 2-9. The Catalyst 3550 can support 8 policers per 10/100 Ethernet port and so can support this Advanced Model.

The Catalyst 3550 configuration for the Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model is shown below. In this example, the same Server-to-Client applications are used as in the Untrusted Multi-Application Server example. However, notice that the Source/Destination ports are reversed for the Client-to-Server direction of traffic flow. Also, due to the limit of the number of policers per FastEthernet port (8), there is no explicit policer for SoftPhone call signaling traffic; to work around this limitation, SoftPhone call signaling traffic is included in the Mission-Critical Data applications access list .

Example 2-21 Catalyst 3550—Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model Configuration

```
CAT3550(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
    ! Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF
CAT3550(config)#mls qos map policed-dscp 0 10 18 24 25 34 to 8
! Excess DVLAN traffic marked 0, AF11, AF21, CS3, DSCP 25,
! and AF41 will be remarked to Scavenger (CS1)
CAT3550(config)#
CAT3550(config)#class-map match-all VOICE
CAT3550(config-cmap)#  match ip dscp 46                                ! DSCP EF (voice)
CAT3550(config-cmap)#class-map match-any CALL SIGNALING          ! Need ‘match-any’ here
CAT3550(config-cmap)#  match ip dscp 26                 ! DSCP AF31 (old Call-Signaling)
CAT3550(config-cmap)#  match ip dscp 24                 ! DSCP CS3 (new Call-Signaling)
CAT3550(config-cmap)#class-map match-all PC-VIDEO
CAT3550(config-cmap)#  match access-group name PC-VIDEO
CAT3550(config-cmap)#class-map match-all MISSION-CRITICAL-DATA
CAT3550(config-cmap)#  match access-group name MISSION-CRITICAL-DATA
CAT3550(config-cmap)#class-map match-all TRANSACTIONAL-DATA
CAT3550(config-cmap)#  match access-group name TRANSACTIONAL-DATA
CAT3550(config-cmap)#class-map match-all BULK-DATA
CAT3550(config-cmap)#  match access-group name BULK-DATA
CAT3550(config-cmap)#class-map match-all ANY
CAT3550(config-cmap)#  match access-group name ANY                     ! Workaround ACL
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-VOICE
CAT3550(config-cmap)#  match vlan  110                             ! VLAN 110 is VVLAN
CAT3550(config-cmap)#  match class-map VOICE                   ! Matches VVLAN DSCP EF
CAT3550(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT3550(config-cmap)#  match vlan  110                             ! VLAN 110 is VVLAN
CAT3550(config-cmap)#  match class-map CALL SIGNALING          ! Matches VVLAN AF31/CS3
CAT3550(config-cmap)#class-map match-all VVLAN-ANY
CAT3550(config-cmap)#  match vlan  110                             ! VLAN 110 is VVLAN
CAT3550(config-cmap)#  match class-map ANY              ! Matches any other VVLAN traffic
CAT3550(config-cmap)#
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-PC-VIDEO
CAT3550(config-cmap)#  match vlan  10                                   ! VLAN 10 is DVLAN
CAT3550(config-cmap)#  match class-map PC-VIDEO         ! Matches PC IP/VC or SoftPhone
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-MISSION-CRITICAL-DATA
CAT3550(config-cmap)#  match vlan  10                                   ! VLAN 10 is DVLAN
CAT3550(config-cmap)#  match class-map MISSION-CRITICAL-DATA
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-TRANSACTIONAL-DATA
CAT3550(config-cmap)#  match vlan  10                                   ! VLAN 10 is DVLAN
CAT3550(config-cmap)#  match class-map TRANSACTIONAL-DATA
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-BULK-DATA
CAT3550(config-cmap)#  match vlan  10                                   ! VLAN 10 is DVLAN
CAT3550(config-cmap)#  match class-map BULK-DATA
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-ANY
CAT3550(config-cmap)#  match vlan  10                                   ! VLAN 10 is DVLAN
```

```
CAT3550(config-cmap)#  match class-map ANY              ! Matches all other DVLAN traffic
CAT3550(config-cmap)#
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map IPPHONE+PC-ADVANCED
CAT3550(config-pmap)#class VVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 46                                 ! DSCP EF (Voice)
CAT3550(config-pmap-c)# police 128000 8000 exceed-action drop
    ! Only one voice call is permitted per switchport VVLAN
CAT3550(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24                      ! DSCP CS3 (Call-Signaling)
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile call signaling is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class VVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
! Unauthorized VVLAN traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class DVLAN-PC-VIDEO
CAT3550(config-pmap-c)# set ip dscp 34                  ! DSCP AF41 (Interactive-Video)
CAT3550(config-pmap-c)# police 500000 8000 exceed-action policed-dscp-transmit
    ! Only one IP/VC stream will be permitted per switchport
CAT3550(config-pmap-c)#class DVLAN-MISSION-CRITICAL-DATA
CAT3550(config-pmap-c)# set ip dscp 25                  ! Interim Mission-Critical Data
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Mission-Critical Data is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class DVLAN-TRANSACTIONAL-DATA
CAT3550(config-pmap-c)# set ip dscp 18                  ! DSCP AF21 (Transactional Data)
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Transactional Data is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class DVLAN-BULK-DATA
CAT3550(config-pmap-c)# set ip dscp 10                          ! DSCP AF11 (Bulk Data)
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Bulk Data is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class DVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)# exit
CAT3550(config-pmap)#exit
CAT3550(config)#
CAT3550(config)#interface FastEthernet0/1
CAT3550(config-if)# switchport access vlan 10                                  ! DVLAN
CAT3550(config-if)# switchport voice vlan 110                                  ! VVLAN
CAT3550(config-if)# mls qos trust device cisco-phone                ! Conditional Trust
CAT3550(config-if)# service-policy input IPPHONE+PC-ADVANCED           ! Attaches policy
CAT3550(config-if)#exit
CAT3550(config)#
CAT3550(config)#ip access list  standard ANY                           ! Workaround ACL
CAT3550(config-std-nacl)# permit any
CAT3550(config-std-nacl)#
CAT3550(config-std-nacl)#ip access list  extended PC-VIDEO          ! IP/VC or SoftPhone
CAT3550(config-ext-nacl)# permit udp any any range 16384 32767
CAT3550(config-ext-nacl)#
CAT3550(config-ext-nacl)#ip access list  extended MISSION-CRITICAL-DATA
CAT3550(config-ext-nacl)# permit tcp any any range 3200 3203                    ! SAP
CAT3550(config-ext-nacl)# permit tcp any any eq 3600                            ! SAP
CAT3550(config-ext-nacl)# permit tcp any any range 2000 2002            ! SoftPhone SCCP
CAT3550(config-ext-nacl)#
CAT3550(config-ext-nacl)#ip access list  extended TRANSACTIONAL-DATA
CAT3550(config-ext-nacl)# permit tcp any any eq 1352                            ! Lotus
CAT3550(config-ext-nacl)#
CAT3550(config-ext-nacl)#ip access list  extended BULK-DATA
CAT3550(config-ext-nacl)# permit tcp any any eq 143                             ! IMAP
CAT3550(config-ext-nacl)# permit tcp any any eq 220                             ! IMAP
CAT3550(config-ext-nacl)#end
```

```
CAT3550#
```

Catalyst MLS QoS Verification Commands

The Catalyst MLS QoS verification commands for Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model include the following:

- show mls qos
- show mls qos map
- show mls qos interface
- show mls qos interface policers
- show mls qos statistics
- show class-map
- show policy-map
- show policy interface

Catalyst 3550—Queuing and Dropping

This section includes the following topics:

- Configuration
- Advanced Tuning Options
- Catalyst MLS QoS Verification Commands

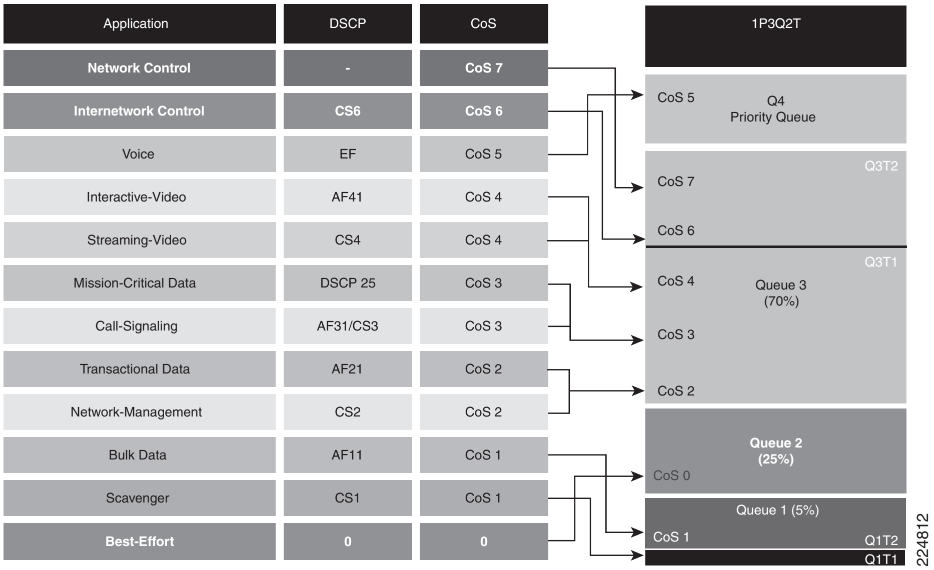
Configuration

Like the Catalyst 2950, the Catalyst 3550 supports a 1P3Q1T queuing model for all ports. GigabitEthernet ports have the additional option of being configured as 1P3Q2T, with either tail-drop or WRED thresholds. However, unlike the Catalyst 2950, the Catalyst 3550 queuing parameters are set on a per-interface basis and not globally. Nonetheless, uniform queuing policies can be expeditiously deployed via the **interface range** configuration command.

The strict-priority queue is enabled on a per-interface basis on the Catalyst 3550 with the **priority-queue out** interface command. Bandwidth is allocated among the remaining queues via the **wrr-queue bandwidth** command. A twist with the Catalyst 3550 is that Queue 4’s WRR weight is set to 1 (indicating that it does not participate in the WRR scheduler since it is configured as a strict-priority queue), instead of 0 (as is the case on the Catalyst 2950). Recommended remaining bandwidth allocations (after the PQ has been fully serviced) are 5% for the Scavenger queue (Q1), 25% for the Best-Effort queue (Q2), and 70% for the preferential application queue (Q3).

Following this, CoS 1 (Scavenger/Bulk) would be assigned to Q1; CoS 0 (Best Effort) would be assigned to Q2; CoS values 2 (Transactional Data and Network Management), 3 (call signaling and Mission-Critical Data), 4 (Interactive and Streaming-Video, 6 (Internetwork Control) and 7 (Network Control/Spanning-Tree) would be assigned to Q3; CoS 5 (voice) would be assigned to the strict-priority Q4. These assignments and allocations are illustrated in Figure 2-15 (the thresholds shown in Q1 and Q3 are discussed shortly).

Figure 2-15 Catalyst 3550 1P3Q2T Queuing Model



Application	DSCP	CoS
Network Control	-	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive-Video	AF41	CoS 4
Streaming-Video	CS4	CoS 4
Mission-Critical Data	DSCP 25	CoS 3
Call-Signaling	AF31/CS3	CoS 3
Transactional Data	AF21	CoS 2
Network-Management	CS2	CoS 2
Bulk Data	AF11	CoS 1
Scavenger	CS1	CoS 1
Best-Effort	0	0

The interface-mode configuration commands to configure this 1P3Q1T queuing model, for either FastEthernet or GigabitEthernet Catalyst 3550 interfaces, are shown below.

Example 2-22 Catalyst 3550 FastEthernet and/or GigabitEthernet Interface Queuing Configuration—1P3Q1T

```
CAT3550(config)#interface range FastEthernet0/1 - 48
CAT3550(config-if)# wrr-queue bandwidth 5 25 70 1           ! Q1-5% Q2-25% Q3-70% Q4=PQ
CAT3550(config-if)# wrr-queue cos-map 1 1                   ! Assigns Scavenger to Q1
CAT3550(config-if)# wrr-queue cos-map 2 0                   ! Assigns Best Effort to Q2
CAT3550(config-if)# wrr-queue cos-map 3 2 3 4 6 7           ! Assigns CoS 2,3,4,6,7 to Q3
CAT3550(config-if)# wrr-queue cos-map 4 5                   ! Assigns VoIP to Q4 (PQ)
CAT3550(config-if)# priority-queue out                      ! Enables Q4 as PQ
CAT3550(config-if)#exit
CAT3550(config)#
```

Advanced Tuning Options

The Catalyst 3550 offers some advanced “nerd-knob” queuing options on 10/100 interfaces, such as tuning Minimum Reserve Thresholds. However, testing has shown that such tuning, which rarely factors into play, makes a highly-negligible difference at best. Therefore, tuning Minimum Reserve Thresholds is recommended only for advanced network administrators or via automated tools, such as AutoQoS.

Some advanced “nerd-knobs” also exist for GigabitEthernet interfaces. A couple of these advanced tuning options include Queue-Limit tuning and the enabling of WRED thresholds for 1P3Q2T operation. In the event of DoS/worm attacks, the GigabitEthernet uplinks will likely be the first to congest, therefore its worthwhile examining these advanced options.

In the example below, the queue-limits for both GigabitEthernet interfaces are tuned to correspond to the WRR weights of the queues (the bandwidth allocations). This is achieved with the **wrr-queue queue-limit** interface command. However, unlike the WRR weight bandwidth ratio for Q4 (which is set to 1 to indicate that Q4 is a PQ), the queue limit for Q4 needs to be explicitly set to a more representative value, such as 30%.

Note The default queue limits are such that each queue is assigned 25% of the available buffer space. It should be noted that when the queue limits are modified, the queue is temporarily shutdown during the hardware reconfiguration and the switch may drop newly-arrived packets destined to the queue. Thus, it may be advisable not to tune the queue limits on Catalyst 3550 switches already in production networks.

Additionally, WRED is enabled on each (non-priority) queue. This allows for the preferential treatment of Bulk Data (DSCP AF11) over Scavenger (CS1) within Q1, as well as the preferential treatment of Internetworking/Networking protocols (DSCP CS6 and CS7, respectively) over all other applications assigned to Q3. Even though Q2 has only Best Effort traffic assigned to it, enabling WRED on this queue increases the efficiency of TCP applications within this queue during periods of congestion.

A low WRED threshold, such as 40%, can be set for Q1 to aggressively drop Scavenger traffic in order to preferentially service Bulk Data. The WRED thresholds for Q2 and Q3 can be set to higher levels, such as 80%.

By default all DSCP values are mapped to the first WRED threshold of the queue to which their CoS values are assigned. Therefore, only DSCP values that are to be mapped to the second WRED thresholds (of their respective queues) need to be manually configured. In this case, Bulk Data (DSCP AF11/10), Internetwork Control (DSCP CS6/48), and Network Control (DSCP CS7/56) all need to be explicitly mapped to the second WRED threshold via the **wrr-queue dscp-map** interface configuration command.

Note Network control traffic in the campus primarily refers to Spanning Tree Protocol (STP) traffic, such as Bridge Protocol Data Units (BPDUs). While these Layer 2 Ethernet frames are marked CoS 7, they (obviously) do not have any capability to carry Layer 3 DSCP markings. Thus, it may seem moot to map DSCP CS7 (56) to a higher WRED threshold. However, it should be kept in mind that Catalyst switches generate *Internal DSCP* values for all frames (regardless of whether they are carrying IP or not). These Internal DSCP values are used for QoS decisions, such as WRED in this case. Therefore, since STP BPDU frames (marked CoS 7) generate an Internal DSCP value of 56, mapping DSCP 56 to the second threshold of Q3 provides preferential treatment for these important Layer 2 frames.

The configuration for these tuning options, which are available only on GigabitEthernet interfaces on the Catalyst 3550, is shown below.

Example 2-23 Catalyst 3550 GigabitEthernet Interface Queuing and Dropping Configuration—1P3Q2T

```
CAT3550(config)#interface range GigabitEthernet 0/1 - 2
CAT3550(config-if-range)# wrr-queue bandwidth 5 25 70 1
! Q1 gets 5% BW, Q2 gets 25% BW, Q3 gets 70% BW, Q4 is the PQ
CAT3550(config-if-range)# wrr-queue queue-limit 5 25 40 30
    ! Tunes buffers to 5% for Q1, 25% for Q2, 40% for Q3 and 30% for Q4
CAT3550(config-if-range)# wrr-queue random-detect max-threshold 1 40 100
    ! Sets Q1 WRED threshold 1 to 40% and threshold 2 to 100%
CAT3550(config-if-range)# wrr-queue random-detect max-threshold 2 80 100
! Sets Q2 WRED threshold 1 to 80% and threshold 2 to 100%
CAT3550(config-if-range)# wrr-queue random-detect max-threshold 3 80 100
! Sets Q3 WRED threshold 1 to 80% and threshold 2 to 100%
CAT3550(config-if)# wrr-queue cos-map 1 1                   ! Assigns Scavenger to Q1
CAT3550(config-if)# wrr-queue cos-map 2 0                   ! Assigns Best Effort to Q2
CAT3550(config-if)# wrr-queue cos-map 3 2 3 4 6 7           ! Assigns CoS 2,3,4,6,7 to Q3
CAT3550(config-if)# wrr-queue cos-map 4 5                   ! Assigns VoIP to Q4 (PQ)
CAT3550(config-if-range)# wrr-queue dscp-map 2 10 48 56
    ! Maps Bulk Data (10), Routing (48) and Spanning Tree (Internal DSCP 56)
    ! to WRED threshold 2 of their respective queues - all other DSCP values
    ! are mapped (by default) to WRED threshold 1 of their respective queues
CAT3550(config-if)# priority-queue out                      ! Enables Q4 as PQ
```

```
CAT3550(config-if-range)#end
CAT3550#
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for queuing and dropping include the following:

- show mls qos interface buffers
- show mls qos interface queueing

show mls qos interface buffers

The **show mls qos interface buffers** verification command displays the queue sizes (as per-queue buffer allocation percentages of the total buffer space). Also the command displays if WRED has been enabled on a queue, and if so, it displays the first and second thresholds (as percentages of the queue's depth).

In the example below, the queue-limits are set to 5%, 25%, 40%, and 30% of the total queuing buffer space for Queues 1 through 4 (respectively). Additionally, WRED is enabled on queues 1 through 3 (but not Q4, as it is the priority queue). The first WRED threshold is set to 5% on Q1 and is set to 80% on queues 2 and 3.

Example 2-24 Show MLS QoS Interface Buffers Verification for a Catalyst 3550 Switch

```
CAT3550#show mls qos interface GigabitEthernet0/1 buffers
GigabitEthernet0/1
Notify Q depth:
qid-size
 1 - 5                       ! Q1 queue-limit is set to 5% of total buffer space
 2 - 25                      ! Q2 queue-limit is set to 25% of total buffer space
 3 - 40                      ! Q3 queue-limit is set to 40% of total buffer space
 4 - 30                      ! Q4 queue-limit is set to 30% of total buffer space
qid WRED thresh1 thresh2
1   ena  40      100         ! WRED is enabled on Q1 - first threshold is set to 40%
2   ena  80      100         ! WRED is enabled on Q2 - first threshold is set to 80%
3   ena  80      100         ! WRED is enabled on Q3 - first threshold is set to 80%
4   dis  100     100         ! WRED is disabled on Q4 (as it is the PQ)

CAT3550#
```

show mls qos interface queueing

The **show mls qos interface queuing** verification command displays the CoS-to-Queuing mappings that have been configured in addition to the bandwidth allocations per queue. On GigabitEthernet interfaces with WRED enabled, the output also includes the DSCP-to-WRED Threshold mappings. This information is displayed in a table form, with the first digit of the decimal DSCP value along the Y-Axis (in rows) and the second digit of the decimal DSCP value along the X-Axis (in columns).

In the example below, the output verifies that the egress expedite queue (priority queue: Q4) is enabled. Also, the WRR Bandwidth Weights show that, of the remaining bandwidth, Q1 is allocated 5%, Q2 is allocated 25%, and Q3 is allocated 70%.

Additionally, the DSCP-to-WRED table verifies that Bulk Data (AF11/10), Internetwork Control (DSCP CS6/48), and Network Control (DSCP CS7/56) are each mapped to the second WRED thresholds (T2) of their respective queues (as determined by the CoS-to-Queue mappings).

Finally, the CoS-to-Queue map shows that CoS 0 (Best Effort) is assigned to Q2, CoS 1 (Scavenger) has been assigned to Q1, CoS values 2, 3, 4, 6 and 7 have all been assigned to Q3, and CoS 5 (Voice) has been assigned to the priority-queue, Q4.

Example 2-25 Show MLS QoS Interface Verification for a Catalyst 3550 Switch

```
CAT3550#show mls qos interface GigabitEthernet0/1 queueing
GigabitEthernet0/1
Egress expedite queue: ena                                  ! Q4 is enabled as a PQ
wrr bandwidth weights:
qid-weights
 1 - 5                                                      ! Q1 is allocated 5%
 2 - 25                                                     ! Q2 is allocated 25%
 3 - 70                                                     ! Q3 is allocated 70&
 4 - 1    when expedite queue is disabled
Dscp-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
      1 :    02 01 01 01 01 01 01 01 01 01              ! DSCP 10 is mapped to WRED T2
      2 :    01 01 01 01 01 01 01 01 01 01
      3 :    01 01 01 01 01 01 01 01 01 01
      4 :    01 01 01 01 01 01 01 01 02 01              ! DSCP 48 is mapped to WRED T2
      5 :    01 01 01 01 01 01 02 01 01 01              ! DSCP 56 is mapped to WRED T2
      6 :    01 01 01 01
Cos-queue map:
cos-qid
 0 - 2                    ! Best-Effort is assigned to Q2
 1 - 1                    ! Scavenger and Bulk are assigned to Q1
 2 - 3                    ! Transactional Data and Network Management are assigned to Q3
 3 - 3                    ! Mission-Critical Data and call signaling are assigned to Q3
 4 - 3                    ! Interactive- and Streaming-Video are assigned to Q3
 5 - 4                    ! Voice is assigned to the priority queue: Q4
 6 - 3                    ! Internetwork Control (Routing) is assigned to Q3
 7 - 3                    ! Network Control (Spanning Tree) is assigned to Q3

CAT3550#
```

Catalyst 2970/3560/3750—QoS Considerations and Design

This section includes the following topics:

- Catalyst 2970/3560/3750—Trusted Endpoint Model
- Catalyst 2970/3560/3750—Auto QoS VoIP Model
- Catalyst 2970/3560/3750—Untrusted PC + SoftPhone with Scavenger-Class QoS Model
- Catalyst 2970/3560/3750—Untrusted Server with Scavenger-Class QoS Model
- Catalyst 2970/3560/3750—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model
- Catalyst 2970/3560/3750—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model
- Catalyst 2970/3560/3750—Queuing and Dropping

The Catalyst 2970 does not support Layer 3 routing and, as such, is restricted to the role of an access-layer switch. The 3560 does support Layer 3 routing as well as inline power— a feature that is rarely, if ever, required at the distribution layer—and so is only considered in an access-layer context. The Catalyst 3750 also supports Layer 3 routing and may be found in either the access layer or the distribution layer.

Figure 2-16 shows the QoS design options for access-layer Catalyst 2970s, 3560s, or 3750s, and Figure 2-17 shows the QoS design recommendations for a distribution-layer Catalyst 3750.

Figure 2-16 Access Layer Catalyst 2970/3560/3750 QoS Design Options

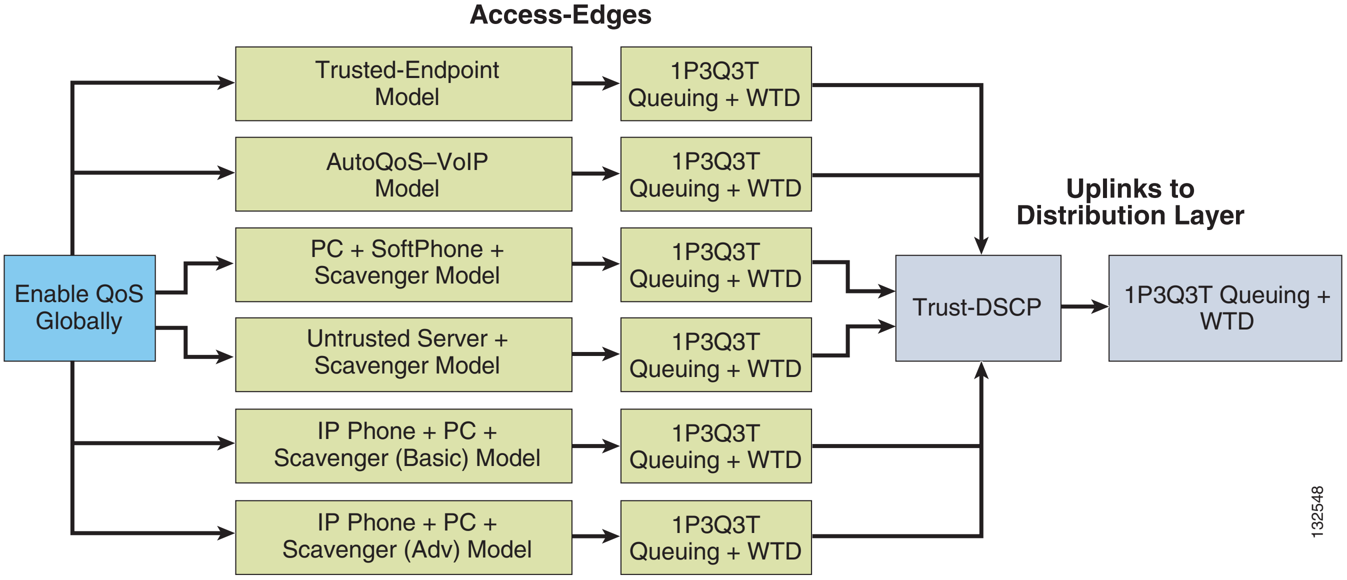
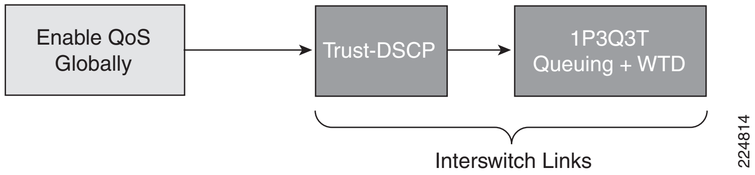


Figure 2-17 Distribution Layer Catalyst 3750 QoS Design



Since the QoS features and configuration syntax are identical for the Catalyst 2970, 3560 and 3750, from a QoS design recommendation perspective, they are subsequently addressed as a single switch.

As with the Catalyst 3550, QoS is globally disabled by default on the Catalyst 2970/3560/3750. While QoS is disabled, all frames/packets are passed-through the switch unaltered (which is equivalent to a trust CoS and trust DSCP state on all ports). When QoS is globally enabled, however, all DSCP and CoS values are (by default) set to 0 (which is equivalent to an untrusted state on all ports).

QoS must be enabled globally for configured policies to become effective. The example below shows how to verify if QoS has been enabled or not and also how it can be globally enabled.

Example 2-26 Enabling QoS Globally on the Catalyst 2970/3560/3750

```
CAT2970#show mls qos
QoS is disabled

CAT2970#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
CAT2970(config)#mls qos
CAT2970(config)#end
CAT2970#

CAT2970#show mls qos
QoS is enabled

CAT2970#
```

Catalyst 2970/3560/3750—Trusted Endpoint Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

The Trusted Endpoint model configuration for the Catalyst 2970/3550 is identical to the switches previously discussed (namely, the Catalyst 2950 and 3550) and is shown below.

Example 2-27 Catalyst 2970/3560/3750—Trusted Endpoint Model Configuration

```
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)#mls qos trust dscp
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for the Trusted Endpoint model include the following:

- show mls qos
- show mls qos interface

Catalyst 2970/3560/3750—Auto QoS VoIP Model

The Catalyst 2970/3560/3750 supports AutoQoS VoIP with the following keyword options:

- **auto qos voip cisco-phone**
- **auto qos voip cisco-softphone**
- **auto qos voip trust**

When you enable AutoQoS VoIP on the Catalyst 2970/3560/3750 by using the **auto qos voip cisco-phone**, the **auto qos voip cisco-softphone**, or the **auto qos voip trust** interface configuration command, the switch automatically generates a QoS configuration based on the traffic type and ingress packet label and applies the commands listed in Table 2-3 to the interface.

Table 2-3 Catalyst 2970/3560/3750 Auto-QoS Generated Configuration

Description	Automatically Generated Command

The switch automatically enables standard QoS and configures the CoS-to-DSCP map (maps CoS values in incoming packets to a DSCP value).	`C2970(config)# mls qos`
	`C2970(config)# mls qos map cos-dscp 0 8 16 26 32 46 48 56`

Table 2-3 Catalyst 2970/3560/3750 Auto-QoS Generated Configuration

The switch automatically maps CoS values to an ingress queue and to a threshold ID.	C2970(config)# **no mls qos srr-queue input cos-map** C2970(config)# **mls qos srr-queue input cos-map queue 1 threshold 3 0** C2970(config)# **mls qos srr-queue input cos-map queue 1 threshold 2 1** C2970(config)# **mls qos srr-queue input cos-map queue 2 threshold 1 2** C2970(config)# **mls qos srr-queue input cos-map queue 2 threshold 2 4 6 7** C2970(config)# **mls qos srr-queue input cos-map queue 2 threshold 3 3 5**
The switch automatically maps CoS values to an egress queue and to a threshold ID.	C2970(config)# **no mls qos srr-queue output cos-map** C2970(config)# **mls qos srr-queue output cos-map queue 1 threshold 3 5** C2970(config)# **mls qos srr-queue output cos-map queue 2 threshold 3 3 6 7** C2970(config)# **mls qos srr-queue output cos-map queue 3 threshold 3 2 4** C2970(config)# **mls qos srr-queue output cos-map queue 4 threshold 2 1** C2970(config)# **mls qos srr-queue output cos-map queue 4 threshold 3 0**
The switch automatically maps DSCP values to an ingress queue and to a threshold ID.	C2970(config)# **no mls qos srr-queue input dscp-map** C2970(config)# **mls qos srr-queue input dscp-map queue 1 threshold 2 9 10 11 12 13 14 15** C2970(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 0 1 2 3 4 5 6 7** C2970(config)# **mls qos srr-queue input dscp-map queue 1 threshold 3 32** C2970(config)# **mls qos srr-queue input dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23** C2970(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 33 34 35 36 37 38 39 48** C2970(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 49 50 51 52 53 54 55 56** C2970(config)# **mls qos srr-queue input dscp-map queue 2 threshold 2 57 58 59 60 61 62 63** C2970(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** C2970(config)# **mls qos srr-queue input dscp-map queue 2 threshold 3 40 41 42 43 44 45 46 47**

Table 2-3 Catalyst 2970/3560/3750 Auto-QoS Generated Configuration

The switch automatically maps DSCP values to an egress queue and to a threshold ID.	C2970(config)# **no mls qos srr-queue output dscp-map** C2970(config)# **mls qos srr-queue output dscp-map queue 1 threshold 3 40 41 42 43 44 45 46 47** C2970(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 24 25 26 27 28 29 30 31** C2970(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55** C2970(config)# **mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63** C2970(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 16 17 18 19 20 21 22 23** C2970(config)# **mls qos srr-queue output dscp-map queue 3 threshold 3 32 33 34 35 36 37 38 39** C2970(config)# **mls qos srr-queue output dscp-map queue 4 threshold 1 8** C2970(config)# **mls qos srr-queue output dscp-map queue 4 threshold 2 9 10 11 12 13 14 15** C2970(config)# **mls qos srr-queue output dscp-map queue 4 threshold 3 0 1 2 3 4 5 6 7**
The switch automatically sets up the ingress queues, with queue 2 as the priority queue and queue 1 in shared mode. The switch also configures the bandwidth and buffer size for the ingress queues.	C2970(config)# **no mls qos srr-queue input priority-queue 1** C2970(config)# **no mls qos srr-queue input priority-queue 2** C2970(config)# **mls qos srr-queue input bandwidth 90 10** C2970(config)# **mls qos srr-queue input threshold 1 8 16** C2970(config)# **mls qos srr-queue input threshold 2 34 66** C2970(config)# **mls qos srr-queue input buffers 67 33**
The switch automatically configures the egress queue buffer sizes. It configures the bandwidth and the SRR mode (shaped or shared) on the egress queues mapped to the port.	C2970(config)# **mls qos queue-set output 1 threshold 1 138 138 92 138** C2970(config)# **mls qos queue-set output 1 threshold 2 138 138 92 400** C2970(config)# **mls qos queue-set output 1 threshold 3 36 77 100 318** C2970(config)# **mls qos queue-set output 1 threshold 4 20 50 67 400** C2970(config)# **mls qos queue-set output 2 threshold 1 149 149 100 149** C2970(config)# **mls qos queue-set output 2 threshold 2 118 118 100 235** C2970(config)# **mls qos queue-set output 2 threshold 3 41 68 100 272** C2970(config)# **mls qos queue-set output 2 threshold 4 42 72 100 242** C2970(config)# **mls qos queue-set output 1 buffers 10 10 26 54** C2970(config)# **mls qos queue-set output 2 buffers 16 6 17 61** C2970(config-if)# **srr-queue bandwidth shape 10 0 0 0** C2970(config-if)# **srr-queue bandwidth share 10 10 60 20**

Table 2-3 Catalyst 2970/3560/3750 Auto-QoS Generated Configuration

If you entered the **auto qos voip trust** command, the switch automatically sets the ingress classification to trust the CoS value received in the packet on a nonrouted port by using the **mls qos trust cos** command.	`C2970(config-if)#` **`mls qos trust cos`**
	`C2970(config-if)#` **`mls qos trust dscp`**

If you entered the **auto qos voip cisco-phone** command, the switch automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP Phone.	`C2970(config-if)#` **`mls qos trust device cisco-phone`**

If you entered the **auto qos voip cisco-softphone** command, the switch automatically creates class maps and policy maps.	`C2970(config)#` **`mls qos map policed-dscp 24 26 46 to 0`**
	`C2970(config)#` **`class-map match-all AutoQoS-VoIP-RTP-Trust`**
	`C2970(config-cmap)#` **`match ip dscp ef`**
	`C2970(config)#` **`class-map match-all AutoQoS-VoIP-Control-Trust`**
	`C2970(config-cmap)#` **`match ip dscp cs3 af31`**
	`C2970(config)#` **`policy-map AutoQoS-Police-SoftPhone`**
	`C2970(config-pmap)#` **`class AutoQoS-VoIP-RTP-Trust`**
	`C2970(config-pmap-c)#` **`set dscp ef`**
	`C2970(config-pmap-c)#` **`police 320000 8000 exceed-action policed-dscp-transmit`**
	`C2970(config-pmap)#` **`class AutoQoS-VoIP-Control-Trust`**
	`C2970(config-pmap-c)#` **`set dscp cs3`**
	`C2970(config-pmap-c)#` **`police 32000 8000 exceed-action policed-dscp-transmit`**

After creating the class maps and policy maps, the switch automatically applies the policy map called *AutoQoS-Police-SoftPhone* to an ingress interface on which auto-QoS with the Cisco SoftPhone feature is enabled.	`C2970(config-if)#` **`service-policy input AutoQoS-Police-SoftPhone`**

Catalyst 2970/3560/3750—Untrusted PC + SoftPhone with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

The Untrusted PC + SoftPhone + Scavenger model configuration for the Catalyst 2970/3560/3750 is identical to the Catalyst 3550 for the same access edge model and is shown below.

Example 2-28 Catalyst 2970/3560/3750—Untrusted PC + SoftPhone + Scavenger Model Configuration

```
CAT2970(config)#mls qos map policed-dscp  0 24 46 to 8
    ! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT2970(config)#
CAT2970(config)#class-map match-all SOFTPHONE-VOICE
CAT2970(config-cmap)#  match access-group name SOFTPHONE-VOICE
CAT2970(config-cmap)#class-map match-all SOFTPHONE-SIGNALING
CAT2970(config-cmap)#  match access-group name SOFTPHONE-SIGNALING
CAT2970(config-cmap)#exit
CAT2970(config)#
CAT2970(config)#policy-map SOFTPHONE-PC
CAT2970(config-pmap)#class SOFTPHONE-VOICE
CAT2970(config-pmap-c)# set ip dscp 46           ! Softphone VoIP is marked to DSCP EF
CAT2970(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile SoftPhone voice traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class SOFTPHONE-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24               ! Signaling is marked to DSCP CS3
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Signaling traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)#exit
CAT2970(config)#
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)# service-policy input SOFTPHONE-PC            ! Applies policy to int
CAT2970(config-if)#exit
CAT2970(config)#
CAT2970(config)#ip access list  extended SOFTPHONE-VOICE
CAT2970(config-ext-nacl)# permit udp any any range 16384 32767             ! VoIP ports
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list  extended SOFTPHONE-SIGNALING
CAT2970(config-ext-nacl)# permit tcp any any range 2000 2002                ! SCCP ports
CAT2970(config-ext-nacl)#end
CAT2970#
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for the Untrusted PC + SoftPhone model include the following:

- show mls qos
- show mls qos map
- show mls qos interface
- show mls qos interface policers
- show class-map
- show policy-map
- show policy interface

Catalyst 2970/3560/3750—Untrusted Server with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

The Untrusted Multi-Application Server model configuration for the Catalyst 2970/3560/3750 is identical to the Catalyst 3550 and is shown below.

Example 2-29 Catalyst 2970/3560/3750—Untrusted Multi-Application Server with Scavenger-Class QoS Model Configuration

```
CAT2970(config)#mls qos map policed-dscp  0 10 18 25 to 8
  ! Excess traffic marked 0 or AF11 or AF21 or DSCP 25 will be remarked to CS1
CAT2970(config)#
CAT2970(config)#class-map SAP
CAT2970(config-cmap)# match access-group name SAP
CAT2970(config-cmap)#class-map LOTUS
CAT2970(config-cmap)# match access-group name LOTUS
CAT2970(config-cmap)#class-map IMAP
CAT2970(config-cmap)# match access-group name IMAP
CAT2970(config-cmap)#exit
CAT2970(config)#
CAT2970(config)#policy-map UNTRUSTED-SERVER
CAT2970(config-pmap)#class SAP
CAT2970(config-pmap-c)# set ip dscp 25              ! SAP is marked as Mission-Critical
CAT2970(config-pmap-c)# police 15000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile SAP is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class LOTUS
CAT2970(config-pmap-c)# set ip dscp 18              ! Lotus is marked as Transactional
CAT2970(config-pmap-c)# police 35000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile LOTUS is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class IMAP
CAT2970(config-pmap-c)# set ip dscp 10                  ! IMAP is marked as Bulk Data
CAT2970(config-pmap-c)# police 50000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile IMAP is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 1000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile excess data traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)#exit
CAT2970(config)#
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)# service-policy input UNTRUSTED-SERVER
CAT2970(config-if)#exit
CAT2970(config)#
CAT2970(config)#ip access list  extended SAP
CAT2970(config-ext-nacl)# permit tcp any range 3200 3203 any
CAT2970(config-ext-nacl)# permit tcp any eq 3600 any
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list  extended LOTUS
CAT2970(config-ext-nacl)# permit tcp any eq 1352 any
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list  extended IMAP
CAT2970(config-ext-nacl)# permit tcp any eq 143 any
CAT2970(config-ext-nacl)# permit tcp any eq 220 any
CAT2970(config-ext-nacl)#end
CAT2970#
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for the Untrusted Multi-Application Server model include the following:

- show mls qos
- show mls qos map
- show mls qos interface
- show mls qos interface policers
- show class-map
- show policy-map
- show policy interface

Catalyst 2970/3560/3750—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

At the time of writing, the Catalyst 2970/3560/3750 does not fully support per-port/per-VLAN policing due to hardware restrictions. Therefore, access lists are required to match voice and signaling traffic sourced from the VVLAN. These ACLs require the administrator to specify the VVLAN subnet information. The configuration for a Conditionally-Trusted IP Phone and PC (Basic Model) for a Catalyst 2970/3560/3750 is shown below.

Example 2-30 Catalyst 2970/3560/3750—Conditionally-Trusted IP Phone + PC + Scavenger (Basic) Model Configuration

```
CAT2970(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
    ! Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF
CAT2970(config)#mls qos map policed-dscp 0 24 to 8
    ! Excess VVLAN & DVLAN traffic will be remarked to Scavenger (CS1)
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)#  match access-group name VVLAN-VOICE
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#  match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)#  match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)#
CAT2970(config-cmap)#policy-map IPPHONE+PC-BASIC
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46                                 ! DSCP EF (Voice)
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
```

```
    ! Only one voice call is permitted per switchport VVLAN
CAT2970(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24                     ! DSCP CS3 (Call-Signaling)
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile call signaling is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Unauthorized VVLAN traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)#exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)# switchport access vlan 10                                 ! DVLAN
CAT2970(config-if)# switchport voice vlan 110                                 ! VVLAN
CAT2970(config-if)# service-policy input IPPHONE+PC-BASIC          ! Attaches policy
CAT2970(config-if)#exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#ip access list  extended VVLAN-VOICE
CAT2970(config-ext-nacl)#permit udp 10.1.110.0 0.0.0.255
    any range 16384 32767
    ! Voice is matched by VVLAN subnet and VoIP UDP port-range
CAT2970(config-ext-nacl)#exit
CAT2970(config)#
CAT2970(config)#ip access list  extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)#permit tcp 10.1.110.0 0.0.0.255
any range 2000 2002
    ! Call Signaling is matched by VVLAN subnet and Call-Signaling TCP port-range(s)
CAT2970(config-ext-nacl)#exit
CAT2970(config)#
CAT2970(config)#ip access list  extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip 10.1.110.0 0.0.0.255 any
! Matches all other traffic sourced from the VVLAN subnet
CAT2970(config-ext-nacl)#end
CAT2970#
```

Note At the time of writing, the Catalyst 2970/3560/3750 does not support a trust statement (such as **mls qos trust device cisco-phone**) in conjunction with a service-policy input statement applied to given port at the same time. While this may be configurable, if the switch is reset, one or the other statement may be removed when the switch reloads. This limitation is to be addressed; consult the latest Catalyst 2970/3560/3750 QoS documentation for updates on this limitation.

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for the Conditionally-Trusted IP Phone and PC with Scavenger-Class QoS (Basic) model include the following:

- show mls qos
- show mls qos map
- show mls qos interface
- show mls qos interface policers

- show class-map
- show policy-map
- show policy interface

Catalyst 2970/3560/3750—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

Building on the previous model, PC applications such as Interactive Video, Mission-Critical Data, Transactional Data, and Bulk Data are identified by access lists. The configuration for the Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model for the Catalyst 2970/3560/3750 is shown below.

Example 2-31 Catalyst 2970/3560/3750—Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model Configuration

```
CAT2970(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
    ! Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF
CAT2970(config)#mls qos map policed-dscp 0 10 18 24 25 34 to 8
! Excess DVLAN traffic marked 0, AF11, AF21, CS3, DSCP 25
! and AF41 will be remarked to Scavenger (CS1)
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)#  match access-group name VVLAN-VOICE
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#  match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)#  match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all DVLAN-PC-VIDEO
CAT2970(config-cmap)# match access-group name DVLAN-PC-VIDEO
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all DVLAN-MISSION-CRITICAL-DATA
CAT2970(config-cmap)# match access-group name DVLAN-MISSION-CRITICAL-DATA
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all DVLAN-TRANSACTIONAL-DATA
CAT2970(config-cmap)# match access-group name DVLAN-TRANSACTIONAL-DATA
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all DVLAN-BULK-DATA
CAT2970(config-cmap)# match access-group name DVLAN-BULK-DATA
CAT2970(config-cmap)#exit
CAT2970(config)#
CAT2970(config)#policy-map IPPHONE+PC-ADVANCED
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46                                  ! DSCP EF (Voice)
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
    ! Only one voice call is permitted per switchport VVLAN
```

```
CAT2970(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24                      ! DSCP CS3 (Call-Signaling)
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile call signaling is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
    ! Unauthorized VVLAN traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class DVLAN-PC-VIDEO
CAT2970(config-pmap-c)# set ip dscp 34                  ! DSCP AF41 (Interactive-Video)
CAT2970(config-pmap-c)# police 496000 8000 exceed-action policed-dscp-transmit
    ! Only one IP/VC stream will be permitted per switchport
CAT2970(config-pmap-c)#class DVLAN-MISSION-CRITICAL-DATA
CAT2970(config-pmap-c)# set ip dscp 25                  ! Interim Mission-Critical Data
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Mission-Critical Data is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class DVLAN-TRANSACTIONAL-DATA
CAT2970(config-pmap-c)# set ip dscp 18                  ! DSCP AF21 (Transactional Data)
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Transactional Data is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class DVLAN-BULK-DATA
CAT2970(config-pmap-c)# set ip dscp 10                      ! DSCP AF11 (Bulk Data)
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile Bulk Data is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
    ! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)#exit
CAT2970(config)#
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)# switchport access vlan 10                                 ! DVLAN
CAT2970(config-if)# switchport voice vlan 110                                 ! VVLAN
CAT2970(config-if)# service-policy input IPPHONE+PC-ADVANCED       ! Attaches Policy
CAT2970(config-if)#exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#ip access list  extended VVLAN-VOICE
CAT2970(config-ext-nacl)#permit udp 10.1.110.0 0.0.0.255
    any range 16384 32767
    ! Voice is matched by VVLAN subnet and DSCP EF
CAT2970(config-ext-nacl)#exit
CAT2970(config)#
CAT2970(config)#ip access list  extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)#permit tcp 10.1.110.0 0.0.0.255
any range 2000 2002
    ! Call Signaling is matched by VVLAN subnet Call-Signaling TCP port-range(s)
CAT2970(config-ext-nacl)#exit
CAT2970(config)#
CAT2970(config)#ip access list  extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip 10.1.110.0 0.0.0.255 any
! Matches all other traffic sourced from the VVLAN subnet
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list  extended DVLAN-PC-VIDEO
CAT2970(config-ext-nacl)# permit udp any any range 16384 32767                ! IP/VC
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list  extended DVLAN-MISSION-CRITICAL-DATA
CAT2970(config-ext-nacl)# permit tcp any any range 3200 3203                  ! SAP
CAT2970(config-ext-nacl)# permit tcp any any eq 3600                          ! SAP
CAT2970(config-ext-nacl)# permit tcp any any range 2000 2002                  ! SCCP
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list  extended DVLAN-TRANSACTIONAL-DATA
CAT2970(config-ext-nacl)# permit tcp any any eq 1352                          ! Lotus
```

```
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list  extended DVLAN-BULK-DATA
CAT2970(config-ext-nacl)# permit tcp any any eq 143                            ! IMAP
CAT2970(config-ext-nacl)# permit tcp any any eq 220                            ! IMAP
CAT2970(config-ext-nacl)#end
CAT2970#
```

Note At the time of writing, the Catalyst 2970/3560/3750 does not support a trust statement (such as **mls qos trust device cisco-phone**) in conjunction with a service-policy input statement applied to given port at the same time. While this may be configurable, if the switch is reset, one or the other statement may be removed when the switch reloads. This limitation is to be addressed; consult the latest Catalyst 2970/3560/3750 QoS documentation for updates on this limitation.

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for the Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model include the following:

- show mls qos
- show mls qos map
- show mls qos interface
- show mls qos interface policers
- show class-map
- show policy-map
- show policy interface

Catalyst 2970/3560/3750—Queuing and Dropping

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Configuration

For the most part, the Catalyst 2970/3560/3750 is relatively compatible in QoS features and syntax with the Catalyst 3550, except with respect to queuing and dropping.

The Catalyst 2970/3560/3750 supports four egress queues, which can be configured on a per-interface basis to operate in either 4Q3T or 1P3Q3T modes. Additionally, the Catalyst 2970/3560/3750 supports two queue-sets, allowing certain interfaces to be configured in one manner and others to be configured in a different manner. For example, some interfaces may be assigned to Queue Set (qset) 1 operating in 4Q3T mode, while others may be assigned to Queue Set 2 operating in 1P3Q3T mode.

However, unlike the Catalyst 2950 and 3550, the Catalyst 2970/3560/3750 has Queue 1 (not Queue 4) as the optional priority queue. In a converged campus environment it is recommended to enable the priority queue via the **priority-queue out** interface command.

Note The Catalyst 2970/3560/3750 also supports two configurable ingress queues (normal and expedite). Ingress scheduling, however, is rarely—if ever—required, as it only becomes enabled if the combined input rates from any/all switch ports exceed the switch fabric's capacity. Such cases are extremely difficult to achieve, even in controlled lab environments. In the extreme case where such a scenario develops in a production environment, the default settings of the ingress queues are acceptable to maintain VoIP quality and network availability.

The three remaining egress queues on the Catalyst 2970/3560/3750 are scheduled by a Shaped Round-Robin (SRR) algorithm, which can be configured to operate in shaped mode or in shared mode. In shaped mode, assigned bandwidth is limited to the defined amount; in shared mode, any unused bandwidth is shared among other classes (as needed).

Shaped or Shared bandwidth weights can be assigned to a queue via the **srr-queue bandwidth shape** and **srr-queue bandwidth share** interface commands. Shaped mode weights override shared mode weights and use an inverse ratio (1/weight) to determine the shaping bandwidth for the queue. Furthermore, if shaped weights are set to 0, then the queue is operating in shared mode. For example, the following interface command **srr-queue bandwidth shape 3 0 0 0** would shape Q1 to 1/3 of the available bandwidth and set all other queues to operate in sharing mode.

To make the queuing structure consistent with examples provided for previously discussed platforms, Queues 2 through 4 should be set to operate in shared mode (which is the default mode of operation on Queues 2 through 4). The ratio of the shared weights determines the relative bandwidth allocations (the absolute values are meaningless). The ratio of the shared weights determines the relative bandwidth allocations (the absolute values are meaningless). Since the PQ of the Catalyst 2970/3560/3750 is Q1 (not Q4 as in the Catalyst 3550), the entire queuing model can be flipped upside down, with Q2 representing the Critical Data queue, Q3 representing the Best Effort queue, and Q4 representing the Scavenger/Bulk queue. Therefore, shared weights of 70, 25, and 5 can be assigned to Queues 2, 3, and 4, respectively.

Additionally, the Catalyst 2970/3560/3750 supports three Weighted Tail Drop (WTD) thresholds per queue. Two of these thresholds are configurable (explicit); the third is non-configurable (implicit), as it is set to the queue-full state (100%). These thresholds can be defined with the **mls qos queue-set output** qset-id **threshold** global command. The only queues that these thresholds need defining (away from defaults) are Queues 2 and 4. In Queue 2, it is recommended to set the first threshold to 70% and the second to 80%, which leaves the third (implicit) threshold set at 100% (the tail of the queue). In Queue 4, it is recommended to set the first threshold to 40%, leaving the default values for both the second and third thresholds at 100%.

Once the queues and thresholds have been defined, traffic can be assigned to queues and thresholds either by CoS values or DSCP values, using the **mls qos srr-queue output cos-map queue** and **mls qos srr-queue output dscp-map queue** global commands, respectively. While DSCP-to-Queue/Threshold maps override CoS-to-Queue/Threshold maps, these mappings should be as consistent as possible to ensure predictable behavior and simplify troubleshooting.

That being said, CoS 0/DSCP 0 (Best Effort traffic) should be mapped to Queue 3 Threshold 3 (the tail of the queue), as no other traffic is to be assigned to Queue 3.

CoS 1 (Scavenger and Bulk) should be mapped to Queue 4 Threshold 3. Scavenger traffic can then be further contained by a DSCP-to-Queue/Threshold mapping assigning DSCP CS1 to Queue 4 Threshold 1 (previously set at 40%); Bulk Data using DSCP values AF11, AF12, or AF13 (decimal values 10, 12, and 14, respectively) can then use the remainder of the queue. Bulk Data can use either Threshold 2 or Threshold 3 as its WTD limit (both of which are set to 100%).

CoS 2 and DSCP CS2, AF21, AF22, and AF23 (decimal values 16, 18, 20, and 22, respectively) can be assigned to Queue 2 Threshold 1 (previously set at 70%). This limits Network Management and Transactional Data to a subset of the Queue 2. The temporary marking value for Mission-Critical traffic, DSCP 25, should also be assigned to Queue2 Threshold 1.

CoS 3, along with DSCP CS3 and AF31 (decimal values 24 and 26, respectively) can be assigned to Queue 2 Threshold 2 (previously set to 80%). This allows for preferential treatment of call signaling traffic within Queue 2.

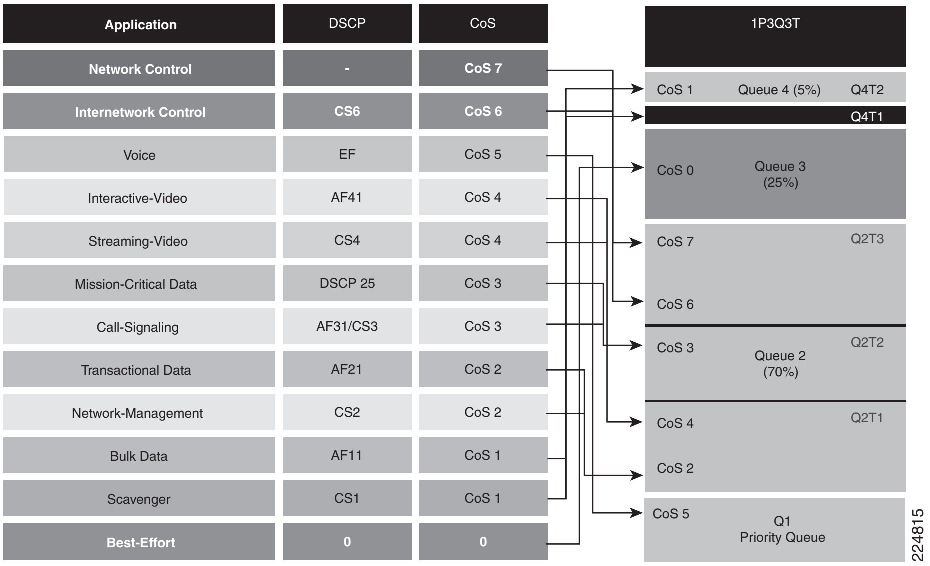
CoS 4 and DSCP CS4, AF41, AF42, and AF43 (decimal values 32, 34, 36, and 38, respectively) can be assigned to Queue 2 Threshold 1. In this manner, video (both Interactive and Streaming) does not drown out call signaling or Network/Internetwork Control traffic within Queue 2.

CoS 5 and DSCP EF (decimal value 46) should be assigned to Queue 1 Threshold 3, as Voice is the only traffic to be assigned to the strict-priority queue.

CoS 6 and DSCP CS6 (decimal value 48) and CoS 7 and DSCP CS7 (decimal value 56) should be assigned to Queue 2 Threshold 3. In this manner, there is always some room available in Queue 2 to service Network and Internetwork Control traffic.

These recommended Catalyst 2970/3560/3750 CoS/DSCP to Queue/Threshold assignments are illustrated in Figure 2-18.

Figure 2-18 Catalyst 2970/3560/3750 1P3Q3T Queuing Model



Application	DSCP	CoS
Network Control	-	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive-Video	AF41	CoS 4
Streaming-Video	CS4	CoS 4
Mission-Critical Data	DSCP 25	CoS 3
Call-Signaling	AF31/CS3	CoS 3
Transactional Data	AF21	CoS 2
Network-Management	CS2	CoS 2
Bulk Data	AF11	CoS 1
Scavenger	CS1	CoS 1
Best-Effort	0	0

The Catalyst 2970/3560/3750 queuing and dropping configuration recommendations are shown below.

Example 2-32 Catalyst 2970/3560/3750—Queuing and Dropping

```
CAT2970(config)#mls qos srr-queue output cos-map queue 1 threshold 3  5
    ! Maps CoS 5 to Queue 1 Threshold 3 (Voice gets all of Queue 1)
CAT2970(config)#mls qos srr-queue output cos-map queue 2 threshold 1  2 4
    ! Maps CoS 2 and CoS 4 to Queue 2 Threshold 1
CAT2970(config)#mls qos srr-queue output cos-map queue 2 threshold 2  3
    ! Maps CoS 3 to Queue 2 Threshold 2
CAT2970(config)#mls qos srr-queue output cos-map queue 2 threshold 3  6 7
    ! Maps CoS 6 and CoS 7 to Queue 2 Threshold 3
CAT2970(config)#mls qos srr-queue output cos-map queue 3 threshold 3  0
    ! Maps CoS 0 to Queue 3 Threshold 3 (Best Efforts gets all of Q3)
```

```
CAT2970(config)#mls qos srr-queue output cos-map queue 4 threshold 3  1
    ! Maps CoS1 to Queue 4 Threshold 3 (Scavenger/Bulk gets all of Q4)
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#mls qos srr-queue output dscp-map queue 1 threshold 3  46
    ! Maps DSCP EF (Voice) to Queue 1 Threshold 3
CAT2970(config)#mls qos srr-queue output dscp-map queue 2 threshold 1  16
    ! Maps DSCP CS2 (Network Management) to Queue 2 Threshold 1
CAT2970(config)#mls qos srr-queue output dscp-map queue 2 threshold 1  18 20 22
    ! Maps DSCP AF21, AF22, AF23 (Transactional Data) to Queue 2 Threshold 1
CAT2970(config)#mls qos srr-queue output dscp-map queue 2 threshold 1  25
    ! Maps DSCP 25 (Mission-Critical Data) to Queue 2 Threshold 1
CAT2970(config)#mls qos srr-queue output dscp-map queue 2 threshold 1  32
    ! Maps DSCP CS4 (Streaming Video) to Queue 2 Threshold 1
CAT2970(config)#mls qos srr-queue output dscp-map queue 2 threshold 1  34 36 38
    ! Maps DSCP AF41, AF42, AF43 (Interactive-Video) to Queue 2 Threshold 1
CAT2970(config)#mls qos srr-queue output dscp-map queue 2 threshold 2  24 26
    ! Maps DSCP CS3 and DSCP AF31 (Call-Signaling) to Queue 2 Threshold 2
CAT2970(config)#mls qos srr-queue output dscp-map queue 2 threshold 3  48 56
    ! Maps DSCP CS6 and CS7 (Network/Internetwork) to Queue 2 Threshold 3
CAT2970(config)#mls qos srr-queue output dscp-map queue 3 threshold 3  0
    ! Maps DSCP 0 (Best Effort) to Queue 3 Threshold 3
CAT2970(config)#mls qos srr-queue output dscp-map queue 4 threshold 1  8
    ! Maps DSCP CS1 (Scavenger) to Queue 4 Threshold 1
CAT2970(config)#mls qos srr-queue output dscp-map queue 4 threshold 3  10 12 14
    ! Maps DSCP AF11, AF12, AF13 (Bulk Data) to Queue 4 Threshold 3
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#mls qos queue-set output 1 threshold 2 70 80 100 100
    ! Sets Q2 Threshold 1 to 70% and Q2 Threshold 2 to 80%
CAT2970(config)#mls qos queue-set output 1 threshold 4 40 100 100 100
    ! Sets Q4 Threshold 1 to 40% and Q4 Threshold 2 to 100%
CAT2970(config)#
CAT2970(config)#interface range GigabitEthernet0/1 - 28
CAT2970(config-if-range)# queue-set 1
    ! Assigns interface to Queue-Set 1 (default)
CAT2970(config-if-range)# srr-queue bandwidth share 1 70 25 5
    ! Q2 gets 70% of remaining BW; Q3 gets 25% and Q4 gets 5%
CAT2970(config-if-range)# srr-queue bandwidth shape  3 0  0  0
    ! Q1 is limited to 1/3 of the total available BW
CAT2970(config-if-range)# priority-queue out
    ! Q1 is enabled as a PQ
CAT2970(config-if-range)#end
CAT2970#
```

Catalyst MLS QoS Verification Commands

Catalyst MLS QoS verification commands for queuing and dropping include the following:

- show mls qos interface buffers
- show mls qos interface queueing
- show mls qos queue-set
- show mls qos maps cos-output-q
- show mls qos maps dscp-output-q

show mls qos queue-set

The **show mls qos queue-set** verification command returns the configured buffer allocations and defined thresholds for each queue-set.

In the example below, each queue has a default buffer allocation of 25%. Additionally, all WTD Thresholds are set to 100% (the tail of the queue), except for Queue 2 Threshold 1 (set to 70%), Queue 2 Threshold 2 (set to 80%), and Queue 4 Threshold 1 (set to 40%).

Example 2-33 Show MLS QoS Queue-Set Verification for a Catalyst 2970/3560/3750 Switch

```
CAT2970#show mls qos queue-set 1
Queueset: 1
Queue     :       1       2       3       4
----------------------------------------------
buffers   :      25      25      25      25
threshold1:     100      70     100      40
threshold2:     100      80     100     100
reserved  :      50     100      50     100
maximum   :     400     100     400     100
CAT2970#
```

show mls qos maps cos-output-q

The **show mls qos maps cos-output-q** verification command truncates the **show mls qos maps** output to only report the CoS-to-Queue/Threshold mappings for egress queues.

In the example below, CoS 0 is mapped to Q3T3, CoS 1 is mapped to Q4T3, CoS 2 is mapped to Q2T1, CoS 3 is mapped to Q2T2, CoS 4 is mapped to Q2T1, CoS 5 is mapped to Q1T3 (the PQ), and CoS 6 and CoS 7 are mapped to Q2T3.

Example 2-34 Show MLS QoS Maps CoS-Output-Q Verification for a Catalyst 2970/3560/3750 Switch

```
CAT2970#show mls qos maps cos-output-q
   Cos-outputq-threshold map:
              cos:  0   1   2   3   4   5   6   7
              ------------------------------------
  queue-threshold: 3-3 4-3 2-1 2-2 2-1 1-3 2-3 2-3


CAT2970#
```

show mls qos maps dscp-output-q

The **show mls qos maps dscp-output-q** verification command truncates the **show mls qos maps** output to only report the DSCP-to-Queue/Threshold mappings for egress queues. The output is shown in tabular form, with the first digit of the decimal DSCP value in rows and the second digit in columns.

In the example below, only standard DSCP PHBs are being mapped away from the default settings (with the exception of the temporary marking of DSCP 25 for Mission-Critical Data). The other non-standard values may be mapped to reflect the CoS-to-Queue mappings, but for example simplicity this has not been done in this case.

Specifically, DSCP 0 is mapped to Q3T3; DSCP CS1 (8) is mapped to Q4T1; DSCP AF11, AF12, and AF13 (10, 12, 14) are mapped to Q4T3; DSCP CS2 (16) is mapped to Q2T1 as are DSCP AF21, AF22, and AF23 (18, 20, 22); DSCP CS3 (24) and AF31 (26) are mapped to Q2T2; DSCP CS4 (32) is mapped to Q2T1 as are DSCP AF41, AF42, and AF43 (34, 36, 38); DSCP EF (46) is mapped to Q1T3 (the PQ); DSCP CS6 (48) and CS7 (56) are mapped to Q2T3. The non-standard DSCP 25 is mapped to Q2T1.

Example 2-35 Show MLS QoS Maps DSCP-Output-Q Verification for a Catalyst 2970/3560/3750 Switch

```
CAT2970#show mls qos maps dscp-output-q
```

```
   Dscp-outputq-threshold map:
     d1 :d2    0     1     2     3     4     5     6     7     8     9
     ------------------------------------------------------------
      0 :    03-03 02-01 02-01 02-01 02-01 02-01 02-01 02-01 04-01 02-01
      1 :    04-03 02-01 04-03 02-01 04-03 02-01 02-01 03-01 02-01 03-01
      2 :    02-01 03-01 02-01 03-01 02-02 02-01 02-02 03-01 03-01 03-01
      3 :    03-01 03-01 02-01 04-01 02-01 04-01 02-01 04-01 02-01 04-01
      4 :    01-01 01-01 01-01 01-01 01-01 01-01 01-03 01-01 02-03 04-01
      5 :    04-01 04-01 04-01 04-01 04-01 04-01 02-03 04-01 04-01 04-01
      6 :    04-01 04-01 04-01 04-01

CAT2970#
```

Catalyst 4500 Supervisor II+/III/IV/V—QoS Considerations and Design

This section includes the following topics:

- Catalyst 4500—Trusted Endpoint Model
- Catalyst 4500—Auto QoS VoIP Model
- Catalyst 4500—Untrusted PC + SoftPhone with Scavenger-Class QoS Model
- Catalyst 4500—Untrusted Server with Scavenger-Class QoS Model
- Catalyst 4500 —Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model
- Catalyst 4500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model
- Catalyst 4500—Queuing

The Catalyst 4500 with Supervisors II+, III, IV, and V can be found at either the access layer or the distribution layer of the campus. Furthermore, due to their high performance, they may also be found at the core layer of some campus networks.

The QoS design options for access layer Catalyst 4500 design are shown in Figure 2-19; the distribution and/or core layer recommendations are shown in Figure 2-20.

Figure 2-19 Access Layer Catalyst 4500 QoS Design Options

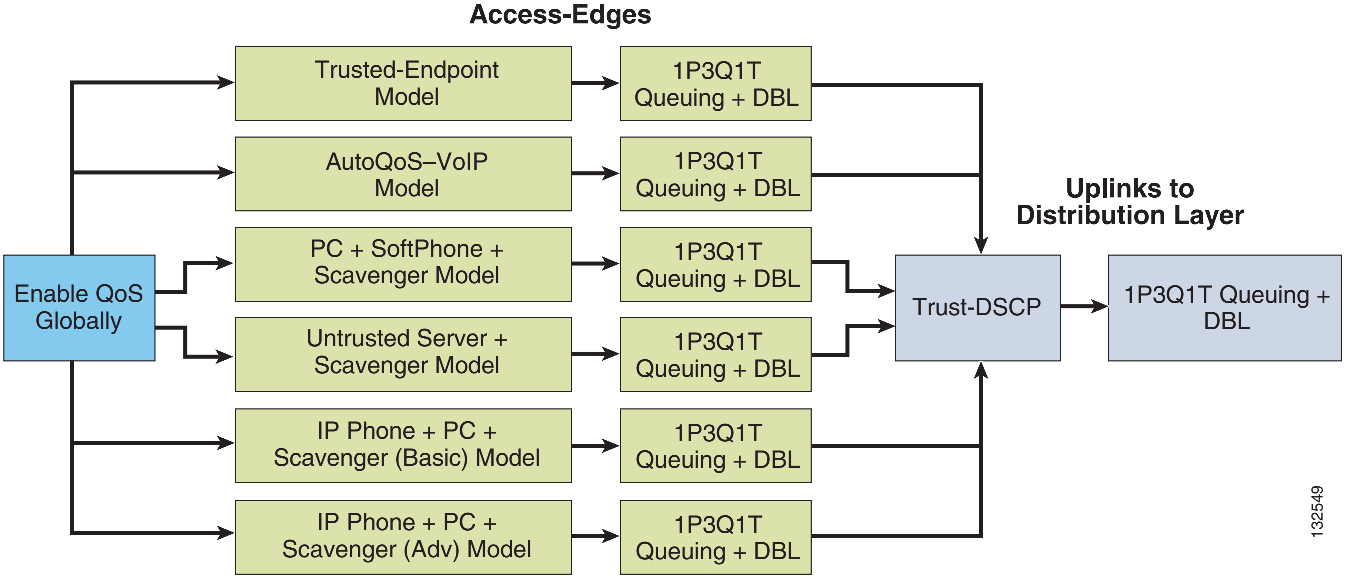
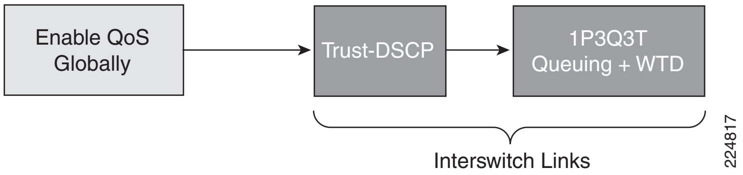


Figure 2-20 Distribution and/or Core Layer Catalyst 4500 QoS Design



Note To narrow the scope of our discussion to the most current and relevant versions of the Catalyst 4500 switch family, only the Catalyst 4500 with Supervisors II+, III, IV and V are examined in this design chapter. For discussions of older versions of Catalyst 4000/4500s, refer to the Cisco Press book, *Cisco Catalyst QoS: Quality of Service in Campus Networks*, by Mike Flannagan, Richard Froom, and Kevin Turek.

Much of the Catalyst MLS QoS syntax is supported on the Catalyst 4500; however, the **mls** prefix keyword is usually omitted from the configuration commands. For example, as with the Catalyst 3550 and 2970/3560/3750, QoS is globally disabled on the Catalyst 4500 by default. However, the command to enable QoS globally on a Catalyst 4500 is simply **qos**, not **mls qos**.

The verification commands are issued in the same manner, with the **mls** keyword omitted. Generally speaking, **show mls qos [...]** verification commands from other Catalyst platforms are translated to **show qos [...]** verification commands on the Catalyst 4500 platforms.

While QoS is globally disabled on the Catalyst 4500, all frames/packets are passed-through the switch unaltered (which is equivalent to a trust CoS and trust DSCP state on all ports). When QoS is globally enabled, however, then all DSCP and CoS values are (by default) set to 0 (which is equivalent to an untrusted state on all ports).

The verification command to check whether QoS has been globally enabled on the Catalyst 4500, along with the configuration command, are shown below.

Example 2-36 Enabling QoS Globally on the Catalyst 4500

```
CAT4500#show qos
QoS is disabled globally
IP header DSCP rewrite is enabled

CAT4500#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
CAT4500(config)#qos
CAT4500(config)#end
CAT4500#

CAT4500#show qos
QoS is enabled globally
IP header DSCP rewrite is enabled

CAT4500#
```

Catalyst 4500—Trusted Endpoint Model

This section includes the following topics:

- Configuration
- Catalyst 4500 QoS Verification Commands

Configuration

To enable a given Catalyst 4500 interface to trust the DSCP markings of an endpoint, the **qos trust dscp** interface command is used as shown below.

Example 2-37 Catalyst 4500—Trusted Endpoint Model Configuration

```
CAT4500(config)#interface FastEthernet2/1
CAT4500(config-if)# qos trust dscp
CAT4500(config-if)#end
CAT4500#
```

Catalyst 4500 QoS Verification Commands

Catalyst 4500 QoS verification commands for the Catalyst 4500 Untrusted Endpoint model include the following:

- show qos
- show qos interface

Note Since most Catalyst 4500 verification commands are reasonably similar to the MLS QoS verification commands previously discussed (albeit without the **mls** keyword), to minimize redundancy MLS QoS verification commands that have already been detailed are not repeated in this section.

Catalyst 4500—Auto QoS VoIP Model

The Catalyst 4500 supports AutoQoS VoIP with the following keyword options:

- **auto qos voip cisco-phone**
- **auto qos voip trust**

When you enable AutoQoS VoIP on the Catalyst 4500 by using the **auto qos voip cisco-phone** or the **auto qos voip trust** interface configuration commands, the switch automatically generates a QoS configuration based on the traffic type and ingress packet label and applies the commands listed in Table 2-4 to the interface.

Table 2-4 Catalyst 4500 AutoQoS Generated Configuration

Description	Automatically Generated Command
The switch automatically enables standard QoS and DBL configures the cos-to-DSCP map (maps CoS values in incoming packets to a DSCP value).	C4500(config)# **qos** C4500(config)# **qos map cos 3 to 26** C4500(config)# **qos dbl** C4500(config)# **qos map cos 5 to 46**
The switch automatically configures the DSCP-to-Tx-queue mapping.	C4500(config)# **qos map dscp 24 25 26 27 b28 29 30 31 to tx-queue 4** C4500(config)# **qos map dscp 32 33 34 35 36 37 38 39 to tx-queue 4**
The switch automatically sets the ingress classification on the interface to trust the CoS/DSCP value received in the packet.	C4500(config-if)# **qos trust cos** or C4500(config-if)# **qos trust dscp**
The switch automatically creates a QoS service policy, enables DBL on the policy, and attaches it to the interface.	C4500(config)# **policy-map autoqos-voip-policy** C4500(config-pmap)# **class class-default** C4500(config-pmap-c)# **dbl**
If you entered the **auto qos voip cisco-phone** command, the switch automatically enables the trusted boundary feature, which uses the CDP to detect the presence or absence of a Cisco IP phone.	C4500(config-if)# **qos trust device cisco-phone**
The switch assigns a higher priority for queue 3. Limit for shaping on queue 3 is selected so that it is 33 percent of the link speed. Configure shaping as 33 percent on those ports where sharing is supported. This procedure ensures that the higher-priority queue does not starve other queues.	C4500(config-if)# **tx-queue 3** C4500(config-if-tx-queue)# **priority high** C4500(config-if-tx-queue)# **shape percent 33** C4500(config-if-tx-queue)# **bandwidth percent 33**

Catalyst 4500—Untrusted PC + SoftPhone with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst 4500 QoS Verification Commands

Configuration

The Untrusted PC + Softphone + Scavenger access edge model for Catalyst 4500s is similar to the examples given on previously discussed platforms. A few distinctions exist, such as the absence of the **mls** keyword in defining the policed-DSCP map (along with some slight syntax variation for this command) and the (optional) use of the **kbps** and **mbps** (denoting kilobits and megabits, respectively) within the policing statements.

Example 2-38 Catalyst 4500—Untrusted PC + SoftPhone + Scavenger Model Configuration

```
CAT4500-SUP4(config)#qos map dscp policed 0 24 46 to dscp 8
! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#class-map match-all SOFTPHONE-SIGNALING
CAT4500-SUP4(config-cmap)#  match access-group name SOFTPHONE-SIGNALING
CAT4500-SUP4(config-cmap)#class-map match-all SOFTPHONE-VOICE
CAT4500-SUP4(config-cmap)#  match access-group name SOFTPHONE-VOICE
CAT4500-SUP4(config-cmap)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#policy-map SOFTPHONE-PC
CAT4500-SUP4(config-pmap)# class SOFTPHONE-VOICE
CAT4500-SUP4(config-pmap-c)# set ip dscp ef
! Softphone VoIP is marked to DSCP EF
CAT4500-SUP4(config-pmap-c)# police 128 kbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile SoftPhone voice traffic is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class SOFTPHONE-SIGNALING
CAT4500-SUP4(config-pmap-c)# set ip dscp cs3
    ! SoftPhone call signaling is marked to DSCP CS3
CAT4500-SUP4(config-pmap-c)# police 32 kbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile Signaling traffic is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class class-default
CAT4500-SUP4(config-pmap-c)# set ip dscp default
CAT4500-SUP4(config-pmap-c)# police 5 mbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#interface FastEthernet2/1
CAT4500-SUP4(config-if)# service-policy input SOFTPHONE-PC             ! Applies policy
CAT4500-SUP4(config-if)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#ip access list  extended SOFTPHONE-VOICE
CAT4500-SUP4(config-ext-nacl)# permit udp any any range 16384 32767             ! VoIP
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended SOFTPHONE-SIGNALING
CAT4500-SUP4(config-ext-nacl)# permit tcp any any range 2000 2002               ! SCCP
CAT4500-SUP4(config-ext-nacl)#end
CAT4500-SUP4#
```

Catalyst 4500 QoS Verification Commands

Catalyst 4500 QoS verification commands for the Catalyst 4500 Untrusted PC + Softphone + Scavenger model include the following:

- show qos
- show qos maps
- show qos interface

- show class-map
- show policy-map
- show policy interface

Catalyst 4500—Untrusted Server with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst 4500 QoS Verification Commands

Configuration

The Catalyst 4500 Untrusted Multi-Application Server with Scavenger-Class QoS model is show below. The main changes for the Catalyst 4500 for this model are the syntax defining the policed-DSCP map and the policer definitions (using the abbreviation **mbps** for megabits per second).

Example 2-39 Catalyst 4500—Untrusted Multi-Application Server with Scavenger-Class QoS Model Configuration

```
CAT4500-SUP4(config)#qos map dscp policed 0 10 18 25 to dscp 8
  ! Excess traffic marked 0 or AF11 or AF21 or DSCP 25 will be remarked to CS1
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#class-map SAP
CAT4500-SUP4(config-cmap)# match access-group name SAP
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map LOTUS
CAT4500-SUP4(config-cmap)# match access-group name LOTUS
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map IMAP
CAT4500-SUP4(config-cmap)# match access-group name IMAP
CAT4500-SUP4(config-cmap)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#policy-map UNTRUSTED-SERVER
CAT4500-SUP4(config-pmap)#class SAP
CAT4500-SUP4(config-pmap-c)# set ip dscp 25
! SAP is marked as Mission-Critical (DSCP 25)
CAT4500-SUP4(config-pmap-c)#  police 15 mbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile SAP is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class LOTUS
CAT4500-SUP4(config-pmap-c)# set ip dscp 18
    ! Lotus is marked as Transactional Data (DSCP AF21)
CAT4500-SUP4(config-pmap-c)#  police 35 mbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile LOTUS is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class IMAP
CAT4500-SUP4(config-pmap-c)# set ip dscp 10
! IMAP is marked as Bulk Data (DSCP AF11)
CAT4500-SUP4(config-pmap-c)#  police 50 mbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile IMAP is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class class-default
CAT4500-SUP4(config-pmap-c)# set ip dscp 0
CAT4500-SUP4(config-pmap-c)#  police 1 mbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile excess data traffic is marked down to Scavenger (CS1)
```

```
CAT4500-SUP4(config-pmap-c)# exit
CAT4500-SUP4(config-pmap)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#interface FastEthernet2/1
CAT4500-SUP4(config-if)# service-policy input UNTRUSTED-SERVER
CAT4500-SUP4(config-if)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#ip access list  extended SAP
CAT4500-SUP4(config-ext-nacl)# permit tcp any range 3200 3203 any
CAT4500-SUP4(config-ext-nacl)# permit tcp any eq 3600 any
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended LOTUS
CAT4500-SUP4(config-ext-nacl)# permit tcp any eq 1352 any
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended IMAP
CAT4500-SUP4(config-ext-nacl)# permit tcp any eq 143 any
CAT4500-SUP4(config-ext-nacl)# permit tcp any eq 220 any
CAT4500-SUP4(config-ext-nacl)#end
CAT4500-SUP4#
```

Catalyst 4500 QoS Verification Commands

Catalyst 4500 QoS verification commands for the Catalyst 4500 Untrusted Server with Scavenger-Class QoS model include the following:

- show qos
- show qos maps
- show qos interface
- show class-map
- show policy-map
- show policy interface

Catalyst 4500 —Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model

This section includes the following topics:

- Configuration
- Catalyst 4500 QoS Verification Commands

Configuration

The Catalyst 4500 does not currently support per-port/per-VLAN policing. Therefore, access lists that include the VVLAN subnet are required to achieve granular policing of the VVLAN and DVLAN subnets, as shown below.

Example 2-40 Catalyst 4500—Conditionally-Trusted IP Phone + PC + Scavenger (Basic) Model Configuration

```
CAT4500-SUP4(config)#qos map cos 5 to dscp 46
! Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF
```

```
CAT4500-SUP4(config)#qos map dscp policed 0 24 to dscp 8
    ! Excess DVLAN & VVLAN traffic will be marked down to Scavenger (CS1)
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#class-map match-all VVLAN-VOICE
CAT4500-SUP4(config-cmap)#  match access-group name VVLAN-VOICE
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-cmap)#  match access-group name VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all VVLAN-ANY
CAT4500-SUP4(config-cmap)#  match access-group name VVLAN-ANY
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#policy-map IPPHONE+PC-BASIC
CAT4500-SUP4(config-pmap)#class VVLAN-VOICE
CAT4500-SUP4(config-pmap-c)# set ip dscp 46                         ! DSCP EF (Voice)
CAT4500-SUP4(config-pmap-c)# police 128 kbps 8000 byte exceed-action drop
    ! Only one voice call is permitted per switchport VVLAN
CAT4500-SUP4(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-pmap-c)# set ip dscp 24                ! DSCP CS3 (Call-Signaling)
CAT4500-SUP4(config-pmap-c)# police 32 kbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Out-of-profile call signaling is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class VVLAN-ANY
CAT4500-SUP4(config-pmap-c)# set ip dscp 0
CAT4500-SUP4(config-pmap-c)# police 32 kbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Unauthorized VVLAN traffic is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class class-default
CAT4500-SUP4(config-pmap-c)# set ip dscp 0
CAT4500-SUP4(config-pmap-c)# police 5 mbps 8000 byte exceed-action
 policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)# exit
CAT4500-SUP4(config-pmap)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#interface FastEthernet2/1
CAT4500-SUP4(config-if)# switchport access vlan 10                          ! DVLAN
CAT4500-SUP4(config-if)# switchport voice vlan 110                          ! VVLAN
CAT4500-SUP4(config-if)# qos trust device cisco-phone             ! Conditional Trust
CAT4500-SUP4(config-if)# service-policy input IPPHONE+PC-BASIC
CAT4500-SUP4(config-if)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#ip access list  extended VVLAN-VOICE
CAT4500-SUP4(config-ext-nacl)# permit udp 10.1.110.0 0.0.0.255 any
 range 16384 32767
    ! Voice is matched by VVLAN subnet and UDP port-range
CAT4500-SUP4(config-ext-nacl)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#ip access list  extended VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-ext-nacl)# permit tcp 10.1.110.0 0.0.0.255 any
range 2000 2002
    ! Call Signaling is matched by VVLAN subnet and TCP port-range
CAT4500-SUP4(config-ext-nacl)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#ip access list  extended VVLAN-ANY
CAT4500-SUP4(config-ext-nacl)# permit ip 10.1.110.0 0.0.0.255 any
! Matches all other traffic sourced from the VVLAN subnet
CAT4500-SUP4(config-ext-nacl)#end
CAT4500-SUP4#
```

Catalyst 4500 QoS Verification Commands

Catalyst 4500 QoS verification commands for the Conditionally-Trusted IP Phone + PC + Scavenger (Basic) model include the following:

- show qos
- show qos maps
- show qos interface
- show class-map
- show policy-map
- show policy interface

Catalyst 4500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model

This section includes the following topics:

- Configuration
- Catalyst 4500 QoS Verification Commands

Configuration

Building on the previous model, PC applications, such as Interactive-Video, Mission-Critical Data, Transactional-Data, and Bulk-Data, are identified by access lists. The configuration for the Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model for the Catalyst 4500 is shown below.

Example 2-41 Catalyst 4500—Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model Configuration

```
CAT4500-SUP4(config)#qos map cos 5 to dscp 46
    ! Modifies CoS-to-DSCP mapping to map CoS 5 to DSCP EF
CAT4500-SUP4(config)#qos map dscp policed 0 10 18 24 25 34 to dscp 8
! Excess DVLAN traffic marked 0, AF11, AF21, CS3, DSCP 25
! and AF41 will be remarked to Scavenger (CS1)
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#class-map match-all VVLAN-VOICE
CAT4500-SUP4(config-cmap)#  match access-group name VVLAN-VOICE
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-cmap)#  match access-group name VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all VVLAN-ANY
CAT4500-SUP4(config-cmap)#  match access-group name VVLAN-ANY
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all DVLAN-PC-VIDEO
CAT4500-SUP4(config-cmap)# match access-group name DVLAN-PC-VIDEO
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all DVLAN-MISSION-CRITICAL-DATA
CAT4500-SUP4(config-cmap)# match access-group name DVLAN-MISSION-CRITICAL-DATA
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all DVLAN-TRANSACTIONAL-DATA
```

```
CAT4500-SUP4(config-cmap)# match access-group name DVLAN-TRANSACTIONAL-DATA
CAT4500-SUP4(config-cmap)#
CAT4500-SUP4(config-cmap)#class-map match-all DVLAN-BULK-DATA
CAT4500-SUP4(config-cmap)# match access-group name DVLAN-BULK-DATA
CAT4500-SUP4(config-cmap)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#policy-map IPPHONE+PC-ADVANCED
CAT4500-SUP4(config-pmap)#class VVLAN-VOICE
CAT4500-SUP4(config-pmap-c)# set ip dscp 46                             ! DSCP EF (Voice)
CAT4500-SUP4(config-pmap-c)# police 128 kbps 8000 byte exceed-action drop
    ! Only one voice call is permitted per switchport VVLAN
CAT4500-SUP4(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-pmap-c)# set ip dscp 24                 ! DSCP CS3 (Call-Signaling)
CAT4500-SUP4(config-pmap-c)# police 32 kbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Out-of-profile call signaling is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class VVLAN-ANY
CAT4500-SUP4(config-pmap-c)# set ip dscp 0
CAT4500-SUP4(config-pmap-c)# police 32 kbps 8000 byte exceed-action
 policed-dscp-transmit
! Unauthorized VVLAN traffic is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class DVLAN-PC-VIDEO
CAT4500-SUP4(config-pmap-c)# set ip dscp 34                 ! DSCP AF41 (Int-Video)
CAT4500-SUP4(config-pmap-c)# police 500 kbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Only one IP/VC stream will be permitted per switchport
CAT4500-SUP4(config-pmap-c)#class DVLAN-MISSION-CRITICAL-DATA
CAT4500-SUP4(config-pmap-c)# set ip dscp 25                 ! Interim Mission-Critical
CAT4500-SUP4(config-pmap-c)# police 5 mbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Out-of-profile Mission-Critical Data is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class DVLAN-TRANSACTIONAL-DATA
CAT4500-SUP4(config-pmap-c)# set ip dscp 18                                ! DSCP AF21
CAT4500-SUP4(config-pmap-c)# police 5 mbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Out-of-profile Transactional Data is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class DVLAN-BULK-DATA
CAT4500-SUP4(config-pmap-c)# set ip dscp 10                                ! DSCP AF11
CAT4500-SUP4(config-pmap-c)# police 5 mbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Out-of-profile Bulk Data is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#class class-default
CAT4500-SUP4(config-pmap-c)# set ip dscp 0
CAT4500-SUP4(config-pmap-c)# police 5 mbps 8000 byte exceed-action
 policed-dscp-transmit
    ! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT4500-SUP4(config-pmap-c)#exit
CAT4500-SUP4(config-pmap)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#interface FastEthernet2/1
CAT4500-SUP4(config-if)# switchport access vlan 10                             ! DVLAN
CAT4500-SUP4(config-if)# switchport voice vlan 110                             ! VVLAN
CAT4500-SUP4(config-if)# qos trust device cisco-phone               ! Conditional Trust
CAT4500-SUP4(config-if)# service-policy input IPPHONE+PC-ADVANCED
CAT4500-SUP4(config-if)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#ip access list  extended VVLAN-VOICE
CAT4500-SUP4(config-ext-nacl)# permit udp 10.1.110.0 0.0.0.255 any
 range 16384 32767
    ! Voice is matched by VVLAN subnet and UDP port-range
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended VVLAN-CALL-SIGNALING
CAT4500-SUP4(config-ext-nacl)# permit tcp 10.1.110.0 0.0.0.255 any
```

```
 range 2000 2002
   ! Call Signaling is matched by VVLAN subnet and TCP port-range
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended VVLAN-ANY
CAT4500-SUP4(config-ext-nacl)# permit ip 10.1.110.0 0.0.0.255 any
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended DVLAN-PC-VIDEO
CAT4500-SUP4(config-ext-nacl)# permit udp any any range 16384 32767
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended DVLAN-MISSION-CRITICAL-DATA
CAT4500-SUP4(config-ext-nacl)# permit tcp any any range 3200 3203             ! SAP
CAT4500-SUP4(config-ext-nacl)# permit tcp any any eq 3600                     ! SAP
CAT4500-SUP4(config-ext-nacl)# permit tcp any any range 2000 2002             ! SCCP
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended DVLAN-TRANSACTIONAL-DATA
CAT4500-SUP4(config-ext-nacl)# permit tcp any any eq 1352                     ! Lotus
CAT4500-SUP4(config-ext-nacl)#
CAT4500-SUP4(config-ext-nacl)#ip access list  extended DVLAN-BULK-DATA
CAT4500-SUP4(config-ext-nacl)# permit tcp any any eq 143                      ! IMAP
CAT4500-SUP4(config-ext-nacl)# permit tcp any any eq 220                      ! IMAP
CAT4500-SUP4(config-ext-nacl)#end
CAT4500-SUP4#
```

Catalyst 4500 QoS Verification Commands

Catalyst 4500 QoS verification commands for the Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) model include the following:

- show qos
- show qos maps
- show qos interface
- show class-map
- show policy-map
- show policy interface

Catalyst 4500—Queuing

This section includes the following topics:

- Configuration
- Catalyst 4500 QoS Verification Commands

Configuration

The Catalyst 4500 supports four egress queues for scheduling, which may be configured in either 4Q1T or 1P3Q1T modes. The strict-priority queue on the Catalyst 4500 is transmit-queue 3.

While tail-drop or WRED thresholds are not supported on the Catalyst 4500, it does support one of the most advanced congestion avoidance mechanisms in the Catalyst family. This congestion avoidance feature is performed by Dynamic Buffer Limiting (DBL). DBL tracks the queue length for each traffic flow in the switch and when the queue length of a flow exceeds its limit, DBL drops packets or sets the (RFC 3168) Explicit Congestion Notification (ECN) bits in the IP packet headers. DBL can be enabled globally with the **qos dbl** global command, as well as on a per-class basis within a policy-map with the **dbl** policy command. A default DBL policy can be applied to all transmit queues, as is shown in the example below.

By default, all queues are scheduled in a round robin manner. The third transmit queue can be designated as an optional strict-priority queue. This can be enabled with the **tx-queue 3** interface command followed by the **priority high** interface transmit-queue sub-command. This queue can be defined to be shaped to a peak limit, such as 30%, to allow bandwidth to be available to non-voice applications. This would be valuable in the event that a trust boundary has been compromised and a DoS/worm attack is saturating voice queues.

Bandwidth allocations can also be assigned to queues (for certain interfaces) using the **tx-queue** interface command followed by the **bandwidth** sub-command. Bandwidth allocations to queues can only be assigned on the following interface types:

- Uplink ports on supervisor engines
- Ports on the WS-X4306-GB linecard
- The 2 1000BASE-X ports on the WS-X4232-GB-RJ linecard
- The first 2 ports on the WS-X4418-GB linecard
- The two 1000BASE-X ports on the WS-X4412-2GB-TX linecard

The Catalyst 4500 does not support CoS-to-Queue mappings, only DSCP-to-Queue mappings. These can be defined with the **qos map dscp to tx-queue** global command.

Given these features and the objective to make queuing consistent across platforms, it is recommended to enable DBL globally on the Catalyst 4500, as well as enable Q3 as the strict-priority queue on all interfaces (such that the switch operates in 1P3Q1T mode). This queue can be shaped to 30% of the link's capacity. Furthermore, Q1 can then be used as the Scavenger/Bulk queue, Q2 as the Best-Effort queu,e and Q4 as the preferential queue.

On interfaces that support bandwidth allocation, 5% could be assigned to Q1, 25% to Q2, and 40% to Q3. Unlike bandwidth-weights that are used on other platforms, these bandwidth allocations are defined in absolute bps or as relative percentages of the link's bandwidth. In either case, they should not total in excess of the link's bandwidth-limit (1 Gbps or 100%), including the priority-bandwidth allocation for Q3.

By default, the DSCP-to-Queue assignments are as follows:

- DSCP 0-15 Queue 1
- DSCP 16-31 Queue 2
- DSCP 32-47 Queue 3
- DSCP 48-63 Queue 4

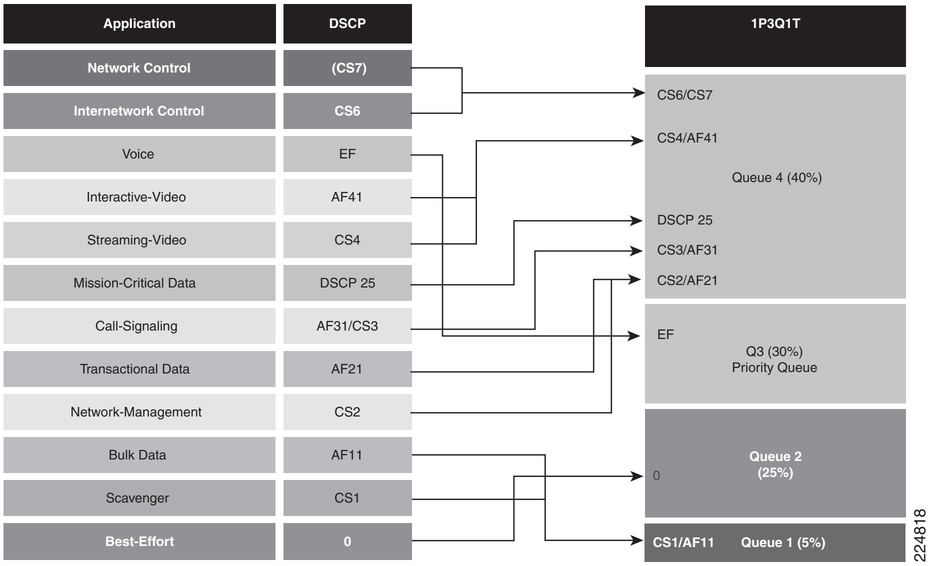
The recommended DSCP-to-Queue assignments for the Catalyst 4500 are as follows:

- DSCP 0 should be assigned to Q2
- DSCP CS1 (Scavenger) and DSCP AF11/AF12/AF13 (Bulk Data) should be assigned to Q1
- DSCP CS2 (Network Management) as well as AF21/AF22/AF23 (Transactional Data) should be assigned to Q4
- DSCP CS3 and AF31 (Call-Signaling) should be assigned to Q4
- DSCP 25 (temporary marking for Mission-Critical Data) should be assigned to Q4
- DSCP CS4 (Streaming Video) and AF41/AF42/AF43 (Interactive Video) should be assigned to Q4
- DSCP EF (Voice) should be assigned to Q3 (the strict priority queue)

- DSCP CS6 (Internetwork Control) and CS7 (Network Control/STP) should be assigned to Q4

The queuing recommendations for the Catalyst 4500 (Supervisors II+, III, IV and V) are shown in Figure 2-21.

Figure 2-21 Catalyst 4500-SupII+/III/IV/V 1P3Q1T Queuing Model



The configurations for enabling queuing on the Catalyst 4500 per these recommendations are shown below. Two separate examples are given, one for a FastEthernet interface that does not support bandwidth allocations and another for a GigabitEthernet interface that does. Some of the DSCP-to-Queue mappings are not required (as they overlap with the default settings), but are shown nonetheless to complete the logic of the example.

Example 2-42 Catalyst 4500—Queuing and Dropping

```
CAT4500-SUP4(config)#qos dbl
    ! Globally enables DBL
CAT4500-SUP4(config)#qos dbl exceed-action ecn
    ! Optional: Enables DBL to mark RFC 3168 ECN bits in the IP ToS Byte
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#qos map dscp 0 to tx-queue 2
    ! Maps DSCP 0 (Best Effort) to Q2
CAT4500-SUP4(config)#qos map dscp 8 10 12 14 to tx-queue 1
    ! Maps DSCP CS1 (Scavenger) and AF11/AF12/AF13 (Bulk) to Q1
CAT4500-SUP4(config)#qos map dscp 16 18 20 22 to tx-queue 4
    ! Maps DSCP CS2 (Net-Mgmt) and AF21/AF22/AF23 (Transactional) to Q4
CAT4500-SUP4(config)#qos map dscp 24 25 26 to tx-queue 4
    ! Maps DSCP CS3 and AF31 (Call-Signaling) and DSCP 25 (MC Data) to Q4
CAT4500-SUP4(config)#qos map dscp 32 34 36 38 to tx-queue 4
    ! Maps DSCP CS4 (Str-Video) and AF41/AF42/AF43 (Int-Video) to Q4
CAT4500-SUP4(config)#qos map dscp 46 to tx-queue 3
    ! Maps DSCP EF (VoIP) to Q3 (PQ)
CAT4500-SUP4(config)#qos map dscp 48 56 to tx-queue 4
    ! Maps DSCP CS6 (Internetwork) and CS7 (Network) Control to Q4
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#policy-map DBL
CAT4500-SUP4(config-pmap)#class class-default
CAT4500-SUP4(config-pmap-c)# dbl                    ! Enables DBL on all traffic flows
CAT4500-SUP4(config-pmap-c)# exit
```

```
CAT4500-SUP4(config-pmap)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#interface range FastEthernet2/1 - 48
CAT4500-SUP4(config-if-range)# service-policy output DBL            ! Applies DBL policy
CAT4500-SUP4(config-if-range)# tx-queue 3
CAT4500-SUP4(config-if-tx-queue)# priority high                     ! Enables Q3 as PQ
CAT4500-SUP4(config-if-tx-queue)# shape percent 30                  ! Shapes PQ to 30%
CAT4500-SUP4(config-if-tx-queue)# exit
CAT4500-SUP4(config-if-range)#exit
CAT4500-SUP4(config)#
CAT4500-SUP4(config)#interface range GigabitEthernet1/1 - 2
CAT4500-SUP4(config-if-range)# service-policy output DBL            ! Applies DBL policy
CAT4500-SUP4(config-if-range)# tx-queue 1
CAT4500-SUP4(config-if-tx-queue)# bandwidth percent 5               ! Q1 gets 5%
CAT4500-SUP4(config-if-tx-queue)# tx-queue 2
CAT4500-SUP4(config-if-tx-queue)# bandwidth percent 25              ! Q2 gets 25%
CAT4500-SUP4(config-if-tx-queue)# tx-queue 3
CAT4500-SUP4(config-if-tx-queue)# priority high                     ! Enables Q3 as PQ
CAT4500-SUP4(config-if-tx-queue)# bandwidth percent 30              ! PQ gets 30%
CAT4500-SUP4(config-if-tx-queue)# shape percent 30                  ! Shapes PQ to 30%
CAT4500-SUP4(config-if-tx-queue)# tx-queue 4
CAT4500-SUP4(config-if-tx-queue)# bandwidth percent 40              ! Q4 gets 40%
CAT4500-SUP4(config-if-tx-queue)#end
CAT4500-SUP4#
```

Catalyst 4500 QoS Verification Commands

Catalyst 4500 QoS verification commands for queuing include the following:

- show qos dbl
- show qos maps dscp tx-queue
- show qos interface

show qos dbl

The Catalyst 4500 **show qos dbl** verification command returns whether or not DBL has been enabled, as well as some of the operating parameters that have been defined for its operation. These parameters include allowing DBL to set RFC 3168 ECN bits in IP headers, as shown in the example below.

Example 2-43 Show QoS DBL Verification for a Catalyst 4500 Switch

```
CAT4500-SUP4#show qos dbl
QOS is enabled globally
DBL is enabled globally
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

CAT4500-SUP4#
```

show qos maps dscp tx-queue

The Catalyst 4500 **show qos maps dscp tx-queue** verification command truncates the **show qos maps** output to only report the DSCP-to-Queue mappings for egress queues. The output is shown in tabular form, with the first digit of the decimal DSCP value in rows and the second digit in columns.

In the example below, only DSCP 0 is mapped to Q2; DSCP CS1 (8) and AF11/AF12/AF13 (10/12/14) are mapped to Q1; DSCP CS2 (16) and AF22/AF22/AF23 (18/20/22) are mapped to Q4; DSCP CS3 (24) and AF31 (26) are mapped to Q4, as is the non-standard DSCP 25. DSCP CS4 (32) and AF41/AF42/AF43 (34/36/38) are mapped to Q4, as are DSCP CS6 (48) and CS7 (56). DSCP EF (46) is mapped to Q3.

Example 2-44 Show QoS Maps DSCP Tx-Queue Verification for a Catalyst 4500 Switch

```
CAT4500-SUP4#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                ! DSCP 0 => Q2; DSCP CS1 => Q1
 1 :    01 01 01 01 01 01 04 02 04 02                ! DSCP AF11/AF12/AF13 => Q1
                                                     ! DSCP CS2 and AF21 => Q4
 2 :    04 02 04 02 04 04 04 02 02 02                ! DSCP AF22/AF23 => Q4
                                                     ! DSCP CS3, 25 and AF31 => Q4
 3 :    02 02 04 03 04 03 04 03 04 03                ! DSCP CS4 and AF41/AF42/AF43 => Q4
 4 :    03 03 03 03 03 03 03 03 04 04                ! DSCP EF => Q3; DSCP CS6 => Q4
 5 :    04 04 04 04 04 04 04 04 04 04                ! DSCP CS7 => Q4
 6 :    04 04 04 04

CAT4500-SUP4#
```

show qos interface

The Catalyst 4500 **show qos interface** verification command displays the global state of QoS (enabled or not), the trust state of an interface, as well as any queuing/shaping parameters that have been defined for the interface.

In the first example below, the **show qos interface** command is being applied on an access-edge FastEthernet interface that has been configured to conditionally-trust Cisco IP Phones. Furthermore, the output reports that Q3 has been enabled as the priority-queue on this interface and is shaped to 30 Mbps (30%). Bandwidth cannot be assigned for non-priority queues on this interface, as is indicated by the "N/A" entries under the bandwidth column.

In the second example below, the **show qos interface** command is being applied to a GigabitEthernet uplink interface which as been configured to trust-DSCP. As before, Q3 has been enabled as the priority-queue and has been shaped to 30%, which now translates to 300 Mbps. Bandwidth is assignable on this interface and therefore Q1 is allocated 50 Mbps (5%), Q2 is allocated 250 Mbps (25%), Q3 is allocated 300 Mbps (30%), and Q4 is allocated 400 Mbps (40%).

Example 2-45 Show QoS Interface Verification for a Catalyst 4500 Switch

```
CAT4500-SUP4#show qos interface FastEthernet2/1
QoS is enabled globally
Port QoS is enabled
Administrative Port Trust State: 'cos'
Operational Port Trust State: 'cos'
Trust device: cisco-phone
Default DSCP: 0 Default CoS: 0
Appliance trust: none
Tx-Queue   Bandwidth   ShapeRate   Priority   QueueSize
```

```
             (bps)       (bps)                  (packets)
   1        N/A         disabled    N/A         240
   2        N/A         disabled    N/A         240
   3        N/A         30000000    high        240
   4        N/A         disabled    N/A         240

CAT4500-SUP4#
```

```
CAT4500-SUP4#show qos interface GigabitEthernet1/1
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         1920
   2        250000000   disabled    N/A         1920
   3        300000000   300000000   high        1920
   4        700000000   disabled    N/A         1920

CAT4500-SUP4#
```

Catalyst 6500 PFC2/PFC3—QoS Considerations and Design

This section includes the following topics:

- Catalyst 6500 QoS Configuration and Design Overview
- Catalyst 6500—CatOS Defaults and Recommendations
- Catalyst 6500—Trusted Endpoint Model
- Catalyst 6500 Auto QoS VoIP Model
- Catalyst 6500—Untrusted PC + SoftPhone with Scavenger-Class QoS Model
- Catalyst 6500—Untrusted Server with Scavenger-Class QoS Model
- Catalyst 6500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model
- Catalyst 6500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model
- Catalyst 6500—Queuing and Dropping
- Catalyst 6500—PFC3 Distribution-Layer (IOS) Per-User Microflow Policing

Catalyst 6500 QoS Configuration and Design Overview

The Catalyst 6500 is the undisputed flagship of the Cisco family of LAN switches, as it is the most powerful and flexible switching platform. As such, it can be found in all three layers of a campus network (Access, Distribution, and Core).

When configured as an access layer switch, the recommended software for the Supervisor is CatOS; when configured as a distribution or core layer switch, the recommended software is Cisco IOS. Furthermore, at the time of writing, Catalyst 6500 IOS does not yet support AutoQoS nor the conditional-trust feature, therefore only CatOS examples of these models are given. However, both

AutoQoS VoIP and conditional trust have been committed for future releases of Catalyst 6500 IOS. The QoS design recommendations for a Catalyst 6500 switch at the access layer are summarized in Figure 2-22; the corresponding recommendations for Catalyst 6500s deployed in the distribution or core layers is shown in Figure 2-23.

Figure 2-22 Access Layer (CatOS) Catalyst 6500 QoS Design Options

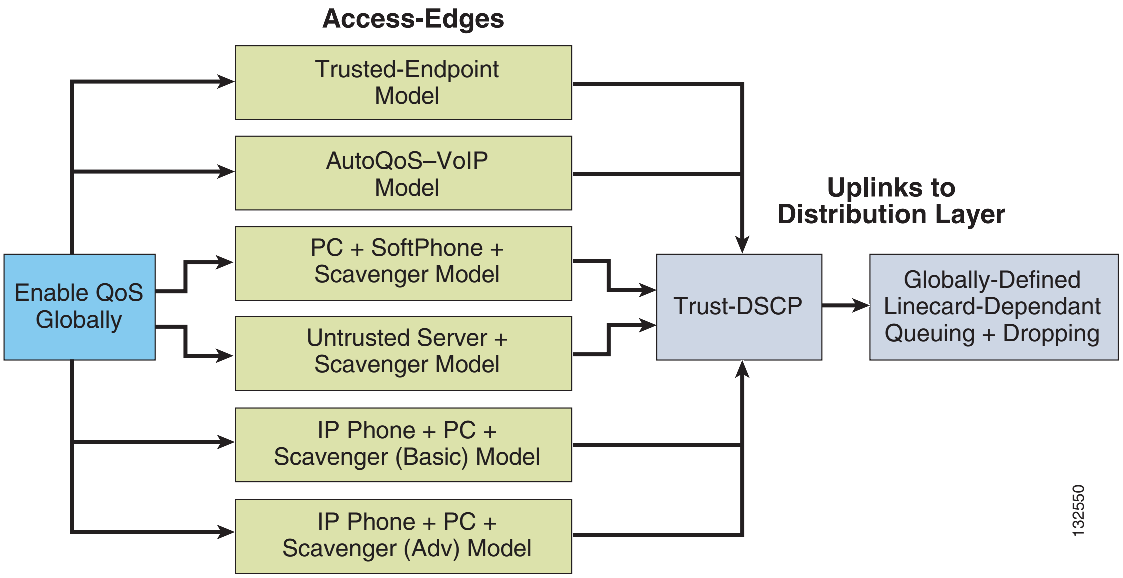
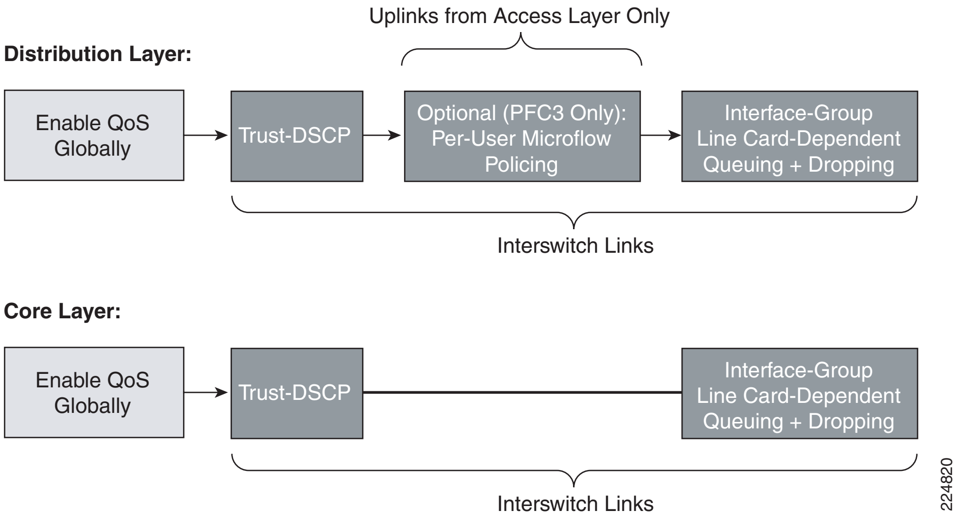

Access-Edges
Enable QoS Globally
Trusted-Endpoint Model
AutoQoS–VoIP Model
PC + SoftPhone + Scavenger Model
Untrusted Server + Scavenger Model
IP Phone + PC + Scavenger (Basic) Model
IP Phone + PC + Scavenger (Adv) Model
Uplinks to Distribution Layer
Trust-DSCP
Globally-Defined Linecard-Dependant Queuing + Dropping
132550

Figure 2-23 Distribution and/or Core Layer (IOS) Catalyst 6500 QoS Design


Uplinks from Access Layer Only
Distribution Layer:
Enable QoS Globally
Trust-DSCP
Optional (PFC3 Only): Per-User Microflow Policing
Interface-Group Line Card-Dependent Queuing + Dropping
Interswitch Links
Core Layer:
Enable QoS Globally
Trust-DSCP
Interface-Group Line Card-Dependent Queuing + Dropping
Interswitch Links
224820

Note To narrow the scope of our discussion to the most current and relevant versions of the Catalyst 6500 switch-family, only the Catalyst 6500 with Supervisor 2 (PFC2) and Supervisor 720 (PFC3) be examined in this design chapter. For discussions of older versions of Catalyst 6000/6500s (such as Supervisor 1, 1a with/without a PFC), refer to the Cisco Press book, *Cisco Catalyst QoS: Quality of Service in Campus Networks*, by Mike Flannagan, Richard Froom and Kevin Turek.

QoS is globally disabled by default on Catalyst 6500s running either CatOS or IOS. When QoS is globally disabled, then all frames/packets that are passed-through the switch remain unaltered (which is equivalent to a trust CoS and trust DSCP state on all ports). When QoS is globally enabled, however, then all DSCP and CoS values are (by default) set to 0 (which is equivalent to an untrusted state on all ports).

The commands to enable and verify QoS globally on both CatOS and IOS Catalyst 6500s are shown below.

Example 2-46 Enabling QoS Globally on a Catalyst 6500—CatOS

```
CAT6500-PFC2-CATOS> (enable) set qos enable
QoS is enabled.
CAT6500-PFC2-CATOS> (enable)



CAT6500-PFC2-CATOS> (enable) show qos status
QoS is enabled on this switch.
CAT6500-PFC2-CATOS> (enable)
```

Example 2-47 Enabling QoS Globally on a Catalyst 6500—IOS

```
CAT6500-PFC2-IOS(config)#mls qos
CAT6500-PFC2-IOS(config)#end
CAT6500-PFC2-IOS#



CAT6500-PFC2-IOS#show mls qos
  QoS is enabled globally
  Microflow policing is enabled globally
Vlan or Portchannel(Multi-Earl) policies supported: Yes

 ----- Module [2] -----
  QoS global counters:
    Total packets: 65
    IP shortcut packets: 0
    Packets dropped by policing: 0
    IP packets with TOS changed by policing: 0
    IP packets with COS changed by policing: 0
    Non-IP packets with COS changed by policing: 0

CAT6500-PFC2-IOS#
```

Catalyst 6500—CatOS Defaults and Recommendations

CatOS specifies a number of default QoS settings per-port, which do not appear in the normal configuration output. However it is beneficial to be aware of what these defaults are and what they do, so as not to override them by mistake.

For example, CatOS allows the QoS policy-source to be defined by the local configuration or by the Common Open Policy Source (COPS) protocol, referring to a COPS Policy-Decision Point (PDP) Server. COPS is a QoS administration protocol that is both dynamic and scalable, but unfortunately it never gained mainstream acceptance. It is recommended to leave the switch's default policy-source as local (except of course in the extremely rare occurrence that COPS is actually deployed on the network).

Additionally, QoS policies may be applied to VLANs or to ports. There was never any significant advantage of using one base over the other; however, AutoQoS tools favor port-based QoS, as it is marginally simpler to configure. Port-based QoS is the default per-port setting and all examples in this chapter are configured using port-based QoS.

All ports (once QoS has been globally enabled) are set to an untrusted state by default. Also, by default, the trust-extension state is set to untrusted and the extended-CoS is correspondingly set to 0.

All packets received through an untrusted port (whether the untrusted port is the actual switch port or the extended switch port in the back of a Cisco IP Phone) are marked to a CoS value of 3, by default. This default marking should be set instead to 0 on all ports connected to untrusted endpoints by using the command **set port qos** *mod/port* **cos 0**. Furthermore, on all ports that are connected to conditionally-trusted endpoints (like Cisco IP Phones) it is recommended to use the command **set port qos** *mod/port* **cos 0** in conjunction with the command **set port qos** *mod/port* **cos-ext 0**.

It is recommended to leave all these port QoS settings at their defaults, with the exception of trust and cos/cos-ext—depending on the access edge model to be applied to the port, as is discussed in additional detail below.

Another Catalyst-OS default behavior to keep in mind is that ACLs and aggregate policers cannot be applied to more than one port in the same manner as these can when configured in IOS. For example, if an aggregate policer called **POLICE-VOIP** was defined to rate-limit flows to 128 kbps and if this policer were applied to two separate ports in CatOS, then it would rate limit flows from **both** ports to combined total of 128 kbps, instead of (the preferred behavior of) limiting flows to 128 kbps on a per-port basis (as is the case when configured in IOS). To work around this default behavior, ACLs and aggregate policers have to be uniquely defined on a per-port basis. To facilitate the administration of this additional configuration complexity, it is recommended that all CatOS ACLs and aggregate policers be defined with names that include the module and port they are to be applied to. For example, the previously defined aggregate policer **POLICE-VOIP** would become **POLICE-VOIP-3-1** when applied to port 3/1 and **POLICE-VOIP-3-2** when applied to port 3/2. This is the nomenclature adopted in the examples to follow in this chapter.

Note Administrators should keep in mind the maximum number of aggregate policers that can be configured via CatOS on a given Catalyst 6500 switch (currently 1023) when designing their access-edge policies. Depending on the chassis/linecard combination, this maximum number of aggregate policers may present scaling limitations to the advanced models presented in this design chapter.

Catalyst 6500—Trusted Endpoint Model

This section includes the following topics:

- Configuration
- Catalyst 6500 CatOS QoS Verification Commands

Configuration

For most Catalyst 6500 switch ports, setting the trust state to trust DSCP is a relatively straightforward command (in either CatOS or in IOS).

In this first example, DSCP trust is configured on a port in CatOS; in the second, DSCP trust is configured on a port/interface in IOS.

Example 2-48 Catalyst 6500 CatOS—Trusted Endpoint Model

```
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust trust-dscp
Port  3/1 qos set to trust-dscp.
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands

Catalyst 6500 CatOS QoS verification commands include the following:

- show port qos
- show qos status

show port qos

The Catalyst 6500 CatOS **show port qos** verification command returns the configured and runtime QoS states of a port. These may differ, as certain commands need to be committed (programmed into hardware) before they become effective.

In the example below, the switch has QoS globally enabled and the source of QoS policy decisions is the local configuration, as opposed to a Common-Open Policy Source Policy-Decision Point (COPS PDP).

Furthermore, the output shows that the port is configured for port-based QoS (by default) and has been set to trust DSCP from connected endpoints. No trust-extension has been configured, as this is not a conditionally-trusted endpoint model.

The output includes the linecard's queuing capabilities: 1P3Q1T (Transmit) and 1P1Q0T (Receive), as well as any ACLs that may be mapped to the port (however, no ACLs have been mapped to this port in this particular example).

Example 2-49 Show Port QoS Verification for a Catalyst 6500—CatOS Switch

```
CAT6500-PFC2-CATOS> (enable) show port qos 3/1
QoS is enabled for the switch.
QoS policy source for the switch set to local.

Port  Interface Type Interface Type Policy Source Policy Source
      config         runtime        config        runtime
----- -------------- -------------- ------------- -------------
 3/1      port-based     port-based          COPS         local

Port  TxPort Type  RxPort Type  Trust Type   Trust Type    Def CoS Def CoS
                                config       runtime       config  runtime
----- ------------ ------------ ------------ ------------- ------- -------
 3/1        1p3q1t       1p1q0t   trust-dscp   trust-dscp        0       0

Port  Ext-Trust Ext-Cos Trust-Device
----- --------- ------- ------------
 3/1  untrusted       0         none

(*)Runtime trust type set to untrusted.

Config:
Port  ACL name                         Type
----- -------------------------------- ----
No ACL is mapped to port 3/1.

Runtime:
Port  ACL name                         Type
----- -------------------------------- ----
```

```
No ACL is mapped to port 3/1.
CAT6500-PFC2-CATOS> (enable)
```

On non-GigabitEthernet linecards that use 2Q2T Transmit Queuing and 1Q4T Receive queuing (such as the WS-X6248-RJ-xx and WS-X6348-RJ-xx linecards), a hardware limitation prevents the proper functioning of port-based trust (which affects trust-cos, trust-ipprec, and trust-dscp). The **show port qos** command can be used to determine if the linecard is a 2Q2T-Tx/1Q4T-Rx linecard. These cards also listed in Table 2-5.

On such linecards, a workaround ACL can be used to achieve trust-functionality for trust-cos, trust-ipprec, and trust-dscp. The workaround ACL for trust-DSCP functionality on such linecards is shown below.

Example 2-50 Trust-DSCP Workaround ACL for Catalyst 6500 2Q2T-TX/1Q4T-Rx Non-Gigabit Linecards

```
CAT6500-PFC2-CATOS> (enable) set qos acl ip TRUST-DSCP trust-dscp any
TRUST-DSCP editbuffer modified. Use 'commit' command to apply changes.
CAT6500-PFC2-CATOS> (enable) commit qos acl TRUST-DSCP

QoS ACL 'TRUST-DSCP' successfully committed.
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl map TRUST-DSCP 4/1
```

Note To apply the QoS ACL you have defined (above), the ACL must be committed to hardware. The process of committing copies the ACL from a temporary editing buffer to the PFC hardware. Once resident in the PFC memory, the policy defined in the QoS ACL can be applied to all traffic that matches the Access Control Entries (ACEs). For ease of configuration, most administrators issue a **commit all** command, however you can commit a specific ACL (by name) to be sent from the editing buffer to PFC memory, as shown above.

In this second example, DSCP trust is configured on a port/interface in IOS.

Example 2-51 Catalyst 6500 IOS—Trusted Endpoint Example

```
CAT6500-PFC2-IOS(config)#interface FastEthernet3/1
CAT6500-PFC2-IOS(config-if)#mls qos trust dscp
```

Other Catalyst 6500 CatOS QoS verification commands include the following:

- show mls qos
- show mls qos interface

Note The ACL Trust workaround to the 2Q2T non-GigabitEthernet linecards (such as the such as the WS-X6248-RJ-xx and WS-X6348-RJ-xx) limitation of not supporting trust only applies in the access Layer of the campus (where CatOS is the recommended software for the Catalyst 6500). In the distribution and core layers, where IOS is the preferred software, all interfaces are recommended to be GigabitEthernet or higher.

Catalyst 6500 Auto QoS VoIP Model

At the time of writing, AutoQoS VoIP is only supported on the Catalyst 6500 in CatOS.

The AutoQoS VoIP macro for the Catalyst 6500 CatOS is divided into these two separate components:

- Global AutoQoS command (**set qos auto**)—Deals with all switch-wide related QoS settings that are not specific to any given interface, including CoS-to-queue maps, CoS-to-DSCP maps, and WRED settings for specific port types and global mappings.
- Port-specific automatic QoS command (**set port qos** *mod/port* **autoqos**)—Configures all inbound QoS parameters for a particular port to support IP Telephony devices.

The port-specific AutoQoS VoIP command for the Catalyst 6500 in CatOS supports the the following keyword options:

- **autoqos voip ciscoipphone**
- **autoqos voip ciscosoftphone**
- **autoqos trust [cos | dscp]**

The effects of enabling the Global AutoQoS command **set qos auto** on the Catalyst 6500 in CatOS are as follows.

Example 2-52 Catalyst 6500 Global AutoQoS Generated Configuration

```
set qos autoqos
---------------

set qos enable

set qos policy-source local
set qos ipprec-dscp-map 0 10 18 26 34 46 48 56
set qos cos-dscp-map 0 10 18 26 34 46 48 56
set qos dscp-cos-map 0-7:0 8-15:1 16-23:2 24-31:3 32-39:4 40-47:5 48-55:6 56-63:7
set qos acl default-action ip dscp 0
set qos map 2q2t tx queue 2 2 cos 5,6,7
set qos map 2q2t tx queue 2 1 cos 1,2,3,4
set qos map 2q2t tx queue 1 1 cos 0
set qos drop-threshold 2q2t tx queue 1 100 100
set qos drop-threshold 2q2t tx queue 2 80 100
set qos drop-threshold 1q4t rx queue 1 50 60 80 100
set qos txq-ratio 2q2t 80 20
set qos wrr 2q2t 100 255


set qos map 1p3q1t tx 1 1 cos 0
set qos map 1p3q1t tx 2 1 cos 1,2
set qos map 1p3q1t tx 3 1 cos 3,4
set qos map 1p3q1t tx 3 0 cos 6,7
set qos map 1p3q1t tx 4 cos 5
set qos wrr 1p3q1t 20 100 200
set qos wred 1p3q1t queue 1 70:100
set qos wred 1p3q1t queue 2 70:100
set qos wred 1p3q1t queue 3 70:90
set qos map 1p1q0t rx 1 cos 0,1,2,3,4
set qos map 1p1q0t rx 2 cos 5,6,7
set qos rxq-ratio 1p1q0t 80 20
set qos map 1p2q2t tx 1 2 cos 0
set qos map 1p2q2t tx 2 1 cos 1,2,3,4
set qos map 1p2q2t tx 2 2 cos 6,7
set qos map 1p2q2t tx 3 cos 5
set qos txq-ratio 1p2q2t 75 15 15
set qos wrr 1p2q2t 50 255
set qos wred 1p2q2t queue 1 1 40:70
set qos wred 1p2q2t queue 1 2 70:100
set qos wred 1p2q2t queue 2 1 40:70
set qos wred 1p2q2t queue 2 2 70:100
set qos map 1p1q4t rx 1 1 cos 0
set qos map 1p1q4t rx 1 3 cos 1,2,3,4
set qos map 1p1q4t rx 1 4 cos 6,7
set qos map 1p1q4t rx 2 cos 5
set qos drop-threshold 1p1q4t rx queue 1 50 60 80 100

set qos map 1p2q1t tx 1 1 cos 0
set qos map 1p2q1t tx 2 1 cos 1,2,3,4
set qos map 1p2q1t tx 2 cos 6,7
set qos map 1p2q1t tx 3 cos 5
set qos txq-ratio 1p2q1t 75 15 15
set qos wrr 1p2q1t 50 255
set qos wred 1p2q1t queue 1 70:100
set qos wred 1p2q1t queue 2 70:100
set qos map 1p1q8t rx 1 1 cos 0
set qos map 1p1q8t rx 1 5 cos 1,2
set qos map 1p1q8t rx 1 8 cos 3,4
set qos map 1p1q8t rx 2 cos 5,6,7
set qos wred 1p1q8t queue 1 1 40:70
set qos wred 1p1q8t queue 1 5 60:90
set qos wred 1p1q8t queue 1 8 70:100
set qos rxq-ratio 1p1q8t 80 20

set qos policed-dscp-map 0:0
set qos policed-dscp-map 1:1
set qos policed-dscp-map 2:2
```

<repetitive output truncated>

```
set qos policed-dscp-map 61:61
set qos policed-dscp-map 62:62
set qos policed-dscp-map 63:63


set qos policed-dscp-map excess-rate 0:0
set qos policed-dscp-map excess-rate 1:1
set qos policed-dscp-map excess-rate 2:2
```

<repetitive output truncated>

```
set qos policed-dscp-map excess-rate 61:61
set qos policed-dscp-map excess-rate 62:62
set qos policed-dscp-map excess-rate 63:63
```

The effects of enabling the port-specific **set port qos** *mod/port* **autoqos voip ciscoipphone** command on the Catalyst 6500 in CatOS are as follows.

Example 2-53 Catalyst 6500 Port-Specific AutoQoS VoIP CiscoIPPhone Generated Configuration

```
set port qos mod/port autoqos voip ciscoipphone
---------------
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device ciscoipphone
```

If the port is on a 2Q2T-Tx/1Q4T-Rx (non-GigabitEthernet) linecard, the configuration is as follows:

```
set qos acl ip ACL_IP-PHONES trust-cos any
```

```
commit qos acl ACL_IP-PHONES
set qos acl map ACL_IP-PHONES mode/port
set port qos mod/port trust trust-cos
```

If the port type is another port type, the configuration is as follows:

```
set port qos mod/port trust trust-cos
```

The effects of enabling the port-specific set port qos mod/port autoqos voip ciscosoftphone command on the Catalyst 6500 in CatOS are as follows.

Example 2-54 Catalyst 6500 Port-Specific AutoQoS VoIP CiscoSoftPhone Generated Configuration

```
set port qos mod/port autoqos voip ciscosoftphone
---------------
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none
set port qos mod/port trust untrusted
set qos policer aggregate POLICE_SOFTPHONE-DSCP46-mod-port rate 320 burst 20 policed-dscp
set qos policer aggregate POLICE_SOFTPHONE-DSCP26-mod-port rate 32  burst 8 policed-dscp
set qos acl ip ACL_IP-SOFTPHONE-mod-port trust-dscp aggregate
POLICE_SOFTPHONE-DSCP46-mod-port any dscp-field 46
set qos acl ip ACL_IP-SOFTPHONE-mod-port trust-dscp aggregate
POLICE_SOFTPHONE-DSCP26-mod-port any dscp-field 26
commit qos acl ACL_IP-SOFTPHONE-mod-port
set qos acl map ACL_IP-SOFTPHONE-mod-port mod/port
```

The effects of enabling the port-specific **set port qos** *mod/port* **autoqos voip trust cos** command on the Catalyst 6500 in CatOS are as follows.

Example 2-55 Catalyst 6500 Port-Specific AutoQoS VoIP Trust CoS Generated Configuration

```
set port qos mod/port autoqos trust cos
---------------
set port qos mod/port policy-source local
set port qos mod/port port-based
set port qos mod/port cos 0
set port qos mod/port cos-ext 0
set port qos mod/port trust-ext untrusted
set port qos mod/port trust-device none
```

If the port is on a 2Q2T-Tx/1Q4T-Rx (non-GigabitEthernet) linecard, the configuration is as follows:

```
set qos acl ip ACL_IP-TRUSTCOS trust-cos any
commit qos acl ACL_IP-TRUSTCOS
set qos acl map ACL_IP-TRUSTCOS mode/port
set port qos mod/port trust trust-cos
```

If the port type is another port type, the configuration is as follows:

```
set port qos mod/port trust trust-cos
```

The AutoQoS VoIP command with the Trust-DSCP option is virtually identical to the Trust-CoS option (albeit the final configuration commands are **set port qos** `mod/port` **trust trust-dscp** instead of **trust-cos**).

Catalyst 6500—Untrusted PC + SoftPhone with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst 6500 CatOS QoS Verification Commands

Configuration

The radical difference in syntax between CatOS and IOS becomes increasingly apparent as more complex access edge models are presented.

In the Untrusted PC + SoftPhone + Scavenger Model, shown below, per-application aggregate policers are defined—one each for SoftPhone VoIP traffic, SoftPhone call signaling traffic, and PC Data traffic. Then an ACL (titled “SOFTPHONE-PC-mod-port”) with multiple ACEs is defined, with each ACE referencing its associated aggregate policer. Once complete, the ACL is committed to PFC memory and then mapped to the desired switch port(s). Switch responses to the commands have been omitted to simplify the example.

Example 2-56 Catalyst 6500 CatOS—Untrusted PC + SoftPhone + Scavenger Model Configuration

```
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map 0,24,46:8
! Excess traffic marked DSCP 0 or CS3 or EF will be remarked to CS1
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate SOFTPHONE-VOICE-3-1
 rate 128 burst 8000 policed-dscp
! Defines the policer for SoftPhone VoIP traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate SOFTPHONE-SIGNALING-3-1
 rate 32 burst 8000 policed-dscp
! Defines the policer for SoftPhone call signaling traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate PC-DATA-3-1
 rate 5000 burst 8000 policed-dscp
! Defines the policer for PC Data traffic
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip SOFTPHONE-PC-3-1 dscp 46
 aggregate SOFTPHONE-VOICE-3-1 udp any any range 16384 32767
! Binds ACL to policer and marks in-profile SoftPhone VoIP to DSCP EF
CAT6500-PFC2-CATOS> (enable) set qos acl ip SOFTPHONE-PC-3-1 dscp 24
 aggregate SOFTPHONE-SIGNALING-3-1 tcp any any range 2000 2002
! Binds ACL to policer marks in-profile call signaling to DSCP CS3
CAT6500-PFC2-CATOS> (enable) set qos acl ip SOFTPHONE-PC-3-1 dscp 0
 aggregate PC-DATA-3-1 any
! Binds ACL to policer and marks in-profile PC Data traffic to DSCP 0
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) commit qos acl SOFTPHONE-PC-3-1
    ! Commits ACL to PFC hardware
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 cos 0
    ! Sets CoS to 0 for all untrusted packets
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust untrusted
    ! Sets the port trust state to untrusted
CAT6500-PFC2-CATOS> (enable) set qos acl map SOFTPHONE-PC-3-1 3/1
    ! Attaches ACL to switch port
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS verification commands for the Untrusted PC + Softphone + Scavenger model include the following:

- show qos status

- show qos maps
- show port qos
- show qos acl
- show qos policer
- show qos statistics

show qos maps

The Catalyst 6500 CatOS **show qos maps** verification command is fairly similar to the **show mls qos maps** MLS QoS verification command. It returns the configured CoS-DSCP, IPPrec-DSCP, DSCP-CoS, and Normal-Rate and Excess-Rate Policed-DSCP Maps. The command can return configured maps (which may or may not be committed to the PFC) or runtime maps.

In the (truncated) runtime example below, all maps are at their default states, with the exception of the Normal-Rate Policed-DSCP map, which has DSCP 0, CS3 (24), and EF (46) mapped for out-of-profile markdown to DSCP CS1 (8).

Example 2-57 Show QoS Maps Verification for Catalyst 6500 Switch—CatOS

```
CAT6500-PFC2-CATOS> (enable) show qos maps runtime
CoS - DSCP map:
CoS   DSCP
---   ----
  0   0
  1   8
  2   16
  3   24
  4   32
  5   40
  6   48
  7   56

IP-Precedence - DSCP map:
IP-Prec   DSCP
-------   ----
      0   0
      1   8
      2   16
      3   24
      4   32
      5   40
      6   48
      7   56

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

DSCP - Policed DSCP map normal-rate:
DSCP                              Policed DSCP
-------------------------------   ------------
```

```
                               1  1
                               2  2
                               3  3
                               4  4
                               5  5
                               6  6
                               7  7
                       0,8,24,46  8
                               9  9
                              10  10
<output truncated>
                              63  63
DSCP - Policed DSCP map excess-rate:
DSCP                              Policed DSCP
--------------------------------  ------------
                               0  0
                               1  1
                               2  2
                               3  3
                               4  4
                               5  5
<output truncated>
                              63  63

CAT6500-PFC2-CATOS> (enable)
```

show qos acl

The Catalyst 6500 CatOS **show qos acl** verification command returns information about ACLs and ACEs that have been configured for QoS purposes. ACL information can be displayed for configuration ACLs or runtime ACLs.

In the example below, three variations of the **show qos acl** command are displayed.

The first one displays the QoS ACLs that are still in the edit-buffer and indicates whether or not the ACL(s) have been committed to PFC hardware. In this example, the ACL "SOFTPHONE-PC-3-1" has been committed to the PFC.

The second example displays runtime ACE level information for a given ACL (or all ACLs, if the keyword **all** is used instead of the ACL name). Each ACE's DSCP markings, associated aggregate policer, and filtering criteria are displayed.

The third example displays the VLANs and/or ports that the ACL has been applied to. In this specific example, port 3/1 has the SOFTPHONE-PC-3-1 ACL applied to it.

Example 2-58 Show QoS ACL Verification for Catalyst 6500 Switch—CatOS

```
CAT6500-PFC2-CATOS> (enable) show qos acl editbuffer
ACL                               Type Status
--------------------------------  ---- ----------
SOFTPHONE-PC-3-1 IP   Committed
CAT6500-PFC2-CATOS> (enable)

CAT6500-PFC2-CATOS> (enable) show qos acl info runtime SOFTPHONE-PC-3-1

set qos acl IP SOFTPHONE-PC-3-1
----------------------------------------------
1. dscp 46 aggregate SOFTPHONE-VOICE-PC-3-1 udp any any range 16384 32767
2. dscp 24 aggregate SOFTPHONE-SIGNALING-PC-3-1 tcp any any range 2000 2002
3. dscp 0 aggregate PC-DATA-PC-3-1 any
CAT6500-PFC2-CATOS> (enable)
```

```
CAT6500-PFC2-CATOS> (enable) show qos acl map runtime SOFTPHONE-PC-3-1
QoS ACL mappings on input side:
ACL name                         Type Vlans
-------------------------------- ---- ---------------------------------
SOFTPHONE-PC-3-1               IP
ACL name                         Type Ports
-------------------------------- ---- ---------------------------------
SOFTPHONE-PC-3-1               IP 3/1
CAT6500-PFC2-CATOS> (enable)
```

show qos policer

The Catalyst 6500 CatOS **show qos policer** verification command displays the Normal and Excess Rates and Burst for any/all policers.

In the example below, three aggregate policers have been defined: SOFTPHONE-VOICE-3-1, SOFTPHONE-SIGNALING-3-1, and PC-DATA-3-1, with Normal Rates of 128 kbps, 32 kbps, and 5 Mbps, respectively. Each of these policers will markdown excess traffic according to the Policed-DSCP Normal-Rate and are attached to the ACL: SOFTPHONE-PC-3-1.

Example 2-59 Show QoS Policer Verification for Catalyst 6500 Switch—CatOS

```
CAT6500-PFC2-CATOS> (enable) show qos policer runtime all
Warning: Runtime information may differ from user configured setting due to hard
ware granularity.
QoS microflow policers:
QoS aggregate policers:
Aggregate name        Avg. rate (kbps) Burst size (kb) Normal action
--------------------- ---------------- --------------- -------------
SOFTPHONE-VOICE-3-1            128            7936  policed-dscp
                      Excess rate (kbps) Excess burst size (kb) Excess action
                      ------------------ ---------------------- -------------
                                31457280                  31744  policed-dscp
                                ACL attached
                                ------------------------------------
                                SOFTPHONE-PC-3-1

Aggregate name        Avg. rate (kbps) Burst size (kb) Normal action
--------------------- ---------------- --------------- -------------
SOFTPHONE-SIGNALING-3-1        32            7936 policed-dscp
                      Excess rate (kbps) Excess burst size (kb) Excess action
                      ------------------ ---------------------- -------------
                                31457280                  31744  policed-dscp
                                ACL attached
                                ------------------------------------
                                SOFTPHONE-PC-3-1

Aggregate name        Avg. rate (kbps) Burst size (kb) Normal action
--------------------- ---------------- --------------- -------------
PC-DATA-3-1                    4864            7936  policed-dscp
                      Excess rate (kbps) Excess burst size (kb) Excess action
                      ------------------ ---------------------- -------------
                                31457280                  31744  policed-dscp
                                ACL attached
                                ------------------------------------
                                SOFTPHONE-PC-3-1

CAT6500-PFC2-CATOS> (enable)
```

show qos statistics

The Catalyst 6500 CatOS **show qos statistics** verification command displays various dynamic statistics regarding the QoS policies.

In the three part example below, the first variation of the command **show qos statistics <mod/port>** returns queuing statistics for the port. Specifically it reports any drops due to queue buffer overfill and breaks these drops down by queues/thresholds—depending on the queuing structure of the module. In this first part of the example, no drops have occurred due to queuing buffer overfills.

In the second example, aggregate policing statistics are displayed via the **show qos statistics aggregate-policer** variation of the command. The number of packets conforming or exceeding a given policer is reported. In this part of the example, the command reports that no packets have exceeded the SOFTPHONE-VOIP-3-1 or SOFTPHONE-SIGNALING-3-1 policer, but a few have exceeded the PC-DATA-3-1 policer.

And finally, in the third example, the number of packets that have been dropped due to policing and/or remarked at Layer 3 or Layer 2 are reported with the **show qos statistics l3stats** command. In this final part of the example, the command reports that no packets have been dropped due to policing, but thousands of packets have had their Layer 3 and Layer 2 markings modified by the configured policy.

Example 2-60 Show QoS Statistics Verification for Catalyst 6500 Switch—CatOS

```
CAT6500-PFC2-CATOS> (enable) show qos statistics 3/1
Tx port type of port 3/1 : 1p3q1t
WRED and tail drops are accumulated in one counter per queue.
Q #  Packets dropped
---  -----------------------------------------------
1    0 pkts
2    0 pkts
3    0 pkts
4    0 pkts

Rx port type of port 3/1 : 1p1q0t
For untrusted ports all the packets are sent to the same queue,
Rx thresholds are disabled, tail drops are reported instead.
Q #  Threshold #:Packets dropped
---  -----------------------------------------------
1    0:0 pkts
2    0:0 pkts

CAT6500-PFC2-CATOS> (enable)

CAT6500-PFC2-CATOS> (enable) show qos statistics aggregate-policer
QoS aggregate-policer statistics:
Aggregate policer               Allowed packet Packets exceed
                                count          excess rate
------------------------------- -------------- --------------
SOFTPHONE-VOICE-3-1                   27536             0
SOFTPHONE-SIGNALING-3-1               224             0
PC-DATA-3-1                           470069           645
CAT6500-PFC2-CATOS> (enable)

CAT6500-PFC2-CATOS> (enable) show qos statistics l3stats
Packets dropped due to policing:                0
IP packets with ToS changed:               169286
IP packets with CoS changed:                83507
Non-IP packets with CoS changed:                0
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500—Untrusted Server with Scavenger-Class QoS Model

This section includes the following topics:

- Configuration
- Catalyst 6500 CatOS QoS Verification Commands

Additional flexibility is offered to the Untrusted Server + Scavenger Model due to the Catalyst 6500 PFC2/PFC3's support of Dual-Rate Policing (as described in RFC 2698 "A Two Rate Three Color Marker" and as illustrated in Figure 4-5).

Using a Dual-Rate policer, three colors are used to indicate:

- *Conforming traffic* (within the normal rate)
- *Excess traffic* (exceeding the normal rate but less than the excess rate)
- *Violating traffic* (exceeding both the normal and excess rate)

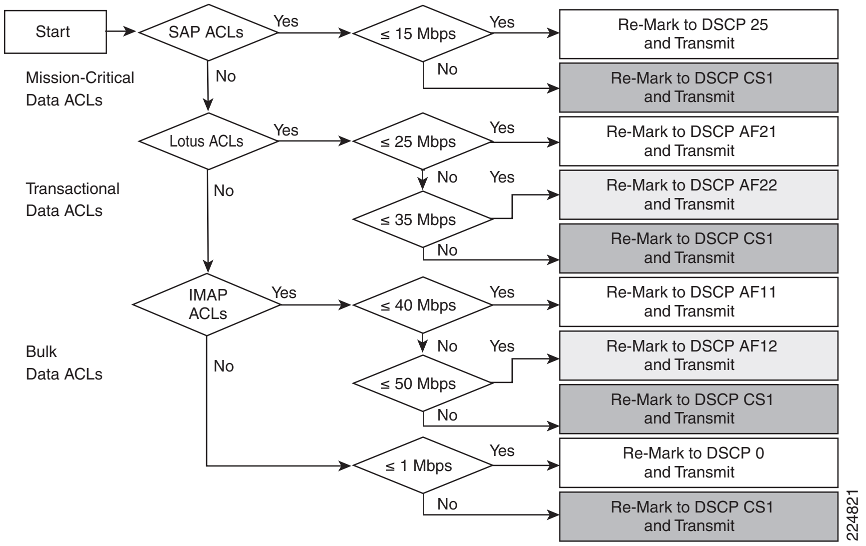
The Dual-Rate policer is intended to complement the RFC 2597 Assured Forwarding Groups Diff-Serv marking scheme. To illustrate, consider Transactional Data traffic, which is marked to AF Class 2. Conforming Transactional Data should be marked to AF21, Excess Transactional Data traffic should be marked-down to AF22, and Violating Transactional Data traffic should be marked-down further to AF23.

Such a markdown scheme is intended to be complemented further by DSCP-based WRED congestion avoidance. In this manner, in the event of congestion, AF23 is dropped more aggressively than AF22 which, in turn, is dropped more aggressively than AF21.

However, since Catalyst 6500 queuing and congestion-avoidance is determined primary by CoS markings, the standards-based DSCP model cannot be followed completely at this time on this platform (since AF21/AF22/AF23 all share CoS 3, this does not allow for granular sub-class QoS). Therefore, the use of Scavenger class markings for violating traffic could be used to achieve a similar overall effect, while maintaining consistency with QoS designs previously presented for other Catalyst platforms.

Under such a modified Untrusted Multi-Application Server with Scavenger-Class QoS Model, Excess Transactional Data traffic can be marked down to AF22 and Violating Transactional Data traffic can be marked down to DSCP CS1 (Scavenger). Similarly, Excess Bulk Data traffic can be marked down to AF12 and Violating Bulk Data traffic can be marked down to DSCP CS1 (Scavenger). This modified model is shown in Figure 2-24.

Figure 2-24 Catalyst 6500 PFC2/PFC3 Untrusted Endpoint—Multi-Application Server with Scavenger-Class QoS (Dual-Rate Policing) Model


Start
SAP ACLs
Yes
≤ 15 Mbps
Yes
Re-Mark to DSCP 25 and Transmit
Mission-Critical Data ACLs
No
No
Re-Mark to DSCP CS1 and Transmit
Lotus ACLs
Yes
≤ 25 Mbps
Yes
Re-Mark to DSCP AF21 and Transmit
Transactional Data ACLs
No
No
Yes
Re-Mark to DSCP AF22 and Transmit
≤ 35 Mbps
No
Re-Mark to DSCP CS1 and Transmit
IMAP ACLs
Yes
≤ 40 Mbps
Yes
Re-Mark to DSCP AF11 and Transmit
Bulk Data ACLs
No
No
Yes
Re-Mark to DSCP AF12 and Transmit
≤ 50 Mbps
No
Re-Mark to DSCP CS1 and Transmit
≤ 1 Mbps
Yes
Re-Mark to DSCP 0 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
224821

Configuration

The configuration for a Catalyst 6500 CatOS Untrusted Endpoint Dual-Rate Policing of a Multi-Application Server with Scavenger-Class QoS example is shown below.

Example 2-61 Catalyst 6500 CatOS—Untrusted Multi-Application Server with Scavenger-Class QoS (Dual-Rate Policing) Model Configuration

```
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map normal-rate 0,25:8
    ! Excess SAP and Data traffic is marked down to DSCP CS1 (Scavenger)
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map normal-rate 18:20
    ! Excess Transactional Data traffic is marked down from DSCP AF21 to AF22
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map excess-rate 18:8
    ! Violating Transactional Data traffic is marked down to CS1
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map normal-rate 10:12
    ! Excess Bulk Data traffic is marked down from DSCP AF11 to AF12
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map excess-rate 10:8
! Violating Bulk Data traffic is marked down to CS1
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate SAP-3-1
rate 15000 burst 8000 policed-dscp
! Defines the policer for Mission-Critical Data (SAP) traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate LOTUS-3-1
rate 25000 policed-dscp erate 35000 policed-dscp burst 8000
! Defines the dual-rate policer for Transactional Data (Lotus) traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate IMAP-3-1
rate 40000 policed-dscp erate 50000 policed-dscp burst 8000
! Defines the dual-rate policer for Bulk Data (IMAP) traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate DATA-3-1
rate 1000 burst 8000 policed-dscp
! Defines the policer for other data traffic
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip UNTRUSTED-SERVER-3-1 dscp 25
aggregate SAP-3-1 tcp any range 3200 3203 any
! Binds ACL to policer and marks in-profile SAP to DSCP 25
CAT6500-PFC2-CATOS> (enable) set qos acl ip UNTRUSTED-SERVER-3-1 dscp 25
```

```
aggregate SAP-3-1 tcp any eq 3600 any
! Binds ACL to policer and marks in-profile SAP to DSCP 25
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip UNTRUSTED-SERVER-3-1 dscp 18
aggregate LOTUS-3-1 tcp any eq 1352 any
! Binds ACL to dual-rate policer and marks in-profile Lotus to DSCP AF21
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip UNTRUSTED-SERVER-3-1 dscp 10
aggregate IMAP-3-1 tcp any eq 143 any
! Binds ACL to dual-rate policer and marks in-profile IMAP to DSCP AF11
CAT6500-PFC2-CATOS> (enable) set qos acl ip UNTRUSTED-SERVER-3-1 dscp 10
aggregate IMAP-3-1 tcp any eq 220 any
! Binds ACL to dual-rate policer and marks in-profile IMAP to DSCP AF11
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip UNTRUSTED-SERVER-3-1 dscp 0
aggregate DATA-3-1 any
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) commit qos acl UNTRUSTED-SERVER-3-1
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 cos 0
    ! Sets CoS to 0 for all untrusted packets
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust untrusted
    ! Sets the port trust state to untrusted
CAT6500-PFC2-CATOS> (enable) set qos acl map UNTRUSTED-SERVER-3-1 3/1
    ! Attaches ACL to switch port
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands

Catalyst 6500 CatOS QoS verification commands for the Untrusted Server + Scavenger model include the following:

- show qos status
- show qos maps
- show port qos
- show qos acl
- show qos policer
- show qos statistics

Catalyst 6500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Basic) Model

This section includes the following topics:

- Configuration
- Catalyst 6500 CatOS QoS Verification Commands

Configuration

In the Conditionally-Trusted IP Phone + PC + Scavenger (Basic) Model for the Catalyst 6500 (CatOS), four aggregate policers are defined, one each for Voice from the VVLAN, call signaling from the VVLAN, all other traffic from the VVLAN, and for all PC Data traffic. Conditional trust is extended to the IP Phones via the trust-device command, as shown below.

Example 2-62 Catalyst 6500 CatOS—Conditionally-Trusted IP Phone + PC + Scavenger (Basic) Model Configuration

```
CAT6500-PFC2-CATOS> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
    ! Modifies default CoS-DSCP mapping so that CoS 5 is mapped to DSCP EF
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map 0,24:8
! Excess traffic marked DSCP 0 or CS3 is remarked to CS1
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-VOICE-3-1
rate 128 burst 8000 drop
! Defines the policer for IP Phone VoIP traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-SIGNALING-3-1
rate 32 burst 8000 policed-dscp
! Defines the policer for IP Phone call signaling traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-ANY-3-1
rate 32 burst 8000 policed-dscp
! Defines the policer for any other traffic sourced from the VVLAN
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate PC-DATA-3-1
rate 5000 burst 8000 policed-dscp
! Defines the policer for PC Data traffic
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC-3-1 dscp 46
aggregate VVLAN-VOICE-3-1 udp 10.1.110.0 0.0.0.255 any range 16384 32767
! Binds ACL to policer and marks in-profile VVLAN VoIP to DSCP EF
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC-3-1 dscp 24
aggregate VVLAN-SIGNALING-3-1 udp 10.1.110.0 0.0.0.255 any range 2000 2002
! Binds ACL to policer marks in-profile VVLAN call signaling to DSCP CS3
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC-3-1 dscp 0
aggregate VVLAN-ANY-3-1 10.1.110.0 0.0.0.255
! Binds ACL to policer and marks all other VVLAN traffic to DSCP 0
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-BASIC-3-1 dscp 0
aggregate PC-DATA-3-1 any
! Binds ACL to policer and marks in-profile PC Data traffic to DSCP 0
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) commit qos acl IPPHONE-PC-BASIC-3-1
    ! Commits ACL to PFC hardware
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 cos 0
    ! Sets CoS to 0 for all untrusted packets (when there is no IP Phone on the port)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 cos-ext 0
    ! Sets CoS to 0 for all untrusted PC-generated packets (behind an IP Phone)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust-ext untrusted
    ! Ignore any CoS values for all PC-generated packets (behind an IP Phone)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust-device ciscoipphone
    ! Conditional trust (for Cisco IP Phones only)
CAT6500-PFC2-CATOS> (enable) set qos acl map IPPHONE-PC-BASIC-3-1 3/1
    ! Attaches ACL to switch port
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands

Catalyst 6500 CatOS QoS verification commands for the Conditionally-Trusted IP Phone + PC + Scavenger (Basic) Model

include the following:

- show qos status
- show qos maps
- show port qos
- show qos acl
- show qos policer
- show qos statistics

Note As previously mentioned, on non-GigabitEthernet linecards that use 2Q2T Transmit Queuing and 1Q4T Receive queuing (such as the WS-X6248-RJ-xx and the WS-X6348-RJ-xx), a hardware limitation prevents the proper functioning of port-based trust (which affects trust-cos, trust-ipprec, and trust-dscp). On such linecards, a workaround ACL can be used to achieve trust functionality. For such an example, see the Catalyst 6500 Trusted Endpoint Model section (Example 2-50) of this chapter.

Catalyst 6500—Conditionally-Trusted IP Phone + PC with Scavenger-Class QoS (Advanced) Model

This section includes the following topics:

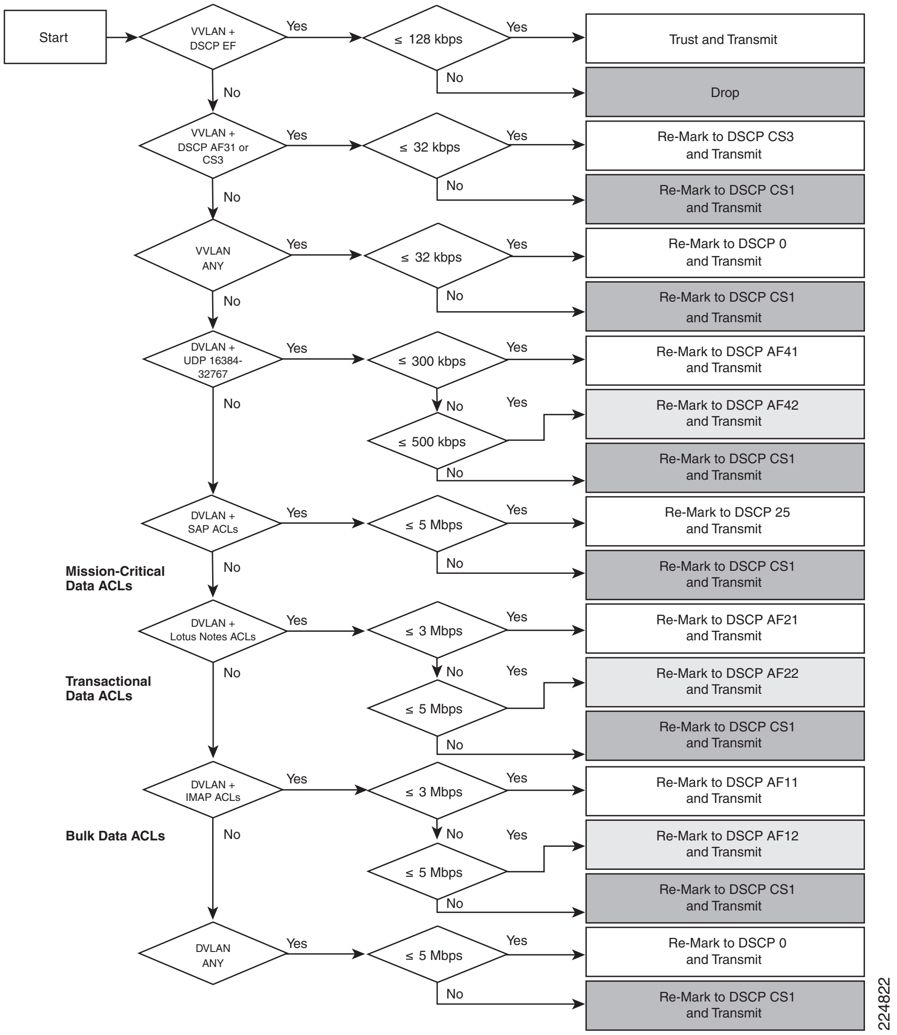
- Configuration
- Catalyst 6500 CatOS QoS Verification Commands

The Catalyst 6500 Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model leverages the Dual-Rate Policing capabilities of the PFC2/PFC3. This feature is described in the Catalyst 6500 Untrusted Server + Scavenger section of this chapter (which applies the feature to Server-to-Client flows). In this example, the Dual-Rate Policing feature is applied to Client-to-Server flows to complement the Untrusted Server + Scavenger Model.

Dual-Rate Policing, in this context, allows for graduated markdown of Interactive-Video (from PCs), Transactional Data, and Bulk Data. Specifically, in this example Interactive-Video is marked down to AF42 if it is in excess of 300 kbps but less than 500 kbps; if it is greater than 500 kbps, it is marked down to Scavenger (CS1). Similarly, Transactional Data and Bulk Data are marked down to AF22 and AF12 (respectively) if they are in excess of 3 Mbps but less than 5 Mbps; if they are in excess of 5 Mbps, then they are both marked down to Scavenger (CS1). All other policers are consistent with the single-rate policer model.

The Catalyst 6500 PFC2/PFC3 Conditionally-Trusted Endpoint Dual-Rate Policing—IP Phone + PC + Scavenger (Advanced) Model is illustrated in Figure 2-25.

Figure 2-25 Catalyst 6500 PFC2/PFC3 Conditionally-Trusted Endpoint Dual-Rate Policing—IP Phone + PC + Scavenger (Advanced) Model


Start
VVLAN + DSCP EF
Yes
≤ 128 kbps
Yes
Trust and Transmit
No
Drop
No
VVLAN + DSCP AF31 or CS3
Yes
≤ 32 kbps
Yes
Re-Mark to DSCP CS3 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
No
VVLAN ANY
Yes
≤ 32 kbps
Yes
Re-Mark to DSCP 0 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
No
DVLAN + UDP 16384-32767
Yes
≤ 300 kbps
Yes
Re-Mark to DSCP AF41 and Transmit
No
No
Yes
≤ 500 kbps
Re-Mark to DSCP AF42 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
DVLAN + SAP ACLs
Yes
≤ 5 Mbps
Yes
Re-Mark to DSCP 25 and Transmit
Mission-Critical Data ACLs
No
No
Re-Mark to DSCP CS1 and Transmit
DVLAN + Lotus Notes ACLs
Yes
≤ 3 Mbps
Yes
Re-Mark to DSCP AF21 and Transmit
Transactional Data ACLs
No
No
Yes
≤ 5 Mbps
Re-Mark to DSCP AF22 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
DVLAN + IMAP ACLs
Yes
≤ 3 Mbps
Yes
Re-Mark to DSCP AF11 and Transmit
Bulk Data ACLs
No
No
Yes
≤ 5 Mbps
Re-Mark to DSCP AF12 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
DVLAN ANY
Yes
≤ 5 Mbps
Yes
Re-Mark to DSCP 0 and Transmit
No
Re-Mark to DSCP CS1 and Transmit
224822

Legend for Figure 2-25:

- MCD = Mission Critical Data
- TD = Transactional Data
- BD = Bulk Data

Note The discrete traffic watermarks at which graduated markdown should occur are at the network administrator's discretion and will vary from enterprise to enterprise and application to application.

Configuration

An example configuration for a Catalyst 6500 CatOS Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model is shown below.

Example 2-63 Catalyst 6500 CatOS—Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) Model Configuration

```
CAT6500-PFC2-CATOS> (enable) set qos cos-dscp-map 0 8 16 24 32 56 48 56
    ! Modifies default CoS-DSCP mapping so that CoS 5 is mapped to DSCP EF
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map normal-rate 0,24,25:8
    ! Excess Data, call signaling and MC-Data traffic is marked down to CS1
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map normal-rate 10:12
    ! Excess Bulk traffic is marked down from DSCP AF11 to AF12
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map excess-rate 10:8
    ! Violating Bulk traffic is marked down to DSCP CS1
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map normal-rate 18:20
    ! Excess Transactional Data traffic is marked down from AF21 to AF22
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map excess-rate 18:8
    ! Violating Transactional Data traffic is marked down to DSCP CS1
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map normal-rate 34:36
    ! Excess Interactive-Video traffic is marked down from AF41 to AF42
CAT6500-PFC2-CATOS> (enable) set qos policed-dscp-map excess-rate 34:8
    ! Violating Interactive-Video traffic is marked down to DSCP CS1
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-VOICE-3-1
rate 128 burst 8000 drop
! Defines the policer for IP Phone VoIP traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-SIGNALING-3-1
rate 32 burst 8000 policed-dscp
! Defines the policer for IP Phone call signaling traffic
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate VVLAN-ANY-3-1
rate 32 burst 8000 policed-dscp
! Defines the policer for any other traffic sourced from the VVLAN
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate PC-VIDEO-3-1
rate 300  policed-dscp erate 500 policed-dscp burst 8000
! Defines the Dual-Rate policer for Interactive-Video
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate MISSION-CRITICAL-3-1
rate 5000 burst 8000 policed-dscp
! Defines the policer for Mission-Critical Data
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate TRANSACTIONAL-3-1
rate 3000 policed-dscp erate 5000 policed-dscp burst 8000
! Defines the Dual-Rate policer for Transactional Data
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate BULK-3-1
rate 3000 policed-dscp erate 5000 policed-dscp burst 8000
! Defines the Dual-Rate policer for Bulk Data
CAT6500-PFC2-CATOS> (enable) set qos policer aggregate PC-DATA-3-1
rate 5000 burst 8000 policed-dscp
! Defines the policer for all other PC Data traffic
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 46
aggregate VVLAN-VOICE-3-1 udp 10.1.110.0 0.0.0.255 any range 16384 32767
! Binds ACL to policer and marks in-profile VVLAN VoIP to DSCP EF
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 24
aggregate VVLAN-SIGNALING-3-1 tcp 10.1.110.0 0.0.0.255 any range 2000 2002
! Binds ACL to policer marks in-profile VVLAN call signaling to DSCP CS3
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 0
aggregate VVLAN-ANY-3-1 10.1.110.0 0.0.0.255
! Binds ACL to policer and marks all other VVLAN traffic to DSCP 0
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 34
aggregate PC-VIDEO-3-1 udp any any range 16384 32767
! Binds ACL to Dual-Rate policer and marks in-profile PC Video to AF41
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 25
aggregate MISSION-CRITICAL-3-1 tcp any any range 3200 3203
! Binds ACL to policer and marks in-profile SAP to DSCP 25
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 25
aggregate MISSION-CRITICAL-3-1 tcp any any eq 3600
```

```
! Binds ACL to policer and marks in-profile SAP to DSCP 25
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 18
aggregate TRANSACTIONAL-3-1 tcp any any eq 1352
! Binds ACL to Dual-Rate policer and marks in-profile Lotus to AF21
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 10
aggregate BULK-3-1 tcp any any eq 143
! Binds ACL to Dual-Rate policer and marks in-profile IMAP to AF11
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 10
aggregate BULK-3-1 tcp any any eq 220
! Binds ACL to Dual-Rate policer and marks in-profile IMAP to AF11
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos acl ip IPPHONE-PC-ADVANCED-3-1 dscp 0
aggregate PC-DATA-3-1 any
! Binds ACL to policer and marks other in-profile PC data to DSCP 0
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) commit qos acl IPPHONE-PC-ADVANCED-3-1
    ! Commits ACL to PFC hardware
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 cos 0
    ! Sets CoS to 0 for all untrusted packets (when there is no IP Phone on the port)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 cos-ext 0
    ! Sets CoS to 0 for all untrusted PC-generated packets (behind an IP Phone)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust-ext untrusted
    ! Ignore any CoS values for all PC-generated packets (behind an IP Phone)
CAT6500-PFC2-CATOS> (enable) set port qos 3/1 trust-device ciscoipphone
    ! Conditional trust (for Cisco IP Phones only)
CAT6500-PFC2-CATOS> (enable) set qos acl map IPPHONE-PC-ADVANCED-3-1 3/1
    ! Attaches ACL to switch port
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands

Catalyst 6500 CatOS QoS verification commands for the Conditionally-Trusted IP Phone + PC + Scavenger (Advanced) model include the following:

- show qos status
- show qos maps
- show port qos
- show qos acl
- show qos policer
- show qos statistics

Note As previously mentioned, on non-GigabitEthernet linecards that use 2Q2T Transmit Queuing and 1Q4T Receive queuing (such as the WS-X6248-RJ-xx and the WS-X6348-RJ-xx), a hardware limitation prevents the proper functioning of port-based trust (which affects trust-cos, trust-ipprec, and trust-dscp). On such linecards, a workaround ACL can be used to achieve trust functionality. For such an example, see Catalyst 6500—Trusted Endpoint Model (Example 2-50).

Catalyst 6500—Queuing and Dropping

This section includes the following topics:

- Catalyst 6500 Queuing and Dropping Overview
- Catalyst 6500 Transmit Queuing and Dropping Linecard Options
- Catalyst 6500—2Q2T Queuing and Dropping
- Catalyst 6500—1P2Q1T Queuing and Dropping
- Catalyst 6500—1P2Q2T Queuing and Dropping
- Catalyst 6500—1P3Q1T Queuing and Dropping
- Catalyst 6500—1P3Q8T Queuing and Dropping
- Catalyst 6500—1P7Q8T Queuing and Dropping

Catalyst 6500 Queuing and Dropping Overview

While the Catalyst 6500 PFC performs classification, marking, mapping, and policing functions, all queuing and congestion avoidance policies are administered by the Catalyst 6500 linecards. This inevitably leads to per-linecard hardware-specific capabilities and syntax when it comes to configuring queuing and dropping.

As previously discussed in relation to other platforms that support ingress queuing, receive queues are extremely difficult to congest, even in controlled lab environments. This is especially so if access edge policies, as detailed in this chapter, are used on all access layer switches.

Ingress congestion implies that the combined ingress rates of traffic exceed the switch fabric channel speed, and thus would need to be queued simply to gain access to the switching fabric. On newer platforms, such as the Catalyst 6500 Sup720, this means that a combined ingress rate of up to 40 Gbps per slot would be required to create such an event.

However, to obviate such an extreme event, the Catalyst 6500 schedules ingress traffic through the receive queues based on CoS values. In the default configuration, the scheduler assigns all traffic with CoS 5 to the strict-priority queue (if present); in the absence of a strict priority queue, the scheduler assigns all traffic to the standard queues. All other traffic is assigned to the standard queue(s) (with higher CoS values being assigned preference over lower CoS values, wherever supported). Additionally, if a port is configured to trust CoS, then the ingress scheduler implements CoS-value-based receive-queue drop thresholds to avoid congestion in received traffic. Thus, even if the extremely unlikely event of ingress congestion should occur, the default settings for the Catalyst 6500 linecard receive queues are more than adequate to protect VoIP and network control traffic.

Therefore, the focus of this section is on Catalyst 6500 egress/transmit queuing design recommendations.

Catalyst 6500 Transmit Queuing and Dropping Linecard Options

There are **currently** six main transmit queuing/dropping options for Catalyst 6500 linecards:

- 2Q2T—Indicates two standard queues, each with two configurable tail-drop thresholds.
- 1P2Q1T—Indicates one strict-priority queue and two standard queues, each with one configurable WRED-drop threshold (however, each standard queue also has one nonconfigurable tail-drop threshold).

- 1P2Q2T—Indicates one strict-priority queue and two standard queues, each with two configurable WRED-drop thresholds.
- 1P3Q1T—Indicates one strict-priority queue and three standard queues, each with one configurable WRED-drop threshold (however, each standard queue also has one nonconfigurable tail-drop threshold).
- 1P3Q8T—Indicates one strict-priority queue and three standard queues, each with eight configurable WRED-drop thresholds (however, each standard queue also has one nonconfigurable tail-drop threshold).
- 1P7Q8T—Indicates one strict-priority queue and seven standard queues, each with eight configurable WRED-drop thresholds (on 1p7q8t ports, each standard queue also has one nonconfigurable tail-drop threshold).

Almost all Catalyst 6500 linecards support a strict-priority queue and when supported, the switch services traffic in the strict-priority transmit queue before servicing the standard queues. When the switch is servicing a standard queue, after transmitting a packet, it checks for traffic in the strict-priority queue. If the switch detects traffic in the strict-priority queue, it suspends its service of the standard queue and completes service of all traffic in the strict-priority queue before returning to the standard queue.

Additionally, Catalyst 6500 linecards implement CoS-value-based transmit-queue drop thresholds to avoid congestion in transmitted traffic. WRED thresholds can also be defined on certain linecards, where the CoS value of the packet (not the IP Precedence value, although they likely match) determines the WRED weight. WRED parameters include a lower and upper threshold: the low WRED threshold is the queue level where (assigned) traffic begins to be selectively-dropped and the high WRED threshold is the queue level above which all (assigned) traffic is dropped. Furthermore, packets in the queue between the low and high WRED thresholds have an increasing chance of being dropped as the queue fills.

The Transmit Queuing/Dropping capabilities can be returned by using the following commands.

- CatOS:
  - show port capabilities
  - show port qos
  - show qos info
- IOS:
  - show queueing interface

Table 2-5 shows the Catalyst 6500 linecards that are currently available and their respective queuing/dropping structures.

Table 2-5 Catalyst 6500 Linecard Queuing Structures

C2 (xCEF720) Modules	Description	Receive Queue Structure	Transmit Queue Structure	Buffer Size
WS-X6704-10GE	Catalyst 6500 4-port 10 GigabitEthernet Module	1Q8T (8Q8T with DFC3a)	1P7Q8T	16MB per port
WS-X6724-SFP	Catalyst 6500 24-port GigabitEthernet SFP Module	1Q8T; (2Q8T with DFC3a)	1P3Q8T	1MB per port

WS-X6748-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Module	1Q8T; (2Q8T with DFC3a)	1P3Q8T	1MB per port
WS-X6748-SFP	Catalyst 6500 48-port GigabitEthernet SFP Module	1Q8T; (2Q8T with DFC3a)	1P3Q8T	1MB per port
Classic/CEF256 Ethernet Modules	**Description**	**Receive Queue Structure**	**Transmit Queue Structure**	**Buffer Size**
WS-X6024-10FL-MT	Catalyst 6000 24-port 10BaseFL MT-RJ Module	1Q4T	2Q2T	64KB per port
WS-X6148-RJ21	Catalyst 6500 48-Port 10/100 RJ-21 Module (Upgradable to Voice)	1Q4T	2Q2T	128KB per port
WS-X6148-RJ21V	Catalyst 6500 48-port 10/100 Inline Power RJ-21 Module	1Q4T	2Q2T	128KB per port
WS-X6148-RJ45	Catalyst 6500 48-Port 10/100; RJ-45 Module (Upgradable to Voice)	1Q4T	2Q2T	128KB per port
WS-X6148-RJ45V	Catalyst 6500 48-port 10/100 Inline Power RJ-45 Module	1Q4T	2Q2T	128KB per port
WS-X6148-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Module	1Q2T	1P2Q2T	1MB per 8 ports
WS-X6148V-GE-TX	Catalyst 6500 48-port 10/100/1000 Inline Power RJ-45 Module	1Q2T	1P2Q2T	1MB per 8 ports
WS-X6316-GE-TX	Catalyst 6000 16-port 1000TX GigabitEthernet RJ-45 Module	1P1Q4T	1P2Q2T	512KB per port
WS-X6324-100FX-MM	Catalyst 6000 24-port 100FX MT-RJ MMF Module (with Enhanced QoS)	1Q4T	2Q2T	128KB per port
WS-X6324-100FX-SM	Catalyst 6000 24-port 100FX MT-RJ SMF Module (with Enhanced QoS)	1Q4T	2Q2T	128KB per port
WS-X6348-RJ-21	Catalyst 6000 48-port 10/100 RJ-21 Module	1Q4T	2Q2T	128KB per port
WS-X6348-RJ21V	Catalyst 6000 48-port 10/100 Inline Power RJ-21 Module	1Q4T	2Q2T	128KB per port
WS-X6348-RJ-45	Catalyst 6500 48-port 10/100 RJ-45 Module (Upgradable to Voice)	1Q4T	2Q2T	128KB per port
WS-X6348-RJ45V	Catalyst 6500 48-port 10/100 Inline Power RJ-45 Module	1Q4T	2Q2T	128KB per port
WS-X6408A-GBIC	Catalyst 6000 8-port GigabitEthernet Module (with Enhanced QoS; Requires GBICs)	1P1Q4T	1P2Q2T	512KB per port
WS-X6416-GBIC	Catalyst 6000 16-port GigabitEthernet Module (Requires GBICs)	1P1Q4T	1P2Q2T	512KB per port
WS-X6416-GE-MT	Catalyst 6000 16-port GigabitEthernet MT-RJ Module	1P1Q4T	1P2Q2T	512KB per port
WS-X6501-10GEX4	1-port 10 GigabitEthernet Module	1P1Q8T	1P2Q1T	64MB per port

WS-X6502-10GE	Catalyst 6500 10 GigabitEthernet Base Module (Requires OIM)	1P1Q8T	1P2Q1T	64MB per port
WS-X6516A-GBIC	Catalyst 6500 16-port GigabitEthernet Module (Fabric-enabled; Requires GBICs)	1P1Q4T	1P2Q2T	1MB per port
WS-X6516-GBIC	Catalyst 6500 16-port GigabitEthernet Module (Fabric-Enabled; Requires GBICs)	1P1Q4T	1P2Q2T	512KB per port
WS-X6516-GE-TX	Catalyst 6500 16-port GigabitEthernet Copper Module; (Crossbar-enabled)	1P1Q4T	1P2Q2T	512KB per port
WS-X6524-100FX-MM	Catalyst 6500 24-port 100FX MT-RJ Module (Fabric-enabled)	1P1Q0T	1P3Q1T	1MB per port
WS-X6548-RJ-21	Catalyst 6500 48-port 10/100 RJ-21 Module (Fabric-enabled)	1P1Q0T	1P3Q1T	1MB per port
WS-X6548-RJ-45	Catalyst 6500 48-port 10/100 RJ-45 Module (Crossbar-enabled)	1P1Q0T	1P3Q1T	1MB per port
WS-X6548V-GE-TX	Catalyst 6500 48-port 10/100/1000 Inline Power RJ-45 Module (Fabric-enabled)	1Q2T	1P2Q2T	1MB per 8 ports
WS-X6548-GE-TX	Catalyst 6500 48-port 10/100/1000 RJ-45 Module (Fabric-enabled)	1Q2T	1P2Q2T	1MB per 8 ports
WS-X6816-GBIC	Catalyst 6500 16-port GigabitEthernet Module (Fabric-Enabled; Requires GBICs)	1P1Q4T	1P2Q2T	512KB per port

Design recommendations for each of these six main Catalyst 6500 queuing structures follow.

Catalyst 6500—2Q2T Queuing and Dropping

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

Linecards that only support 2Q2T queuing models have no provision for priority-queuing. Nonetheless, tuning the Weighted Round-Robin (WRR) weights and the queue sizes can help offset this limitation.

For example, if Q1 is to service Scavenger/Bulk (CoS 1) and Best Effort (CoS 0) traffic, then assigning 30% of the buffer space to the first queue is adequate; the remaining 70% can be assigned to Q2.

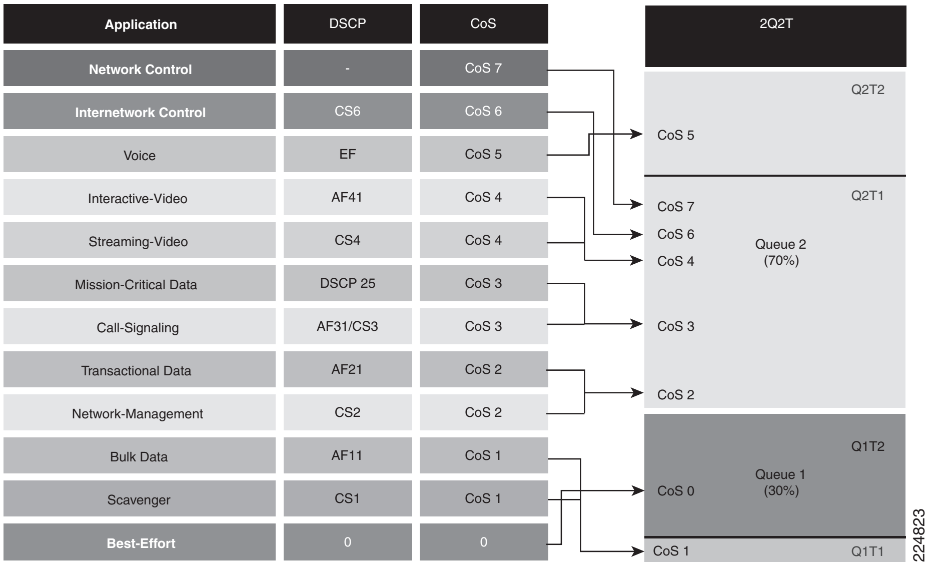
The WRR weights can be set to the same ratio of 30:70 for servicing Q1:Q2.

Since the 2Q2T model supports configurable Tail-Drop thresholds, these can be tuned to provide an additional layer of QoS granularity. For example, the first queue's first threshold can be set at 40% to prevent Scavenger/Bulk traffic from dominating Q1. Similarly, the second queue's first threshold can be set to 80% to always allow some room in the queue for VoIP. The second threshold of each queue should *always* be set to the tail of the queue (100%).

Once the queues and thresholds have been defined as above, then CoS 1 (Scavenger/Bulk) can be assigned to Q1T1; CoS 0 (Best Effort) can be assigned to Q1T2; CoS 2 (Network Management and Transactional Data), CoS 3 (call signaling and Mission-Critical Data), CoS 4 (Interactive and Streaming Video), and CoS 6 and 7 (Internetwork and Network Control) can be assigned to Q21T; and CoS 5 (VoIP) can be assigned to Q2T2.

These 2Q2T queuing recommendations are illustrated in Figure 2-26.

Figure 2-26 Catalyst 6500 2Q2T Queuing Model



Application	DSCP	CoS
Network Control	-	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive-Video	AF41	CoS 4
Streaming-Video	CS4	CoS 4
Mission-Critical Data	DSCP 25	CoS 3
Call-Signaling	AF31/CS3	CoS 3
Transactional Data	AF21	CoS 2
Network-Management	CS2	CoS 2
Bulk Data	AF11	CoS 1
Scavenger	CS1	CoS 1
Best-Effort	0	0

Configuration

The Catalyst 6500 CatOS configurations to configure 2Q2T queuing recommendations are shown below.

Example 2-64 Catalyst 6500 CatOS—2Q2T Queuing Example

```
CAT6500-PFC2-CATOS> (enable) set qos txq-ratio 2q2t 30 70
    ! Sets the buffer allocations to 30% for Q1 and 70% for Q2
CAT6500-PFC2-CATOS> (enable) set qos wrr 2q2t 30 70
    ! Sets the WRR weights for 30:70 (Q1:Q2) bandwidth servicing
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos drop-threshold 2q2t tx queue 1 40 100
    ! Sets Q1T1 to 5% to limit Scavenger/Bulk from dominating Q1
CAT6500-PFC2-CATOS> (enable) set qos drop-threshold 2q2t tx queue 2 80 100
    ! Sets Q2T1 to 80% to always have room in Q2 for VoIP
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos map 2q2t tx 1 1 cos 1
    ! Assigns Scavenger/Bulk to Q1T1
CAT6500-PFC2-CATOS> (enable) set qos map 2q2t tx 1 2 cos 0
    ! Assigns Best Effort to Q1T2
CAT6500-PFC2-CATOS> (enable) set qos map 2q2t tx 2 1 cos 2,3,4,6,7
    ! Assigns CoS 2,3,4,6 and 7 to Q2T1
CAT6500-PFC2-CATOS> (enable) set qos map 2q2t tx 2 2 cos 5
    ! Assigns VoIP to Q2T2
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands:

- show qos info config 2q2t tx
- show qos info runtime
- show qos statistics

Catalyst 6500 CatOS QoS Verification Command: show qos info config 2q2t tx

The Catalyst 6500 CatOS **show qos info config 2q2t tx** verification command displays the queuing and dropping parameters for 2Q2T linecards.

In the example below, CoS 1 is assigned to Q1T1; CoS 0 is assigned to Q1T2; CoS values 2,3,4,6 and 7 are assigned to Q2T1 and CoS 5 is assigned to Q2T2. The first thresholds are set to 40% and 80%of their respective queues, and the second thresholds set to the tail of the queue. The size ratio has been allocated 30% for Q1 and 70% for Q2 and the WRR weights are set to 30:70 to service Q1 and Q2, respectively.

Example 2-65 Show QoS Info Config 2Q2T Tx Verification for a Catalyst 6500-CatOS Switch

```
CAT6500-PFC2-CATOS> (enable) show qos info config 2q2t tx
QoS setting in NVRAM for 2q2t transmit:
QoS is enabled
Queue and Threshold Mapping for 2q2t (tx):
Queue Threshold CoS
----- --------- ---------------
1     1         1
1     2         0
2     1         2 3 4 6 7
2     2         5
Tx drop thresholds:
Queue #  Thresholds - percentage
-------  ------------------------------------
1        40%  100%
2        80% 100%
Tx WRED thresholds:
WRED feature is not supported for this port type.
Tx queue size ratio:
Queue #  Sizes - percentage
-------  ------------------------------------
1        30%
2        70%
Tx WRR Configuration of ports with 2q2t:
Queue #  Ratios
-------  ------------------------------------
1        30
2        70
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Command: show qos info runtime

The Catalyst 6500 CatOS **show qos info runtime** verification command reports similar information as the **show qos info config** command, but displays the runtime information (committed to the PFC and linecard) as opposed to only the configured information.

In the example below, CoS 1 is assigned to Q1T1; CoS 0 is assigned to Q1T2; CoS values 2,3,4,6 and 7 are assigned to Q2T1 and CoS 5 is assigned to Q2T2. The first thresholds are set to 40% and 80% of their respective queues, and the second thresholds set to the tail of the queue. The size ratio has been allocated 30% for Q1 and 70% for Q2 and the WRR weights are set to 30:70 to service Q1 and Q2, respectively.

Example 2-66 Show QoS Info Runtime Verification for a Catalyst 6500-CatOS Switch

```
CAT6500-PFC3-CATOS> (enable) show qos info runtime 3/1
Run time setting of QoS:
QoS is enabled
Policy Source of port 3/1: Local
Tx port type of port 3/1 : 2q2t
Rx port type of port 3/1 : 1q4t
Interface type: port-based
ACL attached:
The qos trust type is set to untrusted.
Default CoS = 0
Queue and Threshold Mapping for 2q2t (tx):
Queue Threshold CoS
----- --------- ---------------
1     1         1
1     2         0
2     1         2 3 4 6 7
2     2         5
Queue and Threshold Mapping for 1q4t (rx):
All packets are mapped to a single queue.
Rx drop thresholds:
Rx drop thresholds are disabled.
Tx drop thresholds:
Queue #  Thresholds - percentage (* abs values)
-------  ------------------------------------
1        40% (6144 bytes) 100% (15360 bytes)
2        80% (28672 bytes) 100% (35840 bytes)
Rx WRED thresholds:
Rx WRED feature is not supported for this port type.
Tx WRED thresholds:
WRED feature is not supported for this port type.
Tx queue size ratio:
Queue #  Sizes - percentage (* abs values)
-------  ------------------------------------
1        30% (17408 bytes)
2        70% (37888 bytes)
Rx queue size ratio:
Rx queue size-ratio feature is not supported for this port type.
Tx WRR Configuration of ports with speed 10Mbps:
Queue #  Ratios (* abs values)
-------  ------------------------------------
1        30 (7648 bytes)
2        70 (17840 bytes)
(*) Runtime information may differ from user configured setting due to hardware
granularity.
CAT6500-PFC3-CATOS> (enable)
```

The Catalyst 6500 IOS configurations to configure 2Q2T queuing recommendations are shown below.

Example 2-67 Catalyst 6500 IOS—2Q2T Queuing Example

```
CAT6500-PFC3-IOS(config)# interface range FastEthernet6/1 - 48
CAT6500-PFC3-IOS(config-if)# wrr-queue queue-limit 30 70
    ! Sets the buffer allocations to 30% for Q1 and 70% for Q2
CAT6500-PFC3-IOS(config-if)# wrr-queue bandwidth 30 70
    ! Sets the WRR weights for 30:70 (Q1:Q2) bandwidth servicing
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue threshold 1 40 100
    ! Sets Q1T1 to 5% to limit Scavenger/Bulk from dominating Q1
CAT6500-PFC3-IOS(config-if)# wrr-queue threshold 2 80 100
    ! Sets Q2T1 to 80% to always have room in Q2 for VoIP
CAT6500-PFC3-IOS(config-if)#
```

```
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 1 1 1
    ! Assigns Scavenger/Bulk to Q1T1
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 1 2 0
    ! Assigns Best Effort to Q1T2
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 2 1 2 3 4 6 7
    ! Assigns CoS 2,3,4,6 and 7 to Q2T1
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 2 2 5
    ! Assigns VoIP to Q2T2
CAT6500-PFC3-IOS(config-if)#end
CAT6500-PFC3-IOS#
```

Catalyst 6500 MLS QoS Verification Commands:

- show queueing interface

Catalyst 6500 IOS QoS Verification Command: show queueing interface

The Catalyst 6500 IOS **show queueing interface** verification command displays the queuing parameters for a given interface (according to the linecard's capabilities).

In the example below, the linecard has 2Q2T transmit queuing. The WRR scheduling weights are set to 30:70 to service Q1 and Q2, respectively. The transmit queue size ratios have been allocated 30% for Q1 and 70 percent for Q2. The first queue's tail-drop thresholds are set to 40% and 100%, while the second queue's tail-drop thresholds are set to 80% and 100%. CoS 1 is assigned to Q1T1; CoS 0 is assigned to Q1T2; CoS values 2,3,4,6 and 7 are assigned to Q2T1 and CoS 5 is assigned to Q2T2.

Example 2-68 Show Queueing Interface Verification for a Catalyst 6500-IOS Switch

```
CAT6500-PFC3-IOS#show queueing interface FastEthernet6/1
Interface FastEthernet6/1 queueing strategy:  Weighted Round-Robin
  Port QoS is enabled
  Port is untrusted
  Extend trust state: not trusted [COS = 0]
  Default COS is 0
    Queueing Mode In Tx direction: mode-cos
    Transmit queues [type = 2q2t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       1         WRR low             2
       2         WRR high            2

    WRR bandwidth ratios:   30[queue 1]  70[queue 2]
    queue-limit ratios:     30[queue 1]  70[queue 2]

    queue tail-drop-thresholds
    --------------------------
    1     40[1] 100[2]
    2     80[1] 100[2]

    queue thresh cos-map
    ---------------------------------------
    1     1      1
    1     2      0
    2     1      2 3 4 6 7
    2     2      5

    <output truncated>

CAT6500-PFC3-IOS#
```

Catalyst 6500—1P2Q1T Queuing and Dropping

This section includes the following topics:

- Configuration
- Catalyst MLS QoS Verification Commands

The 1P2Q1T queuing model builds on the previous 2Q2T model, bringing with it the advantages of strict-priority queuing (for VoIP) as well as a tunable WRED (not Tail-Drop) threshold per queue.

The term "1P2Q1T" is a bit of a misnomer in the CatOS version of this queuing structure because in CatOS there are actually two thresholds per queue: the tunable WRED threshold and the non-configurable tail-of-the-queue (100%) tail-drop threshold.

Under such a model, buffer space can be allocated as follows: 30% for Scavenger/Bulk with Best Effort queue (Q1), 40% for Q2, and 30% for the PQ (Q3)

The WRR weights for Q1 and Q2 (for dividing the remaining bandwidth, after the priority queue has been fully serviced) can be set to 30:70 respectively for Q1:Q2.

Under the 1P2Q1T model, each queue's WRED threshold is defined with a lower and upper limit. For example, the WRED threshold 40:80 indicates that packets assigned to this WRED threshold will *begin* being randomly dropped when the queue fills to 40 percent *and* that these packets will be tail-dropped if the queue fills beyond 80 percent.

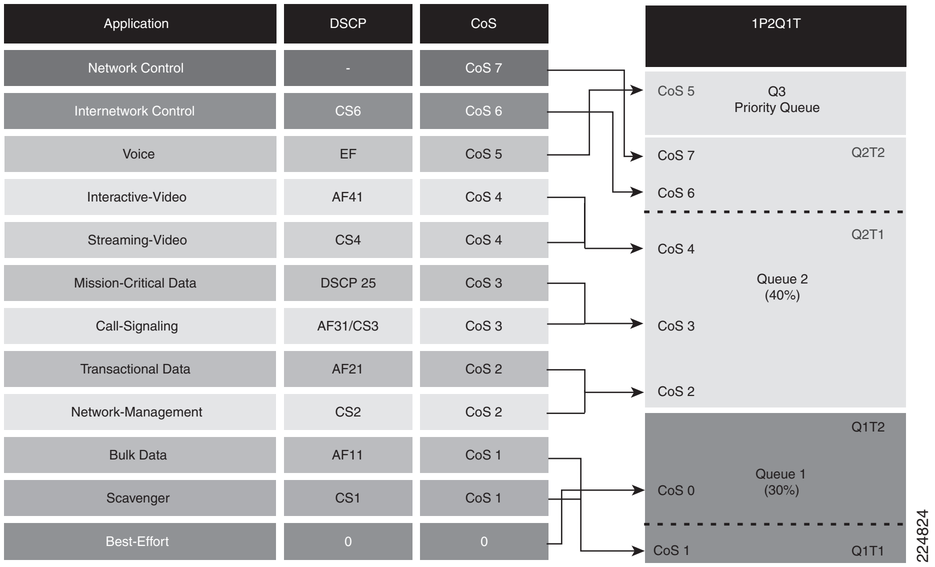
Furthermore, in CatOS within the 1P2Q1T queuing structure, each CoS value can be assigned to queue *and* a WRED threshold or just to a queue. When assigned to a queue (only), then the CoS value is limited only by the tail of the queue (in other words, it is assigned to the queue with a tail-drop threshold of 100%).

Thus (in CatOS), the tunable WRED threshold for Q1 can be set to 40:80, meaning that Scavenger/Bulk Data will be WRED-dropped if Q1 fills to 40 percent and will be tail-dropped if Q1 fills past 80 percent of capacity. This prevents Scavenger/Bulk Data from drowning out Best-Effort traffic in Q1. The WRED threshold for Q2 can be set to 70:80 to provide congestion avoidance for all applications assigned to it and to ensure that there will always be room in the queue to service Network and Internetwork Control traffic.

Therefore, once the queues and thresholds have been defined as above, then CoS 1 (Scavenger/Bulk) can be assigned to Q1T1; CoS 0 (Best Effort) to Q1-only (tail); CoS 2 (Network Management and Transactional Data), CoS 3 (call signaling and Mission-Critical Data) and CoS 4 (Interactive and Streaming Video) can be assigned to Q2T1; CoS 6 and 7 (Internetwork and Network Control) can be assigned to Q2-only (tail); CoS 5 (VoIP) can be assigned to Q3 (the PQ).

These 1P2Q1T queuing recommendations are illustrated in Figure 2-27.

Figure 2-27 Catalyst 6500 1P2Q1T Queuing Model (CatOS Supports 1P2Q2T)



Application	DSCP	CoS
Network Control	-	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive-Video	AF41	CoS 4
Streaming-Video	CS4	CoS 4
Mission-Critical Data	DSCP 25	CoS 3
Call-Signaling	AF31/CS3	CoS 3
Transactional Data	AF21	CoS 2
Network-Management	CS2	CoS 2
Bulk Data	AF11	CoS 1
Scavenger	CS1	CoS 1
Best-Effort	0	0

Configuration

The Catalyst 6500 CatOS configurations to configure 1P2Q1T queuing recommendations are shown below.

Example 2-69 Catalyst 6500 CatOS—1P2Q1T Queuing Example (technically 1P2Q2T)

```
CAT6500-PFC2-CATOS> (enable) set qos txq-ratio 1p2q1t 30 40 30
! Sets the buffer allocations to 30% for Q1, 40% for Q2, 30% for Q3 (PQ)
CAT6500-PFC2-CATOS> (enable) set qos wrr 1p2q1t 30 70
! Sets the WRR weights for 30:70 (Q1:Q2) bandwidth servicing
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos wred 1p2q1t tx queue 1 40:80
! Sets Q1 WRED Threshold to 40:80 to limit Scavenger/Bulk from dominating Q1
CAT6500-PFC2-CATOS> (enable) set qos wred 1p2q1t tx queue 2 70:80
! Sets Q2 WRED Threshold to 70:80 to force room for Network Control traffic
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q1t tx 1 1 cos 1
    ! Assigns Scavenger/Bulk to Q1 WRED Threshold
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q1t tx 1 cos 0
    ! Assigns Best Effort to Q1 tail (100%) threshold
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q1t tx 2 1 cos 2,3,4
    ! Assigns CoS 2,3,4 to Q2 WRED Threshold
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q1t tx 2 cos 6,7
    ! Assigns Network/Internetwork Control to Q2 tail (100%) threshold
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q1t tx 3 cos 5
    ! Assigns VoIP to PQ (Q3)
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands:

- show qos info config 1p2q1t tx
- show qos info runtime
- show qos statistics

Note The Catalyst 6500 CatOS **show qos info** verification commands are reasonably similar for each queuing structure and as such (to minimize redundancy) are not detailed for each queuing model example.

In IOS, for any 1P*x*Q*y*T queuing structure, setting the size of the priority queue is not supported. The only exception to this is within the 1P2Q2T structure, where the priority queue (Q3) is indirectly set to equal Q2's size. Therefore, in all examples of Catalyst 6500 IOS queuing structure configurations to follow (that support a PQ) only the sizes of the standard queues are being set.

Furthermore, specific to the 1P2Q1T queuing structure, CoS values cannot be mapped to the tail of the queue, as in CatOS. CoS values can be mapped only to the single WRED threshold for each queue. Therefore, the 1P2Q1T queuing and dropping recommendation requires some slight alterations for Cisco IOS. These include changing Q1T1's WRED threshold to 80:100 and, likewise, changing Q2T1's WRED threshold to 80:100.

The syntax-logic for setting WRED thresholds in IOS is different from CatOS. In CatOS, minimum and maximum WRED thresholds were set on the same line; in IOS, minimum and maximum WRED thresholds are set on different lines.

After these WRED thresholds have been altered, then CoS 1 (Scavenger/Bulk) and CoS 0 (Best Effort) can be assigned to Q1T1; CoS 2 (Network Management and Transactional Data), CoS 3 (call signaling and Mission-Critical Data), CoS 4 (Interactive and Streaming Video) and CoS 6 and 7 (Internetwork and Network Control) can be assigned to Q2T1; CoS 5 (VoIP) can be assigned to Q3 (the PQ).

The Catalyst 6500 IOS configurations to configure 1P2Q1T queuing recommendations are shown below.

Example 2-70 Catalyst 6500 IOS—1P2Q1T Queuing Example

```
CAT6500-PFC3-IOS(config)#interface TenGigabitEthernet1/1
CAT6500-PFC3-IOS(config-if)# wrr-queue queue-limit 30 40
! Sets the buffer allocations to 30% for Q1 and 40% for Q2
CAT6500-PFC3-IOS(config-if)# wrr-queue bandwidth 30 70
! Sets the WRR weights for 30:70 (Q1:Q2) bandwidth servicing
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 1 80
    ! Sets Min WRED Threshold for Q1T1 to 80%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 1 100
    ! Sets Max WRED Threshold for Q1T1 to 100%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 2 80
    ! Sets Min WRED Threshold for Q2T1 to 80%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 2 100
    ! Sets Max WRED Threshold for Q2T1 to 100%
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 1 1 1 0
    ! Assigns Scavenger/Bulk and Best Effort to Q1 WRED Threshold 1
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 2 1 2 3 4 6 7
    ! Assigns CoS 2,3,4,6 and 7 to Q2 WRED Threshold 1
CAT6500-PFC3-IOS(config-if)# priority-queue cos-map 1 5
    ! Assigns VoIP to PQ (Q3)
CAT6500-PFC3-IOS(config-if)#end
CAT6500-PFC3-IOS(config-if)#
```

Catalyst 6500 MLS QoS Verification Commands:

- show queueing interface

Catalyst 6500—1P2Q2T Queuing and Dropping

This section includes the following topics:

- Recommendations
- Configuration
- Catalyst MLS QoS Verification Commands

Recommendations

The 1P2Q2T queuing model is essentially identical to the 1P2Q1T model, except that it supports two configurable WRED thresholds per queue. Under this model, CoS values cannot be mapped to the tail of the queue, as with the 1P2Q1T model, and so there are (as the name correctly implies this time) two effective thresholds per queue.

Under a 1P2Q2T model, buffer space can be allocated as follows: 30% for Q1 (the Scavenger/Bulk with Best Effort queue), 40% for Q2 (the preferential queue), and 30% for the Q3 (the priority queue).

The WRR weights for Q1 and Q2 (for dividing the remaining bandwidth, after the priority queue has been fully serviced) remain at 30:70 respectively for Q1:Q2.

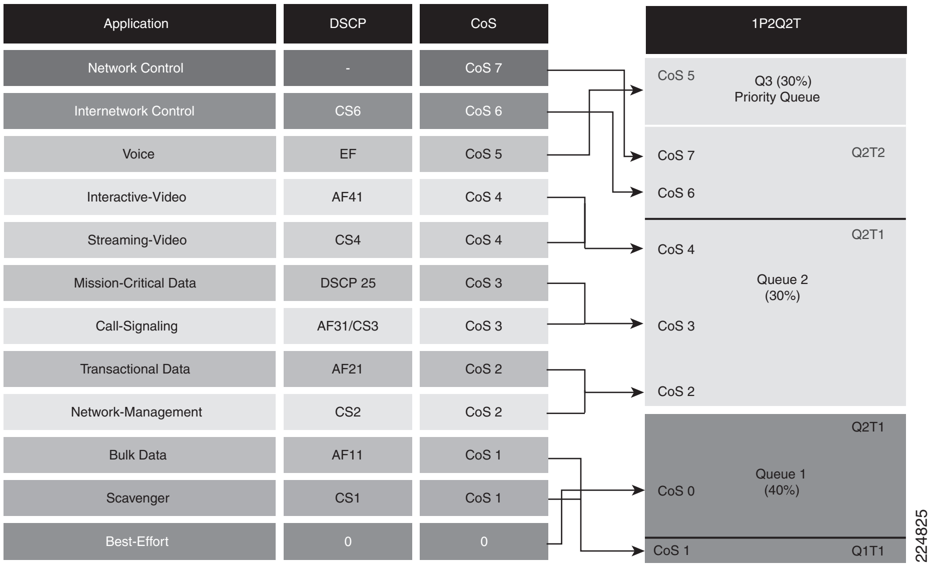
Under the 1P2Q2T model, each WRED threshold is defined with a lower and upper limit. Therefore, the first WRED threshold for Q1 can be set to 40:80, so that Scavenger/Bulk Data traffic can be WRED-dropped if Q1 hits 40 percent and can be tail-dropped if Q1 exceeds 80 percent of its capacity (this prevents Scavenger/Bulk Data from drowning out Best-Effort traffic in Q1). The second WRED threshold for Q1 can be set to 80:100 to provide congestion avoidance for Best-Effort traffic.

Similarly, the first WRED threshold of Q2 can be set to 70:80, and the second can be set to 80:100. In this manner, congestion avoidance will be provided for all traffic types in Q2, and there will always be room in the queue to service Network and Internetwork Control traffic.

Therefore, once the queues have been defined as above, then CoS 1 (Scavenger/Bulk) can be assigned to Q1T1; CoS 0 (Best Effort) to Q1T2; CoS 2 (Network Management and Transactional Data), CoS 3 (call signaling and Mission-Critical Data) and CoS 4 (Interactive and Streaming Video) can be assigned to Q2T1; CoS 6 and 7 (Internetwork and Network Control) can be assigned to Q2T2; CoS 5 (VoIP) can be assigned to Q3T1 (the PQ).

These 1P2Q2T queuing recommendations are illustrated in Figure 2-28.

Figure 2-28 Catalyst 6500 1P2Q2T Queuing Model



Configuration

The Catalyst 6500 CatOS configurations to configure 1P2Q1T queuing recommendations are shown below.

Example 2-71 Catalyst 6500 CatOS—1P2Q2T Queuing Example

```
CAT6500-PFC2-CATOS> (enable) set qos txq-ratio 1p2q2t 30 40 30
! Sets the buffer allocations to 30% for Q1, 40% for Q2, 30% for Q3 (PQ)
CAT6500-PFC2-CATOS> (enable) set qos wrr 1p2q2t 30 70
! Sets the WRR weights for 30:70 (Q1:Q2) bandwidth servicing
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos wred 1p2q2t tx queue 1 40:80 80:100
! Sets Q1 WRED T1 to 40:80 to limit Scavenger/Bulk from dominating Q1
! Sets Q1 WRED T2 to 80:100 to provide congestion-avoidance for Best Effort
CAT6500-PFC2-CATOS> (enable) set qos wred 1p2q2t tx queue 2 70:80 80:100
! Sets Q2 WRED T1 to 70:80 to provide congestion-avoidance
! Sets Q2 WRED T2 to 80:100 to force room for Network Control traffic
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q2t tx 1 1 cos 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q2t tx 1 2 cos 0
! Assigns Best Effort to Q1 WRED Threshold 2
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q2t tx 2 1 cos 2,3,4
! Assigns CoS 2,3,4 to Q2 WRED Threshold 1
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q2t tx 2 2 cos 6,7
! Assigns Network/Internetwork Control to Q2 WRED Threshold 2
CAT6500-PFC2-CATOS> (enable) set qos map 1p2q2t tx 3 1 cos 5
! Assigns VoIP to PQ
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands:

- show qos info config 1p2q2t tx
- show qos info runtime
- show qos statistics

The compatible Catalyst 6500 IOS configurations to configure 1P2Q1T queuing recommendations are shown below. Notice that the buffer allocation for the PQ (Q3) is not configurable, but is, by default (for the 1P2Q2T queuing structure only) set to equal the size defined for Q2. Therefore, the queue size ratios have been slightly altered from the CatOS version of this queuing model to take this default IOS behavior into account; specifically Q1 is set to 40% and Q2 is set to 30% (which indirectly sets Q3 to match, at 30%).

The Catalyst 6500 IOS configurations to configure 1P2Q2T queuing recommendations are shown below.

Example 2-72 Catalyst 6500 IOS—1P2Q2T Queuing

```
CAT6500-PFC3-IOS(config)#interface range GigabitEthernet4/1 - 8
CAT6500-PFC3(config-if-range)# wrr-queue queue-limit 40 30
! Sets the buffer allocations to 40% for Q1 and 30% for Q2
! Indirectly sets PQ (Q3) size to equal Q2 (which is set to 30%)
CAT6500-PFC3(config-if-range)# wrr-queue bandwidth 30 70
! Sets the WRR weights for 30:70 (Q1:Q2) bandwidth servicing
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)# wrr-queue random-detect min-threshold 1 40 80
    ! Sets Min WRED Thresholds for Q1T1 and Q1T2 to 40 and 80, respectively
CAT6500-PFC3(config-if-range)# wrr-queue random-detect max-threshold 1 80 100
    ! Sets Max WRED Thresholds for Q1T1 and Q1T2 to 80 and 100, respectively
CAT6500-PFC3(config-if-range)#
```

```
CAT6500-PFC3(config-if-range)# wrr-queue random-detect min-threshold 2 70 80
    ! Sets Min WRED Thresholds for Q2T1 and Q2T2 to 70 and 80, respectively
CAT6500-PFC3(config-if-range)# wrr-queue random-detect max-threshold 2 80 100
    ! Sets Max WRED Thresholds for Q2T1 and Q2T2 to 80 and 100, respectively
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 1 1 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 1 2 0
! Assigns Best Effort to Q1 WRED Threshold 2
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 2 1 2 3 4
! Assigns CoS 2,3,4 to Q2 WRED Threshold 1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 2 2 6 7
! Assigns Network/Internetwork Control to Q2 WRED Threshold 2
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)# priority-queue cos-map 1 5
! Assigns VoIP to PQ
CAT6500-PFC3(config-if-range)#end
CAT6500-PFC3-IOS#
```

Catalyst 6500 MLS QoS Verification Commands:

- show queueing interface

Catalyst 6500—1P3Q1T Queuing and Dropping

This section includes the following topics:

- Recommendations
- Configuration
- Catalyst MLS QoS Verification Commands

Recommendations

The 1P3Q1T queuing structure is identical to the 1P2Q1T structure, except that an additional standard queue has been added to it and it does not support tuning the Transmit Size Ratios. Under this model, Q4 is the strict-priority queue.

The WRR weights for the standard queues (Q1, Q2, Q3), for dividing the remaining bandwidth, after the priority queue has been fully serviced, can be set to 5:25:70 respectively for Q1:Q2:Q3.

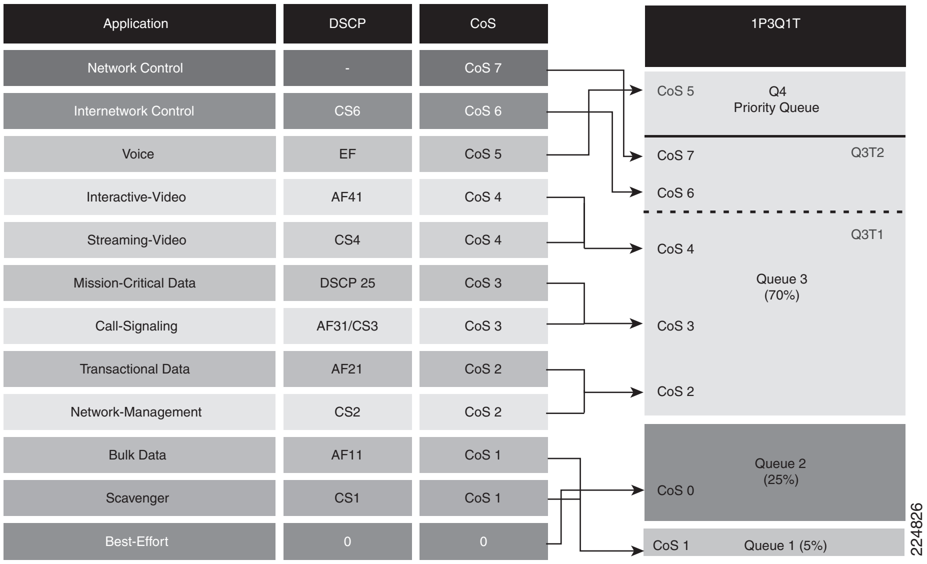
In CatOS, within the 1P3T1T queuing structure each CoS value can be assigned to queue *and* a WRED threshold or just to a queue. When assigned to a queue (only), then the CoS value is limited only by the tail of the queue (in other words, it is assigned to the queue with a tail-drop threshold of 100%).

Thus, the tunable WRED threshold for Q1 can be set to 80:100 to provide congestion avoidance for Scavenger/Bulk Data traffic. The WRED threshold for Q2 similarly can be set to 80:100 to provide congestion avoidance on all Best-Effort flows. The WRED threshold for Q3 can be set to 70:80, to provide congestion avoidance for all applications assigned to it and to ensure that there will always be room in the Q3 to service Network and Internetwork Control traffic.

Therefore, once the queues and thresholds have been defined as above, then CoS 1 (Scavenger/Bulk) can be assigned to Q1T1; CoS 0 (Best Effort) to Q2T1; CoS 2 (Network Management and Transactional Data), CoS 3 (call signaling and Mission-Critical Data) and CoS 4 (Interactive and Streaming Video) can be assigned to Q3T1; CoS 6 and 7 (Internetwork and Network Control) can be assigned to Q3 (tail); CoS 5 (VoIP) can be assigned to Q4 (the PQ).

These 1P3Q1T queuing recommendations are illustrated in Figure 2-29.

Figure 2-29 Catalyst 6500 1P3Q1T Queuing Model (CatOS supports 1P3Q2T)



Configuration

The Catalyst 6500 CatOS configurations to configure 1P3Q1T queuing recommendations are shown below.

Example 2-73 Catalyst 6500 CatOS—1P3Q1T Queuing Example (technically 1P3Q2T)

```
CAT6500-PFC2-CATOS> (enable) set qos wrr 1p3q1t 5 25 70
! Sets the WRR weights for 5:25:70 (Q1:Q2:Q3) bandwidth servicing
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos wred 1p3q1t tx queue 1 80:100
    ! Sets Q1 WRED T1 to 80:100 to provide congestion-avoidance for Scavenger/Bulk
CAT6500-PFC2-CATOS> (enable) set qos wred 1p3q1t tx queue 2 80:100
    ! Sets Q2 WRED T1 to 80:100 to provide congestion-avoidance for Best Effort
CAT6500-PFC2-CATOS> (enable) set qos wred 1p3q1t tx queue 3 70:80
! Sets Q3 WRED T1 to 70:80 to provide congestion-avoidance for CoS 2,3,4
! and to force room (via tail-drop) for Network Control traffic
CAT6500-PFC2-CATOS> (enable)
CAT6500-PFC2-CATOS> (enable) set qos map 1p3q1t tx 1 1 cos 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1 (80:100)
CAT6500-PFC2-CATOS> (enable) set qos map 1p3q1t tx 2 1 cos 0
! Assigns Best Effort to Q2 WRED Threshold 1 (80:100)
CAT6500-PFC2-CATOS> (enable) set qos map 1p3q1t tx 3 1 cos 2,3,4
! Assigns CoS 2,3,4 to Q3 WRED Threshold 1 (70:80)
CAT6500-PFC2-CATOS> (enable) set qos map 1p3q1t tx 3 cos 6,7
! Assigns Network/Internetwork Control to Q3 Tail (100%)
CAT6500-PFC2-CATOS> (enable) set qos map 1p3q1t tx 4 cos 5
! Assigns VoIP to PQ (Q4)
CAT6500-PFC2-CATOS> (enable)
```

Catalyst 6500 CatOS QoS Verification Commands:

- show qos info config 1p3q1t tx
- show qos info runtime
- show qos statistics

In IOS, the 1P3Q1T, 1P3Q8T, and 1P7Q8T queuing structures can be configured to use tail-drop or WRED. By default, WRED is disabled. Therefore, it is good practice to always explicitly enable WRED on a queue before setting WRED thresholds for these queuing structures.

Additionally, in Cisco IOS, the 1P3Q1T queuing structure does not support mapping CoS values to the tail of the queue (only to the single WRED threshold). Therefore, the queuing recommendation requires slight alterations for Cisco IOS: changing all three WRED thresholds to 80:100 and mapping CoS values 2, 3, 4, 6, and 7 to Q3T1.

The Catalyst 6500 IOS configurations to configure 1P3Q1T queuing recommendations are shown below.

Example 2-74 Catalyst 6500 IOS—1P3Q1T Queuing Example

```
CAT6500-PFC3-IOS(config)# interface range FastEthernet3/1 - 48
CAT6500-PFC3-IOS(config-if)# wrr-queue bandwidth 5 25 70
! Sets the WRR weights for 5:25:70 (Q1:Q2:Q3) bandwidth servicing
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 1
    ! Enables WRED on Q1
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 2
! Enables WRED on Q2
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 3
! Enables WRED on Q3
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 1 80
    ! Sets Min WRED Threshold for Q1T1 to 80%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 1 100
    ! Sets Max WRED Threshold for Q1T1 to 100%
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 2 80
    ! Sets Min WRED Threshold for Q2T1 to 80%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 2 100
    ! Sets Max WRED Threshold for Q2T1 to 100%
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 3 80
    ! Sets Min WRED Threshold for Q3T1 to 80%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 3 100
    ! Sets Max WRED Threshold for Q3T1 to 100%
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 1 1 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1 (80:100)
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 2 1 0
! Assigns Best Effort to Q2 WRED Threshold 1 (80:100)
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 3 1 2 3 4 6 7
! Assigns CoS 2,3,4,6 and 7 to Q3 WRED Threshold 1 (80:100)
CAT6500-PFC3-IOS(config-if)# priority-queue cos-map 1 5
! Assigns VoIP to PQ (Q4)
CAT6500-PFC3-IOS(config-if)#end
CAT6500-PFC3-IOS#
```

Catalyst 6500 MLS QoS Verification Commands:

- show queueing interface

Catalyst 6500—1P3Q8T Queuing and Dropping

The 1P3Q8T queuing structure is identical to the 1P3Q1T structure, except it has eight tunable WRED thresholds per queue (instead of one) and it also supports tuning the Transmit Size Ratios. Under this model, Q4 is the strict-priority queue.

Under a 1P3Q8T model, buffer space can be allocated as follows: 5% for the Scavenger/Bulk queue (Q1), 25% for the Best Effort queue (Q2), 40% for the preferential queue (Q3), and 30% for the strict priority queue (Q4).

The WRR weights for the standard queues (Q1, Q2, Q3), for dividing the remaining bandwidth, after the priority queue has been fully serviced, can be set to 5:25:70 respectively for Q1:Q2:Q3.

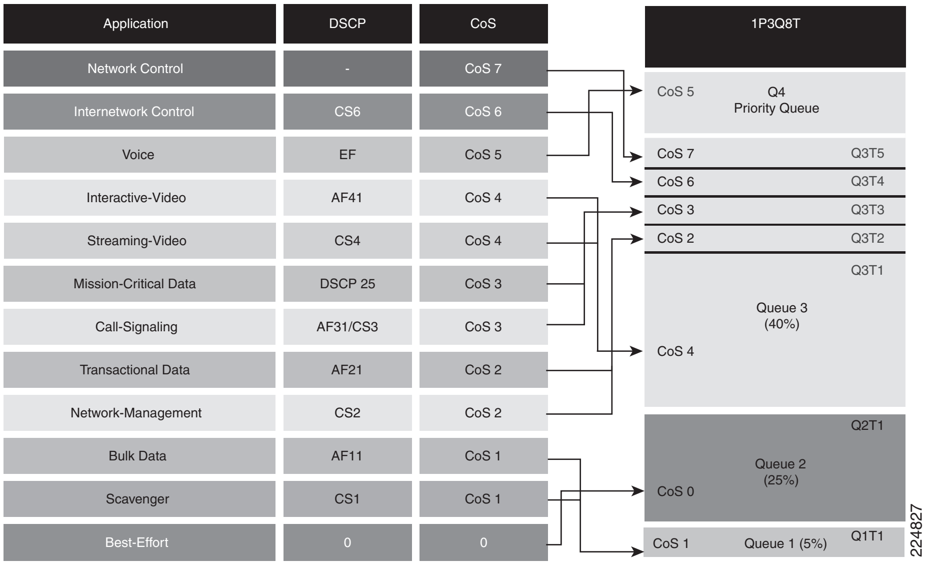
The tunable WRED threshold for Q1 can be set to 80:100 to provide congestion avoidance to Scavenger/Bulk Data traffic. The WRED threshold for Q2 similarly can be set to 80:100 to provide congestion avoidance on all Best-Effort flows.

The 1P3Q8T queuing structure's support for up to eight WRED thresholds per queue allows for additional QoS granularity for the applications sharing Q3. Because only five discrete CoS values are sharing this queue, only five of eight thresholds need to be defined for subqueue QoS. For example, Q3T1 could be set to 50:60, Q3T2 could be set to 60:70, Q3T3 could be set to 70:80, Q3T4 could be set to 80:90, and Q3T5 could be set to 90:100.

Therefore, once the queues and thresholds have been defined as above, CoS 1 (Scavenger/Bulk) can be assigned to Q1T1; CoS 0 (Best Effort) to Q2T1; CoS 4 (Interactive and Streaming Video) can be assigned to Q3T1; CoS 2 (Network Management and Transactional Data) could be assigned to Q3T2; CoS 3 (call signaling and Mission-Critical Data) could be assigned to Q3T3; CoS 6 (Internetwork Control) could be assigned to Q3T4; CoS 7 (Internetwork and Network Control) can be assigned to Q3T5; CoS 5 (VoIP) can be assigned to Q4 (the PQ).

These 1P3Q8T queuing recommendations are illustrated in Figure 2-30.

Figure 2-30 Catalyst 6500 1P3Q8T Queuing Model



Application	DSCP	CoS
Network Control	-	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive-Video	AF41	CoS 4
Streaming-Video	CS4	CoS 4
Mission-Critical Data	DSCP 25	CoS 3
Call-Signaling	AF31/CS3	CoS 3
Transactional Data	AF21	CoS 2
Network-Management	CS2	CoS 2
Bulk Data	AF11	CoS 1
Scavenger	CS1	CoS 1
Best-Effort	0	0

The Catalyst 6500 (PFC3) CatOS configurations to configure 1P3Q8T queuing recommendations are shown below.

Example 2-75 Catalyst 6500 (PFC3) CatOS—1P3Q8T Queuing Example

```
CAT6500-PFC3-CATOS> (enable) set qos txq-ratio 1p3q8t 5 25 40 30
! Allocates 5% for Q1, 25% for Q2, 40% for Q3 and 30% for Q4 (PQ)
CAT6500-PFC3-CATOS> (enable) set qos wrr 1p3q8t 5 25 70
! Sets the WRR weights for 5:25:70 (Q1:Q2:Q3) bandwidth servicing
CAT6500-PFC3-CATOS> (enable)
```

```
CAT6500-PFC3-CATOS> (enable) set qos wred 1p3q8t tx queue 1 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q1 WRED T1 to 80:100 and all other Q1 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p3q8t tx queue 2 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q2 WRED T1 to 80:100 and all other Q2 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p3q8t tx queue 3 50:60 60:70 70:80
80:90 90:100 100:100 100:100 100:100
! Sets Q3 WRED T1 to 50:60, Q3T2 to 60:70, Q3T3 to 70:80,
! Q3T4 to 80:90, Q3T5 to 90:100
! All other Q3 WRED Thresholds are set to 100:100
CAT6500-PFC3-CATOS> (enable)
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 1 1 cos 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 2 1 cos 0
! Assigns Best Effort to Q2 WRED Threshold 1
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 3 1 cos 4
    ! Assigns Video to Q3 WRED Threshold 1
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 3 2 cos 2
    ! Assigns Net-Mgmt and Transactional Data to Q3 WRED T2
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 3 3 cos 3
! Assigns call signaling and Mission-Critical Data to Q3 WRED T3
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 3 4 cos 6
! Assigns Internetwork-Control (IP Routing) to Q3 WRED T4
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 3 5 cos 7
! Assigns Network-Control (Spanning Tree) to Q3 WRED T5
CAT6500-PFC3-CATOS> (enable) set qos map 1p3q8t tx 4 cos 5
    ! Assigns VoIP to the PQ (Q4)
CAT6500-PFC3-CATOS> (enable)
```

Catalyst 6500 (PFC3) CatOS QoS Verification Commands:

- show qos info config 1p3q8t tx
- show qos info runtime
- show qos statistics

The Catalyst 6500 (PFC3) IOS configurations to configure 1P3Q8T queuing recommendations are shown below.

Example 2-76 Catalyst 6500 IOS—1P3Q8T Queuing Example

```
CAT6500-PFC3-IOS(config)# interface range GigabitEthernet1/1 - 48
CAT6500-PFC3-IOS(config-if)# wrr-queue queue-limit 5 25 40
! Allocates 5% for Q1, 25% for Q2 and 40% for Q3
CAT6500-PFC3-IOS(config-if)# wrr-queue bandwidth 5 25 70
! Sets the WRR weights for 5:25:70 (Q1:Q2:Q3) bandwidth servicing
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 1
    ! Enables WRED on Q1
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 2
! Enables WRED on Q2
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 3
! Enables WRED on Q3
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 1 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q1T1 to 80% and all others to 100%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 1 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q1T1 to 100% and all others to 100%
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 2 80
```

```
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q2T1 to 80% and all others to 100%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 2 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q2T1 to 100% and all others to 100%
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect min-threshold 3 50
60 70 80 90 100 100 100
! Sets Min WRED Threshold for Q3T1 to 50%, Q3T2 to 60%, Q3T3 to 70%
! Q3T4 to 80%, Q3T5 to 90% and all others to 100%
CAT6500-PFC3-IOS(config-if)# wrr-queue random-detect max-threshold 3 60
70 80 90 100 100 100 100
! Sets Max WRED Threshold for Q3T1 to 60%, Q3T2 to 70%, Q3T3 to 80%
! Q3T4 to 90%, Q3T5 to 100% and all others to 100%
CAT6500-PFC3-IOS(config-if)#
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 1 1 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 2 1 0
! Assigns Best Effort to Q2 WRED Threshold 1
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 3 1 4
    ! Assigns Video to Q3 WRED Threshold 1
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 3 2 2
    ! Assigns Net-Mgmt and Transactional Data to Q3 WRED T2
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 3 3 3
! Assigns call signaling and Mission-Critical Data to Q3 WRED T3
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 3 4 6
! Assigns Internetwork-Control (IP Routing) to Q3 WRED T4
CAT6500-PFC3-IOS(config-if)# wrr-queue cos-map 3 5 7
! Assigns Network-Control (Spanning Tree) to Q3 WRED T5
CAT6500-PFC3-IOS(config-if)# priority-queue cos-map 1 5
    ! Assigns VoIP to the PQ (Q4)
CAT6500-PFC3-IOS(config-if)#end
CAT6500-PFC3-IOS#
```

Catalyst 6500 MLS QoS Verification Commands:

- show queueing interface

Catalyst 6500—1P7Q8T Queuing and Dropping

This section includes the following topics:

- Recommendations
- Configuration
- Catalyst MLS QoS Verification Commands

Recommendations

The 1P7Q8T queuing structure adds four additional standard queues to the 1P3Q8T structure and moves the PQ from Q4 to Q8, but otherwise is identical.

Under a 1P7Q8T model, buffer space can be allocated as follows: 5% for the Scavenger/Bulk queue (Q1), 25% for the Best Effort queue (Q2), 10% for the Video queue (Q3), 10% for the Network-Management/Transactional Data queue (Q4), 10% for the Call-Signaling/Mission-Critical Data queue (Q5), 5% for the Internetwork-Control queue (Q6), 5% for the Network Control queue (Q7), and 30% for the PQ (Q8).

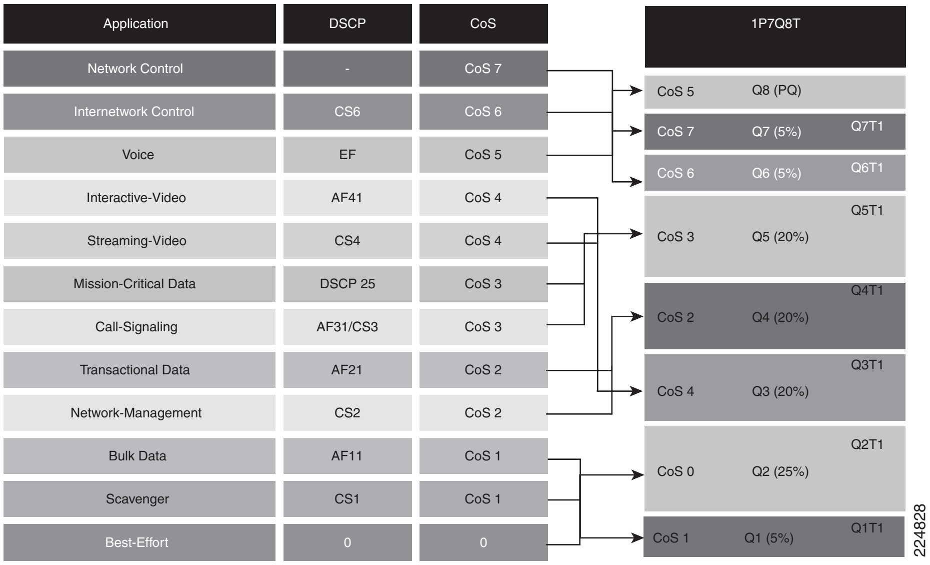
The WRR weights for the standard queues (Q1 through Q7) for dividing the remaining bandwidth after the priority queue has been fully serviced, can be set to 5:25:20:20:20:5:5 respectively for Q1 through Q7.

Since eight queues are available, each CoS value can be assigned to its own exclusive queue. WRED can be enabled on each queue to provide it with congestion avoidance by setting the first WRED threshold of each queue to 80:100. All other WRED thresholds can remain at 100:100.

Therefore, once the queues and thresholds have been defined as above, then CoS 1 (Scavenger/Bulk) can be assigned to Q1T1; CoS 0 (Best Effort) to Q2T1; CoS 4 (Interactive and Streaming Video) can be assigned to Q3T1; CoS 2 (Network Management and Transactional Data) could be assigned to Q4T1; CoS 3 (call signaling and Mission-Critical Data) could be assigned to Q5T1; CoS 6 (Internetwork Control) could be assigned to Q6T1; CoS 7 (Internetwork and Network Control) can be assigned to Q7T1; CoS 5 (VoIP) can be assigned to Q8 (the PQ).

These 1P7Q8T queuing recommendations are illustrated in Figure 2-31.

Figure 2-31 Catalyst 6500 1P7Q8T Queuing Model



Application	DSCP	CoS
Network Control	-	CoS 7
Internetwork Control	CS6	CoS 6
Voice	EF	CoS 5
Interactive-Video	AF41	CoS 4
Streaming-Video	CS4	CoS 4
Mission-Critical Data	DSCP 25	CoS 3
Call-Signaling	AF31/CS3	CoS 3
Transactional Data	AF21	CoS 2
Network-Management	CS2	CoS 2
Bulk Data	AF11	CoS 1
Scavenger	CS1	CoS 1
Best-Effort	0	0

Configuration

The Catalyst 6500 (PFC3) CatOS configurations to configure 1P7Q8T queuing recommendations are shown below.

Example 2-77 Catalyst 6500 (PFC3) CatOS—1P7Q8T Queuing Example

```
CAT6500-PFC3-CATOS> (enable) set qos txq-ratio 1p7q8t 5 25 10 10 10 5 5 30
    ! Allocates 5% to Q1, 25% to Q2, 10% to Q3, 10% to Q4,
    ! Allocates 10% to Q5, 5% to Q6, 5% to Q7 and 30% to the PQ (Q8)
CAT6500-PFC3-CATOS> (enable) set qos wrr 1p7q8t 5 25 20 20 20 5 5
! Sets the WRR weights for 5:25:20:20:20:5:5 (Q1 through Q7)
CAT6500-PFC3-CATOS> (enable)
CAT6500-PFC3-CATOS> (enable)
CAT6500-PFC3-CATOS> (enable) set qos wred 1p7q8t tx queue 1 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q1 WRED T1 to 80:100 and all other Q1 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p7q8t tx queue 2 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q2 WRED T1 to 80:100 and all other Q2 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p7q8t tx queue 3 80:100 100:100
```

```
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q3 WRED T1 to 80:100 and all other Q3 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p7q8t tx queue 4 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q4 WRED T1 to 80:100 and all other Q4 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p7q8t tx queue 5 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q5 WRED T1 to 80:100 and all other Q5 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p7q8t tx queue 6 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q6 WRED T1 to 80:100 and all other Q6 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable) set qos wred 1p7q8t tx queue 7 80:100 100:100
100:100 100:100 100:100 100:100 100:100 100:100
! Sets Q7 WRED T1 to 80:100 and all other Q7 WRED Thresholds to 100:100
CAT6500-PFC3-CATOS> (enable)
CAT6500-PFC3-CATOS> (enable)
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 1 1 cos 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 2 1 cos 0
! Assigns Best Effort to Q2 WRED Threshold 1
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 3 1 cos 4
    ! Assigns Video to Q3 WRED Threshold 1
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 4 1 cos 2
    ! Assigns Net-Mgmt and Transactional Data to Q4 WRED T1
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 5 1 cos 3
! Assigns call signaling and Mission-Critical Data to Q5 WRED T1
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 6 1 cos 6
! Assigns Internetwork-Control (IP Routing) to Q6 WRED T1
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 7 1 cos 7
! Assigns Network-Control (Spanning Tree) to Q7 WRED T1
CAT6500-PFC3-CATOS> (enable) set qos map 1p7q8t tx 8 cos 5
    ! Assigns VoIP to the PQ (Q4)
CAT6500-PFC3-CATOS> (enable)
```

Catalyst 6500 (PFC3) CatOS QoS Verification Commands:

- show qos info config 1p7q8t tx
- show qos info runtime
- show qos statistics

The Catalyst 6500 (PFC3) IOS configurations to configure 1P7Q8T queuing recommendations are shown below.

Example 2-78 Catalyst 6500 (PFC3) IOS—1P7Q8T Queuing Example

```
CAT6500-PFC3-IOS(config)#interface range TenGigabitEthernet4/1 - 4
CAT6500-PFC3(config-if-range)# wrr-queue queue-limit 5 25 10 10 10 5 5
    ! Allocates 5% to Q1, 25% to Q2, 10% to Q3, 10% to Q4,
    ! Allocates 10% to Q5, 5% to Q6 and 5% to Q7
CAT6500-PFC3(config-if-range)# wrr-queue bandwidth 5 25 20 20 20 5 5
! Sets the WRR weights for 5:25:20:20:20:5:5 (Q1 through Q7)
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 1
    ! Enables WRED on Q1
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 2
! Enables WRED on Q2
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 3
! Enables WRED on Q3
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 4
    ! Enables WRED on Q4
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 5
```

```
! Enables WRED on Q5
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 6
! Enables WRED on Q6
CAT6500-PFC3(config-if-range)# wrr-queue random-detect 7
! Enables WRED on Q7
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)# wrr-queue random-detect min-threshold 1 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q1T1 to 80% and all others to 100%
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect max-threshold 1 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q1T1 to 100% and all others to 100%
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect min-threshold 2 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q2T1 to 80% and all others to 100%
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect max-threshold 2 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q2T1 to 100% and all others to 100%
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect min-threshold 3 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q3T1 to 80% and all others to 100%
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect max-threshold 3 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q3T1 to 100% and all others to 100%
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect min-threshold 4 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q4T1 to 80% and all others to 100%
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect max-threshold 4 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q4T1 to 100% and all others to 100%
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect min-threshold 5 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q5T1 to 80% and all others to 100%
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect max-threshold 5 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q5T1 to 100% and all others to 100%
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect min-threshold 6 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q6T1 to 80% and all others to 100%
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect max-threshold 6 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q6T1 to 100% and all others to 100%
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect min-threshold 7 80
100 100 100 100 100 100 100
! Sets Min WRED Threshold for Q7T1 to 80% and all others to 100%
CAT6500-PFC3(config-if-range)#  wrr-queue random-detect max-threshold 7 100
100 100 100 100 100 100 100
! Sets Max WRED Threshold for Q7T1 to 100% and all others to 100%
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)#
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 1 1 1
! Assigns Scavenger/Bulk to Q1 WRED Threshold 1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 2 1 0
! Assigns Best Effort to Q2 WRED Threshold 1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 3 1 4
    ! Assigns Video to Q3 WRED Threshold 1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 4 1 2
```

```
    ! Assigns Net-Mgmt and Transactional Data to Q4 WRED T1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 5 1 3
! Assigns call signaling and Mission-Critical Data to Q5 WRED T1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 6 1 6
! Assigns Internetwork-Control (IP Routing) to Q6 WRED T1
CAT6500-PFC3(config-if-range)# wrr-queue cos-map 7 1 7
! Assigns Network-Control (Spanning Tree) to Q7 WRED T1
CAT6500-PFC3(config-if-range)# priority-queue cos-map 1 5
! Assigns VoIP to the PQ (Q4)
CAT6500-PFC3(config-if-range)#end
CAT6500-PFC3-IOS#
```

Catalyst 6500 MLS QoS Verification Commands:

- show queueing interface

Catalyst 6500—PFC3 Distribution-Layer (IOS) Per-User Microflow Policing

In general, superior defense strategies have multiple lines of defense. In the context of the campus designs that have been considered, there is a main line of defense against DoS/worm attack traffic at the access layer edges. This line of defense can be bolstered at the distribution layer whenever Catalyst 6500 Sup720s (PFC3s) are deployed there. This can be done by leveraging the PFC3 feature of Per-User Microflow Policing.

In the example below, traffic has been assumed to be correctly classified. This may or may not be a valid assumption. If it is suspected to be invalid, then ACLs should be used to identify the flows (instead of DSCP markings). In either case, various flow-types can be filtered as they arrive at the distribution layer to see if they conform to the normal limits that have been set for the enterprise. Each flow is examined by source IP Address and if a source is transmitting out-of-profile, the excess traffic can be dropped or marked-down. In this manner, spurious flows can be contained even in the case that access layer switches do not support granular policing (such as the Catalyst 2950, as discussed earlier in this chapter) or in the case that policing has been mis-configured on an access layer switch.

In this manner, the distribution layer Catalyst 6500 PFC3 can catch any DoS/worm attack flows that may have slipped through the access layer net.

Example 2-79 Catalyst 6500 (PFC3) IOS—Distribution-Layer Per-User Microflow Policing

```
CAT6500-PFC3-IOS(config)#mls qos map policed-dscp normal 0 24 26 34 36 to 8
! Excess traffic marked 0,CS3,AF31,AF41 or AF42 will be remarked to CS1
CAT6500-PFC3-IOS(config)#
CAT6500-PFC3-IOS(config)#class-map match-all VOIP
CAT6500-PFC3-IOS(config-cmap)#  match ip dscp ef
CAT6500-PFC3-IOS(config-cmap)#class-map match-all INTERACTIVE-VIDEO
CAT6500-PFC3-IOS(config-cmap)#  match ip dscp af41 af42
CAT6500-PFC3-IOS(config-cmap)#class-map match-all CALL-SIGNALING
CAT6500-PFC3-IOS(config-cmap)#  match ip dscp cs3 af31
CAT6500-PFC3-IOS(config-cmap)#class-map match-all BEST-EFFORT
CAT6500-PFC3-IOS(config-cmap)#  match ip dscp 0
CAT6500-PFC3-IOS(config-cmap)#
CAT6500-PFC3-IOS(config-cmap)#policy-map PER-USER-POLICING
CAT6500-PFC3-IOS(config-pmap)#  class VOIP
CAT6500-PFC3-I(config-pmap-c)# police flow mask src-only 128000 8000
conform-action transmit exceed-action drop
! No source can send more than 128k worth of DSCP EF traffic
CAT6500-PFC3-I(config-pmap-c)#  class INTERACTIVE-VIDEO
CAT6500-PFC3-I(config-pmap-c)# police flow mask src-only 500000 8000
conform-action transmit exceed-action policed-dscp-transmit
! Excess IP/VC traffic from any source is marked down to CS1
```

```
CAT6500-PFC3-I(config-pmap-c)#  class CALL-SIGNALING
CAT6500-PFC3-I(config-pmap-c)# police flow mask src-only 32000 8000
conform-action transmit exceed-action policed-dscp-transmit
  ! Excess call signaling traffic from any source is marked down to CS1
CAT6500-PFC3-I(config-pmap-c)#  class BEST-EFFORT
CAT6500-PFC3-I(config-pmap-c)# police flow mask src-only 5000000 8000
conform-action transmit exceed-action policed-dscp-transmit
! Excess PC Data traffic from any source is marked down to CS1
CAT6500-PFC3-I(config-pmap-c)#  exit
CAT6500-PFC3-IOS(config-pmap)#exit
CAT6500-PFC3-IOS(config)#
CAT6500-PFC3-IOS(config)#interface range GigabitEthernet4/1 - 4
CAT6500-PFC3(config-if-range)# mls qos trust dscp
CAT6500-PFC3(config-if-range)# service-policy input PER-USER-POLICING
    ! Attaches Per-User Microflow policing policy to Uplinks from Access
CAT6500-PFC3(config-if-range)#end
CAT6500-PFC3-IOS#
```

Catalyst 6500 MLS QoS Verification Commands:

- show mls qos
- show class-map
- show policy-map
- show policy interface

WAN Aggregator/Branch Router Handoff Considerations

A final consideration in campus QoS design is the Campus-to-WAN (or VPN) handoff; in the case of a branch, this equates to the Branch Switch to Branch router handoff.

In either case, a major speed mismatch is impending, as GigabitEthernet/FastEthernet campus networks are connecting to WAN links that may only be a few Megabits (if that).

Granted, the WAN Aggregation Routers and the Remote-Branch Routers have advanced QoS mechanisms to prioritize traffic on their links, but it is critical to keep in mind that Cisco router QoS is performed in IOS *software*, while Catalyst switch QoS is performed in ASIC *hardware*.

Therefore, the optimal distribution of QoS operations would be to have as much QoS actions performed on the Catalyst switches as possible, saving the WAN/Branch router valuable CPU cycles. This is an especially critical consideration when deploying DoS/Worm mitigation designs.

For example, some enterprises have deployed advanced QoS policies on their Branch Switches and Routers, only to have DoS/Worm attacks originate from *within* the Branch. Remember, queuing will not engage on a switch unless its links are congested, and even if it does, should the Branch switch hands off 100 Mbps of (correctly queued) traffic to a Branch router, it will more than likely bring it down.

Thus, the following design principles for the Campus-to-WAN handoff can help mitigate these types of scenarios:

First, resist the urge to automatically use a GigabitEthernet connection to the WAN Aggregation router, even if the router supports GE.

It is extremely unlikely that the WAN Aggregator (WAG) is serving anywhere close to a (combined) WAN-circuit-rate of 1 Gbps. Therefore, use one (or more) FastEthernet connections on the distribution layer Catalyst switch to connect to the WAG, so that the aggregate traffic sent to the WAG is not only *limited* (in 100 Mbps increments), but also (since congestion points are now pulled back into the Catalyst switch, thus forcing queuing to engage on the FE switch port) the traffic will be *correctly queued* within these (100 Mbps-increment) limits.

For example, a WAN Aggregation router may support two DS3 WAN connections (totaling 90 Mbps of WAN circuit-capacity). In this case, the Distribution Layer switch port connecting to the WAG should be FastEthernet. Then, if more than 100 Mbps of traffic attempts to traverse the WAN, the Catalyst switch engages queuing on the switch port and aggressively drops flows according to the defined application hierarchies. Only 100 Mbps of correctly-queued traffic is ever handed off to the WAG.

In the case of a WAG supporting over 100 Mbps of WAN circuits, like the case of a WAG running one or more OC-3 ports (at 155 Mbps each), then multiple FastEthernet connections can be used to connect to the WAG from the Distribution Layer switch to achieve the same net effect.

The point is to bring back, as much as possible, the choke point into Catalyst hardware and engage hardware queuing there, rather than overwhelming the software-based policing and/or queueing policies within the WAG.

Second, if the combined WAN circuit-rate is significantly below 100 Mbps, enable egress shaping on the Catalyst switches (when supported).

If there is no hope of engaging queuing on the Catalyst switch because the combined WAN circuit-rates are far below FastEthernet (the minimum port speed of Catalyst switches), then enable shaping on platforms that support this feature. Such platforms include the Catalyst 2970, 3560, 3750, and 4500.

In this manner, the Catalyst switch can hold back traffic and selectively drop (according to defined policies) from flows that would otherwise flood the WAN/Branch router.

For example, if a Branch router is using two ATM-IMA T1 links (3 Mbps combined throughput) to connect the Branch to the WAN, then the Branch switch could be configured to shape all WAN-destined traffic to 3 Mbps or could be configured to shape on a per-application basis to smaller increments.

Refer to the queuing/dropping sections of these platforms in this chapter and Cisco IOS documentation for additional guidance on enabling shaping.

Finally, if the combined WAN circuit-rate is significantly below 100 Mbps and the Catalyst switch does not support shaping, enable egress policing (when supported).

If the Catalyst switch does not support shaping, then egress policing is the next-best alternative for this scenario.

For example, the Catalyst 3550 does not support shaping, but it does support up to 8 policers on all egress ports. Thus it could still protect its Branch Router from being overwhelmed by policing on egress. Egress policing may be done on an aggregate level or on a per-application-basis.

Again, the objective is to discard, as intelligently as possible, traffic that will inevitably be dropped anyway (by the WAN/Branch router) but, whenever possible, perform the dropping within Catalyst hardware (as opposed to IOS software).

Egress policers are configured in the same manner as ingress policers, but the direction specified in the ***service-policy*** interface-configuration statement will be ***out***, not ***in***.

Note The only Catalyst switch discussed in this chapter that did not support either shaping or egress policing is the Catalyst 2950. Unfortunately there is no way that the Catalyst 2950 can offload QoS from the Branch router. If such functionality is required, then a hardware upgrade would be advisable.

Note For a case study example of Campus QoS design, refer to Figure 12-32 and Examples 12-76 through 12-81 of the Cisco Press book, *End-to-End QoS Network Design* by Tim Szigeti and Christina Hattingh.

Summary

This chapter began with establishing the case for Campus QoS by way of three main QoS design principles:

- The first is that applications should be classified and marked as close to their sources as technically and administratively feasible.
- The second is that unwanted traffic flows should be policed as close to their sources as possible.
- The third is that QoS should always be performed in hardware, rather than software, whenever a choice exists.

Furthermore, it was emphasized that the only way to provide service *guarantees* is to enable queuing at any node that has the potential for congestion, including campus uplinks and downlinks.

A proactive approach to mitigating DoS/worm flooding attacks within campus environments was overviewed. This approach focused on access edge policers that could meter traffic rates received from endpoint devices and when these exceed specified watermarks (at which point they are no longer considered normal flows), these policers could markdown excess traffic to the Scavenger class. These policers would be coupled with queuing policies throughout the enterprise that provisioned for a less-than Best-Effort Scavenger class on all links. In this manner, legitimate traffic bursts would not be affected, but DoS/worm generated traffic would be significantly mitigated.

Common endpoints were overviewed and classified into three main groups: 1) Trusted Endpoints, 2) Untrusted Endpoints, and 3) Conditionally-Trusted Endpoints. Untrusted Endpoints were subdivided into two smaller models: Untrusted PCs and Untrusted Servers; similarly, Conditionally-Trusted Endpoints were subdived into two models: Basic and Advanced.

Following these access edge Model definitions, platform-specific recommendations were given to on how to implement these access edge models on Cisco Catalyst 2950, 2970, 3550, 3560, 3750, 4500, and 6500 series switches. Platform-specific limitations, caveats, or nerd-knobs were highlighted to tailor each model to each platforms unique feature sets. All configurations were presented in config-mode to continually highlight what platform was being discussed. Furthermore, many relevant verification commands were discussed in detail (in context) to illustrate how and when these could be used effectively when deploying QoS within the campus.

Recommendations were also given on how to configure queuing on a per-platform/per-linecard basis. These recommendations included configuring 1P3Q1T queuing on the Catalyst 2950, 1P3Q2T queuing on the Catalyst 3550, configuring 1P3Q3T queuing on the Catalyst 2970/3560/3750, and configuring 1P3Q1T queuing (with DBL) on the Catalyst 4500. For the Catalyst 6500, linecard-specific queuing structures were examined in detail, including CatOS and IOS configurations for configuring 2Q2T, 1P2Q1T, 1P2Q2T, 1P3Q1T, 1P3Q8T, and 1P7Q8T queuing.

Following this, the Catalyst 6500 PFC3's Per-User Microflow Policing feature was discussed in the context of how it could be leveraged to provide a second line of policing defense at the distribution layer.

Finally, Campus-to-WAN/VPN handoff considerations were examined. It was recommended:

- First, resist the urge to automatically use a GigabitEthernet connection to the WAN Aggregation router, even if the router supports GE.
- Second, if the combined WAN circuit-rate is significantly below 100 Mbps, enable egress shaping on the Catalyst switches (when supported).
- Third, if the combined WAN circuit-rate is significantly below 100 Mbps and the Catalyst switch does not support shaping, enable egress policing (when supported).

References

Standards

- RFC 2474 "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers

  http://www.ietf.org/rfc/rfc2474
- RFC 2597 "Assured Forwarding PHB Group"

  http://www.ietf.org/rfc/rfc2597
- RFC 2697 "A Single Rate Three Color Marker"

  http://www.ietf.org/rfc/rfc2697
- RFC 2698 "A Two Rate Three Color Marker"

  http://www.ietf.org/rfc/rfc2698
- RFC 3168 "The Addition of Explicit Congestion Notification (ECN) to IP"

  http://www.ietf.org/rfc/rfc3168
- RFC 3246 "An Expedited Forwarding PHB (Per-Hop Behavior)"

  http://www.ietf.org/rfc/rfc3246

Books

- Flannagan, Michael and Richard Froom and Kevin Turek. *Cisco Catalyst QoS: Quality of Service in Campus Networks*. Indianapolis: Cisco Press, 2003.
- Szigeti, Tim and Christina Hattingh. *End-to-End QoS Network Design: Quality of Service in LANs, WANs and VPNs*. Indianapolis: Cisco Press, 2004.

Cisco Catalyst Documentation

- Configuring QoS on the Catalyst 2950 (Cisco IOS Software Release 12.1(19)EA1)

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2950/12119ea1/2950scg/swqos.htm
- Configuring QoS on the Catalyst 3550 (Cisco IOS Software Release 12.1(19)EA1)

  http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/12119ea1/3550scg/swqos.htm
- Configuring QoS on the Catalyst 2970 (Cisco IOS Software Release 12.2(18)SE)

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2970/12218se/2970scg/swqos.htm
- Configuring QoS on the Catalyst 2970 (Cisco IOS Software Release 12.2(18)SE)

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12218se/3750scg/swqos.htm
- Configuring QoS on the Catalyst 4500 (Cisco IOS Software Release 12.2(18)EW)

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_18/config/qos.htm
- Configuring QoS on the Catalyst 6500 (Cisco CatOS Software Release 8.2)

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/qos.htm

- Configuring Automatic QoS on the Catalyst 6500 (Cisco CatOS Software Release 8.2)
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_2/confg_gd/autoqos.htm
- Configuring QoS on the Catalyst 6500 (Cisco IOS Software Release 12.2(17)SX)
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/qos.htm