You make **possible**

Campus QoS Design - Simplified

Roland Saville – Technical Leader Engineering

BRKCRS-2501

Barcelona | January 27-31, 2020

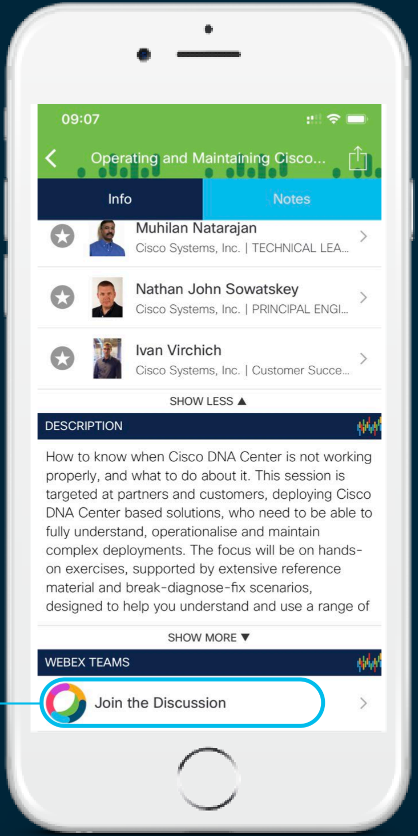
Cisco Webex Teams

Questions?

Use Cisco Webex Teams to chat with the speaker after the session

How

1. Find this session in the Cisco Events Mobile App
2. Click "Join the Discussion"
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

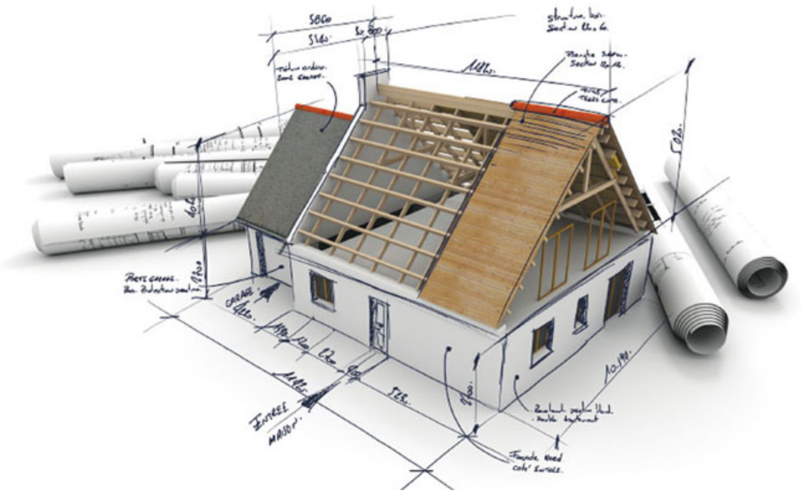


Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Campus QoS Design Considerations and Best Practices

What Do You Consider First?



Where to Begin?

- Always, Always, Always Start with Defining Your Business Goals of QoS
- *Guaranteeing voice quality* meets enterprise standards
- Ensuring a *high Quality of Experience* (QoE) for *video* applications
- *Improving user productivity* by minimizing network response times
- *Managing* business applications that are "*bandwidth hogs*"
- Identifying and *de-prioritizing non-business applications*
- Improving network availability by *protecting the control planes*
- *Hardening the network* infrastructure to deal with abnormal events

Determining Business Relevance

How Important is an Application to Your Business?

Relevant

- These applications directly support business objectives
- Applications should be classified, marked and treated marked according to industry best-practice recommendations

RFC 4594

Default

- These applications may/may not support business objectives (e.g. HTTP/HTTPS/SSL)
- Applications of this type should be treated with a Default Forwarding service

RFC 2474

Irrelevant

- These applications do not support business objectives and are typically consumer-oriented
- Applications of this type should be treated with a “less-than Best Effort” service

RFC 3662

Translating Business-Relevance to QoS Policies

Apply RFC 4594-based Marking / Queuing / Dropping

Application Class	Per-Hop Behavior	Queuing & Dropping	Application Examples

Relevant

Default

Irrelevant

Translating Business-Relevance to QoS Policies

Apply RFC 4594-based Marking / Queuing / Dropping

	Application Class	Per-Hop Behavior	Queuing & Dropping	Application Examples
Relevant	VoIP Telephony	EF	Priority Queue (PQ)	Cisco IP Phones (G.711, G.729)
	Broadcast Video	CS5	(Optional) PQ	Cisco IP Video Surveillance / Cisco Enterprise TV
	Real-Time Interactive	CS4	(Optional) PQ	Cisco TelePresence
	Multimedia Conferencing	AF4	BW Queue + DSCP WRED	Cisco Jabber, Cisco WebEx
	Multimedia Streaming	AF3	BW Queue + DSCP WRED	Cisco Digital Media System (VoDs)
	Network Control	CS6	BW Queue	EIGRP, OSPF, BGP, HSRP, IKE
	Signaling	CS3	BW Queue	SCCP, SIP, H.323
	Ops / Admin / Mgmt (OAM)	CS2	BW Queue	SNMP, SSH, Syslog
	Transactional Data	AF2	BW Queue + DSCP WRED	ERP Apps, CRM Apps, Database Apps
	Bulk Data	AF1	BW Queue + DSCP WRED	E-mail, FTP, Backup Apps, Content Distribution
Default	Default Forwarding	DF	Default Queue + RED	Default Class
Irrelevant	Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

Start by Defining Your QoS Strategy

Articulate Your Business Intent, Relevant Applications and End-to-End Strategy

CISCO Strategic QoS Design

At-A-Glance

The Quality of Service Challenge
Today there is a virtual explosion of rich media applications on the IP network This explosion of content and media types, both managed and un-managed, requires network architects to take a new look at their Quality of Service (QoS) designs.

Step 1: Articulate Business Intent and Application Relevance
The first step may seem obvious and superfluous, but in actuality it is crucial: clearly define the business objectives that your QoS policies are to enable. These may include any/all of the following:
- Guaranteeing voice quality meets enterprise standards
- Ensuring a high Quality of Experience (QoE) for video
- Increasing user productivity by increasing network response times for interactive applications
- Managing applications that are "bandwidth hogs"
- Identifying and de-prioritizing consumer applications
- Improving network availability
- Hardening the network infrastructure

With these goals in mind, network architects can clearly identify which applications are relevant to their business. Conversely, this exercise will also make it apparent which applications are *not* relevant towards achieving business objectives. Such applications may include consumer-oriented and/or entertainment-oriented applications.

Finally, there may be applications/protocols that can fall into either category of business relevance. For example, HTTP/HTTPS may carry business-relevant traffic or consumer-oriented traffic, and as such cannot be clearly classified in either category. Note: in such cases, deep packet inspection technologies may be able to discretely identify the applications being transported, allowing these to be properly classified in line with business objectives.

Figure 1 Determining Application Business Relevance

Step 2: Define an End-to-End QoS Design Strategy
Once applications have been defined as business-relevant (or otherwise), then the network architect must decide how to mark and treat these applications over the IP infrastructure.

To this end, Cisco advocates following relevant industry standards and guidelines, as this extends the effectiveness of your QoS policies beyond your direct administrative control. That being said, it may be helpful to overview a relevant RFC for QoS marking and provisioning: RFC 4594, "Configuration Guidelines for DiffServ Service Classes."

These guidelines are to be viewed as industry best-practice recommendations. As such, enterprises and service providers are encouraged to adopt these marking and provisioning recommendations with the aim of improving QoS consistency, compatibility, and interoperability. However, it should be noted that these guidelines are not standards; as such, modifications can be made to these recommendations as specific needs or constraints require.

Thus, to meet specific business requirements, Cisco has made a minor modification to its adoption of RFC 4594: specifically the swapping of Call-Signaling and Broadcast Video markings (to CS3 and CS5, respectively). A summary of Cisco's implementation of RFC 4594 is presented in Figure 2.

Figure 2 Cisco (RFC 4594-Based) QoS Recommendations

Application Class	Per-Hop Behavior	Queuing and Dropping
Voice	EF	Priority Queue (PQ)
Broadcast Video	CS5	(Optional) PQ
Real-Time Interactive	CS4	(Optional) PQ
Multimedia Conferencing	AF4	BW Queue + DSCP WRED
Multimedia Streaming	AF3	BW Queue + DSCP WRED
Network Control	CS6	BW Queue
Call-Signaling	CS3	BW Queue
Ops/Admin/Mgmt (OAM)	CS2	BW Queue
Transactional Data	AF2	BW Queue + DSCP WRED
Bulk Data	AF1	BW Queue + DSCP WRED
Best Effort	DF	Default Queue + RED
Scavenger	CS1	Min BW Queue

RFC 4594 also provides some application classification rules to help network architects to assign applications to the optimal traffic classes; these are summarized in the following sections:

Business relevant application can be grouped into one of four main categories:
- control plane protocols
- voice applications
- video applications
- data applications

Beginning with the control plane protocols, these may be sub-divided further, as shown in Figure 3.

Figure 3 Control Plane Traffic Classes

- **Network Control**—This traffic class is intended for network control plane traffic, which is required for reliable operation of the enterprise network. Traffic in this class should be marked CS6 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, as network control traffic should not be dropped. Example traffic includes EIGRP, OSPF, BGP, HSRP, IKE, etc.

- **Signaling**—This traffic class is intended for signaling traffic that supports IP voice and video telephony. Traffic in this class should be marked CS3 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, as signaling traffic should not be dropped. Example traffic includes SCCP, SIP, H. 323, etc.

- **Operations/Administration/Management (OAM)**—This traffic class is intended for network operations, administration, and management traffic. This class is critical to the ongoing maintenance and support of the network. Traffic in this class should be marked CS2 and provisioned with a (moderate, but dedicated) guaranteed bandwidth queue. WRED should not be enabled on this class, as OAM traffic should not be dropped. Example traffic includes SSH, SNMP, Syslog, etc.

Provisioning for voice is relatively straightforward:

- **Voice**—This traffic class is intended for voice/audio traffic (VoIP signaling traffic is assigned to the "Call-Signaling" class). Traffic assigned to this class should be marked EF. This class is provisioned with an Expedited Forwarding (EF) Per-Hop Behavior (PHB). The EF PHB-defined in RFC 3246-is a strict-priority queuing service and, as such, admission to this class should be controlled. Example traffic includes G.711 and G.729a, as well as the audio components of multimedia conferencing applications, like Cisco Jabber, WebEx and Spark.

Video—on the other hand—may have unique QoS requirements depending on the type, as illustrated in Figure 4.

Figure 4 Video Traffic Classes

Two key questions need to be answered to determine the optimal traffic classification for a video application :
- is the video unidirectional or bidirectional?
- is the video elastic or inelastic?

"Elastic" flows are able to adapt to network congestion and/or drops (by reducing frame rates, bit rates, compression rates, etc.); "inelastic" flows either do not have such capabilities or—in order to meet specific business configured not to utilize these.

With these two questions answered, video applications may be assigned to their respective traffic classes, including:

- **Broadcast Video**—This traffic class is intended for broadcast TV, live events, video surveillance flows, and similar "inelastic" streaming video flows Traffic in this class should be marked Class Selector 5 (CS5) and may be provisioned with an EF PHB; as such, admission to this class should be controlled. Example traffic includes live Cisco Enterprise TV (ETV) streams, and Cisco IP Video Surveillance.

- **Real-Time Interactive**—This traffic class is intended for inelastic interactive video applications. Whenever possible, signaling and data sub-components of this class should be separated out and assigned to their respective traffic classes. Traffic in this class should be marked CS4 and may be provisioned with an EF PHB; as such, admission to this class should be controlled. An example application is Cisco TelePresence.

- **Multimedia Conferencing**—This traffic class is intended for elastic interactive multimedia collaboration applications. Whenever possible, signaling and data sub-components of this class should be separated out and assigned to their respective traffic classes. Traffic in this class should be marked Assured Forwarding (AF) Class 4 (AF41) and should be provisioned with a guaranteed bandwidth queue with DSCP-based Weighted-Random Early Detect (DSCP-WRED) enabled. Traffic in this class may be subject to policing and re-marking. Example applications include Cisco Jabber, WebEx and Spark.

- **Multimedia Streaming**—This traffic class is intended for elastic streaming video applications, such as Video-on-Demand (VoD). Traffic in this class should be marked AF Class 3 (AF31) and should be provisioned with a guaranteed bandwidth queue with DSCP-based WRED enabled. Example applications include Cisco Digital Media System Video-on-Demand (VoD) streams, E-Learning videos, etc.

Figure 5 Data Traffic Classes

When it comes to data applications, there is really only one key question to answer (as illustrated in Figure 5):
- Is the data application "foreground" or "background"?

"Foreground" refers to applications from which users expect a response—via the network—in order to continue with their tasks; excessive latency to such applications will directly impact user productivity.

Conversely, "background" applications—while business relevant—do not directly impact user productivity and typically consist of machine-to-machine flows.

- **Transactional Data**—This traffic class is intended for interactive, "foreground" data applications Traffic in this class should be marked AF Class 2 (AF21) and should be provisioned with a dedicated bandwidth queue with DSCP-WRED enabled. This traffic class may be subject to policing and re-marking. Example applications include data components of multimedia collaboration applications, Enterprise Resource Planning (ERP) applications, Customer Relationship Management (CRM) applications, database applications, etc.

- **Bulk Data**—This traffic class is intended for non-interactive "background" data applications Traffic in this class should be marked AF Class 1 (AF11) and should be provisioned with a dedicated bandwidth queue with DSCP-WRED enabled. This traffic class may be subject to policing and re-marking. Example applications include: E-mail, backup operations, FTP/SFTP transfers, video and content distribution, etc.

With all business-relevant applications assigned to their respective traffic classes, then only two types of traffic classes are left to be provisioned:

- **Best Effort** (the Default Class)—This traffic class is the default class. The vast majority of applications will continue to default to this Best-Effort service class; as such, this default class should be adequately provisioned. Traffic in this class is marked Default Forwarding (DF or DSCP 0) and should be provisioned with a dedicated queue. WRED is recommended to be enabled on this class.

- **Scavenger**—This traffic class is intended for all applications that have been previously identified as business-irrelevant. These may include video applications that are consumer and/or entertainment-oriented. The approach of a "less-than Best-Effort" service class for non-business applications (as opposed to shutting these down entirely) has proven to be a popular, political compromise. These applications are permitted on business networks when bandwidth is available; however, as soon as the network experiences congestion, this class is the most aggressively dropped. Traffic in this class should be marked CS1 and should be provisioned with a minimal bandwidth queue that is the first to starve should network congestion occur. Example traffic includes Netflix, YouTube, Xbox Live/360 Movies, iTunes, BitTorrent, etc

For more details, see:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html
And the Cisco Press Book: **End-to-End QoS Network Design** (Second Edition)-Chapter 10

Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

The Case for Campus QoS

- The primary role of QoS in campus networks is to *manage packet loss*
  - It takes only a few milliseconds of congestion to cause drops
  - Rich media applications are extremely sensitive to packet drops
  - Queuing policies at every node can prevent packet loss for real-time apps
- The secondary role of QoS in campus networks is to condition traffic at the access edge, which can include any of the following:
  - Trust
  - Classify and Mark
  - Police

Why Is Video So Sensitive to Packet Loss?

1920 lines of Vertical Resolution (Widescreen Aspect Ratio is 16:9)

1080 lines of Horizontal Resolution

1080p60

1080 x 1920 lines =

2,073,600 pixels per frame

x 24 bits of color per pixel

x 60 frames per second

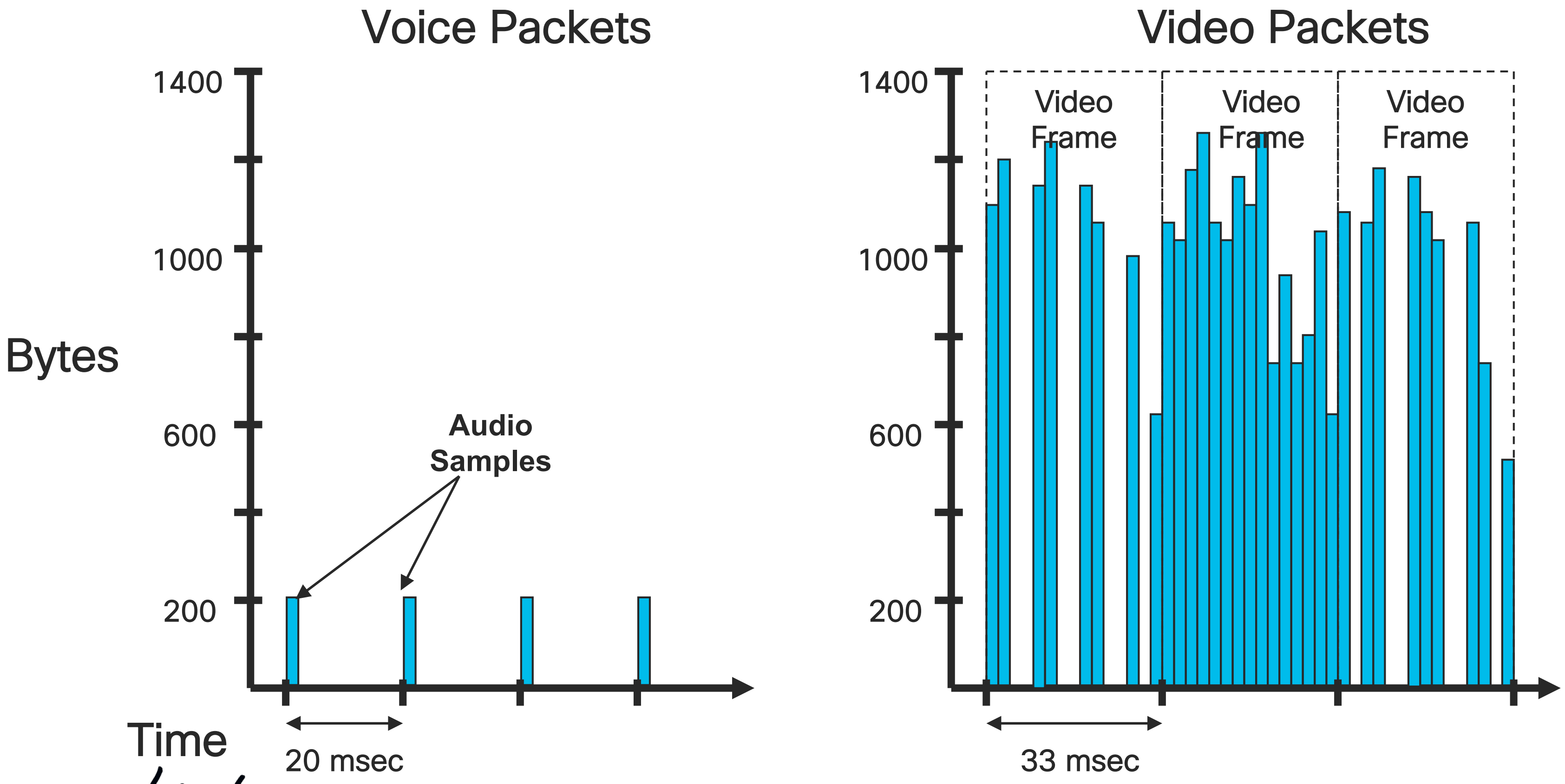
= 2,985,984,000 bps

or 3 Gbps Uncompressed!

Cisco (H264/H.265) codecs transmit 3-5 Mbps per 1080p60 video stream which represents *over* 99.8% *compression (~ 1000:1)*

Packet loss is proportionally magnified by compression ratios. Users can notice a single packet lost in 10,000 – Making HD Video *One Hundred Times More Sensitive to Packet Loss than VoIP!*

VoIP vs. HD Video—At the Packet Level

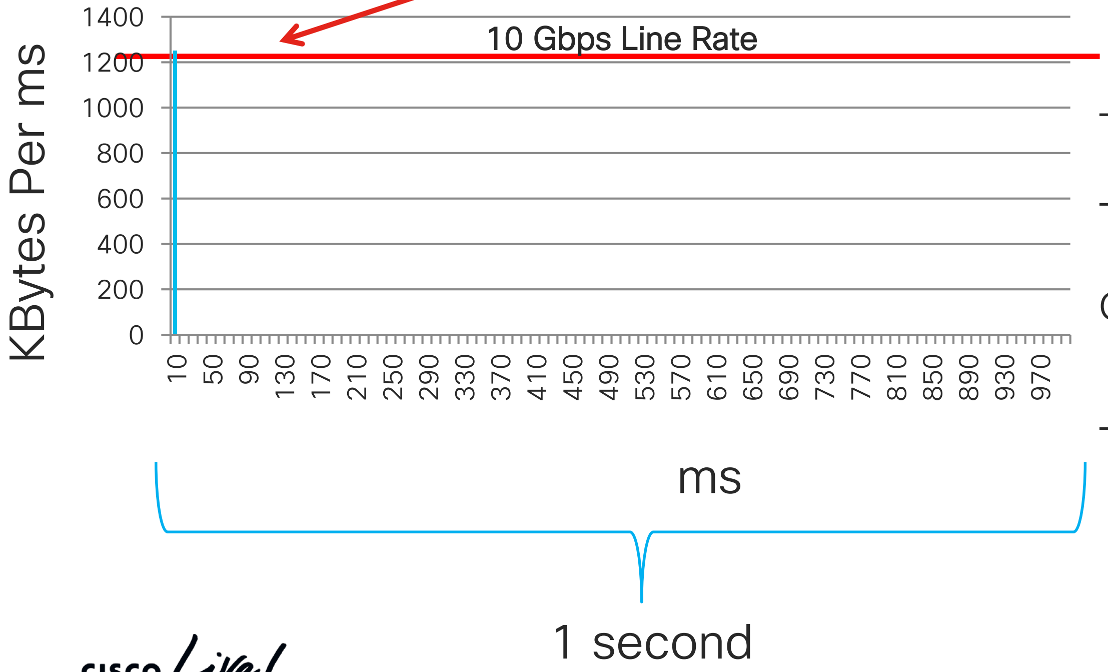


Campus QoS Design Considerations

How Long Can Queue-Buffers Accommodate Line-Rate Bursts?

10-GE Linecard Example

Begin dropping at 9 ms
but overall utilization is still only 1%!



10 GE Linecard Example (WS-X6908)

Total Per-Port Buffer: 90 MB

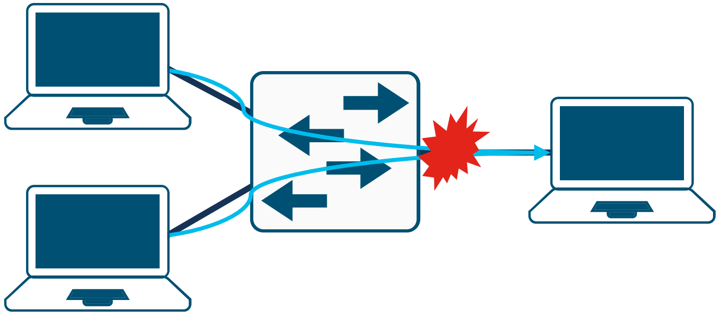
Total Per-Queue Buffer*: 11.25 MB

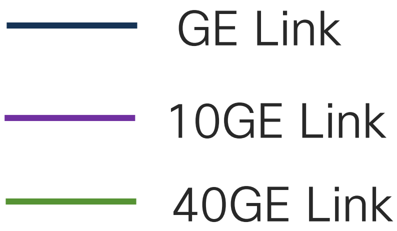
Gbps Line Rate: 10 Gbps = 1.25 GB/s
or 1.25 MB/ms

Total Per-Queue Buffering Capacity: 9.0 ms

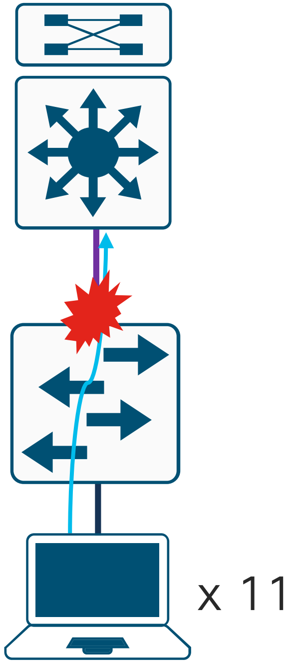
*Assuming (8) equal-sized queues

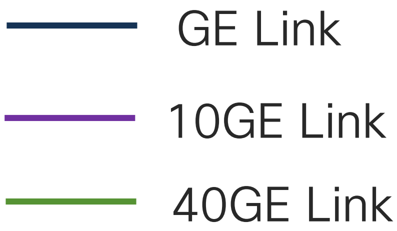
Oversubscription in the Campus



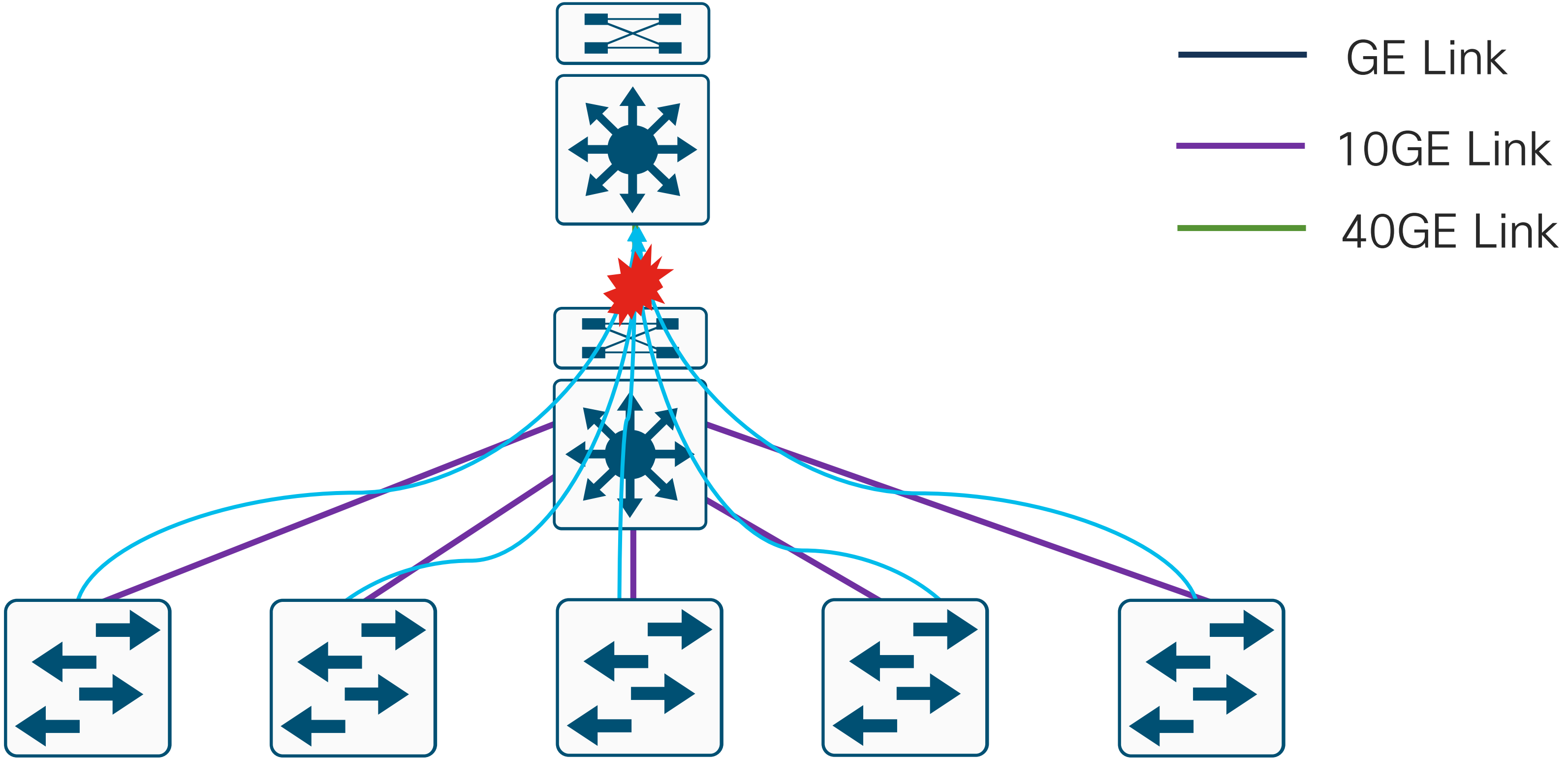


Oversubscription in the Campus

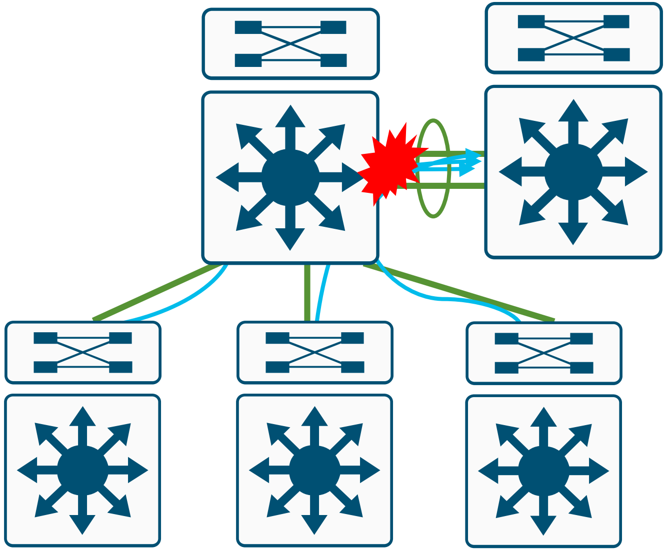




Oversubscription in the Campus



Oversubscription in the Campus



GE Link

10GE Link

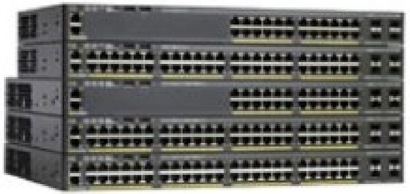
40GE Link

Know Your Tools

- Catalyst switch hardware
- Software and Syntax
- Global Default QoS Settings
- Trust States and Conditional Trust
- Logical vs. Physical Interface QoS
- Ingress and Egress Queuing Models

Hardware Varies

Economy



Utility

Performance

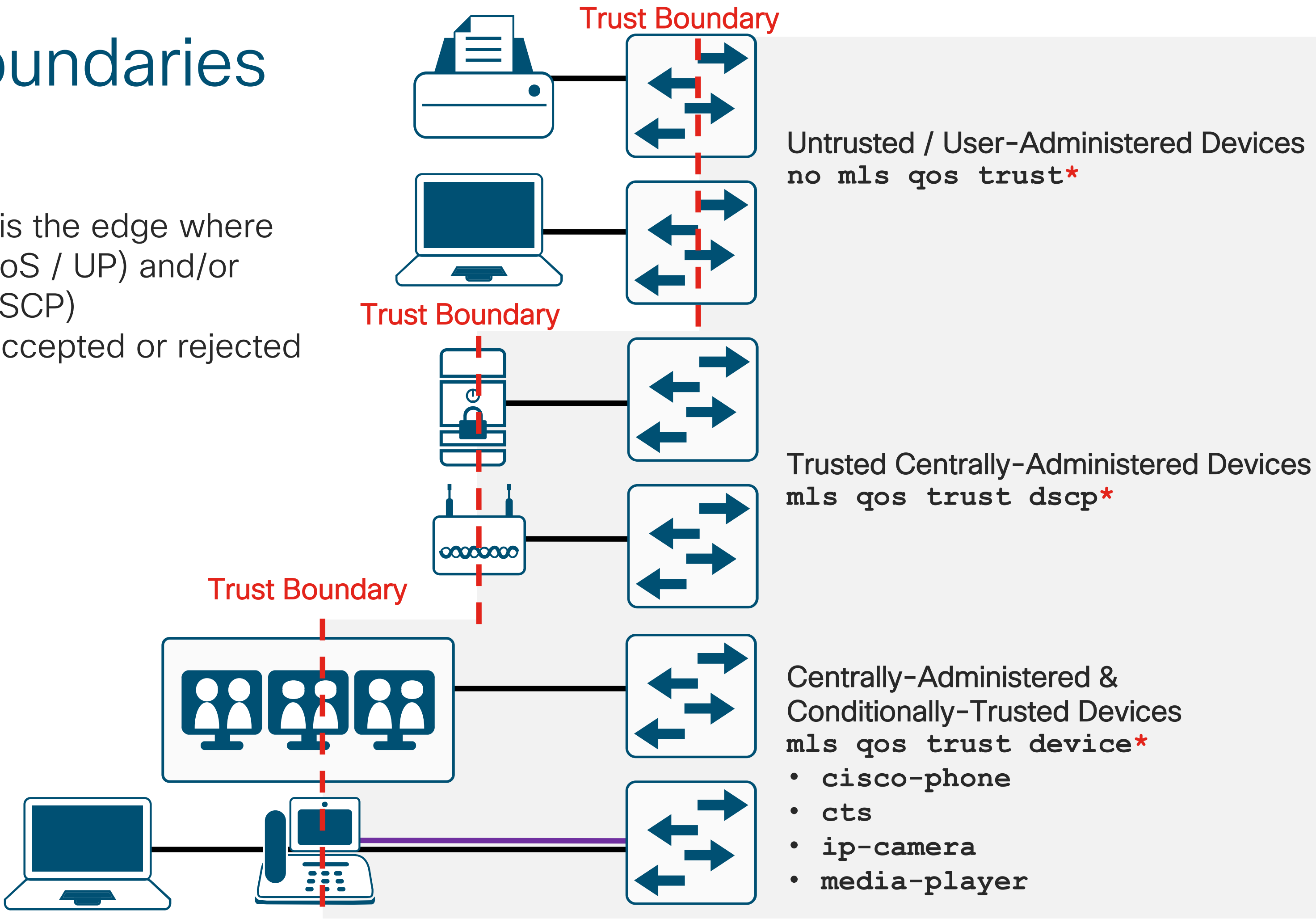
Software and Syntax Variations

- Catalyst 2960-X/3560-X/3750-X are the last platforms to use Multilayer Switch QoS (MLS QoS)
  - QoS is disabled by default and must be globally enabled with the mls qos command
  - Once enabled, all ports are set to an untrusted port-state
- Catalyst 9000, Catalyst 3650/3850, and Catalyst 4500E use IOS Modular QoS Command Line Interface (MQC)
  - QoS is enabled by default
  - All ports trust at layer 2 and layer 3 by default
- Catalyst 6500-E/6800 (Sup6T & Sup2T) use Cisco Common Classification Policy Language (C3PL) QoS
  - QoS is enabled by default
  - All ports trust at layer 2 and layer 3 by default
  - C3PL presents queuing policies similar to MQC, but as a defined “type” of policy
- Nexus 7000/7700 use NX-OS QoS
  - QoS is enabled by default
  - All ports trust at layer 2 and layer 3 by default
  - NX-OS presents queuing policies similar to MQC, but as a defined “type” and with default class-map names

Trust Boundaries

The trust boundary is the edge where
- Layer 2 (CoS / UP) and/or
- Layer 3 (DSCP)

QoS markings are accepted or rejected



*MLS QoS syntax

Conditional Trust

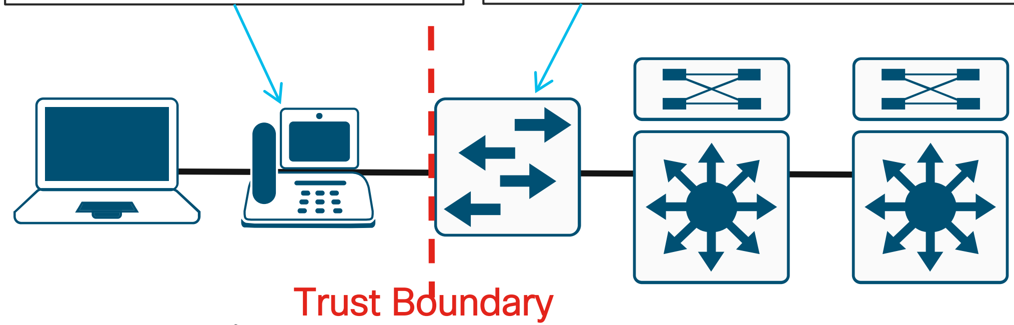
Trust Boundary Extension to Cisco Devices

Access Switch CoS-to-DSCP Mapping Table

```
CoS 7 → DSCP CS7 (56)
CoS 6 → DSCP CS6 (48)
CoS 5 → DSCP EF  (46)*
CoS 4 → DSCP CS4 (32)
CoS 3 → DSCP CS3 (24)
CoS 2 → DSCP CS2 (16)
CoS 1 → DSCP CS1  (8)
CoS 0 → DSCP DF   (0)
```

IP Phone CoS Mapping Table

```
CoS 6-7   → CoS 0
Voice     → CoS 5
Signaling → CoS 3
CoS 0-4   → CoS 0
```



If a Cisco IP Phone is detected then the trust boundary extends to the IP Phone

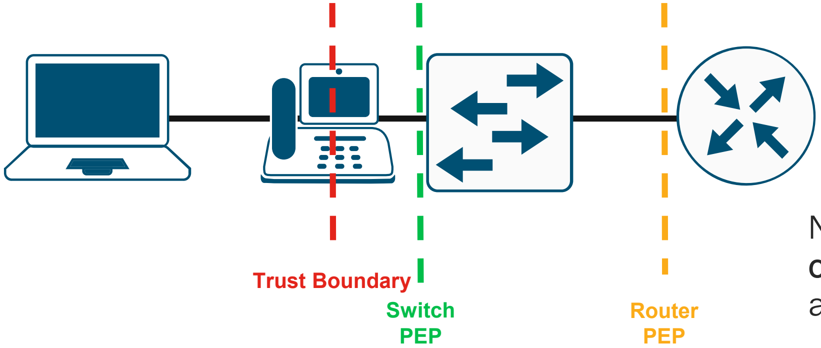
The IP Phone sets CoS for Voice and Signaling and resets all else to 0

The access switch maps CoS-to-DSCP

* Non-Default Mapping

Policy Enforcement Points (PEPs)

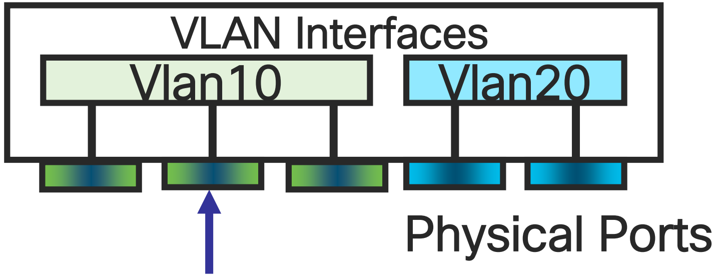
- The Policy Enforcement Point (PEP) is the edge where classification and marking policies are enforced
- The PEP may or *may not be the same as the trust boundary*
- Multiple PEPs may exist for different types of network devices
  - e.g. switch PEP vs. router PEP



Note: For the sake of simplification, in this deck PEP will refer to **classification and marking policy enforcement points** (only) and will not include other policy enforcement points (e.g. queuing).

Per-Port QoS vs. Per-VLAN QoS

Per-Port QoS

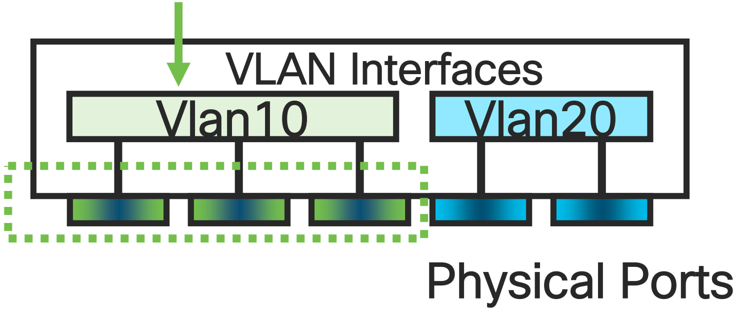


Policy map is applied to the physical switch port

```
interface gig 1/1-48
 service-policy input MARKING
```

Per-VLAN QoS

Policy map is applied to the logical VLAN interface



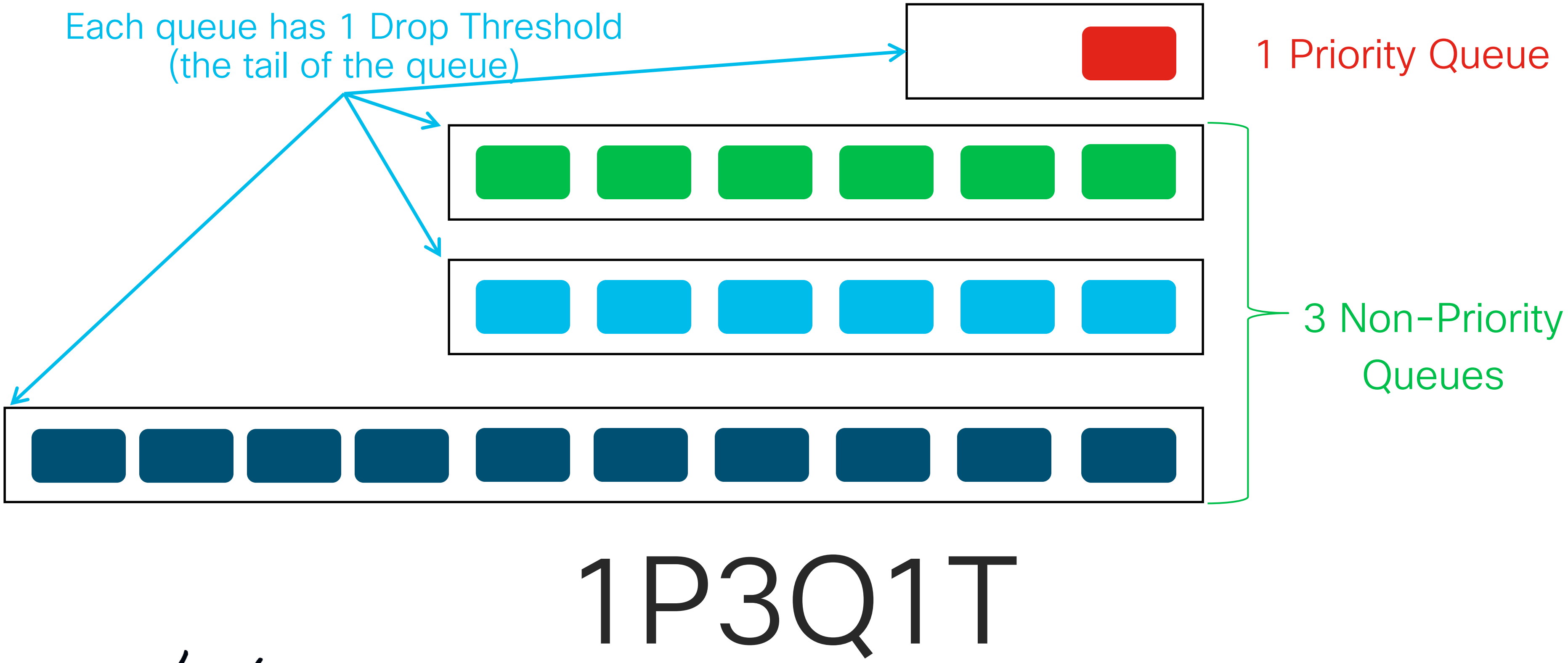

```
interface gig 1/1-48
 mls qos vlan-based

interface Vlan 10
 service-policy input MARKING
```


NBAR2 in Hardware–Today

- UADP-based platforms:
  - Catalyst 3650 and Catalyst 3850 (UADP 1.0 or 1.5)
  - Catalyst 9000 Series (UADP 2.0 or 3.0)
- Supports 1400+ protocols
- Maximum Throughput (Catalyst 3850 / 3650):
  - ~500 connections per second at less than 50% CPU
  - Up to 5,000 bi-directional flows (24 ports) and 10,000 bi-directional flows (48 ports)
- Maximum Throughput (Catalyst 9200):
  - ~500 connections per second at less than 50% CPU
  - Up to 5,000 bi-directional flows (24 and 48 ports)
- Maximum Throughput (Catalyst 9300, and 9400):
  - ~2000 connections per second at less than 50% CPU
  - Up to 10,000 bi-directional flows (24 ports) and 20,000 bi-directional flows (48 ports)

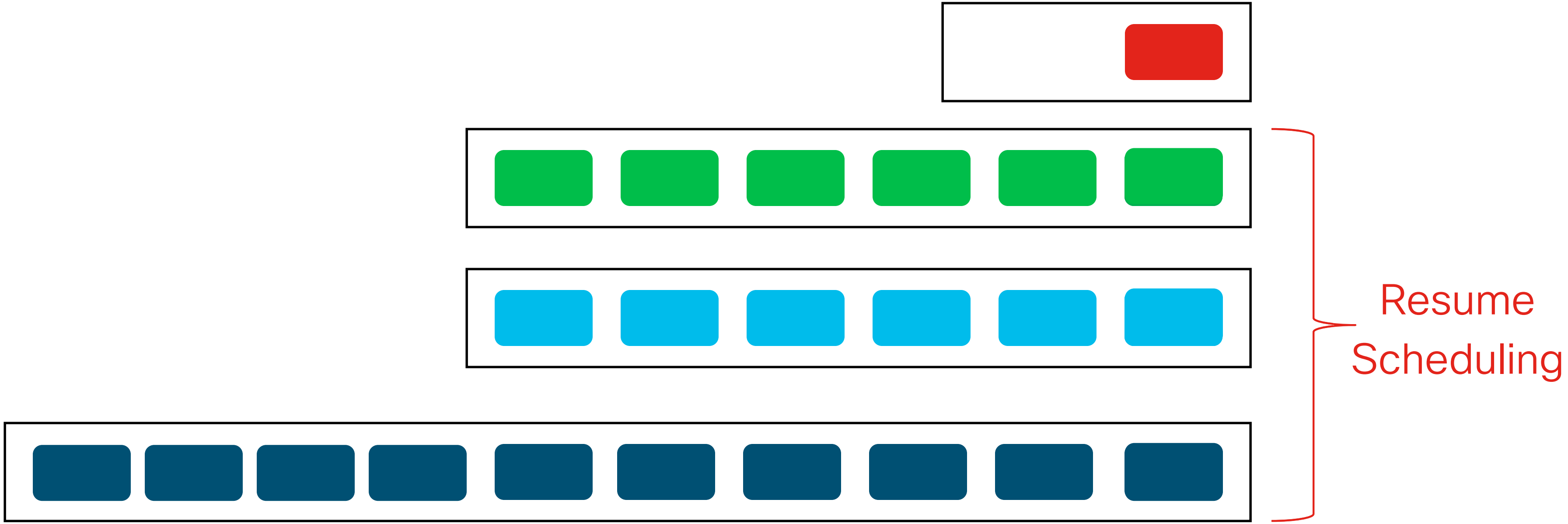
Catalyst Hardware Queuing

1P3Q1T Example



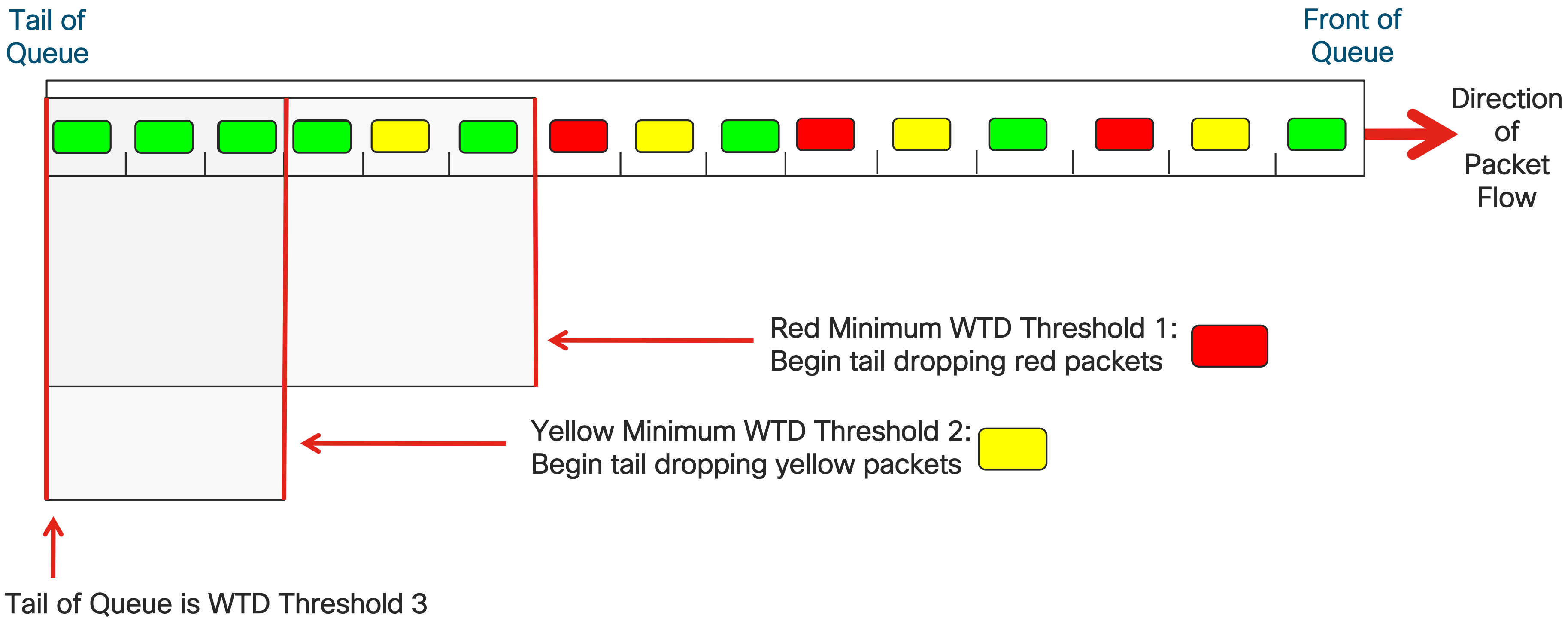
Catalyst Hardware Queuing

1P3Q1T Example



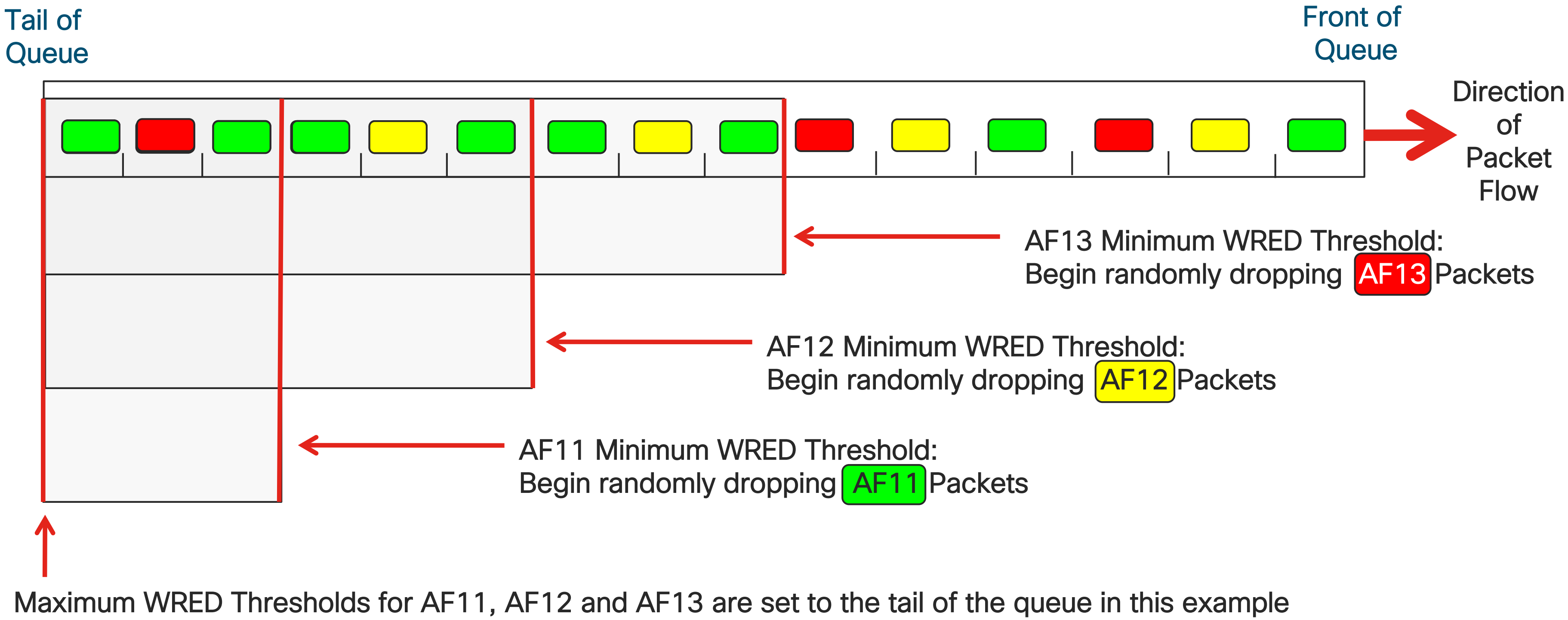
Weighted Tail Drop (WTD) Operation

3T WTD Example



Weighted Random Early Detect (WRED) Operation

3T WRED Example



Auto QoS

- Auto QoS is a macro which provisions pre-defined ingress classification & marking and queuing (egress and/or ingress) policies to switch ports
- Eleven forms of the interface-level Auto QoS command
  - auto qos voip {cisco-phone | cisco-softphone | trust}
  - auto qos video {cts | ip-camera | media-player}
  - auto qos classify [police]
  - auto qos trust [cos | dscp]

QoS Policies for all Auto QoS commands for MLS QoS and MQC platforms are included Appendices D & E

- To remove Auto QoS on an interface preface the command with a “no” (i.e. no auto qos voip cisco-phone)
  - It is not recommended to modify the configuration provisioned by the Auto QoS commands because it may affect the ability of the switch to remove the configuration at the interface-level or globally when removing Auto QoS
- The global command “auto qos srnd4” must be configured to use the current version of Auto QoS on Catalyst 3750-X / 3560-X / 2960-X platforms.

QoS Policies Applied to EtherChannels

Platform	Applied to the (Logical) Port-Channel Interface*	Applied to (Physical) Port-Member Interfaces
Catalyst 2960-X/3560-X/3750-X		Ingress Classification & Marking and Egress Queuing
Catalyst 9000/3850/3650		Ingress Classification & Marking and Egress Queuing
Catalyst 4500E	Ingress Classification & Marking	Egress Queuing
Catalyst 6800/6500-E	Ingress Classification & Marking	Ingress and Egress Queuing
Nexus 7700/7000	Ingress Classification & Marking and Egress Queuing	

*EtherChannels are comprised of logical (Port-Channel) interfaces and physical (port-member) interfaces

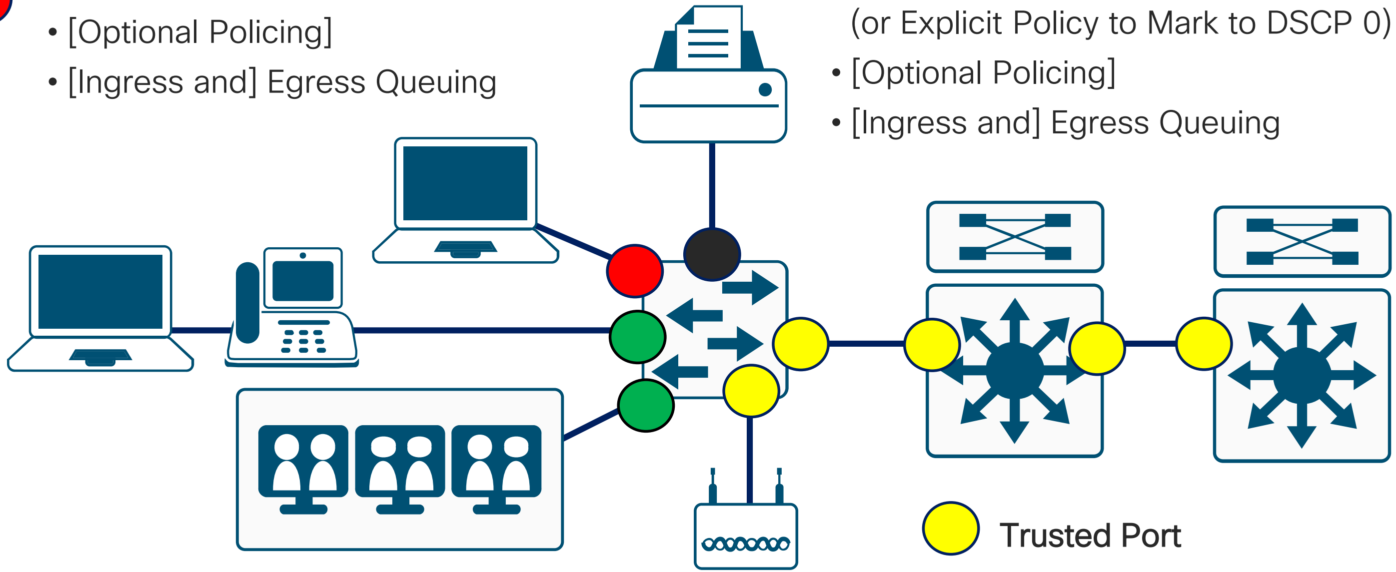
Campus QoS Design Best Practices

- Always perform QoS in hardware rather than software when a choice exists
- Classify and mark applications as close to their sources as technically and administratively feasible
  - Establish the QoS trust boundary at the access-edge of the network
  - Trust QoS within the distribution and core layers of the network
- Police unwanted traffic flows as close to their sources as possible
- Enable queuing policies at every node where the potential for congestion exists

Campus Port QoS Roles

Untrusted Endpoint:
- Ingress Classification and Marking
- [Optional Policing]
- [Ingress and] Egress Queuing

Untrusted Endpoint:
- Port Set to Untrusted State
  (or Explicit Policy to Mark to DSCP 0)
- [Optional Policing]
- [Ingress and] Egress Queuing



Conditionally-Trusted Endpoint
- Conditional-Trust with Trust-CoS or DSCP
- [Optional Ingress Classification, Marking and/or Policing]
- [Ingress and] Egress Queuing

Trusted Port
- Trust DSCP
  (Default on all non-MLS QoS platforms)
- [Ingress and] Egress Queuing

Campus QoS Design—At-A-Glance

Campus QoS Design

The Case for QoS in Campus Networks

The primary role of QoS in campus networks is not to control latency or jitter (as it is in the WAN/VPN), but to manage packet loss. In GE/10GE campus networks, it takes only a few milliseconds of congestion to cause instantaneous buffer overruns resulting in packet drops. Rich media applications—particularly HD video applications—are extremely sensitive to packet drops, to the point where even 1 packet dropped in 10,000 is discernible by the end-user.

Classification, marking, policing, queuing, and congestion avoidance are therefore critical QoS functions that are optimally performed within the campus network.

Four QoS design principles that apply to campus QoS deployments include:

- Always perform QoS in hardware rather than software when a choice exists.
- Classify and mark applications as close to their sources as technically and administratively feasible.
- Police unwanted traffic flows as close to their sources as possible.
- Enable queuing policies at every node where the potential for congestion exists.

Campus QoS Design Considerations

There are several considerations that impact QoS designs within the campus:

- Global Default QoS Setting
- Trust States and Conditional Trust
- Per-Port QoS, Per-VLAN QoS, Per-Port/Per-VLAN QoS
- Ingress QoS Models
- Egress QoS Models
- EtherChannel QoS
- QoS Roles in a campus
- AutoQoS

Global Default QoS Setting

On some platforms QoS is globally disabled by default (such as the Cisco Catalyst 2960/3650/3750). A fundamental first step is to globally enable QoS on these platforms.

Trust States

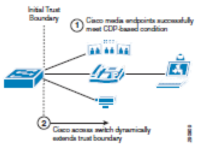
A switch port that is set to trust will accept and preserve either Layer 2 or Layer 3 packet markings. There are four static trust states with which a switch port may be configured:

- Untrusted—The default state with QoS enabled
- Trust CoS—Accepts Layer 2 802.1P CoS markings
- Trust IP Precedence—Accepts Layer 3 IP Precedence markings; largely deprecated
- Trust DSCP—Accepts Layer 3 DSCP markings; this is the most granular and flexible static state and thus the most utilized static trust state in campus networks

Conditional Trust

Trust may also be extended dynamically, provided a successful condition has been met. In Cisco campus networks this condition is a successful Cisco Discovery Protocol (CDP) negotiation between the access switch and the endpoints. Endpoints that can be extended conditional trust by Cisco Catalyst switches include Cisco IP phones, Cisco TelePresence Systems, Cisco IP Surveillance Cameras, and Cisco Digital Media Players. Conditional trust operation is shown in Figure 1.

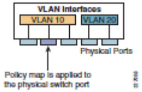
Figure 1 Conditional Trust Operation



Per-Port QoS

When a QoS policy is applied on a per-port basis, it is attached to a specific physical switch port and is active on all traffic received on that specific port (only). QoS policies are applied on a per-port basis by default. Figure 2 illustrates port-based QoS.

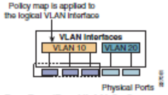
Figure 2 Port-Based QoS



Per-VLAN QoS

When a QoS policy is applied on a per-VLAN basis, it is attached to a logical VLAN interface and is active on all traffic received on all ports that are currently assigned to the VLAN. Figure 3 illustrates VLAN-based QoS.

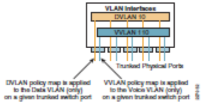
Figure 3 VLAN-Based QoS



Per-Port/Per-VLAN QoS

When a QoS policy is applied on a Per-Port/Per-VLAN basis, it is attached to specific VLAN on a trunked port and is active on all traffic received from that specific VLAN from that specific trunked port (only). Figure 4 illustrates Per-Port/Per-VLAN-based QoS.

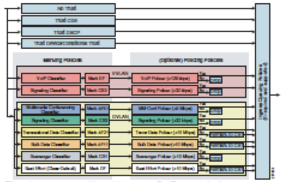
Figure 4 Per-Port-Per-VLAN-Based QoS



Ingress QoS Models

There are many options for an administrator to choose from for ingress QoS models, as shown in Figure 5.

Figure 5 Ingress QoS Models



The three most utilized ingress QoS models for campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Combinations of these may be used at the same time

Egress QoS Models

Cisco Catalyst switches perform queuing in hardware and as such are limited to a fixed number of queues. The nomenclature used to describe these queuing structures is 1PxQyT, where:

- **1P** represents a strict priority queue
- x**Q** represents x-number of non-priority queues
- y**T** represents y-number of drop-thresholds per non-priority queue

No fewer than four hardware queues would be required to support QoS policies in the campus; the following queues would be considered a minimum:

- Realtime queue (RFC 3246 EF PHB)
- Guaranteed bandwidth queue (RFC 2597 AF PHB)
- Default queue (RFC 2474 DF PHB)
- Bandwidth constrained queue (RFC 3662 PDB or "scavenger" service)

Additionally, the following bandwidth allocations are recommended for these queues:

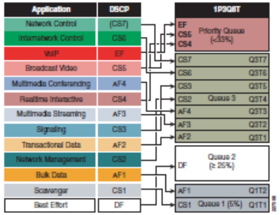
- Realtime queue should not exceed 33% BW
- Default queue should be at least 25% BW
- Bulk/scavenger queue should not exceed 5% BW

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

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

An egress queuing example based on these design considerations is shown in Figure 6.

Figure 6 An Egress Queuing Example Model



EtherChannel QoS

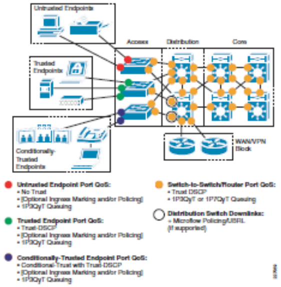
On some platforms ingress QoS policies (such as DSCP trust) are applied on the logical Port-Channel interface; however, on all platforms egress QoS policies (such as queuing policies) are always applied to the physical port-member interfaces.

QoS Roles in a Campus

Access edge switch ports have the most variation in QoS policy roles and these will vary depending on the type of endpoint to which these are connecting.

For all switch-to-switch links the only QoS policies that are required are DSCP-trust (on ingress) and queuing (on egress). QoS roles in a campus network are shown in Figure 7.

Figure 7 Campus Port QoS Roles



AutoQoS

On some Catalyst switching platforms Cisco has already updated and expanded the functionality of its AutoQoS feature to automatically provision QoS best practice designs for voice, IP-based video applications (such as IP Video Surveillance, Cisco TelePresence, conferencing applications, and streaming video applications), as well as for multiple types of data applications.

On these switch platforms, an administrator can automatically provision these best practice designs via a single interface-level command that corresponds to the endpoint to which the switch port is connecting.

For more details, see Campus QoS Design 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html
And the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 13

Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

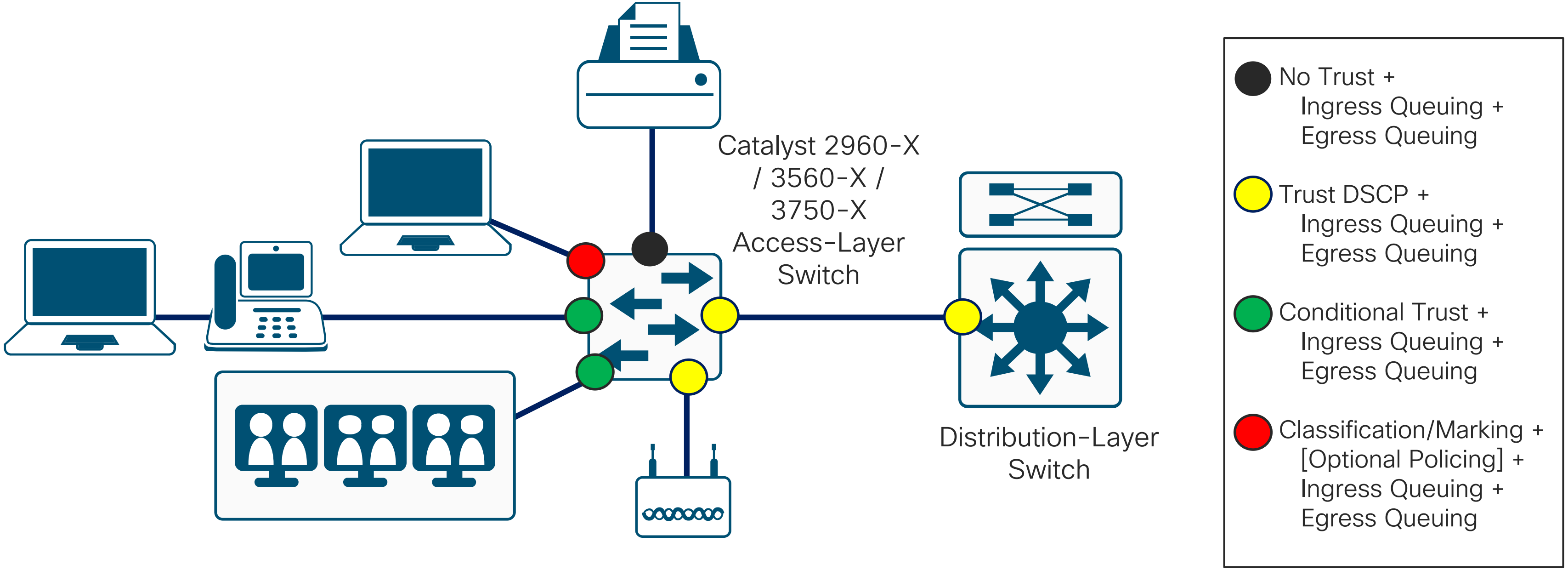
Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design

Catalyst 2960-X / 3560-X / 3750-X

QoS Roles in the Campus Access



Catalyst 2960-X / 3560-X / 3750-X

QoS Design Steps

1. Enable QoS

2. Configure Ingress QoS Model(s):
    - Trust Models
    - Conditional Trust Model
    - Service Policy Models

3. Configure Egress Queuing

4. Configure Ingress Queuing (Catalyst 3560-X & 3750-X)

Note: The Catalyst 3560-X & 3750-X support VLAN-based QoS policies, but the 2960-X does not.

Note: Catalyst 2960-X must be running a LAN Base image (not IP Lite) to support the following QoS features

- Policy maps
- Policing & marking
- Mapping tables
- Weighted Tail Drop (WTD)

Catalyst 2960-X / 3560-X / 3750-X

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Grey shaded commands are global

Trust-CoS Model Example:

```
mls qos map cos-dscp 0 8 16 24 32 46 48 56
```

Key commands/parameters are in RED

```
mls qos trust cos
```

Yellow shaded commands are interface specific

Trust-DSCP Model Example:

```
mls qos trust dscp
```

Note: CoS 5 which is explicitly mapped to DSCP 46

Conditional-Trust Model Example:

```
mls qos trust device cisco-phone   [or]
mls qos trust device cts           [or]
mls qos trust device ip-camera     [or]
mls qos trust device media-player
```

Note: Only one type of device may be configured at a time

Catalyst 2960-X / 3560-X / 3750-X

Conditional Trust Model Example

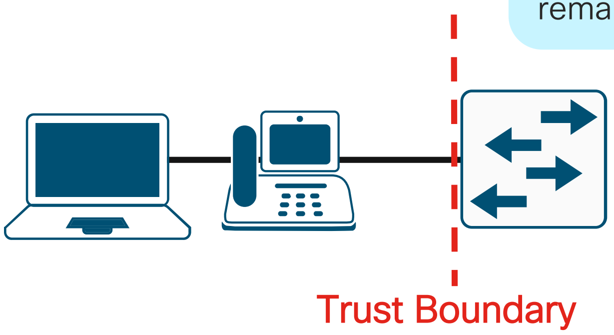
Conditional Trust Policy to a Cisco IP

```
mls qos
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos trust device cisco-phone
mls qos trust cos
```

CoS must be matched as Cisco IP Phones only remark at Layer 2

Note: All CoS-to-DSCP values are left at default (DSCP = CoS * 8)

Except for CoS 5 which is explicitly mapped to DSCP 46 (Expedite Forwarding/EF, per RFC 3246 & 4594).



Catalyst 2960-X / 3560-X / 3750-X

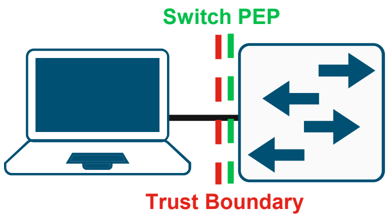
Ingress Classification & Marking Policy Example – Policy-Map

The policy-map definition specifies an ordered list of classes, each with an action, with a default class at the bottom

```
policy-map MARKING-POLICY
 class VOIP-TELEPHONY
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
 class REALTIME-INTERACTIVE
  set dscp cs4
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class MULTIMEDIA-STREAMING
  set dscp af31
 class SIGNALING
  set dscp cs3
 class OAM
  set dscp cs2
 class TRANSACTIONAL-DATA
  set dscp af21
…
```

```
[continued]
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
service-policy input MARKING-POLICY
```

The service-policy is applied inbound (ingress classification & marking policy) and references a policy-map definition



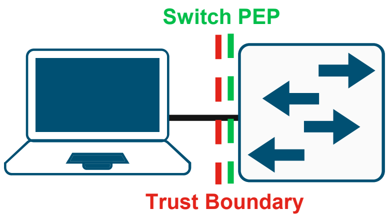
Catalyst 2960-X / 3560-X / 3750-X

Ingress Classification & Marking Policy Example – Class-Maps

```
class-map match-all VOIP-TELEPHONY
 match access-group name VOIP-TELEPHONY
class-map match-all BROADCAST-VIDEO
 match access-group name BROADCAST-VIDEO
class-map match-all REALTIME-INTERACTIVE
 match access-group name REALTIME-INTERACTIVE
class-map match-all MULTIMEDIA-CONFERENCING
 match access-group name MULTIMEDIA-CONFERENCING
class-map match-all MULTIMEDIA-STREAMING
 match access-group name MULTIMEDIA-STREAMING
class-map match-all SIGNALING
 match access-group name SIGNALING
class-map match-all OAM
 match access-group name OAM
class-map match-all TRANSACTIONAL-DATA
 match access-group name TRANSACTIONAL-DATA
class-map match-all BULK-DATA
 match access-group name BULK-DATA
class-map match-all SCAVENGER
 match access-group name SCAVENGER
```

The class-map definitions specify the classes. ‘match-all’ matches all (logical AND) match statements under a class. ‘match-any’ matches any (logical OR) match statements under a class.

‘match access-group’ matches on an access-list definition



Catalyst 2960-X / 3560-X / 3750-X

Ingress Classification & Marking Policy Model Example – Access Control List

```
ip access-list extended SIGNALING
 remark sccp
 permit tcp any any eq 2000
 permit tcp any any eq 2001
 permit tcp any any eq 2002
 remark rtsp
 permit tcp any any eq 554
 permit tcp any any eq 8554
 remark sip
 permit tcp any any eq 5060
 permit udp any any eq 5060
 remark sip-tls
 permit tcp any any eq 5061
 permit udp any any eq 5061
```

The access-list definition can be an standard or extended access-list

Permit statements allow traffic to be matched. Statements can specify source and destination IP addresses and ports.

Comments can be added to the ACL definition to help identify the application

Access-list entries (ACEs) are mapped into TCAM tables within switches for QoS performance.

Catalyst 2960-X

Marking & Policing Policy Example

Note: Remarking is performed by configuring a policed-DSCP map with the global configuration command **mls qos map policed-dscp**, which specifies which DSCP values are subject to remarking if out-of-profile and what value these should be remarked as.

In this example exceeding:

- Best Effort (DSCP 0)
- Bulk (AF11 / DSCP 10)
- Transactional Data (AF21 / DSCP 18)

are remarked to Scavenger (CS1 / DSCP 8).

```
mls qos map policed-dscp 0 10 18 to 8

[class-maps omitted for brevity]
policy-map MARKING&POLICING
 class VVLAN-VOIP
  set dscp ef
  police 128k 8000 exceed-action drop
 class VVLAN-SIGNALING
  set dscp cs3
  police 32k 8000 exceed-action drop
 class MULTIMEDIA-CONFERENCING
  set dscp af41
  police 5m 8000 exceed-action drop
 class SIGNALING
  set dscp cs3
  police 32k 8000 exceed-action drop
 class TRANSACTIONAL-DATA
  set dscp af21
  police 10m 8000 exceed-action policed-dscp-transmit
…
```

```
[continued]
 class BULK-DATA
  set dscp af11
  police 10m 8000 exceed-action policed-dscp-transmit
 class SCAVENGER
  set dscp cs1
  police 10m 8000 exceed-action drop
 class DEFAULT
  set dscp default
  police 10m 8000 exceed-action policed-dscp-transmit
```

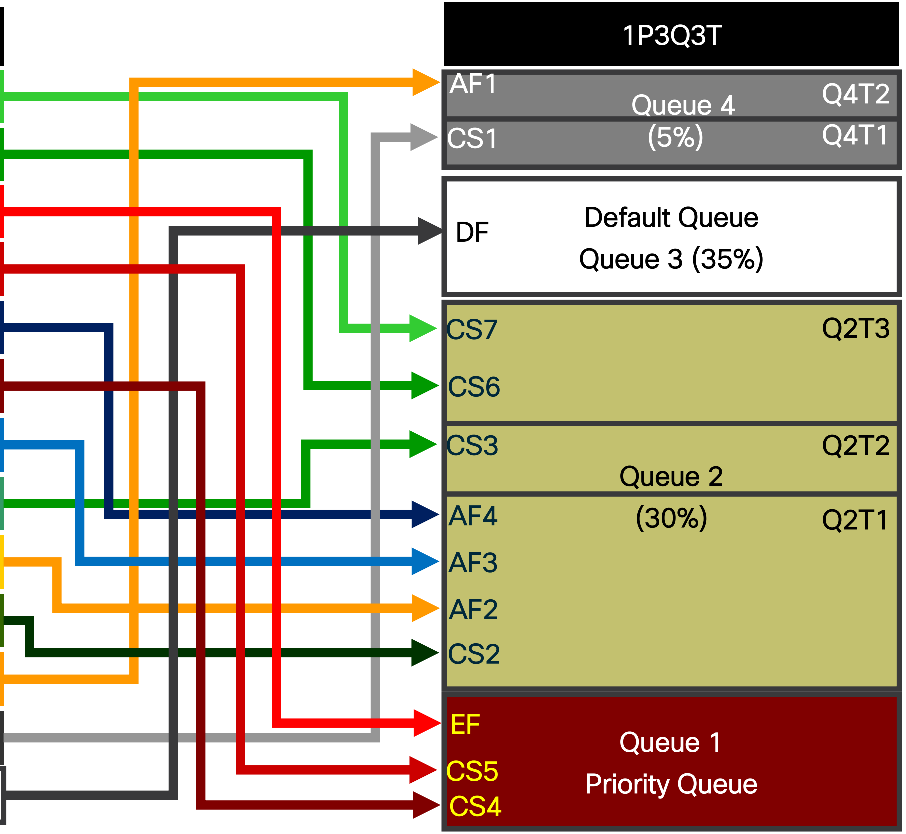
```
service-policy input MARKING&POLICING
```

cisco Live!

Catalyst 2960-X / 3560-X / 3750-X

1P3Q3T Egress Queuing Model

Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF



Catalyst 2960-X / 3560-X / 3750-X

1P3Q3T Egress Queuing Model Config—Part 1 of 2

Note: The Catalyst 2960-X can also be configured to use an 8-queue model; however this model is NOT supported in a stack, nor is it supported if AutoQoS is enabled.

```
! This section configures egress buffers and thresholds
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 400
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 80 100 400
```

Allocates buffers to Q1, Q2, Q3 and Q4 (respectively)

Each queue has 4 thresholds:

- **WTD Threshold 1**
- **WTD Threshold 2**
- **Reserved Threshold**—buffers that may NOT be shared with adjacent port-queues
- **Maximum Threshold**—maximum amount of buffers may be borrowed from common buffer pools (if available)

```
! This section configures egress CoS-to-Queue mappings
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
```

If the packet enters the switch on a port that is set to **trust cos** then these **CoS-to-Queue** mappings will be used to determine how the packet is queued on egress

Catalyst 2960-X / 3560-X / 3750-X

1P3Q3T Egress Queuing Model Config—Part 2 of 2

```
! This section configures egress DSCP-to-Queue mappings
mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36 38
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
```

If the packet enters the switch on a port that is set to **trust dscp** then these **DSCP-to-Queue** mappings will be used to determine how the packet is queued on egress

```
! This section configures interface egress queuing parameters
queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
```

Enables the PQ

Allocates bandwidth to each queue by means of a WRR weight. Q1 weight is ignored, as it's operating as a PQ

Catalyst 2960-X QoS Design At-A-Glance

Cisco Catalyst 2960-X QoS Design

At-A-Glance

Role in Campus Network

The Cisco Catalyst 2960-X series switches are well suited to the role of access switches in campus networks. As such, these switches may connect directly to a variety of endpoints, as well as to distribution-layer switches, as shown in Figure 1.

Figure 1 Cisco Catalyst 2960-X Switches in a Campus Network

QoS Design Steps

There are four main steps to configure QoS on Cisco Catalyst 2960-X series switches:

1. Enable QoS
2. Configure Ingress QoS Model(s):
   - Trust DSCP Model
   - Conditional Trust Model
   - Service Policy Models
3. Configure Egress Queuing

Step 1: Globally Enable QoS

QoS is globally enabled on the Cisco Catalyst 2960-X with the **mls qos** command.

Step 2: Configure Ingress QoS Model(s)

The three most utilized ingress QoS models for campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Combinations of these ingress QoS models may be used at the same time.

Trust DSCP Model

This model is configured with the **mls qos trust dscp** interface-configuration command.

The Trust DSCP model configures the interface to statically accept and preserve the Layer 3 DSCP markings of all incoming packets. This model is suitable for interfaces connecting to endpoints that can mark DSCP values and are administratively controlled (such as WLAN controllers) as well as for any uplinks to distribution layer switches. Switch ports that can be set to trust DSCP are shown as yellow circles in Figure 1.

Conditional Trust Model

This model is configured with the **mls qos trust device** interface-configuration command.

The Conditional Trust model configures the interface to *dynamically* accept markings from endpoints that have met a specific condition (currently based on a successful Cisco Discovery Protocol identification). This model is suitable for switch ports connecting to Cisco IP phones (with the **cisco-phone** option), Cisco TelePresence Systems (with the **cts** option), Cisco IP Video Surveillance cameras (with the **ip-camera** option), and Cisco Digital Media Players (with the **media-player** option). This model is also suitable for PCs and untrusted devices, since the ports connecting to such devices will remain in their default untrusted state. Switch ports that can be set to conditional trust are shown as green circles in Figure 1.

Service Policy Models

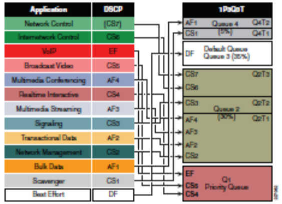
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

- class-maps which identify the flows using packet markings or by access-lists or other criteria
- policy-maps which specify policy actions to be taken on a class-by-class basis
- service-policy statements which apply a specific policy-map to an interface(s) and specify direction

Step 3: Configure Egress Queuing

The egress queuing model for the Cisco Catalyst 2960-X is shown in Figure 2..

Figure 2 Catalyst 2960-X Egress Queuing Model



EtherChannel QoS

QoS policies on the Cisco Catalyst 2960-X are configured on the physical port-member interfaces only (and not on the logical Port-Channel interface).

Cisco Validated Design

The Cisco Validated Design for Cisco Catalyst 2960-X series switches in the role of an access switch in a campus network is presented below.

Step 1: Enable QoS:

```
mls qos
```

Step 2: Configure Ingress QoS Model :

Trust DSCP Model :

```
mls qos trust dscp
```

Conditional Trust Model :

```
mls qos trust device cisco-phone or
mls qos trust device cts or
mls qos trust device ip-camera or
mls qos trust device media-player
```

Service Policy Models :

```
[class-maps omitted for brevity]

policy-map MARKING-POLICY
 class VOIP
  set dscp ef
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class SIGNALING
  set dscp cs3
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class DEFAULT
  set dscp default

service-policy input MARKING-POLICY
```

Note : The Service-Policy Model can be expanded to include policing.

Step 3 : Configure Egress Queuing

```
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 100 100 400
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36 38
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14

queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
```

Egress Queue and Threshold Tuning

Egress CoS-to-Queue Mapping

Egress DSCP-to-Queue Mapping

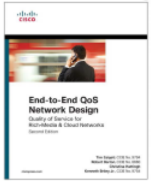
Egress Queuing Interface-Specific Commands

Note: Highlighted commands are interface specific; otherwise these are global.

For more details, see Campus QoS Design 4.0:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html

And the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 14



Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

Catalyst 3560-X/3750-X QoS Design At-A-Glance

Cisco Catalyst 3560-X/3750-X QoS Design

Role in Campus Network

The Cisco Catalyst 3560-X & 3750-X series switches are well suited to the role of access switches in campus networks. As such, these switches may connect directly to a variety of endpoints, as well as to distribution-layer switches, as shown in Figure 1.

Figure 1 Cisco Catalyst 3560-X/3750-X Switches in a Campus Network

QoS Design Steps

There are four main steps to configure QoS on Cisco Catalyst 3560-X and 3750-X series switches:

1. Enable QoS
2. Configure Ingress QoS Model(s):
   - Trust DSCP Model
   - Conditional Trust Model
   - Service Policy Models
3. Configure Ingress Queuing
4. Configure Egress Queuing

Step 1: Globally Enable QoS

QoS is globally enabled on the Cisco Catalyst 3560-X and 3750-X with the **mls qos** command.

Step 2: Configure Ingress QoS Model(s)

The three most utilized ingress QoS models for campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Combinations of these ingress QoS models may be used at the same time.

Trust DSCP Model

This model is configured with the **mls qos trust dscp** interface-configuration command.

The Trust DSCP model configures the interface to statically accept and preserve the Layer 3 DSCP markings of all incoming packets. This model is suitable for interfaces connecting to endpoints that can mark DSCP values and are administratively controlled (such as WLAN controllers) as well as for any uplinks to distribution layer switches. Switch ports that can be set to trust DSCP are shown as yellow circles in Figure 1.

Conditional Trust Model

This model is configured with the **mls qos trust device** interface-configuration command.

The Conditional Trust model configures the interface to ***dynamically*** accept markings from endpoints that have met a specific condition (currently based on a successful Cisco Discovery Protocol identification). This model is suitable for switch ports connecting to Cisco IP phones (with the **cisco-phone** option), Cisco TelePresence Systems (with the **cts** option), Cisco IP Video Surveillance cameras (with the **ip-camera** option), and Cisco Digital Media Players (with the **media-player** option). This model is also suitable for PCs and untrusted devices, since the ports connecting to such devices will remain in their default untrusted state. Switch ports that can be set to conditional trust are shown as green circles in Figure 1.

Service Policy Models

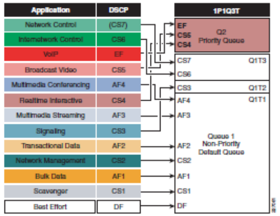
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

- class-maps which identify the flows using packet markings or by access-lists or other criteria
- policy-maps which specify policy actions to be taken on a class-by-class basis
- service-policy statements which apply a specific policy-map to an interface(s) and specify direction

Step 3: Configure Ingress Queuing

The ingress queuing model for the Cisco Catalyst 3560-X/3750X is shown in Figure 2.

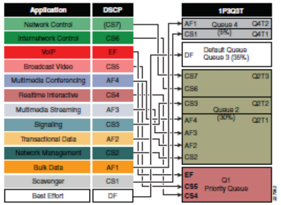
Figure 2 Catalyst 3560-X/3750-X Ingress Queuing Model



Step 4: Configure Egress Queuing

The egress queuing model for the Cisco Catalyst 3560-X/3750X is shown in Figure 3.

Figure 3 Catalyst 3560-X/3750-X Egress Queuing Model



EtherChannel QoS

QoS policies on the Cisco Catalyst 3560-X/3750-X are configured on the physical port-member interfaces only (and not on the logical Port-Channel interface).

Cisco Validated Design

The Cisco Validated Design for Cisco Catalyst 3650-X and 3750-X series switches in the role of an access switch in a campus network is presented below.

Step 1: Enable QoS:

```
mls qos
```

Step 2: Configure Ingress QoS Model :

Trust DSCP Model :

```
mls qos trust dscp
```

Conditional Trust Model :

```
mls qos trust device cisco-phone or
mls qos trust device cts or
mls qos trust device ip-camera or
mls qos trust device media-player
```

Service Policy Models :

```
[class-maps omitted for brevity]

policy-map MARKING-POLICY
 class VOIP
  set dscp ef
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class SIGNALING
  set dscp cs3
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class DEFAULT
  set dscp default

service-policy input MARKING-POLICY
```

Note : The Service-Policy Model can be expanded to include policing.

Step 3 :Configure Ingress Queuing

```
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input buffers 90 10
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4 5
mls qos srr-queue input dscp-map queue 1 threshold 1 0 8 10 12 14
mls qos srr-queue input dscp-map queue 1 threshold 1 16 18 20 22
mls qos srr-queue input dscp-map queue 1 threshold 1 26 28 30 34 36 38
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 56
mls qos srr-queue input dscp-map queue 2 threshold 3 32 40 46
```

Ingress Queue and Threshold Tuning
Ingress CoS-to-Queue Mapping
Ingress DSCP-to-Queue Mapping

Step 4 : Configure Egress Queuing

```
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 100 100 400
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 40 46
mls qos srr-queue output dscp-map queue 2 threshold 1 16 18 20 22
mls qos srr-queue output dscp-map queue 2 threshold 1 26 28 30 34 36 38
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 56
mls qos srr-queue output dscp-map queue 3 threshold 3 0
mls qos srr-queue output dscp-map queue 4 threshold 1 8
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14

queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
```

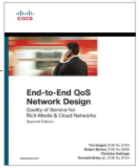
Egress Queue and Threshold Tuning
Egress CoS-to-Queue Mapping
Egress DSCP-to-Queue Mapping
Egress Queuing Interface-Specific Commands

Note: Highlighted commands are interface specific; otherwise these are global.

For more details, see Campus QoS Design 4.0:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html

And the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 14



Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

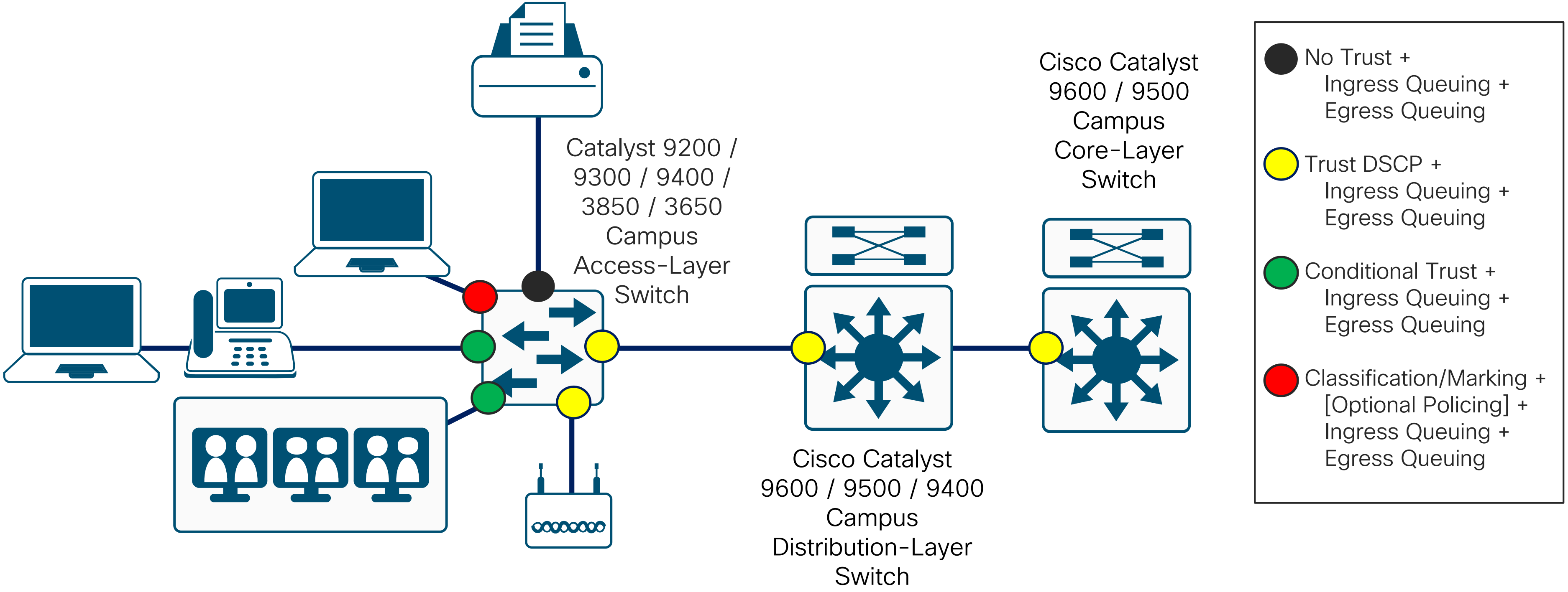
Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design

Catalyst 9000 / 3850 / 3650 Series

QoS Roles in the Campus



Catalyst 9000 / 3850 / 3650 Series

QoS Design Steps

Access-Layer Switch Role

1. Configure Ingress QoS Model(s):
   - ❑ Trust DSCP / CoS Model (Default)
   - ❑ Conditional Trust Models
   - ❑ Service Policy Models
2. Configure Egress Queuing
   - ❑ Wired Queuing Models: 2P6Q3T

Core or Distribution-Layer Switch Role

1. Configure Egress Queuing
   - ❑ Wired Queuing Models: 2P6Q3T

Catalyst 9000 / 3850 / 3650 Series

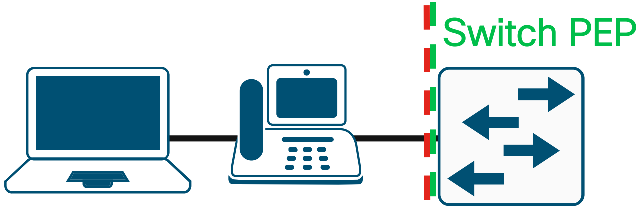
Conditional Trust Models

As of IOS XE 16.5.1 and higher match-all is also supported on Catalyst 3850 and 3650 Series switches. Both match-any and match-all are supported on Catalyst 9000 Series switches.

Conditional-Trust Models:

```
interface GigabitEthernet 1/0/1
 trust device cisco-phone      [or]
 trust device cts              [or]
 trust device ip-camera        [or]
 trust device media-player
```

Only one type of device can be configured for conditional trust on an interface at a given time



Conditional-Trust (Cisco IP Phone) Example:

```
class-map match-any VOICE
 match cos 5
class-map match-any SIGNALING
 match cos 3

policy-map CISCO-IPPHONE
 class VOICE
  set dscp ef
 class SIGNALING
  set dscp cs3
 class class-default
  set dscp default
interface GigabitEthernet 1/0/1
 trust device cisco-phone
 service-policy input CISCO-IPPHONE
```

CoS must be matched as Cisco IP Phones only remark at Layer 2

Catalyst 9000 / 3850 / 3650 Series

Classification Options

- ACL-based classification: match access-group
  - Syntax is identical to Catalyst 2960-X / 3560-X / 3750-X ACL-based classification & marking examples
- NBAR2 classification: match protocol
  - Catalyst 3850 / 3650 IOS XE 16.3.1 and higher
  - Catalyst 9300 IOS XE 16.5.1 and higher
  - Catalyst 9400 IOS XE 16.9.1 and higher
  - Catalyst 9200 IOS XE 16.11.1 and higher
- NBAR2 classification: match protocol attribute business-relevance and match protocol attribute traffic-class
  - Catalyst 9300 / 3850 / 3650 Series running IOS XE 16.8.1 and higher
  - Catalyst 9400 Series running IOS XE 16.9.1 or higher
  - Catalyst 9200 Series running IOS XE 16.11.1 or higher

Catalyst 9000 / 3850 / 3650 Series

Configuring NBAR2 QoS Policies

match protocol enables NBAR2 classification
Note: Up to 16 **match protocol** statements are supported per class-map and up to 255 **match protocol** statements in all policies.

```
class-map match-any VOICE
 match protocol cisco-phone
 match protocol cisco-jabber-audio
 match protocol ms-lync-audio
 match protocol citrix-audio
class-map match-any BROADCAST-VIDEO
 match protocol cisco-ip-camera
class-map match-any REAL-TIME-INTERACTIVE
 match protocol telepresence-media
class-map match-any CALL-SIGNALING
 match protocol skinny
 match protocol telepresence-control
class-map match-any TRANSACTIONAL-DATA
 match protocol citrix
 match protocol sap
…
```

NBAR2 based match protocol is allowed only with marking or policing actions - not queuing.

```
policy-map NBAR-MARKING
 class VOICE
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
 class REAL-TIME-INTERACTIVE
  set dscp cs4
 class CALL-SIGNALING
  set dscp cs3
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
```

Holy Grail QoS Config: NBAR2 1400+ App / 12-Class Model

```
class-map match-all VOICE
   match protocol attribute traffic-class voip-telephony
   match protocol attribute business-relevance business-relevant
class-map match-all BROADCAST-VIDEO
   match protocol attribute traffic-class broadcast-video
   match protocol attribute business-relevance business-relevant
class-map match-all REAL-TIME-INTERACTIVE
   match protocol attribute traffic-class real-time-interactive
   match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-CONFERENCING
   match protocol attribute traffic-class multimedia-conferencing
   match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-STREAMING
   match protocol attribute traffic-class multimedia-streaming
   match protocol attribute business-relevance business-relevant
 class-map match-all SIGNALING
   match protocol attribute traffic-class signaling
   match protocol attribute business-relevance business-relevant
class-map match-all NETWORK-CONTROL
   match protocol attribute traffic-class network-control
   match protocol attribute business-relevance business-relevant
class-map match-all NETWORK-MANAGEMENT
   match protocol attribute traffic-class ops-admin-mgmt
   match protocol attribute business-relevance business-relevant
class-map match-all TRANSACTIONAL-DATA
   match protocol attribute traffic-class transactional-data
   match protocol attribute business-relevance business-relevant
class-map match-all BULK-DATA
   match protocol attribute traffic-class bulk-data
   match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER
   match protocol attribute business-relevance business-irrelevant
```

```
policy-map MARKING
 class VOICE
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
 class REAL-TIME-INTERACTIVE
  set dscp cs4
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class MULTIMEDIA-STREAMING
  set dscp af31
 class SIGNALING
  set dscp cs3
 class NETWORK-CONTROL
  set dscp cs6
 class NETWORK-MANAGEMENT
  set dscp cs2
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
```

Provisioned with Cisco DNA Center 1.2.8+ Application Policy on Catalyst 9000 Series access-layer switches with IOS XE 16.10+ (Switch must support "traffic-class" and "business-relevance" attributes).

Catalyst 9000 / 3850 / 3650

Marking & Policing Policy Example

```
policy-map MARKING&POLICING
 class VVLAN-VOIP
  set dscp ef
  police 128K conform-action transmit  exceed-action drop
 class VVLAN-SIGNALING
  set dscp cs3
  police 32K conform-action transmit  exceed-action drop
 class MULTIMEDIA-CONFERENCING
  set dscp af41
  police 5M conform-action transmit  exceed-action drop
 class SIGNAL
  set dscp c
  police 32K
…
```

Policers can may be set to either remark or **drop** excess traffic

All markdown and/or mapping operations are configured through **table-maps**

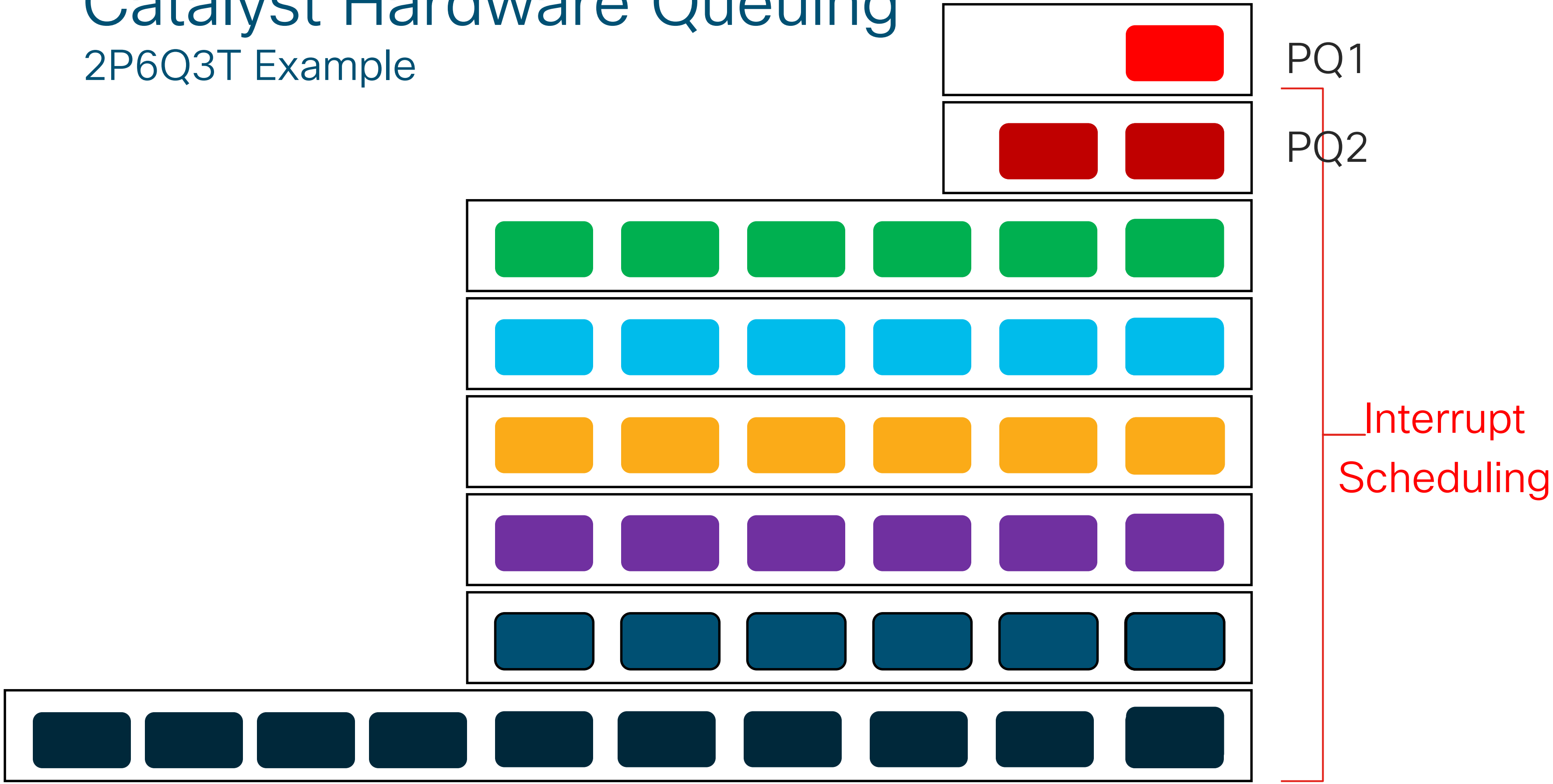
```
table-map TABLE-MAP
 map from 0 to 8
 map from 10 to 8
 map from 18 to 8
```

Policing to remark traffic is done by referencing the previously-configured **table-map**

```
[continued]
class TRANSACTIONAL-DATA
  set dscp af21
  police 10M conform-action transmit  exceed-action set-dscp-transmit dscp table TABLE-MAP
 class BULK-DATA
  set dscp af11
  police 100K conform-action transmit  exceed-action set-dscp-transmit dscp table TABLE-MAP
 class SCAVENGER
  set dscp cs1
  police 10M conform-action transmit  exceed-action drop
 class class-default
  set dscp default
  police 10M conform-action transmit  exceed-action set-dscp-transmit dscp table TABLE-MAP
```


Catalyst Hardware Queuing

2P6Q3T Example



Catalyst 9000 / 3850 / 3650

2P6Q3T with WTD or WRED: Wired Port Egress Queuing Model

Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

2P6Q3T	
EF	PQ Level 1 (10%)
CS5 CS4	PQ Level 2 (20%)
CS7 & CS6 CS3 & CS2	Q6 (BWR 10%)
AF4	Q5 (BWR 15% + DSCP-Based WTD or WRED)
AF3	Q4 (BWR 15% + DSCP-Based WTD or WRED)
AF2	Q3 (BWR 15% + DSCP-Based WTD or WRED)
AF1 CS1	Q2 (BWR 10% + DSCP-Based WTD or WRED)
DF	Q1 (BWR 35% + DSCP-Based WRED)

BWR = Bandwidth Remaining

WTD = Weighted Tail Drop

WRED = Weighted Random Early Detect

WRED supported on Catalyst 9000 Series only

Catalyst 9000 / 3850 / 3650

2P6Q3T with WTD or WRED: Wired Port Egress Queuing Class Maps

```
class-map match-any VOICE-PQ1
 match dscp ef
class-map match-any VIDEO-PQ2
 match dscp cs4
 match dscp cs5
class-map match-any CONTROL-MGMT-QUEUE
 match dscp cs7
 match dscp cs6
 match dscp cs3
 match dscp cs2
class-map match-any MULTIMEDIA-CONFERENCING-Q
 match dscp af41
 match dscp af42
 match dscp af43
…
```

```
[continued]
class-map match-any MULTIMEDIA-STREAMING-QUEUE
 match dscp af31
 match dscp af32
 match dscp af33
class-map match-any TRANSACTIONAL-DATA-QUEUE
 match dscp af21
 match dscp af22
 match dscp af23
class-map match-any SCAVENGER-BULK-DATA-QUEUE
 match dscp af11
 match dscp af12
 match dscp af13
 match dscp cs1
```


Catalyst 9000 / 3850 / 3650

2P6Q3T with WTD: Wired Port Egress Queuing – Policy Map

```
policy-map 2P6Q3T
 class VOICE-PQ1
  priority level 1
  police rate percent 10
  queue-buffers ratio 5
 class VIDEO-PQ2
  priority level 2
  police rate percent 23
  queue-buffers ratio 5
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 5
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 10
  queue-limit dscp af43 percent 80
  queue-limit dscp af42 percent 90
…
```

```
interface GigabitEthernet 1/0/2
 service-policy output 2P6Q3T
```

Two-levels of priority queuing are supported

Policer can be explicit or implicit

```
[continued]
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 10
  queue-limit dscp af33 percent 80
  queue-limit dscp af32 percent 90
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 10
  queue-limit dscp af23 percent 80
  queue-limit dscp af22 percent 90
 class SCAVENGER-BULK-DATA-QUEUE
  bandwidth remaining percent 7
  queue-buffers ratio 10
  queue-limit dscp values af13 cs1 percent 80
  queue-limit dscp values af12 percent 90
 class class-default
  bandwidth remaining percent 38
  queue-buffers ratio 25
```

If a PQ is enabled then non-PQs must use **bandwidth remaining**

Allocates buffers to queues

Enables DSCP-based WTD and tunes tail-drop percentages to align to AF PHBs

Catalyst 9000 (ONLY)

2P6Q3T with DSCP-Based WRED: Wired Port Egress Queuing – Policy Map

```
policy-map 2P6Q3T-WRED
 class VOICE-PQ1
  priority level 1
  police rate percent 10
  queue-buffers ratio 5
 class VIDEO-PQ2
  priority level 2
  police rate percent 23
  queue-buffers ratio 5
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 5
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 15
  queue-limit dscp af43 percent 80
  queue-limit dscp af42 percent 90
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 10
  queue-limit dscp af33 percent 80
  queue-limit dscp af32 percent 90
```

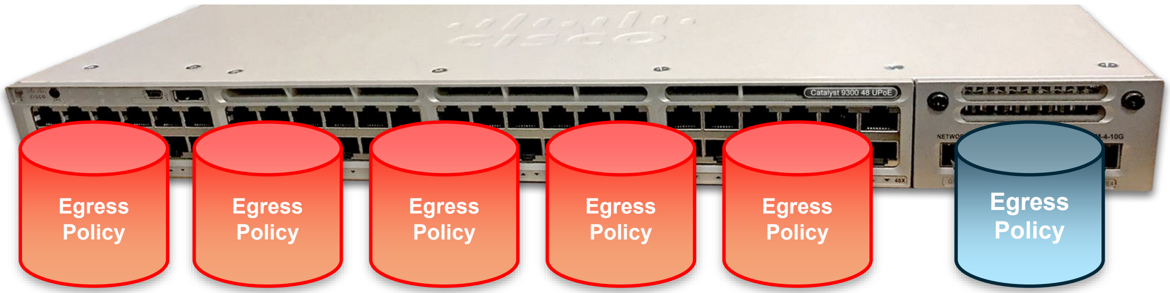
```
class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp af21 percent 80 100
  random-detect dscp af22 percent 70 100
  random-detect dscp af23 percent 60 100
 class SCAVENGER-BULK-DATA-QUEUE
  bandwidth remaining percent 7
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 8 percent 60 100
  random-detect dscp 10 percent 80 100
  random-detect dscp 12 percent 70 100
  random-detect dscp 14 percent 60 100
 class class-default
  bandwidth remaining percent 38
  queue-buffers ratio 25
  random-detect dscp-based
  random-detect dscp default percent 80 100
```

Enables DSCP-based WRED for the queue

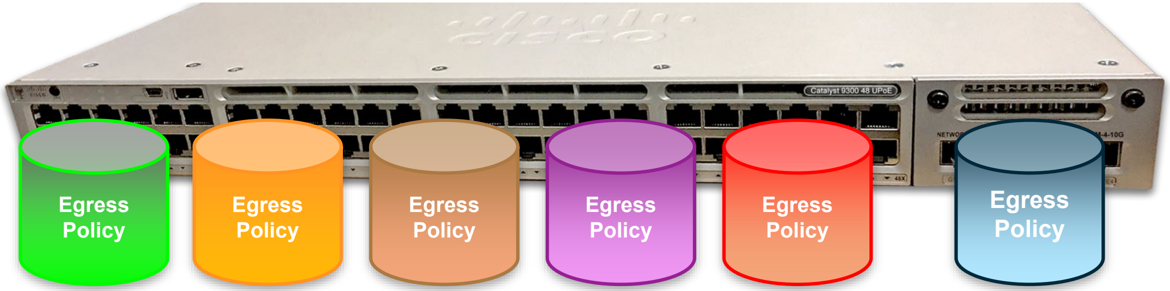
Tunes min and max values of the three drop thresholds to align to AF PHBs

```
interface GigabitEthernet 1/0/3
 service-policy output 2P6Q3T-WRED
```


Catalyst 9000 Series Per-port Policy Allocation



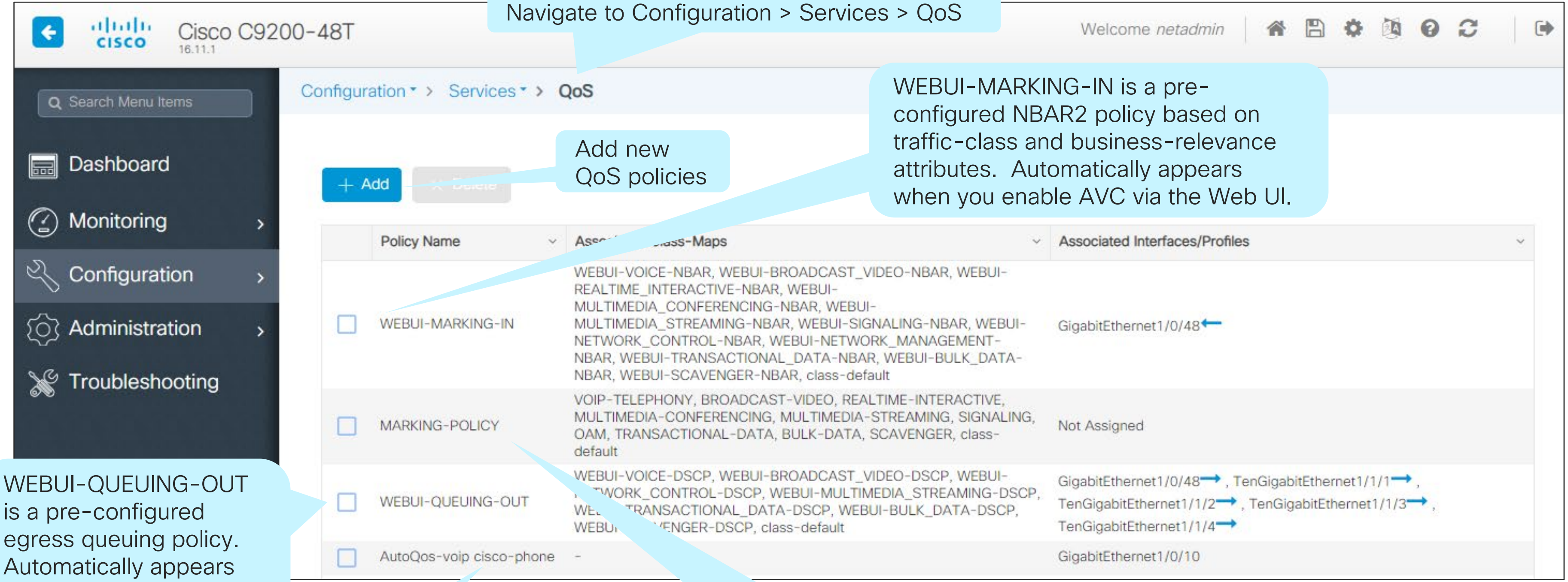
- Catalyst 3850 / 3650 Series supports two egress policies
  - All built-in front panel ports need to share the same egress queueing policy
  - All ports on network modules need to share the same egress queueing policy



- Catalyst 9000 Series supports per port egress policy which adds a lot flexibility

QoS Policy via the Catalyst 9000 Series Web UI

Navigate to Configuration > Services > QoS



Add new QoS policies

WEBUI-MARKING-IN is a pre-configured NBAR2 policy based on traffic-class and business-relevance attributes. Automatically appears when you enable AVC via the Web UI.

WEBUI-QUEUING-OUT is a pre-configured egress queuing policy. Automatically appears when you enable AVC via the Web UI.

Auto QoS policies

Custom QoS policies – AVC/NBAR2 or User Defined (DSCP or ACL)

Additional slides showing QoS configuration using the Catalyst 9000 Series Web UI are in Appendix F

Catalyst 9000 Series QoS Design—At-A-Glance

Cisco Catalyst 9000 Series QoS Design

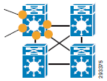
Roles in Campus Network

The Catalyst 9300 & 9400 Series switches are engineered to serve as access-layer switches in campus networks. As such, these switches may connect directly to a variety of endpoints and aggregation-layer switches, as shown in Figure 1.

Figure 1 Cisco Catalyst 9300 & 9400 Series Switches in a Campus Network

The Catalyst 9500 Series switches are engineered to serve as core or aggregation-layer switches in campus networks. As such, these switches may connect directly to other core, aggregation-layer, or access-layer switches, as shown in Figure 2.

Figure 2 Cisco Catalyst 9500 Series Switches in a Campus Network



Trust DSCP
+ Egress Queuing

QoS Design Steps

There are two main steps to configure QoS on Cisco Catalyst 9000 Series switches:

1. Configure Ingress QoS Model(s):
   - Trust DSCP Model
   - Conditional Trust Model
   - Service Policy Models
2. Configure Egress Queuing
   - Queuing Models: 8Q3T, 1P7Q3T or 2P6Q3T

Step 1: Configure Ingress QoS Model(s)

The three most utilized ingress QoS models for campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Combinations of these ingress QoS models may be used at the same time.

Trust DSCP Model

Switch ports on the Catalyst 9000 Series default to a trusted state (shown as orange circles in Figures 1 and 2).

Conditional Trust Model

The Conditional Trust model configures the interface to dynamically accept markings from endpoints that have met a specific condition, such as a successful CDP negotiation (switch ports set to conditional trust are shown as green circles in Figure 1).

This model is suitable for switch ports connecting to:

- Cisco IP phones - **trust device cisco-phone**
- Cisco TelePresence Systems - **trust device cts**
- Cisco IP Video Surveillance cameras - **trust device ip-camera**
- Cisco Digital Media Players - **trust device media-player**

This model is also suitable for PCs and untrusted devices, since the ports connecting to such devices will remain in their default untrusted state (shown as black circles in Figure 1).

Service Policy Models

There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

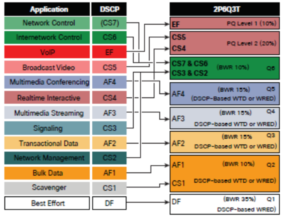
- **class-maps** which identify the flows using packet markings, access-lists, NBAR2 classification, or other criteria
- **policy-maps** which specify policy actions to be taken on a class-by-class basis
- **service-policy** statements which apply a specific policy-map to an interface(s) and specify direction

On the Catalyst 9300 Series, service policies may be applied to switch ports (shown as red circles in Figure 1).

Step 2: Configure Egress Queuing for Switch Ports

Switch ports can be configured with an 8Q3T, 1P7Q3T, or 2P6Q3T egress queuing model. The only difference between the models is the number of priority queues configured via the **prioritylevel 1** or **priority level 2** policy-map action commands.

Figure 3 Cisco Catalyst 9000 Series 2P6Q3T Egress Queuing Model



Both WRED and WTD are supported on Catalyst 9000 Series switches. WRED can be applied on up to four queues only. Additional queues can implement WTD if desired.

IOS XE 16.8.1 AVC / NBAR2 Policy Example

An example design for a Catalyst 9000 Series in the role of an access-layer switch in a campus network, using **match protocol attribute** commands and DSCP-based WRED is presented below.

Step 1: Configure Ingress QoS Model :

Trust DSCP Model:
Switch Ports : <default>

Conditional Trust Model:

```
trust device cisco-phone or
trust device cts or
trust device ip-camera or
trust device media-player
```

Note: Yellow highlighted commands are interface specific; otherwise these are global.

Service Policy Models:

```
class-map match-all VOICE
 match protocol attribute traffic-class voip-telephony
 match protocol attribute business-relevance business-relevant
class-map match-all BROADCAST-VIDEO
 match protocol attribute traffic-class broadcast-video
 match protocol attribute business-relevance business-relevant
class-map match-all REAL-TIME-INTERACTIVE
 match protocol attribute traffic-class real-time-interactive
 match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-CONFERENCING
 match protocol attribute traffic-class multimedia-conferencing
 match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-STREAMING
 match protocol attribute traffic-class multimedia-streaming
 match protocol attribute business-relevance business-relevant
class-map match-all SIGNALING
 match protocol attribute traffic-class signaling
 match protocol attribute business-relevance business-relevant
class-map match-all NETWORK-CONTROL
 match protocol attribute traffic-class network-control
 match protocol attribute business-relevance business-relevant
class-map match-all NETWORK-MANAGEMENT
 match protocol attribute traffic-class ops-admin-mgmt
 match protocol attribute business-relevance business-relevant
class-map match-all TRANSACTIONAL-DATA
 match protocol attribute traffic-class transactional-data
 match protocol attribute business-relevance business-relevant
class-map match-all BULK-DATA
 match protocol attribute traffic-class bulk-data
 match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER
 match protocol attribute business-relevance business-irrelevant

policy-map NBAR-MARKING
 class VOICE
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
[Continued...]
```

```
class REAL-TIME-INTERACTIVE
  set dscp cs4
class MULTIMEDIA-CONFERENCING
  set dscp af41
 class MULTIMEDIA-STREAMING
 set dscp af31
class SIGNALING
  set dscp cs3
 class NETWORK-CONTROL
  set dscp cs6
 class NETWORK-MANAGEMENT
  set dscp cs2
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
```

Switch Port Application:

```
interface GigabitEthernet 1/0/1
 service-policy input NBAR-MARKING
```

Step 2: Configure 8Q3T, 1P7Q3T or 2P6Q3T Egress Queuing on Switch Ports (2P6Q3T Example with WRED is shown) :

```
class-map match-any VOICE-PQ1
 match dscp ef
class-map match-any VIDEO-PQ2
 match dscp cs4
 match dscp cs5
class-map match-any CONTROL-MGMT-QUEUE
 match dscp cs7
 match dscp cs6
 match dscp cs3
 match dscp cs2
class-map match-any MULTIMEDIA-
CONFERENCING-QUEUE
 match dscp af41
 match dscp af42
 match dscp af43
class-map match-any MULTIMEDIA-STREAMING-
QUEUE
 match dscp af31
 match dscp af32
 match dscp af33
[Continued...]
```

```
class-map match-any TRANSACTIONAL-DATA-QUEUE
 match dscp af21
 match dscp af22
 match dscp af23
class-map match-any SCAVENGER-BULK-DATA-QUEUE
 match dscp af11
 match dscp af12
 match dscp af13
 match dscp cs1

policy-map 2P6Q3T-WRED
 class VOICE-PQ1
  priority level 1
  police rate percent 10
 class VIDEO-PQ2
  priority level 2
  police rate percent 20
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 15
  queue-limit dscp af43 percent 80
  queue-limit dscp af42 percent 90
class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 10
  queue-limit dscp af33 percent 80
  queue-limit dscp af32 percent 90
class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 18 percent 80 100
  random-detect dscp 20 percent 70 100
  random-detect dscp 22 percent 60 100
 class SCAVENGER-BULK-DATA-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
  random-detect dscp-based
  random-detect dscp 8 percent 60 100
  random-detect dscp 10 percent 80 100
  random-detect dscp 12 percent 70 100
  random-detect dscp 14 percent 60 100
 class class-default
  bandwidth remaining percent 35
  queue-buffers ratio 25
  random-detect dscp-based
  random-detect dscp 0 percent 80 100
```

Switch Port Application:

```
interface GigabitEthernet 1/0/1
 service-policy output 2P6Q3T-WRED
```


Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

Catalyst 3650 / 3850 QoS Design—At-A-Glance

Cisco Catalyst 3650/3850 QoS Design

At-A-Glance

Role in Campus Network

The Catalyst 3650/3850 series switches are engineered to serve as a converged access switch in wired and wireless campus networks. As such, these switches may connect directly to a variety of endpoints and distribution-layer switches, as shown in Figure 1.

Figure 1 **Cisco Catalyst 3650/3850 Switch in a Campus Network**

QoS Design Steps

There are two main steps to configure QoS on Cisco Catalyst 3650/3850 series switches:

1. Configure Ingress QoS Model(s):
   - Trust DSCP Model
   - Conditional Trust Model (wired ports only)
   - Service Policy Models
2. Configure Egress Queuing
   - Wired Queuing Models: 1P7Q3T or 2P6Q3T
   - Wireless Queuing Model: 2P2Q+AFD

Step 1: Configure Ingress QoS Model(s)

The three most utilized ingress QoS models for campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Combinations of these ingress QoS models may be used at the same time.

Trust DSCP Model

Wired ports on the Catalyst 3650/3850 default to a trusted state (shown as orange circles in Figure 1), but wireless ports default to an untrusted state. Nonetheless, wireless ports can also be configured to be trusted by the global configuration command: **no qos wireless-default-untrust**

Conditional Trust Model

The Conditional Trust model configures the interface to dynamically accept markings from endpoints that have met a specific condition, such as a successful CDP negotiation (switch ports set to conditional trust are shown as green circles in Figure 1).

This model is suitable for switch ports connecting to:

- Cisco IP phones—**trust device cisco-phone**
- Cisco TelePresence Systems—**trust device cts**
- Cisco IP Video Surveillance cameras—**trust device ip-camera**
- Cisco Digital Media Players—**trust device media-player**

This model is also suitable for PCs and untrusted devices, since the ports connecting to such devices will remain in their default untrusted state (shown as black circles in Figure 1).

Service Policy Models

There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

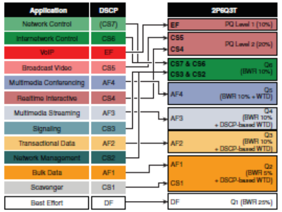
- **class-maps** which identify the flows using packet markings or by access-lists or other criteria
- **policy-maps** which specify policy actions to be taken on a class-by-class basis
- **service-policy** statements which apply a specific policy-map to an interface(s) and specify direction

On the Catalyst 3650/3850, service policies may be applied to wired or wireless ports (shown as red circles in Figure 1) or to individual wireless clients (shown as purple circles in Figure 1).

Step 2a: Configure Egress Queuing for Wired Ports

Wired ports can be configured with either a 1P7Q3T or 2P6Q3T egress queuing model. The only difference between the two models is whether a second priority queue is configured via the **priority level 2** policy-map action command.

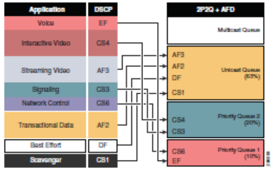
Figure 2 **Catalyst 3650/3850 2P6Q3T (Wired Port) Egress Queuing Model**



Step 2b: Configure Egress Queuing for Wireless Ports

The Catalyst 3650/3850 switch supports two levels of priority queueing on wireless ports, as well as one non-priority queue for unicast traffic and one non-priority queue for multicast traffic. The switch also supports a bandwidth control algorithm, Approximate Fair Drop (AFD), to provide fairness between radios, SSIDs, and even individual clients

Figure 3 **Catalyst 3650/3850 2P2Q+AFD (Wireless Port) Egress Queuing Model**



Cisco Validated Design (CVD)

The Cisco Validated Designs for a Catalyst 3650/3850 series switch in the role of a converged access switch in a campus network are presented below.

Step 1: Configure Ingress QoS Model :

Trust DSCP Model:
Wired Ports : <default>
Wireless Ports:

```
no qos wireless-default-untrust
```

Conditional Trust Model:

```
trust device cisco-phone or
trust device cts or
trust device ip-camera or
mls qos trust device media-player
```

Service Policy Models:

```
[class-maps omitted for brevity]

policy-map MARKER
 class VOIP
  set dscp ef
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class SIGNALING
  set dscp cs3
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class DEFAULT
  set dscp default
```

Wired Port Application:

```
interface GigabitEthernet 1/0/1
 service-policy input MARKER
```

Wireless SSID Application:

```
wlan WLAN-1
 service-policy input MARKER
```

Per-Wireless-Client Application:

```
wlan WLAN-1
 service-policy client input MARKER
```

Step 2a: Configure 1P7Q3T or 2P6Q3T Egress Queuing on Wired Ports (2P6Q3T Example is shown) :

```
policy-map 2P6Q3T
 class PRIORITY-QUEUE
  priority level 1
  police rate percent 10
 class REAL-TIME-VIDEO-QUEUE
  priority level 2
  police rate percent 20
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
  queue-limit dscp af43 percent 80
  queue-limit dscp af42 percent 90
  queue-limit dscp af41 percent 100
class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
  queue-limit dscp af33 percent 80
  queue-limit dscp af32 percent 90
  queue-limit dscp af31 percent 100
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
  queue-limit dscp af23 percent 80
  queue-limit dscp af22 percent 90
  queue-limit dscp af21 percent 100
 class BULK-SCAVENGER-DATA-QUEUE
  bandwidth remaining percent 5
  queue-buffers ratio 10
  queue-limit dscp values af13 cs1 percent 80
  queue-limit dscp values af12 percent 90
  queue-limit dscp values af11 percent 100
 class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25

Wired Port Application:
interface GigabitEthernet 1/0/1
 service-policy output 2P6Q3T
```

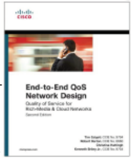
Step 2b: Configure 2P2Q+AFD Egress Queuing on Wireless Ports :

```
policy-map port_child_policy
 class non-client-nrt-class
  bandwidth remaining ratio 7
 class RT1
  priority level 1
  police rate percent 10
     conform-action transmit
     exceed-action drop
 class RT2
  priority level 2
  police rate percent 20
     conform-action transmit
     exceed-action drop
 class class-default
  bandwidth remaining ratio 63
```

Note: This policy is applied automatically to all wireless ports and thus no explicit service-policy attachment statement is needed.

Note: Highlighted commands are interface specific; otherwise these are global.

For more details, see the Cisco Press book: **End-to-End QoS Design** (Second Edition)-Chapter 20



Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

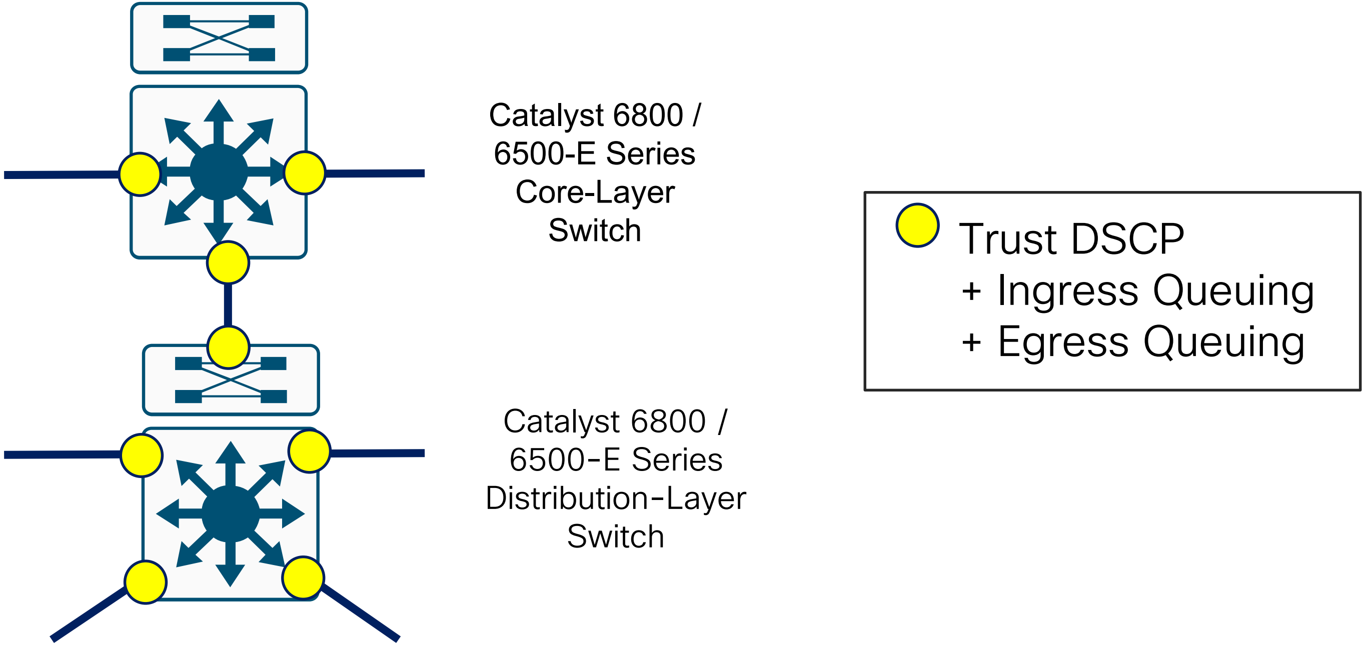
Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Cisco Catalyst 6800 & 6500-E QoS Design

Cisco Catalyst 6800 / 6500-E

QoS Roles in the Campus



Cisco Catalyst 6800 / 6500-E

QoS Design Steps

1. Configure Ingress Queuing
2. Configure Egress Queuing

Catalyst 6800 / 6500-E (Sup6T & Sup2T) are C3PL platforms which trust by default. Therefore no explicit policy is required for DSCP trust.

Cisco Catalyst 6800 / 6500-E

2P6Q4T Ingress & Egress Queuing Models–DSCP-to-Queue

Additional Catalyst 6800 / 6500-E Sup2T/6T queuing models are detailed in Appendix A.

Application-Class	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

2P6Q4T	
EF	Voice-PQ1 (Priority Level 1) (10%)
CS5 CS4	Video-PQ2 (Priority Level 2) (20%)
CS6 & CS7 CS2 & CS3	Control/Mgmt Queue (10% BWR)
AF4	Multimedia-Conferencing Queue (15% BWR + DSCP-WRED)
AF3	Multimedia-Streaming Queue (15% BWR + DSCP-WRED)
AF2	Transactional Data Queue (15% BWR + DSCP-WRED)
AF1 CS1	Bulk Data Queue (10% BWR + DSCP-WRED)
DF	Default Queue (WRED)

Ingress and egress queuing models varies by line card / module.

Refer to the 6500-E / 6800 QoS Configuration Guide or data sheets to ensure that you use the proper queuing module for a given line card.

WS-X6904-40G-2T
WS-X6904-40G-2TXL
C6800-8P10G
C6800-8P10G-XL
C6800-16P10G
C6800-16P10G-XL
C6800-32P10G
C6800-32P10G-XL

http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-1SY/config_guide/sup2T/15_1_sy_swcg_2T/qos_policy_based_queueing.html

Cisco Catalyst 6800 / 6500-E –2P6Q4T Model

Part 1 of 3–Common Ingress & Egress Queuing Class-Maps

```
class-map type lan-queuing match-all VOICE-PQ1
 match dscp ef
class-map type lan-queuing match-all VIDEO-PQ2
 match dscp cs4 cs5
class-map type lan-queuing match-all CONTROL-MGMT-QUEUE
 match dscp cs2 cs3 cs6 cs7
class-map type lan-queuing match-all MULTIMEDIA-CONFERENCING-QUEUE
 match dscp af41 af42 af43
class-map type lan-queuing match-all MULTIMEDIA-STREAMING-QUEUE
 match dscp af31 af32 af33
class-map type lan-queuing match-all TRANSACTIONAL-DATA-QUEUE
 match dscp af21 af22 af23
class-map type lan-queuing match-all SCAVENGER-BULK-DATA-QUEUE
 match dscp cs1 af11 af12 af13
```

Class-maps and policy-maps used for ingress and/or egress queuing policies must be explicitly configured as **type lan-queuing**

Unless specified otherwise, the default C3PL class-map and policy-map **type** is **qos** (classification, marking, policing)

Cisco Catalyst 6800 / 6500-E –2P6Q4T Model

Part 2 of 3–2P6Q4T Queuing Policy-Map

Policy-map must be defined as **type lan-queuing**

```
policy-map type lan-queuing 2P6Q4T
 class VOICE-PQ1
  priority level 1
 class VIDEO-PQ2
  priority level 2
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 15
  random-detect dscp af41 percent 80 100
  random-detect dscp af42 percent 70 100
  random-detect dscp af43 percent 60 100
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 15
  random-detect dscp af31 percent 80 100
  random-detect dscp af32 percent 70 100
  random-detect dscp af33 percent 60 100
…
```

Enables egress Priority Queue 1 (highest level of service)

Enables egress Priority Queue 2 (can only be interrupted by PQ1)

bandwidth remaining is required (as PQs are enabled)

Tunes WRED to better align to the AF PHB

Cisco Catalyst 6800 / 6500-E –2P6Q4T Model

Part 3 of 3–2P6Q4T Queuing Policy-Map (continued)

```
[continued]
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  random-detect dscp-based
  random-detect dscp af21 percent 80 100
  random-detect dscp af22 percent 70 100
  random-detect dscp af23 percent 60 100
 class BULK-DATA-QUEUE
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect dscp af11 percent 80 100
  random-detect dscp af12 percent 70 100
  random-detect dscp cs1 percent 50 100
class class-default
  random-detect dscp-based
  random-detect dscp default percent 80 100
```

```
 service-policy type lan-queuing input 2P6Q4T
 service-policy type lan-queuing output 2P6Q4T
```

type lan-queuing must also be specified in the service-policy statement

Generally Catalyst 6800 / 6500-E Series linecards which support the 2P6Q4T queuing structure also support both ingress and egress queuing

Catalyst 6800/6500-E Sup 6T/2T QoS Design At-A-Glance

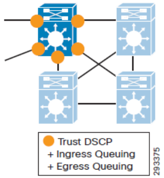
Cisco Catalyst 6800 / 6500-E (Supervisor 6T or 2T) QoS Design

At-A-Glance

Role in Campus Network

The Cisco Catalyst 6800 / 6500-E Series switches with Supervisor 6T or 2T are well-suited to the role of distribution or core-layer switches in campus networks. As such, these switches typically connect directly to other switches or routers, as shown in Figure 1.

Figure 1 Cisco Catalyst 6800 / 6500-E Supervisor 6T or 2T Switches in a Campus Network



QoS Design Steps

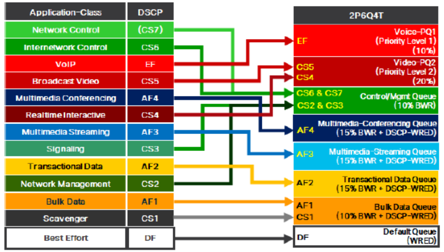
There are two main steps to configure QoS on Cisco Catalyst 6800 / 6500E Series switches with Supervisor 2T:

1. Configure Ingress Queuing
2. Configure Egress Queuing

Steps 1 & 2: Configure Ingress & Egress Queuing:

The 2P6Q4T queuing model for both ingress and egress queuing for the Cisco Catalyst 6800 / 6500-E with Supervisor 6T or 2T is shown in Figure 2.

Figure 2 Catalyst 6800 / 6500-E Sup 6T or 2T (2P6Q4T) Ingress & Egress Queuing Model



EtherChannel QoS

Ingress classification & marking QoS policies on the Cisco Catalyst 6800 /6500-E are configured on the logical port-channel interface (typically these are simply to enable DSCP trust, which is enabled by default on the Sup 6T or 2T). Ingress and egress queuing QoS policies are configured on the physical port-member interfaces.

Cisco Validated Design (CVD)

The Cisco Validated Design for Cisco Catalyst 6800 / 6500-E Series switches with Supervisor 6T or 2T in the role of a distribution or core-layer switch in a campus network is presented below.

Campus Cisco Catalyst 6800 / 6500-E Supervisor 6T or 2T QoS Design

At-A-Glance

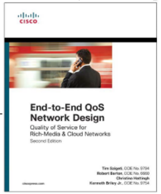
Step 1: Configure (Common) Class-Maps to be used for both Ingress & Egress Queuing Policies

```
class-map type lan-queuing VOICE-PQ1
 match dscp ef
class-map type lan-queuing VIDEO-PQ2
 match dscp cs4 cs5
class-map type lan-queuing CONTROL-MGMT-QUEUE
 match dscp cs2 cs3 cs6 cs7
class-map type lan-queuing MULTIMEDIA-CONFERENCING-QUEUE
 match dscp af41 af42 af43
class-map type lan-queuing MULTIMEDIA-STREAMING-QUEUE
 match dscp af31 af32 af33
class-map type lan-queuing TRANSACTIONAL-DATA-QUEUE
 match dscp af21 af22 af23
class-map type lan-queuing SCAVENGER-BULK-DATA-QUEUE
 match dscp cs1 af11 af12 af13
```

Step 2 Configure 2P6Q4T Ingress & Egress Queuing Policy-Map and apply to Interface(s)

```
policy-map type lan-queuing 2P6Q4T
 class VOICE-PQ1
  priority level 1
 class VIDEO-PQ2
  priority level 2
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 15
  random-detect dscp af41 percent 80 100
  random-detect dscp af42 percent 70 100
  random-detect dscp af43 percent 60 100
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 15
  random-detect dscp af31 percent 80 100
  random-detect dscp af32 percent 70 100
  random-detect dscp af33 percent 60 100
  class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  random-detect dscp-based
  random-detect dscp af21 percent 80 100
  random-detect dscp af22 percent 70 100
  random-detect dscp af23 percent 60 100
 class BULK-DATA-QUEUE
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect dscp af11 percent 80 100
  random-detect dscp af12 percent 70 100
  random-detect dscp cs1 percent 50 100
class class-default
  random-detect dscp-based
  random-detect dscp default percent 80 100

service-policy type lan-queuing input 2P6Q4T
service-policy type lan-queuing output 2P6Q4T
```

Note: Highlighted commands are interface specific; otherwise these are global



For more details, see Campus QoS Design 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html

Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

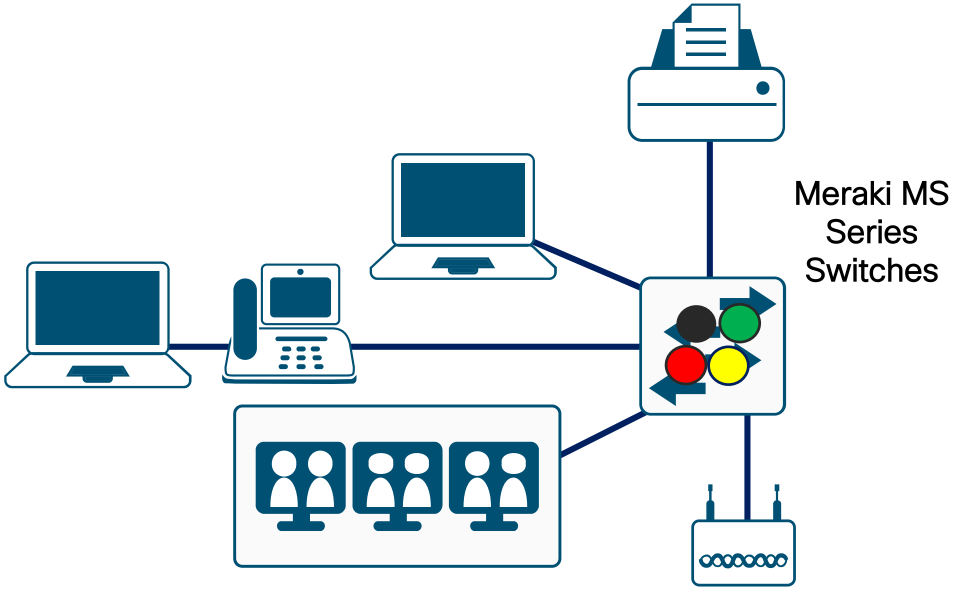
Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Meraki MS Series Switch QoS Design

Meraki MS Series Switches

QoS Role in the Campus



QoS on Meraki switches is configured at the Network level, and applies to all switches in the Meraki Network

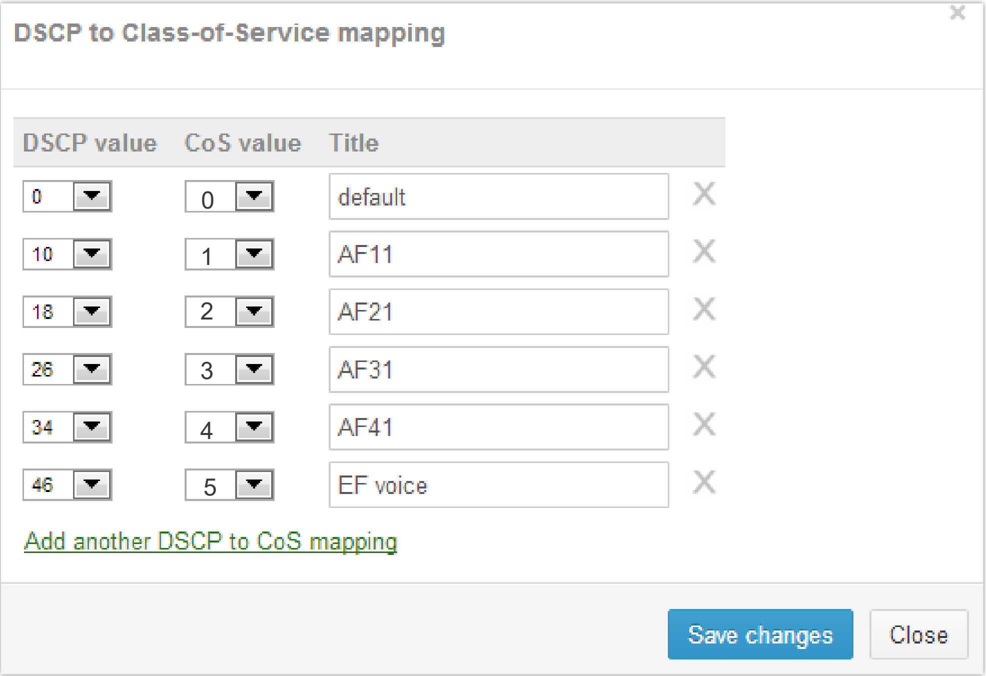
- No Trust
- Ingress Classification/Marking
- Trust DSCP
- Egress Queuing

Meraki MS Series Switch QoS

DSCP to CoS Map

- DSCP markings of incoming packets are mapped to one of the six configurable **CoS queues** on the switch for forwarding
- Multiple DSCP values can be mapped to the same CoS queue
- DSCP values do not have to be assigned to every CoS queue

Switch > Configure > Switch Settings



https://documentation.meraki.com/MS/Other_Topics/MS_Switch_Quality_of_Service_Defined

Meraki MS Series Switch QoS

- Each CoS queue is assigned a weight which determines the ratio of bandwidth assigned to the queue
- QoS guarantees a certain fraction of the uplink to each configured queue when the link is congested
- If a queue is not fully utilized, the bandwidth will be used by other queues
- Note: Meraki MS Series switches do not support strict priority queuing

Cos	Weight
0 (default class)	1
1	2
2	4
3	8
4	16
5	32

Meraki MS Series Switch QoS

Dashboard QoS Rules for the Network

	VLAN	Protocol	Source port	Destination port	DSCP	Edit DSCP to CoS map
1	100	Any			Trust incoming DSCP	
2	200	TCP	Any	6000	Set DSCP to...	26 → class 2 (AF31)

- Rules are user defined and processed from top to bottom
- A rule can apply to any combination of VLAN, protocol, source port, or destination port
  - Meraki MS120 Series switches support QoS rules based on IP range only
- Each rule has one of the following actions – Trust or Set the DSCP marking
- As soon as the first QoS rule is added, the switch will trust DSCP markings on incoming packets that have DSCP to CoS mappings. This rule is invisible and processed last.
- If an incoming packet has a DSCP marking set but no matching QoS rule or DSCP to CoS mapping, it will be placed in the default queue

Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Campus WLAN QoS Design Considerations and Best Practices

The Case for Wireless QoS

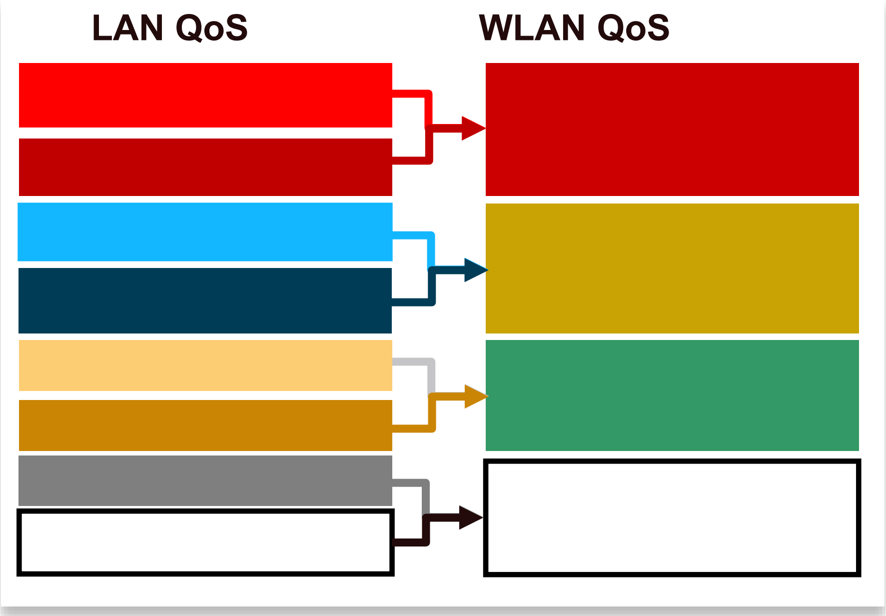
- QoS is like a chain
  - It's only as strong as its weakest link
- The WLAN is one of the weakest links in enterprise QoS designs for three primary reasons:

  1) Typical downshift in speed (and throughput)
  2) Shift from full-duplex to half-duplex media
  3) Shift from dedicated media to shared media

- WLAN QoS policies control *both* jitter and packet loss

Wireless QoS-Specific Limitations

- No priority servicing
- No bandwidth guarantees
- Non-deterministic media access
- Only 4 levels of service



Know Your Tools

- IEEE 802.11
  - User Priorities (UP)
  - Access Categories (AC)
  - Arbitration Inter-frame Spacing (AIFS)
  - Contention Windows (CW)
  - Enhanced Distributed Coordination Function (EDCF)
- DSCP←→UP Mapping
- Trust Boundaries
- Policy-Enforcement Points
- Application Visibility and Control (AVC)

IEEE 802.11 User Priority (UP)

2	2	6	6	6	2	0 or 6	0 or 2	n	4
Frame control	Dur	A1	A2	A3	Seq control	A4	QoS control	Body	FCS

3 Bit Field allows for UP values 0-7

IEEE 802.11 UP Values and Access Categories

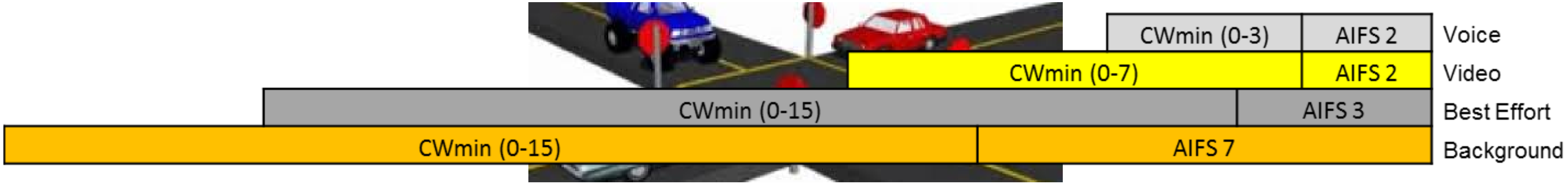
802.11 UP Value	802.11 Access Category	WMM Designation
7	AC_VO	Voice
6		
5	AC_VI	Video
4		
3	AC_BE	Best Effort
0		
2	AC_BK	Background
1		

IEEE 802.11 Arbitration Inter-Frame Spacing (AIFS) and Contention Windows (CW)

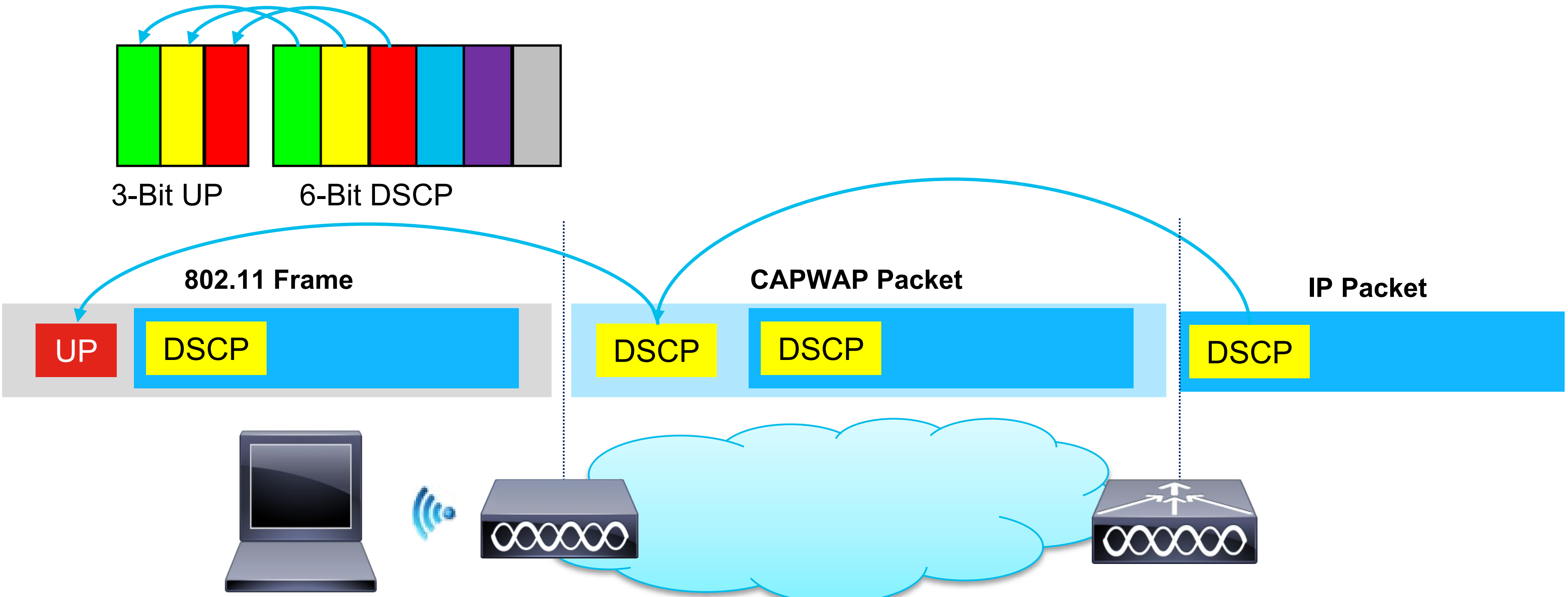
- Due to the nature of wireless as a shared media, a Congestion Avoidance algorithm (CSMA/CA) must be utilized
- Wireless senders have to wait a ***fixed amount of time*** (the AIFS)
- Wireless senders also have to wait a ***random amount of time*** (the Contention Window)
- AIFS and Contention Window timers vary by Access Category

Access Category	AIFS (Slot Times)
Voice	2
Video	2
Best Effort	3
Background	7

Access Category	CWmin (Slot Times)	CWmax (Slot Times)
Voice	3	7
Video	7	15
Best-Effort	15	1023
Background	15	1023



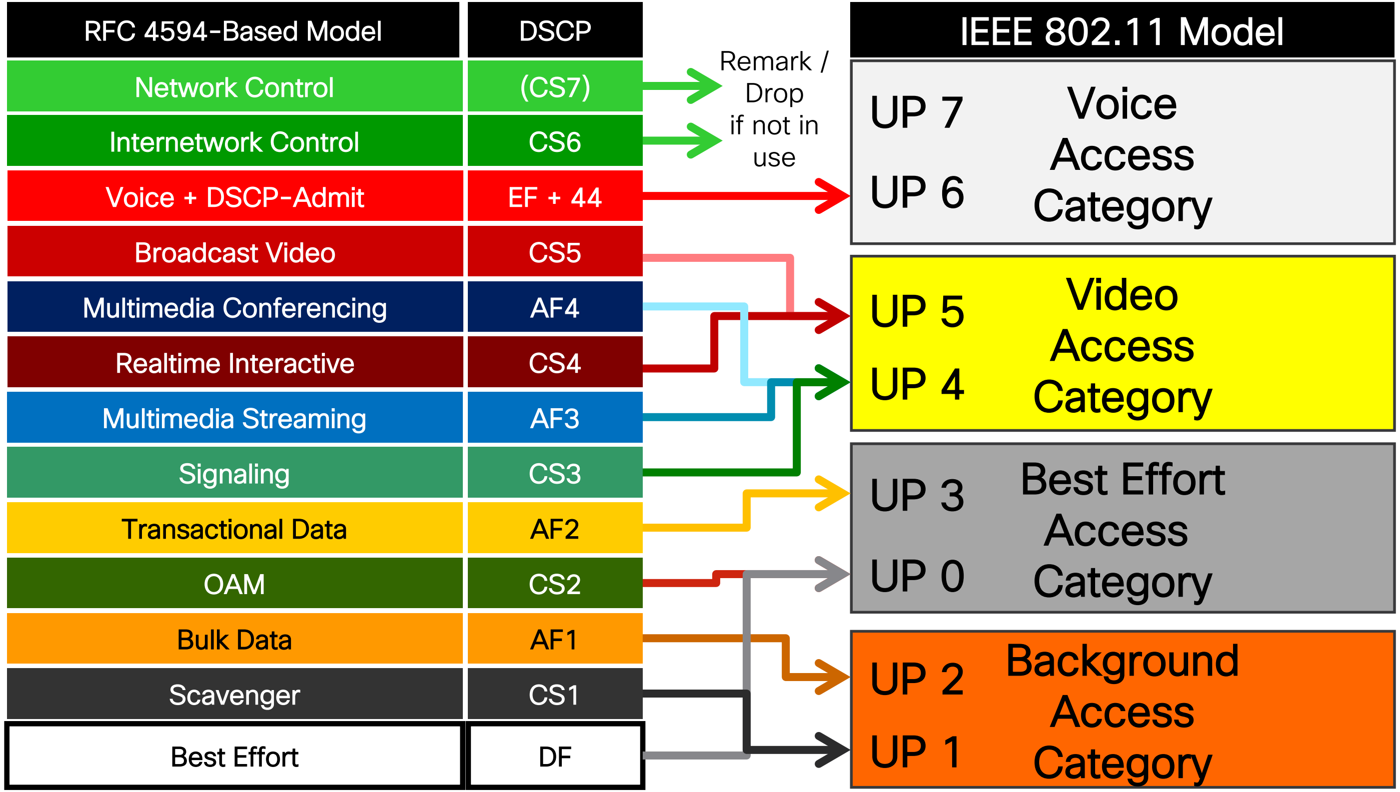
Downstream DSCP-to-UP **Default** Mapping



Downstream DSCP-to-UP Mapping Model

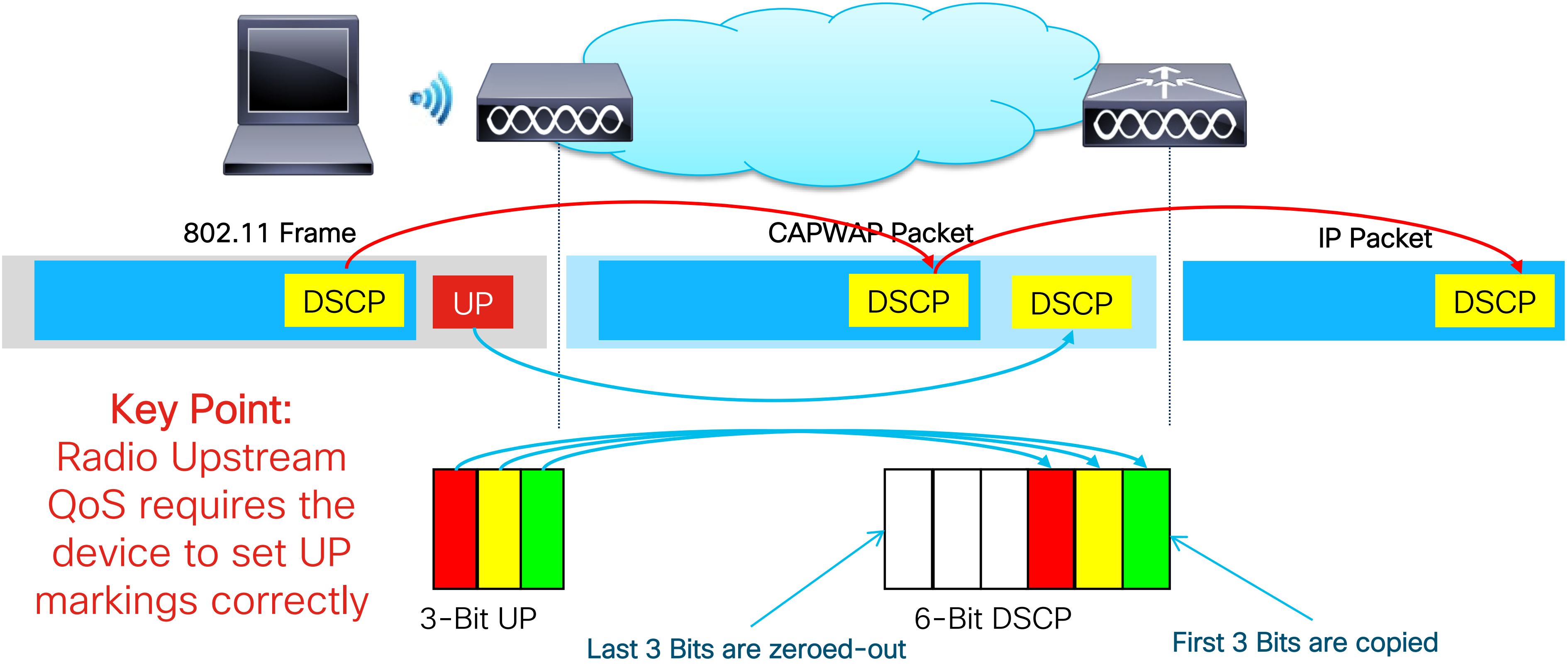
Ratified Cisco Consensus Model (June 2015)

- Provides distinction between elastic and inelastic video classes
- Aligns RFC 4594 recommendations into the IEEE 802.11 model
- Requires several custom DSCP-to-UP mappings



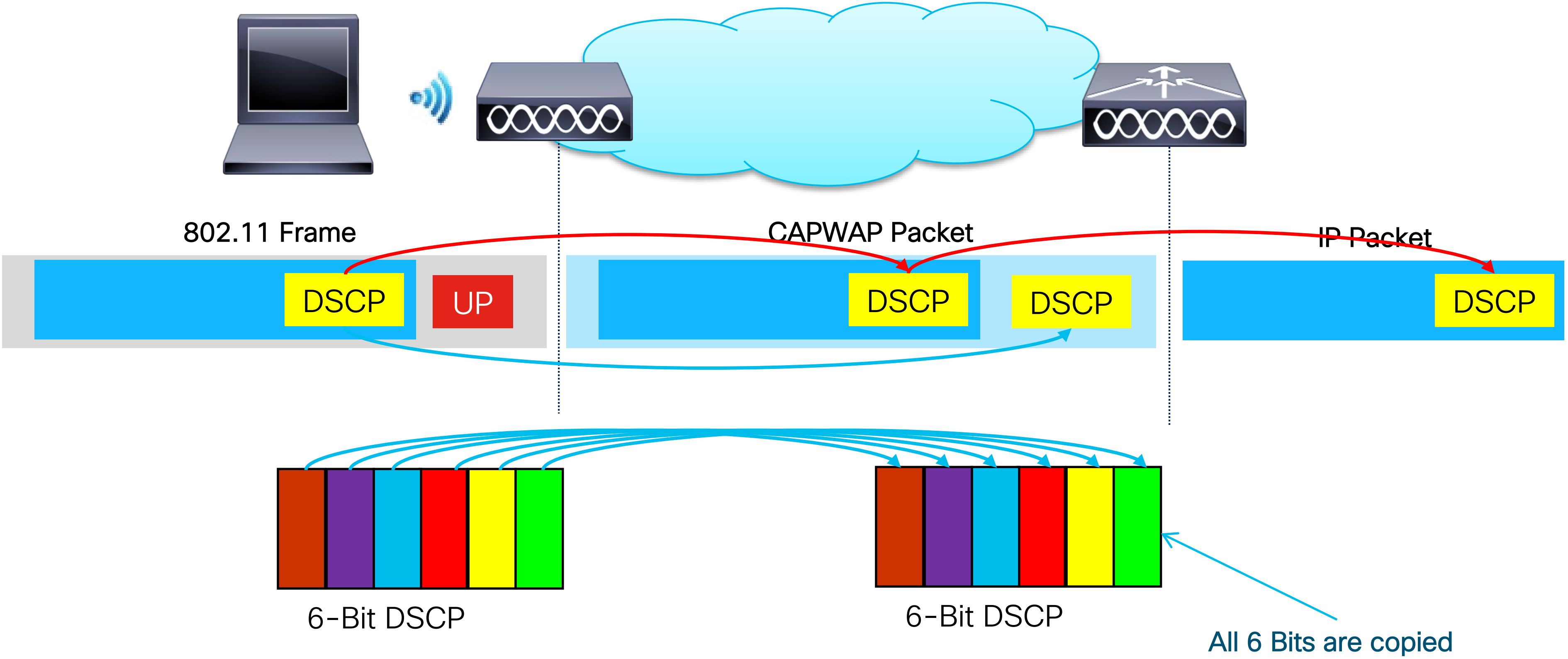
cisco Live!

Upstream UP-to-DSCP **Default** Mapping



Key Point:
Radio Upstream QoS requires the device to set UP markings correctly

Upstream DSCP Trust Model



RFC 8325 – Mapping DiffServ to IEEE 802.11

- Reconciles RFC 4594 with IEEE 802.11
- Summarizes our internal consensus on DSCP-to-UP mapping
- Advocates DSCP-trust in the upstream direction (vs. UP-to-DSCP mapping)

https://tools.ietf.org/html/rfc8325

Internet Engineering Task Force (IETF)
Request for Comments: 8325
Category: Standards Track
ISSN: 2070-1721
February 2018

T. Szigeti
J. Henry
Cisco Systems
F. Baker

Mapping Diffserv to IEEE 802.11

Abstract

As Internet traffic is increasingly sourced from and destined to wireless endpoints, it is crucial that Quality of Service (QoS) be aligned between wired and wireless networks; however, this is not always the case by default. This document specifies a set of mappings from Differentiated Services Code Point (DSCP) to IEEE 802.11 User Priority (UP) to reconcile the marking recommendations offered by the IETF and the IEEE so as to maintain consistent QoS treatment between wired and IEEE 802.11 wireless networks.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc8325.

Cisco WLAN QoS Design At-A-Glance

The Case for QoS in the Wireless LAN

Wireless access points are the second most-likely places in the enterprise network to experience congestion (after LAN-to-WAN links). This is because wireless media:
- is generally presents a downshift in speed/throughput
- is a half-duplex media
- is a shared media

Furthermore, the nature of wireless media presents additional challenges from a QoS provisioning perspective, including:
- No support for strict priority queuing
- No support for guaranteed bandwidth allocations
- Non-deterministic media access
- A maximum of four levels of service

As such, the case for QoS on the WLAN is to minimize packet drops due to congestion, as well as to minimize jitter due to non-deterministic access to the half-duplex, shared media.

WLAN QoS Design Best Practices

Four QoS design principles that apply to WLAN deployments include:
- Classify and mark applications as close to their sources as technically and administratively possible
- Police unwanted traffic flows as close to their sources as possible
- Enable queuing policies at every node where the potential for congestion exists

WLAN QoS Design Considerations

There are several considerations unique to WLANs that must be factored into QoS designs:
- The IEEE 802.11e Enhanced Distributed Coordination Function (EDCF), including:
  - User Priorities
  - Access Categories
  - Arbitration Inter-Frame Spaces (AIFS)
  - Contention Windows (CW)
  - EDCF Operation
  - Transmission Opportunity (TXOP)
  - Transmission Specification (TSpec)
- UP-to-DSCP and DSCP-to-UP Mapping

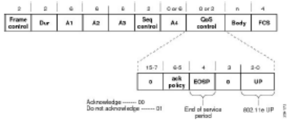
IEEE 802.11e EDCF

The original 802.11 standard described a Distributed Coordination Function (DCF) to avoid collisions over the WLAN. However, this function had no support for QoS. In 2006, the 802.11e task group provided several enhancements to this function to support QoS, hence the term: Enhanced Distributed Coordination Function (EDCF). These enhancements include:

User Priorities (UP)

802.11e introduced a 3 bit marking value in layer 2 wireless frames referred to as User Priority (UP); UP values range from 0-7. UP fields are showin in Figure 1.

Figure 1 IEEE 802.11e User Priority Field



Access Categories (AC)

Pairs of UP values are assigned to 4 access categories, which statistically equate to 4 distinct levels of service over the WLAN. Access categories and their UP pairings are shown in Figure 2.

Figure 2 IEEE 802.11e Access Categories

802.11e UP Value	802.11e Access Category	WMM Designation	Cisco AireOS WLC Designation
7	AC_VO	Voice	Platinum
6			
5	AC_VI	Video	Gold
4			
3	AC_BE	Best Effort	Silver
0			
2	AC_BK	Background	Bronze
1			

Arbitration Interframe Spaces (AIFS)

Each wireless station was wait a fixed (and a variable) amount of time once the medium is clear prior to attempting to transmit. The fixed amount of time is called the AIFS. EDCF skewed these fixed delays on a per-access category basis, such that higher-priority ACs are assigned shorter wait times as compared to the lower-priority ACs. This approach thus gives the high-priority traffic better probability of being transmitted first. AIFS by access category are shown in Figure 3.

Figure 3 IEEE 802.11e AIFS by Access Category

Access Category	AIFS (Slot Times)
Voice	2
Video	2
Best Effort	3
Background	7

Contention Windows

If two or more wireless devices begin transmitting after waiting only a fixed amount of time after the air is clear (the AIFS), then the probability of collisions would be high. However, in addition to waiting a fixed amount of time, each station must also wait a variable amount of time, called a random backoff. The range for these random backoffs is between 0 and the current size of the Contention Window (CW). The CW can increase over time, but begins at an initial minimum value (CWmin). The values for CWmin are skewed by access categories, as are the maximum values for Contention Windows (the CWmax values), as shown in Figure 4.

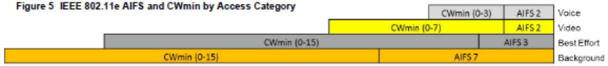
Figure 4 IEEE 802.11e Contention Windows by AC

Access Category	CWmin (Slot Times)	CWmax (Slot Times)
Voice	3	7
Video	7	15
Best-Effort	15	1023
Background	15	1023

EDCF Operation

When the AIFS and random backoff timers are combined, then the skewing of the probability of transmission of each access categories becomes even more apparent, as shown in Figure 5 (right).

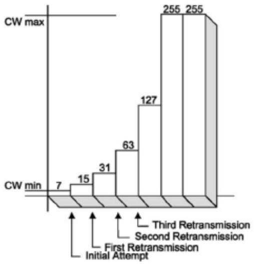
Figure 5 IEEE 802.11e AIFS and CWmin by Access Category



Each wireless station (including the access point, which is competing on equal terms with endpoint devices for airtime) waits until all timers have elapsed before attempting transmission. Statistically, any endpoint transmitting voice traffic will have a better chance at being the next to use the media; however, this is not guaranteed, because of the random value of the CW timers.

If in the event that two (or more) stations still begin transmitting at the same time, then all stations will effectively double their CW sizes and try again. This process repeats (as needed) until the CWmax value for an AC is reached. At this point, Contention Windows remain fixed at the CWmax size until a defined transmission attempt limit is reached (e.g. on Cisco APs this limit is 64 transmission attempts). This operation is shown in Figure 6.

Figure 6 Contention Window Operation



Transmission Opportunity (TXOP)

EDCF provides contention-free period access to the wireless medium, called the Transmission Opportunity (TOXP). The TXOP is a set period of time when a wireless station may send as many frames as possible without having to contend with other stations. With TXOP, each station has a set time limit when it can transmit; once this limt expires, it must give up access to the medium.

Transmission Specification (TSpec)

One last major enhancement introduced by 802.11e is a mechanism for Call Admission Control (CAC) called Transmission Specification (TSpec). TSpec allows real-time applications, such as voice or video calls in-progress, to be prioritized over requests for new calls. To use this feature of EDCF, TSpec must be configured on the AP and optionally on the client stations.

DSCP-to-UP and UP-to-DSCP Mapping

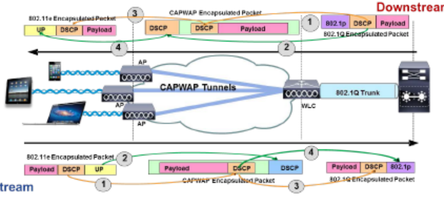
Upstream and downstream DSCP<>UP mapping is shown in Figure 7. By default, 6-bit DSCP values are mapped to 3-bit 802.11e UP values by taking the three Most-Significant Bits (MSB) of the DSCP and copying these as UP values. For example, DSCP EF/46 (binary **101**110) is mapped to CoS or UP 5 (binary **101**), by default.

Conversely, in the reverse direction, the CoS or UP values are simply multiplied by 8 (in order to shift these three binary bits to the left) to generate a DSCP value. Continuing the example, UP 5 (binary **101**) would be mapped (i.e., multiplied by 8) to DSCP 40 (binary **101**000), also referred to as Class Selector 5 (CS5).

As can be seen in the above pair of examples, because information is being truncated from 6-bits to 3-bits, marking details can get lost in translation. In this example, the original voice packet was sent with DSCP EF, but was received as DSCP CS5 (based solely on default Layer 2-to-Layer 3 mapping). This needs to be taken into account when mapping from wired-to-wireless and vice-versa.

Also, it bears explicit mention that (Layer 2) IEEE and (Layer 3) IETF marking recommendations do not always align. For example, DSCP EF/46 is recommended by the IETF for use for voice, which would map by default to UP 5; but the IEEE designates UP 6 for voice. Similarly, the IETF recommends DSCP CS4 or AF4 for real-time or interactive video conferencing, both of which would map by default to UP 4; but the IEEE designates UP 5 for video. Such discrepancies must also be taken into account and reconciled in WLAN QoS designs

Figure 7 Downstream (DSCP-to-UP) Mapping & Upstream (UP-to-DSCP) Mapping



For more details, see the AVC/QoS Design chapter of the BYOD CVD at: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_AVC.html
And/or the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 18

Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

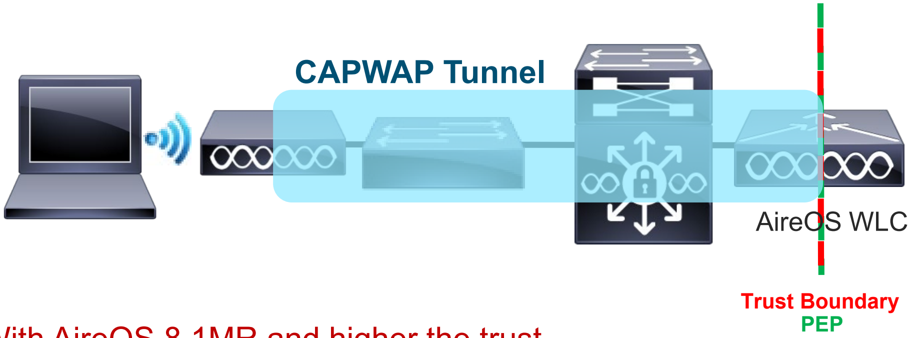
Cisco AireOS WLC AVC/QoS Design

Cisco AireOS WLC

QoS Roles in the Wireless LAN – Centralized Mode

- Customizable DSCP←→UP Mappings (AireOS 8.1MR and higher) modify the QoS Roles of the AP and WLC:
  - Trust Boundary moves to the AP
  - PEP remains at the WLC

Centralized Deployment Model



With AireOS 8.1MR and higher the trust-boundary can be extended to the AP

Cisco AireOS WLC

QoS Design Steps

1. Tune EDCA and CAC
2. Select and Tune the WLAN QoS Profile
3. Configure an AVC Profile
4. Apply the QoS and AVC Profile to the WLAN and Enable Application Visibility
5. Modify default DSCP-to-UP mappings and enable Upstream DSCP-Trust

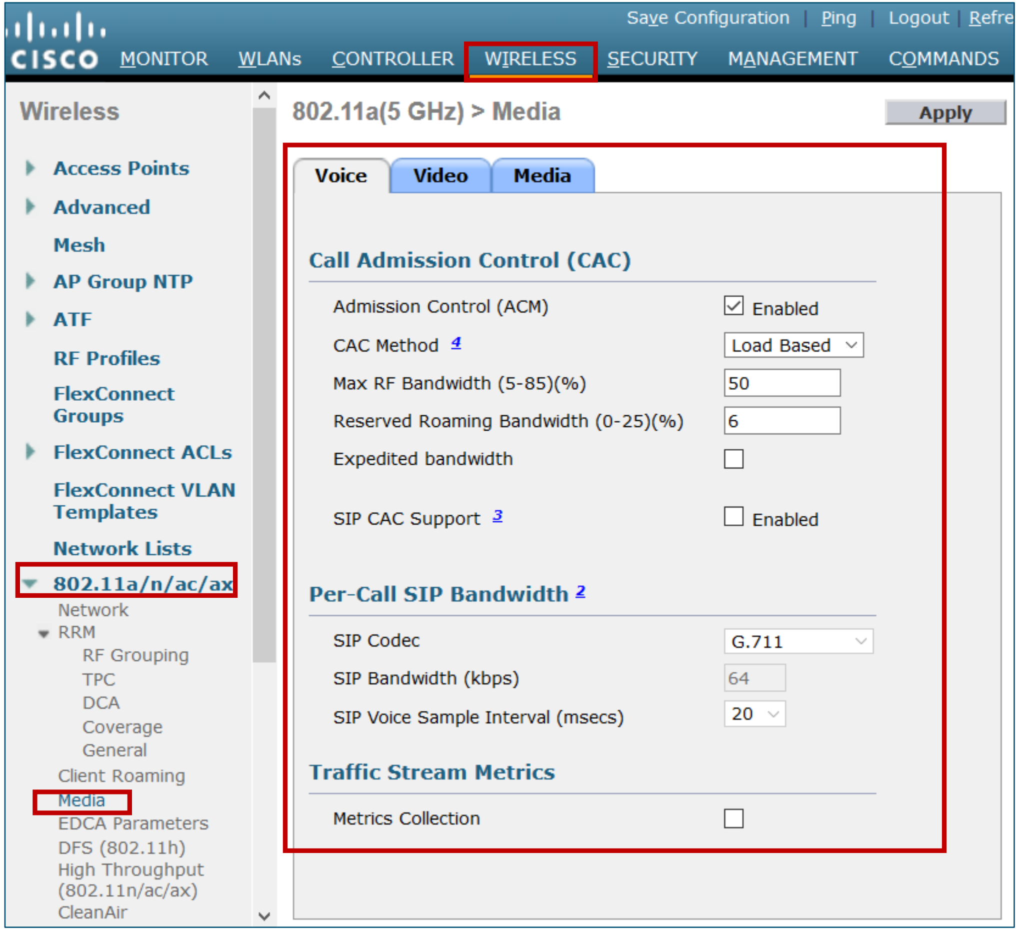
AireOS – EDCA Profiles

EDCA Profiles control access to the wireless media through differentiated contention window (aCWmin & aCWmax), arbitrated interframe space (AIFS), and transmit opportunity (TXOP) settings for each of the access categories (AC_VO, AC_VI, AC_BE, AC_BK)

- Tunable for each radio (5 GHz & 2.4 GHz)
- Radio must be disabled before changing EDCA Profile
- Navigate to **Wireless > 802.11a/n/ac/ax** or **802.11g/n/ax > EDCA Parameters**
- Select the EDCA Profile
  - WMM (Default Setting)
  - Spectralink Voice Priority
  - Voice Optimized
  - Voice & Video Optimized
  - Custom Voice
  - Customized
  - Fastlane

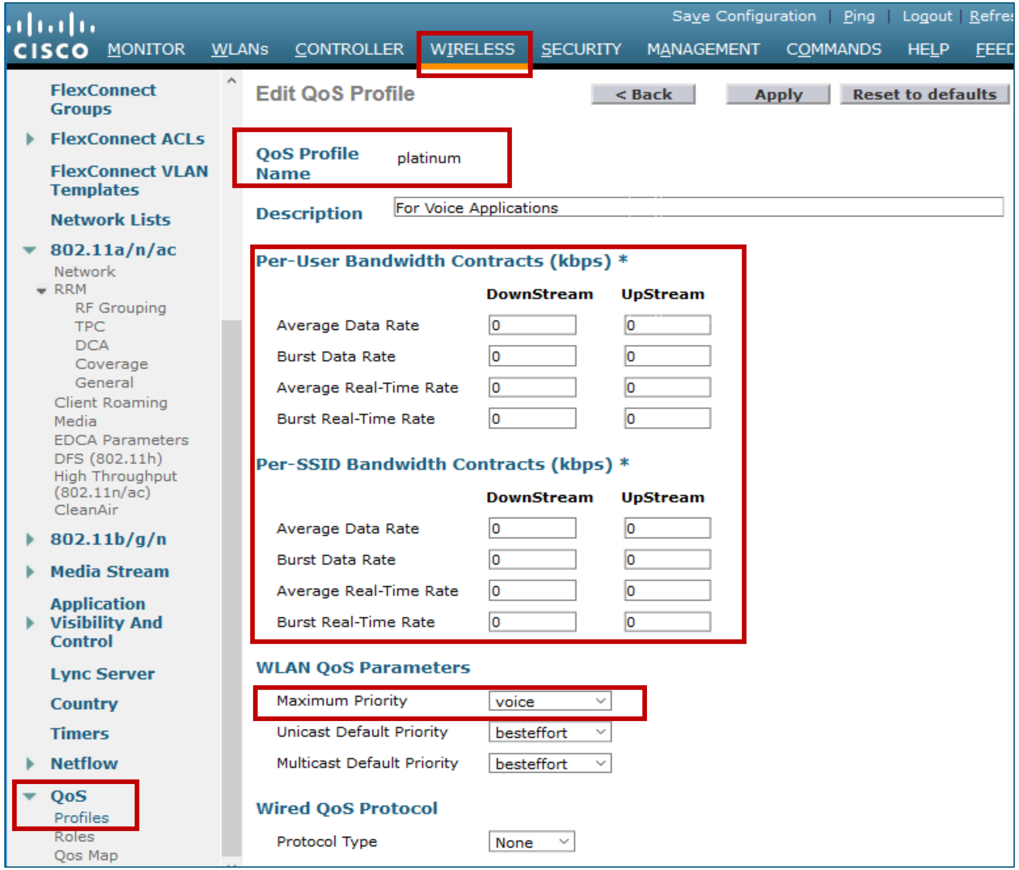
AireOS – CAC

- Supported for Voice, Video, & Media
- Tune for each radio (5 GHz & 2.4 GHz)
- Radio must be disabled before changing CAC settings
- Navigate to **Wireless > 802.11a/n/ac/ax** or **802.11g/n/ax > Media > Voice, Video,** or **Media**
- Load Based CAC takes into account channel loading impact due to interference, other APs, etc. as well as client traffic
- SIP CAC Support is for wireless stations that do not support TSPEC-based admission control



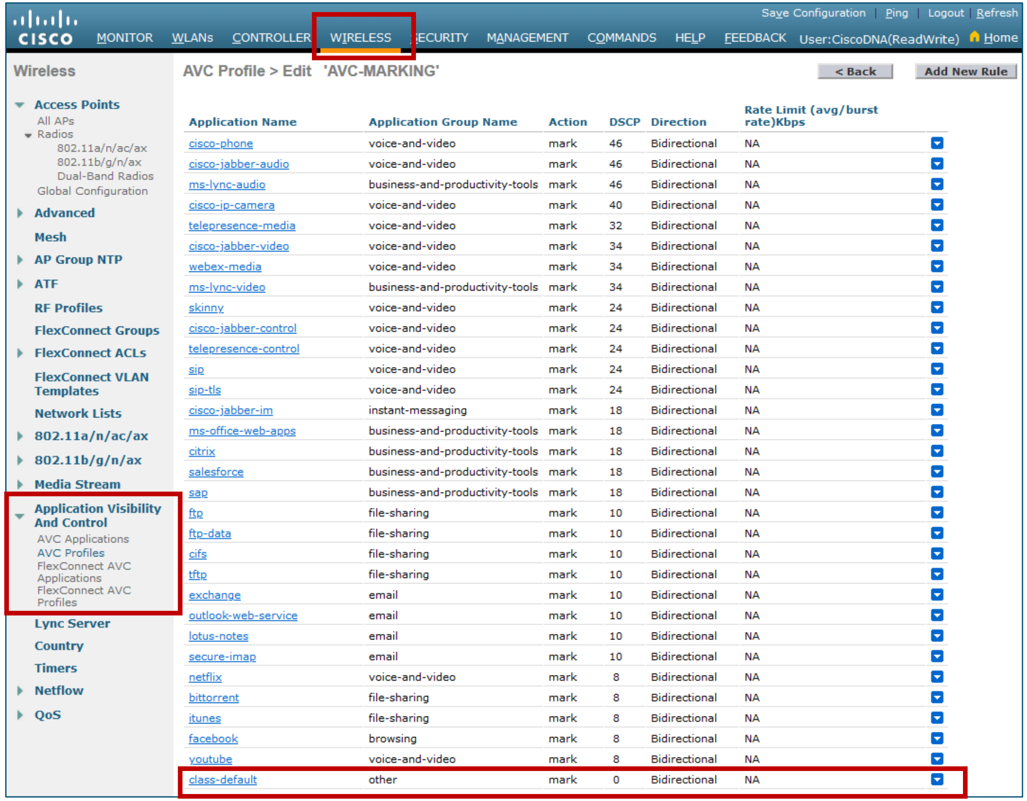
AireOS – QoS Profiles (Precious Metals)

- Platinum, Gold, Silver or Bronze templates which can be applied to WLANs
- The main purpose of the QoS profile is to limit the maximum DSCP allowed and thus limit the 802.11 UP value.
- Per-User or Per-SSID rate limiting
  - Real-Time (UDP) & non-Real-Time (TCP) flows
  - Upstream & Downstream Rates
- Maximum Priority setting controls the maximum DSCP marking of traffic in the CAPWAP header. Unicast/Multicast default is the marking used for non WMM packets
- The Maximum Priority setting should be in alignment with the AVC Profile



AireOS AVC & FlexConnect AVC Profiles

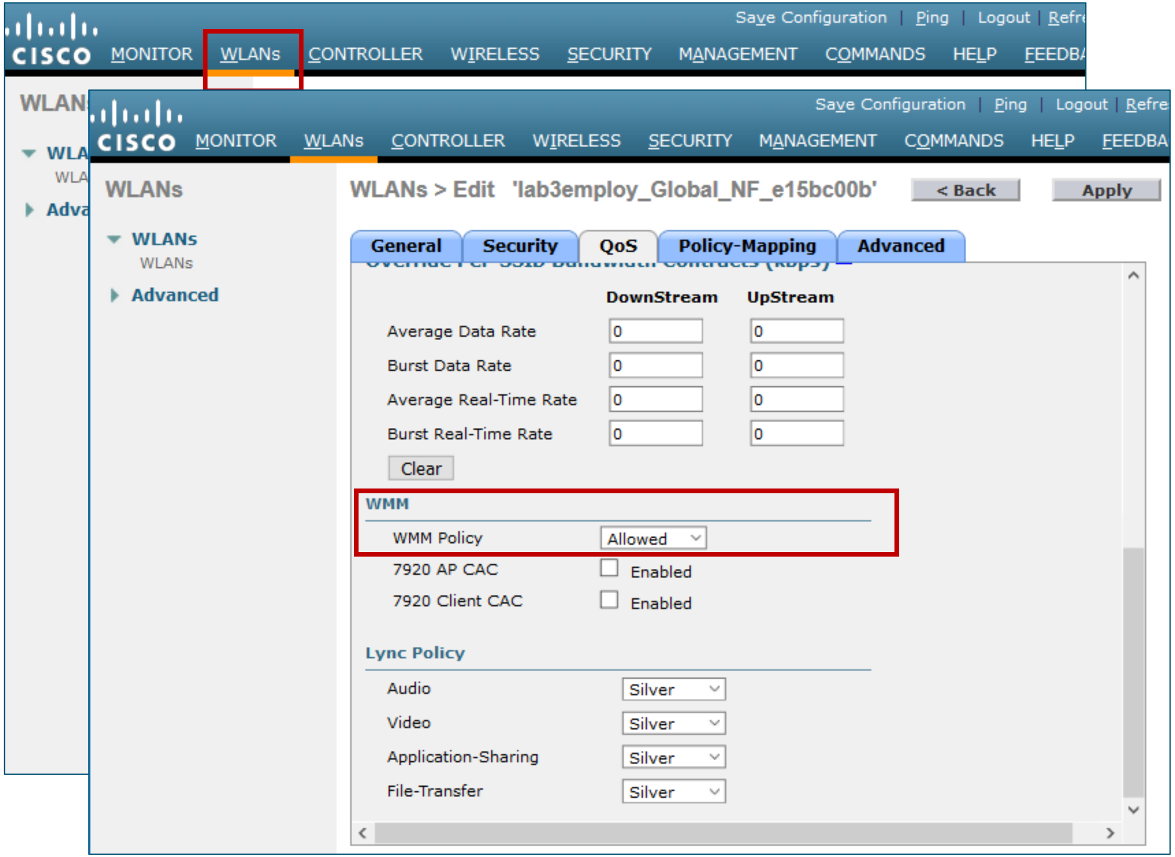
- NBAR-based policies
  - NBAR versions are generally different between the WLC (AVC Profiles) and the AP (FlexConnect Profiles)
- Up to 32 application rules per profile
- Actions of Mark, Drop, or Rate-limit
  - Marking can be Upstream, Downstream, or Bidirectional
  - Up to 3 applications can be rate-limited
- AireOS 8.8 and higher allows a “class-default” rule with marking action applied to all apps which do not match a previous rule
- AVC profiles modify the DSCP markings of the original packet. QoS Profiles modify the DSCP markings of the outer CAPWAP header.
  - Align AVC Profiles with QoS Profiles



Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
cisco-phone	voice-and-video	mark	46	Bidirectional	NA
cisco-jabber-audio	voice-and-video	mark	46	Bidirectional	NA
ms-lync-audio	business-and-productivity-tools	mark	46	Bidirectional	NA
cisco-ip-camera	voice-and-video	mark	40	Bidirectional	NA
telepresence-media	voice-and-video	mark	32	Bidirectional	NA
cisco-jabber-video	voice-and-video	mark	34	Bidirectional	NA
webex-media	voice-and-video	mark	34	Bidirectional	NA
ms-lync-video	business-and-productivity-tools	mark	34	Bidirectional	NA
skinny	voice-and-video	mark	24	Bidirectional	NA
cisco-jabber-control	voice-and-video	mark	24	Bidirectional	NA
telepresence-control	voice-and-video	mark	24	Bidirectional	NA
sip	voice-and-video	mark	24	Bidirectional	NA
sip-tls	voice-and-video	mark	24	Bidirectional	NA
cisco-jabber-im	instant-messaging	mark	18	Bidirectional	NA
ms-office-web-apps	business-and-productivity-tools	mark	18	Bidirectional	NA
citrix	business-and-productivity-tools	mark	18	Bidirectional	NA
salesforce	business-and-productivity-tools	mark	18	Bidirectional	NA
sap	business-and-productivity-tools	mark	18	Bidirectional	NA
ftp	file-sharing	mark	10	Bidirectional	NA
ftp-data	file-sharing	mark	10	Bidirectional	NA
cifs	file-sharing	mark	10	Bidirectional	NA
tftp	file-sharing	mark	10	Bidirectional	NA
exchange	email	mark	10	Bidirectional	NA
outlook-web-service	email	mark	10	Bidirectional	NA
lotus-notes	email	mark	10	Bidirectional	NA
secure-imap	email	mark	10	Bidirectional	NA
netflix	voice-and-video	mark	8	Bidirectional	NA
bittorrent	file-sharing	mark	8	Bidirectional	NA
itunes	file-sharing	mark	8	Bidirectional	NA
facebook	browsing	mark	8	Bidirectional	NA
youtube	voice-and-video	mark	8	Bidirectional	NA
class-default	other	mark	0	Bidirectional	NA

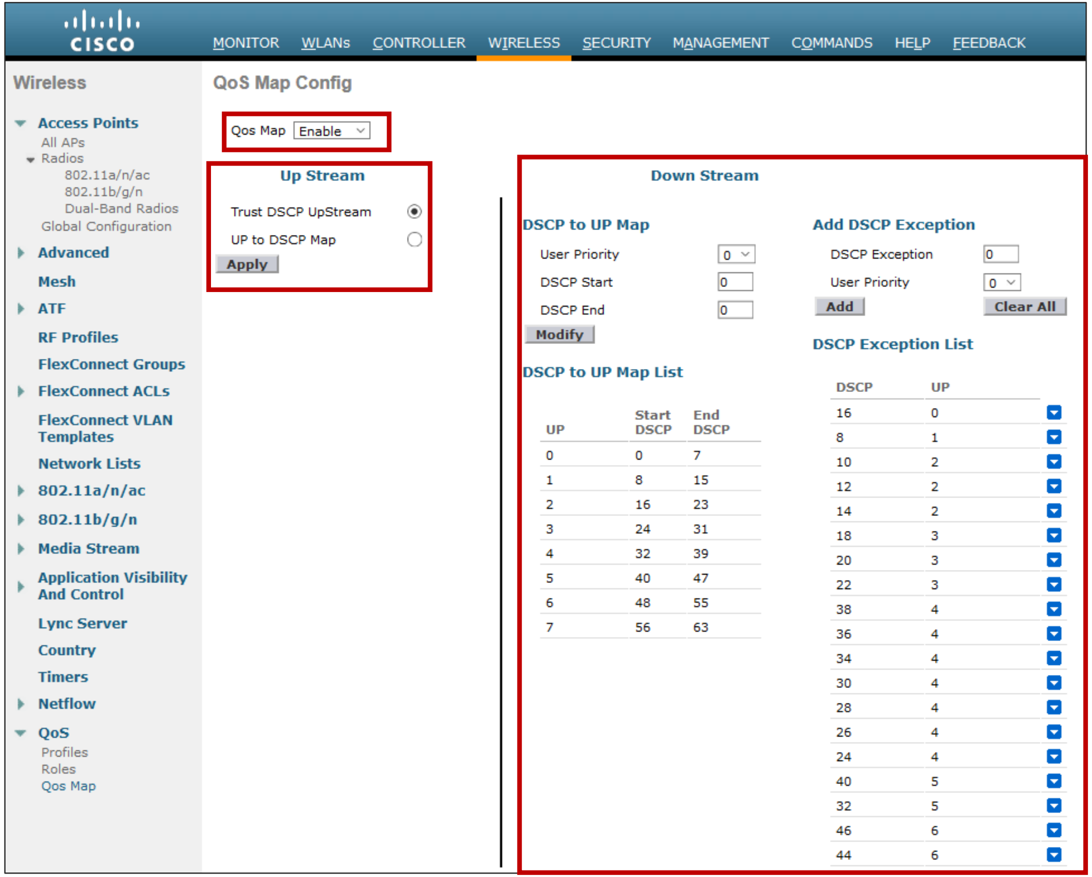
AireOS – Applying QoS & AVC Profiles to WLANs

- Navigate to **WLANs**, select the **WLAN ID**, and select the **QoS** tab
- Select the QoS Profile to apply to the WLAN
- Enable Application Visibility and select the AVC Profile to apply to the WLAN
- You can override per-user and per-SSID rate limiting for the WLAN if you choose
- Set the WMM Policy on the WLAN
  - Disabled
  - Allowed
  - Required



AireOS – DSCP-to-UP Mapping & DSCP Trust

- Disable the QoS Map to change the mappings
- Upstream configuration
  - Trust DSCP UpStream (recommended)
  - UP to DSCP Map
    - A table will appear allowing you to choose the mappings
- Downstream configuration
  - Configure the DSCP to UP Map ranges
  - Add DSCP Exceptions to the map
- Re-enable the QoS Map



Cisco AirOS QoS Design At-A-Glance

AireOS Wireless LAN Controller AVC/QoS Design

At-A-Glance

Role in Wireless Campus Network

Cisco AireOS wireless LAN controllers centrally manage QoS policies on wireless LAN access points, as well as perform advanced QoS operations, such as Application Visibility and Control (AVC) classification, marking and policing.

QoS Design Steps

There are three main steps required to configure AVC/QoS on AireOS WLCs:

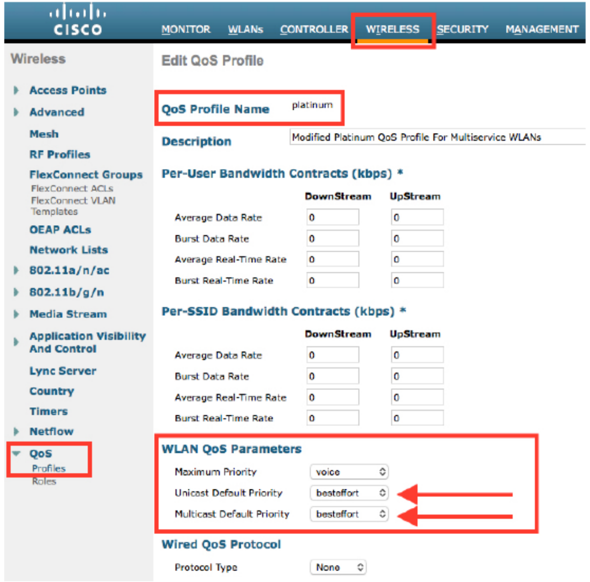
1. Select and tune the desired QoS Profile
2. Configure an AVC Profile
3. Apply the QoS and AVC Profiles on the WLAN and enable Application Visibility

Step 1: Selecting and Tuning the QoS Profile

QoS Profiles are applied to both upstream and downstream flows on WLC egress. The WLAN QoS Profile defines (as shown in Figure 1):

- **Per-User Bandwidth Contracts**—(Optional) per-user limits for average and peak data and realtime traffic rates.
- **Per-SSID Bandwidth Contracts**—(Optional) per-SSID limits for average and peak data and realtime traffic rates.
- **WLAN Maximum Priority**—The highest DSCP marking value that may be used on the WLAN; this value can override AVC policies as well DSCP-values received from the wired network. As such, in multiservice WLANs, it is generally recommended to ensure that the Maximum Priority value be set to voice.
- **Unicast and Multicast Default Priority**—The default DSCP marking value to be used on the WLAN for all traffic not explicitly classified by an overriding AVC Profile. Typically these values are set as best effort; however there may be cases where this default value may be set to background (i.e., bronze), such as if applied to a guest WLAN.
- **Wired QoS Protocol**—Can be set to 802.1p and the maximum CoS value can be defined per WLAN

Figure 1 Design Recommendations for the Platinum QoS Profile for an Employee WLAN



Cisco AireOS WLC AVC/QoS Design

At-A-Glance

Step 2: Configure an AVC Profile

AVC Profiles are applied to both upstream and downstream flows on WLC ingress. While this may simplify the QoS policy configuration on the WLC, it has design implications in upstream/downstream mapping.

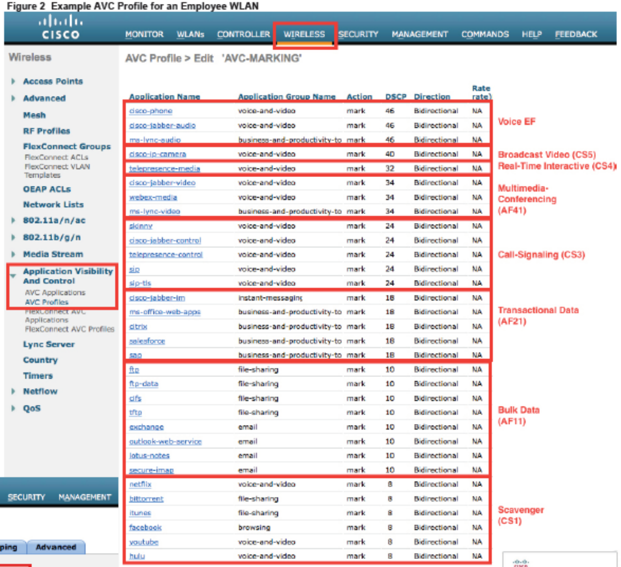
Additionally, each WLAN can have only one AVC profile attached to it to control applications, however an AVC Profile can be attached to multiple WLANs. Also, an AVC Profile can contain a maximum of 32 application rules and a maximum of 16 AVC profiles can be created on a WLC. Also, only 3 AVC applications may be policed in a given profile.

As has been previously discussed, it also is important to note that each WLAN can have both a QoS Profile and an AVC Profile attached to it. The AVC Profile is applied when the packet *enters* the WLC and the QoS policy is applied when packet *exits* the WLC. QoS Profiles may define a Maximum Priority (DSCP value) for packet marking, which will override any AVC Profile marking policy. Thus care should be taken that QoS and AVC Profiles are correctly configured to complement-and not contradict-one another.

An example AVC Profile is shown in Figure 2.

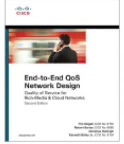
Step 3: Apply the QoS and AVC Profiles on the WLAN and enable Application Visibility With the QoS and AVC Profiles defined, all that remains is to enable these on a given WLAN, as shown in Figure 3. Additionally, by checking the box for AVC, Application Visibility is enabled on the WLAN.

Figure 2 Example AVC Profile for an Employee WLAN



Application Name	Application Group Name	Action	DSCP	Direction	Rate rate)
cisco-phone	voice-and-video	mark	46	Bidirectional	NA
cisco-jabber-audio	voice-and-video	mark	46	Bidirectional	NA
ms-lync-audio	business-and-productivity-to	mark	46	Bidirectional	NA
cisco-ip-camera	voice-and-video	mark	40	Bidirectional	NA
telepresence-media	voice-and-video	mark	32	Bidirectional	NA
cisco-jabber-video	voice-and-video	mark	34	Bidirectional	NA
webex-media	voice-and-video	mark	34	Bidirectional	NA
ms-lync-video	business-and-productivity-to	mark	34	Bidirectional	NA
skinny	voice-and-video	mark	24	Bidirectional	NA
cisco-jabber-control	voice-and-video	mark	24	Bidirectional	NA
telepresence-control	voice-and-video	mark	24	Bidirectional	NA
sip	voice-and-video	mark	24	Bidirectional	NA
sip-tls	voice-and-video	mark	24	Bidirectional	NA
cisco-jabber-im	instant-messaging	mark	18	Bidirectional	NA
ms-office-web-apps	business-and-productivity-to	mark	18	Bidirectional	NA
citrix	business-and-productivity-to	mark	18	Bidirectional	NA
salesforce	business-and-productivity-to	mark	18	Bidirectional	NA
sap	business-and-productivity-to	mark	18	Bidirectional	NA
ftp	file-sharing	mark	10	Bidirectional	NA
ftp-data	file-sharing	mark	10	Bidirectional	NA
cifs	file-sharing	mark	10	Bidirectional	NA
tftp	file-sharing	mark	10	Bidirectional	NA
exchange	email	mark	10	Bidirectional	NA
outlook-web-service	email	mark	10	Bidirectional	NA
lotus-notes	email	mark	10	Bidirectional	NA
secure-imap	email	mark	10	Bidirectional	NA
netflix	voice-and-video	mark	8	Bidirectional	NA
bittorrent	file-sharing	mark	8	Bidirectional	NA
itunes	file-sharing	mark	8	Bidirectional	NA
facebook	browsing	mark	8	Bidirectional	NA
youtube	voice-and-video	mark	8	Bidirectional	NA
hulu	voice-and-video	mark	8	Bidirectional	NA

Figure 3 Example AVC Profile for an Employee WLAN



For more details, see the AVC/QoS Design chapter of the BYOD CVD at:

http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_AVC.html

And the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 19

Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

Cisco AirOS QoS Mapping At-A-Glance

WLAN QoS Mapping for AireOS Wireless LAN Controllers

At-A-Glance

The Case for QoS Mapping in the Wireless LAN

As internet traffic is increasingly sourced-from and destined-to wireless endpoints, it is crucial that Quality of Service be aligned between wired-and-wireless networks; however, this is not always the case by default. This is due to the fact that two independent standards bodies provide QoS guidance on wired and wireless networks: specifically, the IETF offers design recommendations for wired IP networks, while a separate and autonomous standards-body, the IEEE, administers the standards for wireless 802.11 networks. As such, custom QoS mappings are required between IETF Differentiated Services Code Point (DSCP) and IEEE 802.11 User Priority (UP) markings to reconcile the design recommendations offered by these two standards bodies, and, as such, to optimize wired-and-wireless interconnect QoS.

Three are three general options for wired/wireless QoS mapping:
• (Downstream) DSCP-to-UP Mapping
• (Upstream) UP-to-DSCP Mapping
• (Upstream) DSCP-Trust

Note: In AireOS, these options are combined with QoS Profiles, which can limit the maximum marking values in use to/from a given WLAN.

DSCP-to-UP Mapping
Downstream DSCP-to-UP mapping is shown in Figure 1.
By default, 6-bit DSCP values are mapped to 3-bit 802.11e UP values by taking the three Most-Significant Bits (MSB) of the DSCP and copying these as UP values. For example, the IETF recommended marking for voice (DSCP EF/46-binary 101110) is mapped by default to UP 5 (binary 101); which, incidentally is an IEEE recommended marking for video (IEEE marks voice as UP 6).

Note: To partially compensate for IETF/IEEE marking misalignments, AireOS implements some non-default mappings, as specified in the QoS Translation Table at:
http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-1/configuration-guide/b_cg81/b_cg81_chapter_01010111.html

Upstream DSCP-to-UP Mapping
Upstream UP-to-DSCP mapping is shown in Figure 2.
Conversely, in the reverse direction, UP values are simply multiplied by 8 (in order to shift these three binary bits to the left) to generate a DSCP value. Continuing the example, the IEEE recommended marking for voice (UP 6-binary 110) would be mapped by default (i.e., multiplied by 8) to DSCP CS6/48 (binary 110000); which, incidentally is an IETF recommended marking for network control traffic (rather than EF/46, the IETF marking for voice).

Upstream DSCP Trust
Upstream DSCP trust is shown in Figure 3.
To prevent information from being lost in translation (which can happen when converting 6-bit markings to/from 3-bit markings), as well to prevent IEEE UP markings to generate misaligned IETF DSCP markings, Cisco wireless access points can also be configured to Trust DSCP. In this example, a voice packet marked EF can likewise have its CAPWAP outer DSCP set to match.

Figure 1: Default Downstream DSCP-to-UP Mapping

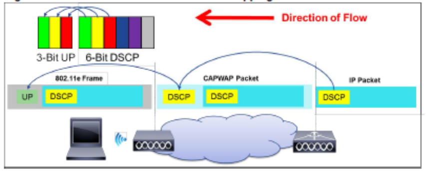


Figure 2: Default Upstream UP-to-DSCP Mapping

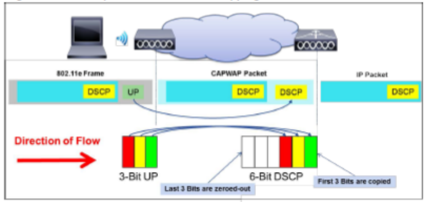
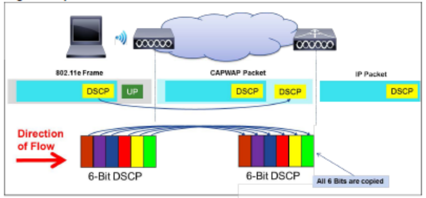


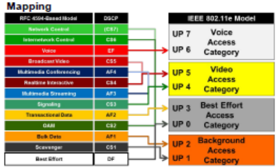
Figure 3: Upstream DSCP Trust



Cisco DSCP<>UP QoS Mapping Recommendations

As previously mentioned, (Layer 2) IEEE and (Layer 3) IETF marking recommendations do not always align. For example, DSCP EF/46 is recommended by the IETF for use for voice, which would map by default to UP 5; but the IEEE designates UP 6 for voice. These discrepancies must be taken into account and reconciled in WLAN QoS designs, as shown in Figure 4 which presents Cisco's Recommended DSCP-to-UP Mappings.

Figure 4: Cisco Recommended DSCP-to-UP Mapping



Note: The details behind Cisco's recommendations for IETF/IEEE QoS Mapping are documented in the Internet Draft: http://tools.ietf.org/html/draft-szigeti-tsvwg-ieee-802-11e-01

In the upstream, Cisco recommends DSCP-trust, for the following reasons:

• This is a standards-based approach (per RFC 2474 and 2475)
• Most wireless device operating systems generate UP values by using the 3 MSB of the encapsulated 6-bit DSCP; then, at the access point, these 3-bit mappings are converted back into DSCP values; in such cases, information is lost in the transitions from 6-bit marking to 3-bit marking and then back to 6-bit marking; trusting the encapsulated DSCP prevents this loss of information
• A practical implementation benefit is also realized, as enabling applications to mark DSCP is much more prevalent and accessible to programmers of wireless applications vis-a-vis trying to explicitly set UP values, which requires special hooks into the wireless device operating system

AireOS Recommended QoS Mapping Configuration
Note: This requires AireOS 8.1MR+

Step 1: Disable the 802.11 Networks and the Current QoS Map

```
(Cisco Controller) > config 802.11a disable network
(Cisco Controller) > config 802.11b disable network
(Cisco Controller) > config qos qosmap disable
```

Step 2: Configure the UP-to-DSCP Maps
Even though DSCP will be trusted in the upstream direction (rather then implementing UP-to-DSCP Maps), specifying the UP-to-DSCP maps is a syntactical requirement. Additionally, the first line also has the additional benefit of mapping the whole DSCP range (0-63) to UP 0.

```
(Cisco Controller) > config qos qosmap up-to-dscp-map 0 0 0 63
(Cisco Controller) > config qos qosmap up-to-dscp-map 1 8
(Cisco Controller) > config qos qosmap up-to-dscp-map 2 16
(Cisco Controller) > config qos qosmap up-to-dscp-map 3 24
(Cisco Controller) > config qos qosmap up-to-dscp-map 4 32
(Cisco Controller) > config qos qosmap up-to-dscp-map 5 40
(Cisco Controller) > config qos qosmap up-to-dscp-map 6 48
(Cisco Controller) > config qos qosmap up-to-dscp-map 7 56
```

Step 3: Configure DSCP-to-UP Mapping Exceptions
Only the exceptions noted in Figure 4 will be explicitly mapped to various UP values; all remaining (unused) DSCPs will continue to be mapped to UP 0.

```
(Cisco Controller) > config qos qosmap dscp-to-up-exception 46 6
(Cisco Controller) > config qos qosmap dscp-to-up-exception 40 5
(Cisco Controller) > config qos qosmap dscp-to-up-exception 38 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 36 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 34 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 32 5
(Cisco Controller) > config qos qosmap dscp-to-up-exception 30 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 28 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 26 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 24 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 22 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 20 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 18 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 16 0
(Cisco Controller) > config qos qosmap dscp-to-up-exception 14 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 12 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 10 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 8 1
```

Step 4: Enable DSCP-Trust, the New Qos Maps and the 802.11 Networks

```
(Cisco Controller) > config qos qosmap trust-dscp-upstream enable
(Cisco Controller) > config qos qosmap enable
(Cisco Controller) > config 802.11a enable network
(Cisco Controller) > config 802.11b enable network
```


Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Cisco Catalyst 9800 WLC QoS Design

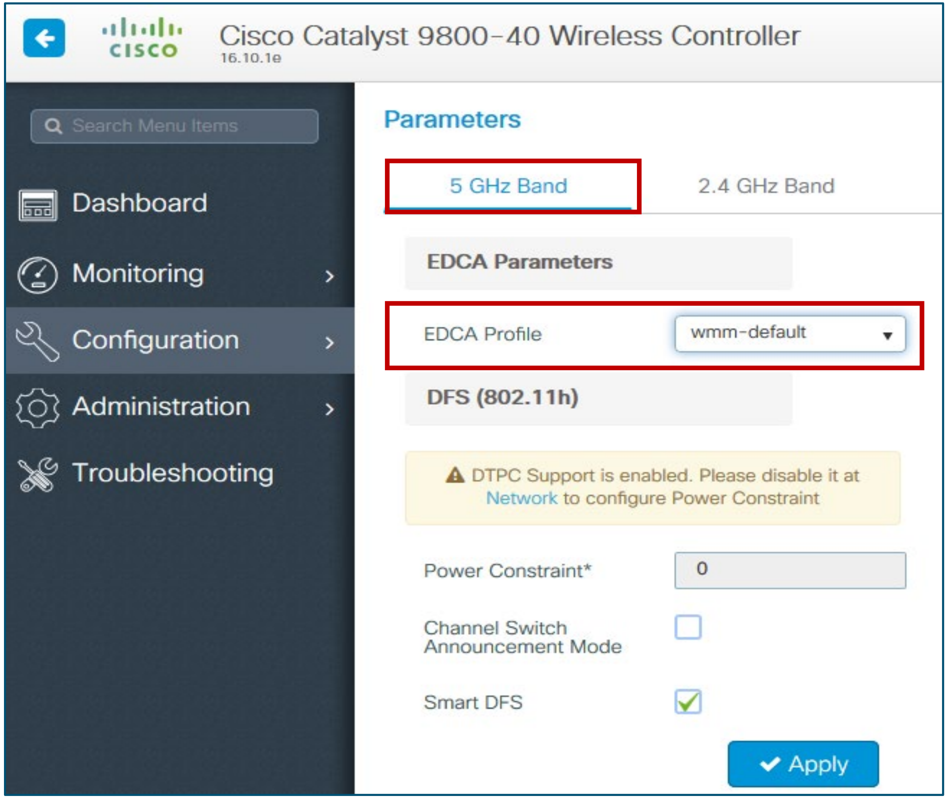
Cisco Catalyst 9800 WLC

QoS Design Steps

1. Tune EDCA and CAC
2. Create QoS Policies (MQC or Web-UI)
   - AVC/NBAR Based
   - ACL Based
3. Apply QoS Policies
   - AVC/NBAR Based, ACL Based, or Precious Metals QoS Profile per SSID
   - AVC/NBAR Based, ACL Based, or AAA Override per Client
   - AutoQoS

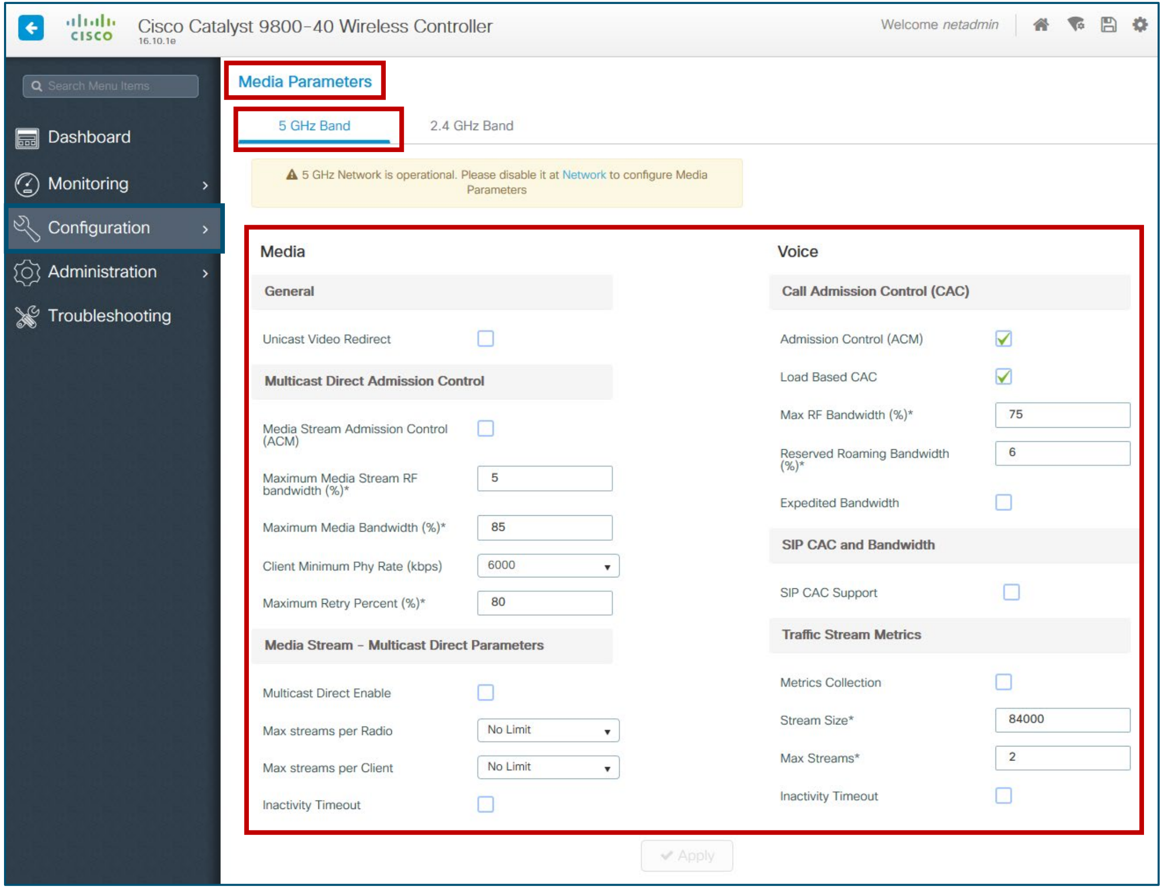
Catalyst 9800 – EDCA Profiles

- Tunable for each radio (5 GHz & 2.4 GHz)
- Radio must be disabled before changing the EDCA Profile
- Navigate to **Configuration > Radio Configurations > Parameters > 5 GHz Band** or **2.4 GHz Band**
- Select the EDCA profile
  - wmm-default
  - svp-voice
  - optimized-voice
  - optimized-video-voice
  - custom-voice
  - fastlane



Catalyst 9800 CAC

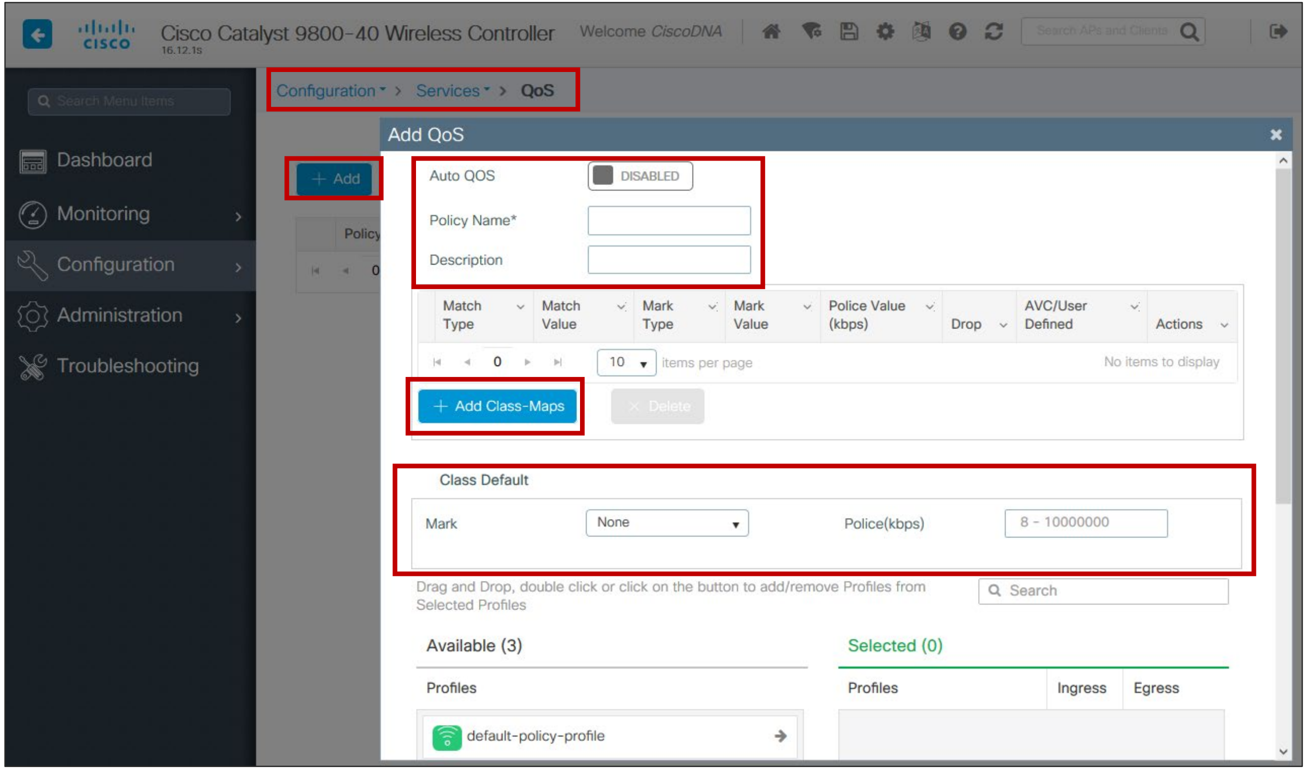
- Only supported for Voice & Media (no Video CAC)
- Tune for each radio (5 GHz & 2.4 GHz)
- Radio must be disabled before changing CAC settings
- Navigate to **Configuration > Media Parameters > 5 GHz Band** or **2.4 GHz Band**
- Load Based CAC takes into account channel loading impact due to interference, other APs, etc. as well as client traffic
- SIP CAC Support is for wireless stations that do not support TSPEC-based admission control



cisco Live!

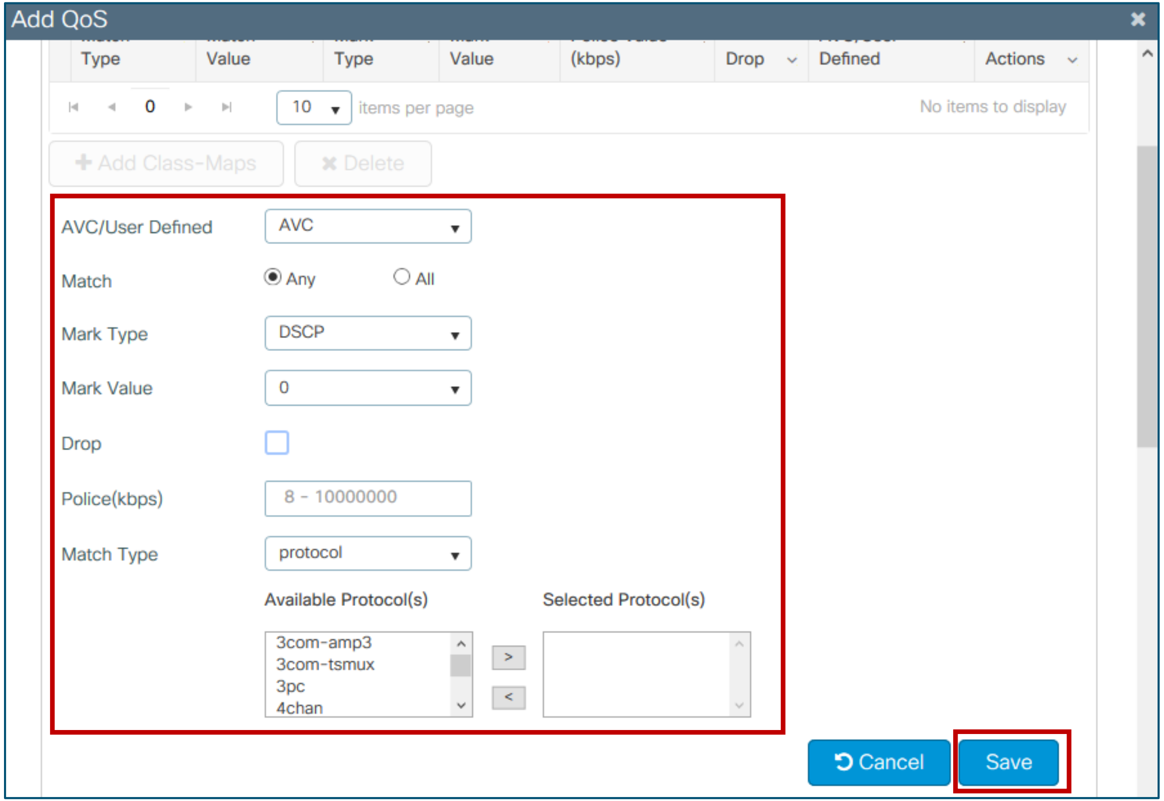
Catalyst 9800 – QoS Policy (Web-UI)

- Navigate to **Configuration > Services > QoS**
- Click **+Add** to add a new QoS policy
- Disable Auto QoS
- Configure a Policy Name (policy-map) and Description
- Click **+Add Class-Maps** to add one or more class-maps
- Two choices for class-maps:
  - AVC – NBAR-based
  - User-Defined – DSCP or ACL
- Determine the behavior of the default traffic-class



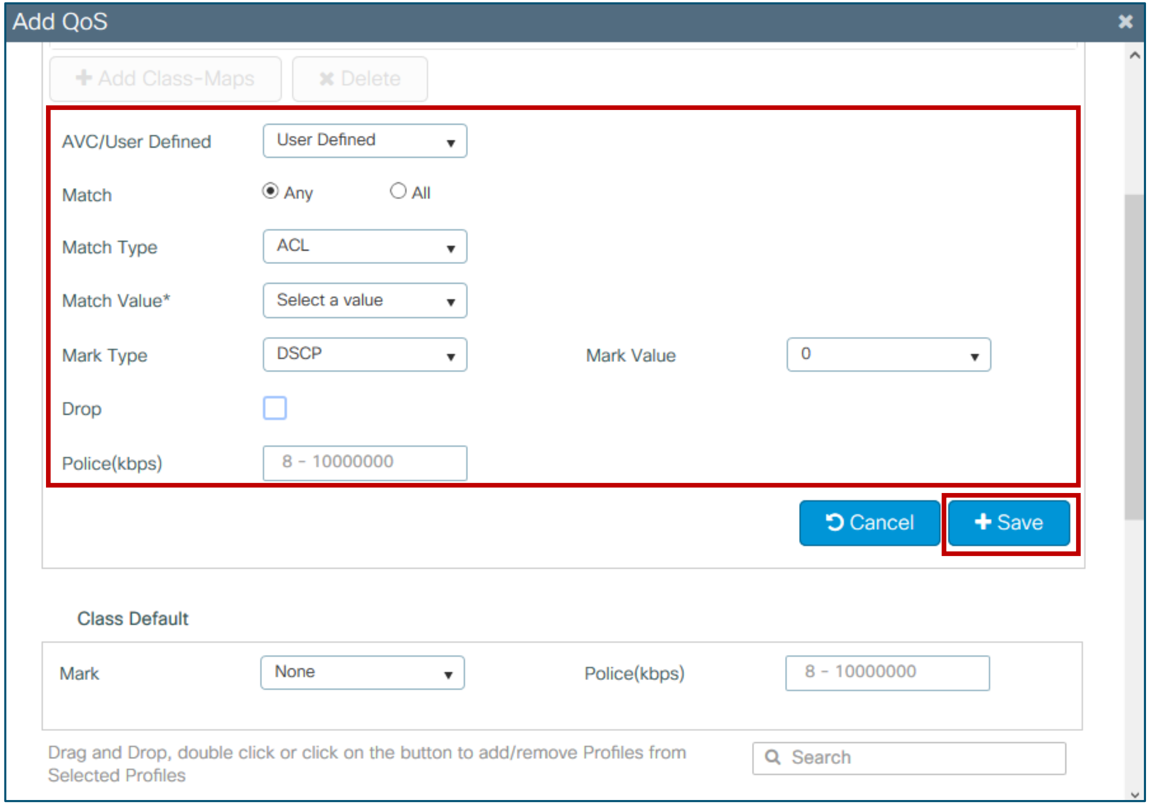
Catalyst 9800 – AVC Class-maps (Web-UI)

- For NBAR-based policies, **select AVC**
- Web-UI supported **match types for AVC class-maps**
  - Protocol, Category, Subcategory, or Application-group (Protocol Attributes supported via CLI)
- Select protocols from the menu and click > to apply to the class-map
- **Select Match Any (logical OR)** if you select multiple protocols
- **Configure the action**(s)
  - Drop, Mark (DSCP Only), or Police (specify the rate)
- Save each class-map to add to the policy-map



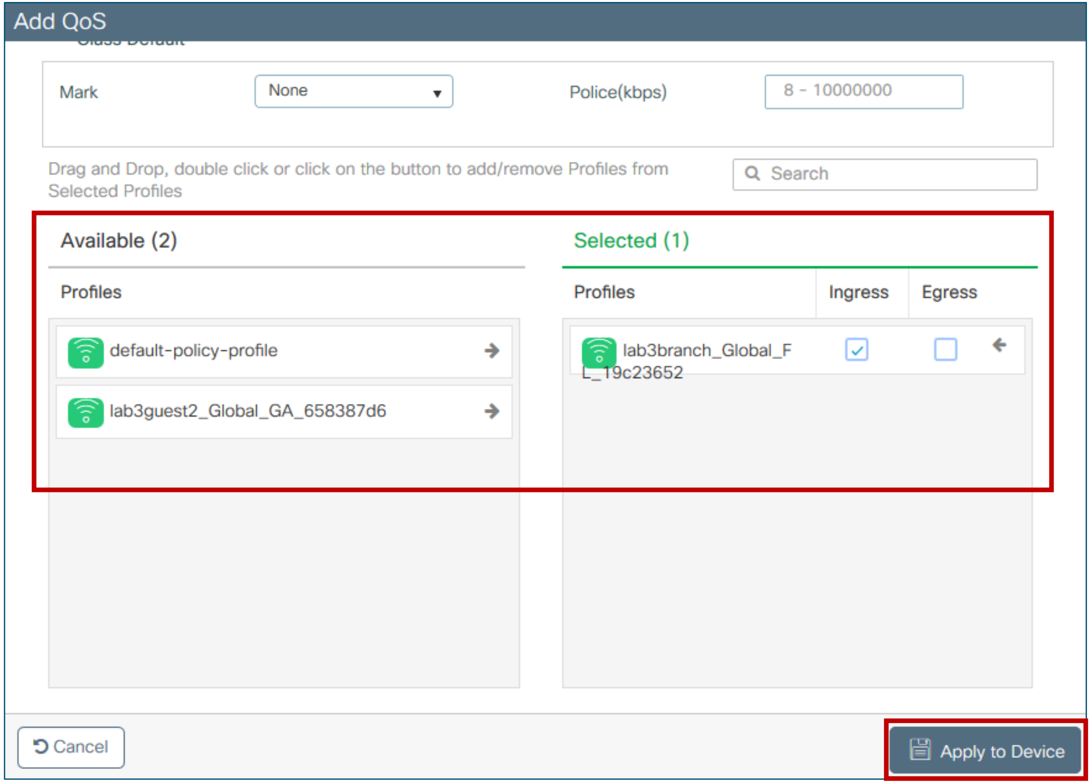
Catalyst 9800- ACL Class-maps (Web-UI)

- For ACL-based policies, select **User Defined**
- Currently supported match types for User Defined class-maps
  - DSCP or ACL
- For match type of ACL, select the ACL from the drop-down list under Match Value
- Select Match Any (logical OR) or Match All (logical AND)
- **Configure the action(s)**
  - Drop, Mark (DSCP Only), or Police (specify the rate)
- Save each class-map to add to the policy-map



Catalyst 9800 – QoS Policy (Web-UI)

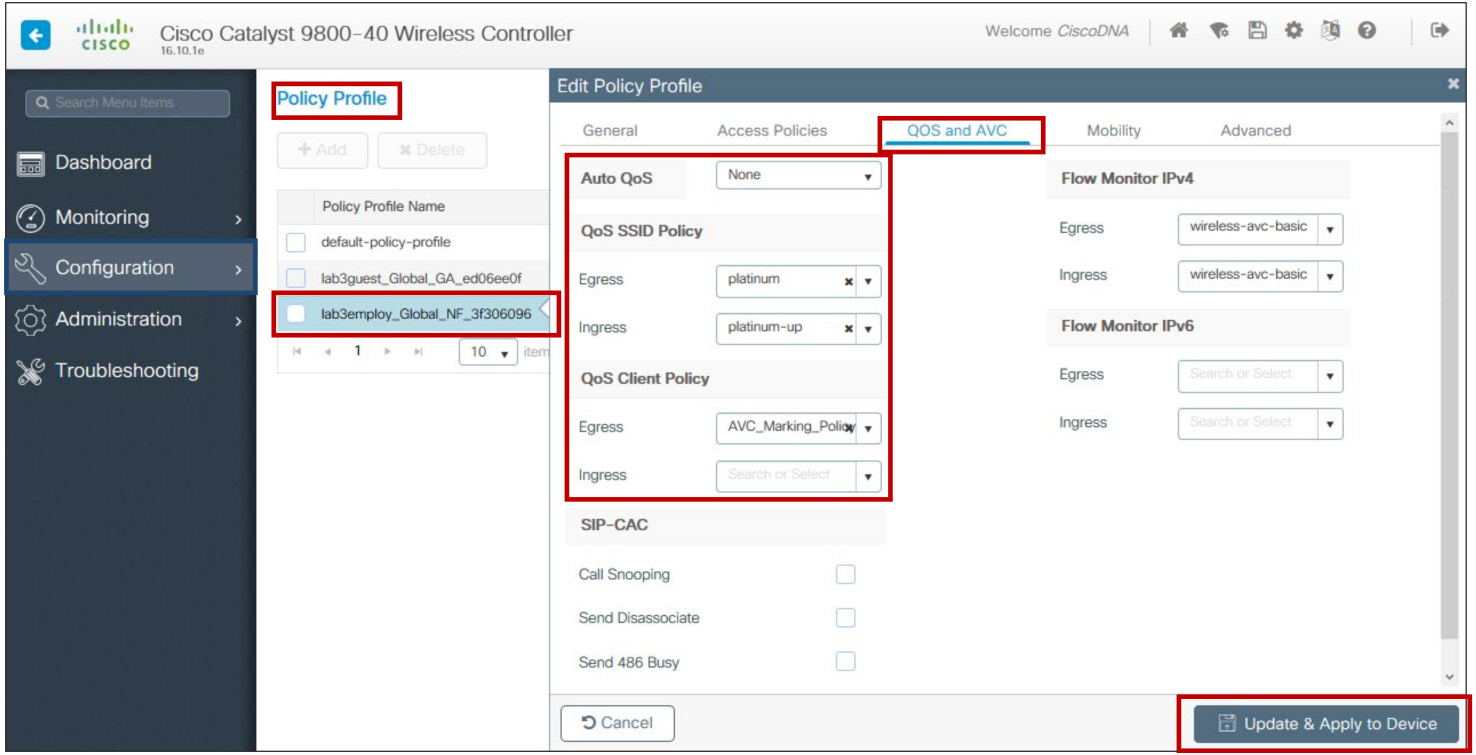
- You can apply the **custom QoS Policy to the Policy Profile** by selecting from the available profiles, clicking on the → button, and checking the ingress and/or egress boxes
- Optionally, you can apply the QoS Policy within the Policy Profile itself (next slide)
- Click the **Apply to Device** button to save the custom QoS policy



Apply QoS Policies to Policy Profiles

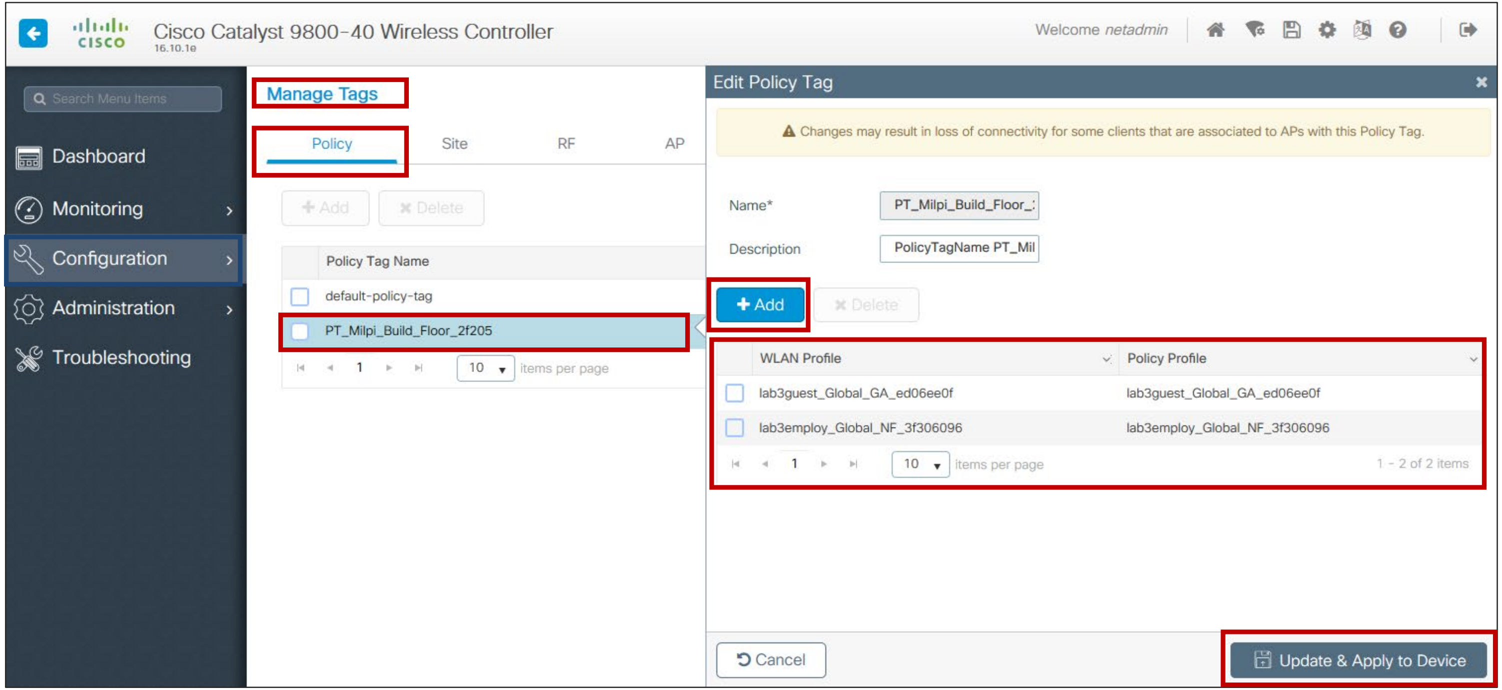
- Navigate to **Configuration > Tags & Profiles > Policy**
- Click on the Policy Profile to edit and then select **QoS and AVC**
- Click the **Update & Apply to Device** button to save the Policy Tag

- Apply QoS policies per SSID
  - Precious Metals
  - Custom Policy
- Apply QoS policies per client
  - Custom Policy
- Optionally apply Auto QoS policy
  - Enterprise
  - Fastlane
  - Guest
  - Voice



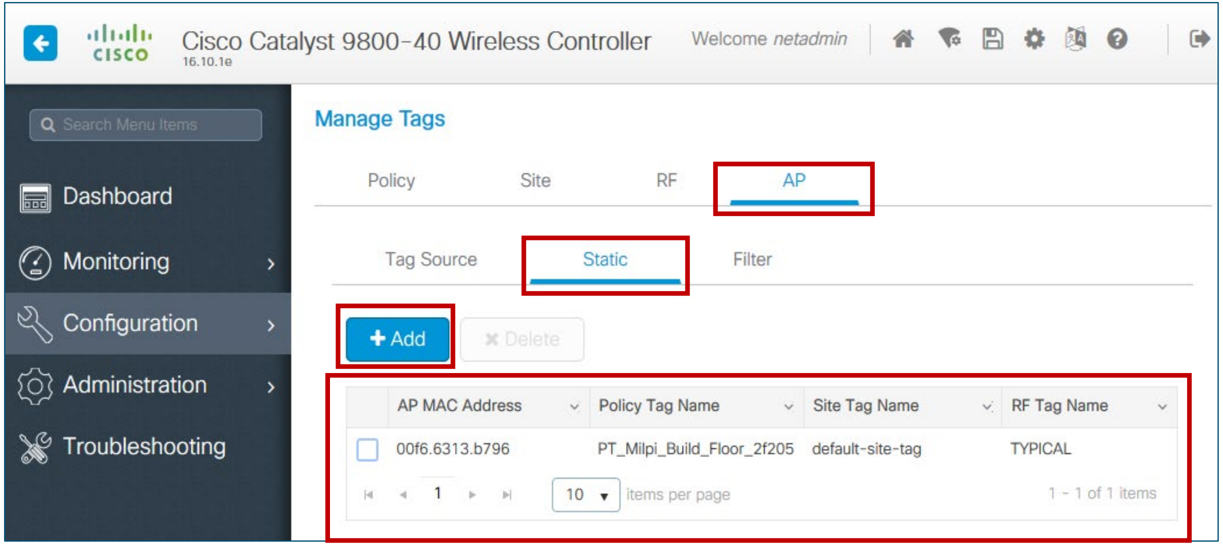
Catalyst 9800 - Apply Policy Profile to Policy Tag

- Navigate to **Configuration > Tags & Profiles > Tags**
- Under the **Policy** tab select the Policy Tag to which you want to apply the QoS Policy Profile
  - Click **+Add** to add WLAN Profile(s) and Policy Profile(s) to the Policy Tag
  - Click the **Update & Apply to Device** button to save the Policy Tag



Catalyst 9800 - Apply the Policy Tag to APs

- One of the way is to use the static method, under the AP tab select the Static tab
- Click +Add to assign a Policy Tag, Site Tag, and RF Tag to an AP. Type in the MAC Address of the AP
- Select the Policy Tag, Site Tag, and RF Tag from the drop-down menus
- Click the Save & Apply to Device button to save the tag assignments



Catalyst 9800 – DSCP-to-UP Mapping & DSCP Trust

- DSCP-to-UP mapping in the downstream direction are statically defined on the Catalyst 9800 WLC
- DSCP Trust is enabled by default in the upstream direction

IETF DiffServ Service Class	DSCP	802.11 User Priority	801.11 Access Category
Network Control	CS6, (CS7)	0	AC_BE
IP Telephony	EF	6	AC_VO
VOICE-ADMIT	44	6	AC_VO
Signaling	CS5	5	AC_VI
Multimedia Conferencing	AF4x	4	AV_VI
Real-Time Interactive	CS4	5	AC_VI
Multimedia Streaming	AF3x	4	AC_VI
Broadcast Video	CS3	4	AC_VI
Low-Latency Data (Transactional Data)	AF2x	3	AC_BE
OAM	CS2	0	AC_BE
High-Throughput Data (Bulk Data)	AF1x	2	AC_BK
Low-Priority Data (Scavenger)	CS1	1	AC_BK
Remaining	Remaining	0	AC_BE

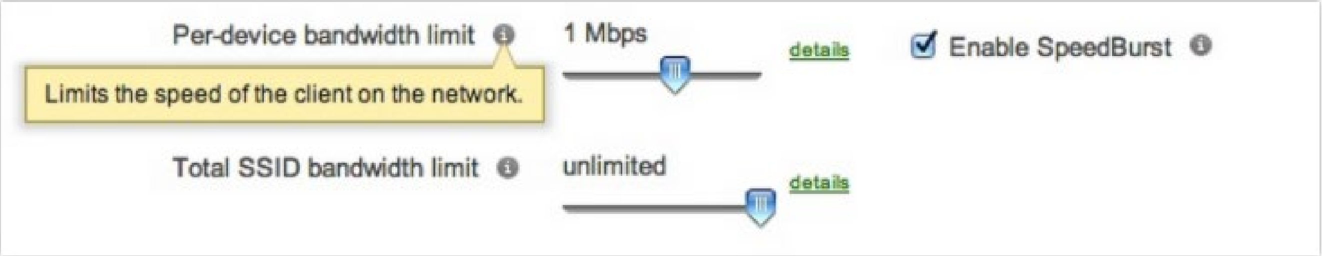
Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Meraki MR Series AP QoS Design

Meraki MR Series AP QoS

Bandwidth Shaping - Configure > Firewall and Traffic shaping



- Supports separate upload and download limits
- Per-SSID and per-device/user limits
  - Support for per-user bandwidth limits when a customer-hosted RADIUS server is used
- SpeedBurst allows up to 4 times the configured rate for 5 seconds

https://documentation.meraki.com/MR/Firewall_and_Traffic_Shaping/Traffic_and_Bandwidth_Shaping

Meraki MR Series AP QoS

Traffic Shaping – Configure > Firewall and Traffic shaping

- Identifies traffic based on Layer 3 or Layer 7 (application) signatures and enforces QoS
- Rule Definition – 2 Options
  - Select from pre-defined application categories
  - Custom rule definitions specifying HTTP hostnames, port number, IP address range, or combinations of IP address range and port
- Rule Action – Shaping and/or Prioritization
  - Allow unlimited bandwidth usage – ignoring limits set for a particular SSID
  - Obey the SSID limits defined on the Access Control page
  - Apply more restrictive limits than specified for the SSID

Meraki MR Series AP QoS

Upstream and Downstream QoS

- Default downstream mapping of DSCP value to 802.11 AC
- Upstream QoS sent by the client is honored.
  - DSCP field within the traffic sent from the client is maintained on the Ethernet network
  - Fastlane support with the ability to install a wireless profile on iOS devices via the Meraki EMM
    - The default configuration accepts all application markings. Select **Restrict QoS marking** to whitelist specific applications

RFC 4594-Based Model	**802.3 DSCP**	**802.3 DSCP** [Decimal]	**IEEE 802.11 Model** [802.11e WMM-AC]
Voice + DSCP-Admit	EF + 44	46	Voice AC (AC_VO)
Broadcast Video	CS5	24	Video AC (AC_VI)
Multimedia Conferencing	AF4*n*	34, 36, 38	Video AC (AC_VI)
Realtime Interactive	CS4	32	Video AC (AC_VI)
Multimedia Streaming	AF3*n*	26, 28, 30	Video AC (AC_VI)
Signaling	CS3	40	Video AC (AC_VI)
Transactional Data	AF2*n*	18, 20, 22	Best Effort AC (AC_BE)
OAM	CS2	16	Best Effort AC (AC_BE)
Bulk Data	AF1*n*	10, 12, 14	Background AC (AC_BK)
Scavenger	CS1	8	Background AC (AC_BK)
Best Effort	DF	0	Best Effort AC (AC_BE)

Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

What are we doing to make this simpler?

How Are We Simplifying Campus QoS?

- Simplifying Hardware – UADP ASIC
- Simplifying Software – IOS XE
- QoS via the Catalyst 9000 Series Web UI
- Cisco Validated Designs & At-A-Glance Documents
- Automating Best Practices
  - Auto QoS
  - Fastlane for iOS
  - Cisco DNA Center Application Policy and Assurance

Cisco DNA Center Application Policy & Application Assurance Demo

Cisco DNA Center - Application Policy & Assurance

Cisco DNA Center   DESIGN   POLICY   PROVISION   ASSURANCE   PLATFORM   24

Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- Add site locations on the network
- Designate golden images for device families
- Create wireless profiles of SSIDs

Policy

Use policies to automate and simplify network management, reducing cost and risk while speeding rollout of new and enhanced services.

- Segment your network as Virtual Networks
- Create scalable groups to describe your critical assets
- Define segmentation policies to meet your policy goals

Provision

Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.

- Onboard and manage unclaimed devices
- Add, update or delete devices managed by the controller
- Provision switches, routers, WLCs and APs in defined site
- Set up Campus Fabric across switches

Assurance

Use proactive monitoring and insights from the network, devices, and applications to predict problems faster and ensure that policy and configuration changes achieve the business intent and the user experience you want.

- Assurance Health
- Assurance Issues

Platform

Use DNA Center Platform, to programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

- View the API Catalog
- Configure DNA Center - to - Third Party Integrations
- Schedule and Download - Data and Reports

Agenda

- Campus QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
  - Cisco Catalyst 6800 / 6500-E QoS Design
  - Meraki MS Series Switch QoS Design
- Campus WLAN QoS Design Considerations and Best Practices
  - Cisco AireOS WLC AVC / QoS Design
  - Cisco Catalyst 9800 WLC QoS Design
  - Meraki MR Series AP QoS Design
- What are we doing to make this simpler?
- Summary and References

Summary and References

Key Takeaways

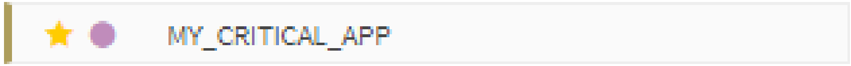
- Start by identifying the business objectives behind implementing QoS
- QoS on the wired side of the campus is needed primarily to control packet drops
- WLAN QoS is needed to control both jitter and packet drops
- Know your QoS toolset, as this varies platform-to-platform
- Cisco provides many At-A-Glance guides to get you up and running quickly and design guides for more detail
- Cisco is continuing to simplify QoS—both in hardware and software
- Cisco DNA Center Application Policy delivers simplicity for Campus QoS through intent-based QoS policy
- Cisco DNA Assurance provides visibility into applications and application performance on the network

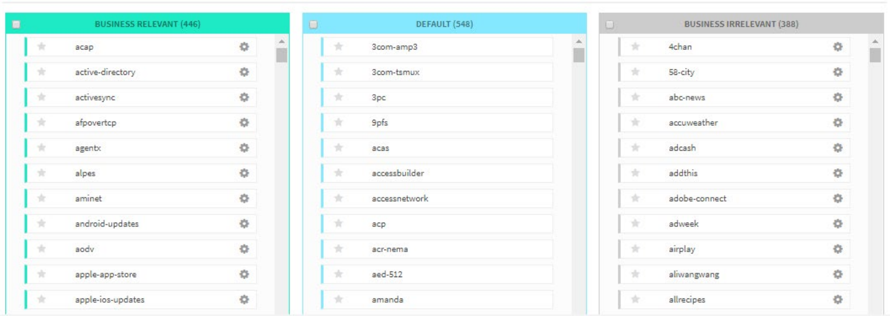
Your Choice

Manual QoS Policy

```
ip access-list extended APIC_EM-MM_STREAM-ACL
 remark citrix - Citrix
 permit tcp any any eq 1494
 permit udp any any eq 1494
 permit tcp any any eq 2598
 permit udp any any eq 2598
 remark citrix-static - Citrix-Static
 permit tcp any any eq 1604
 permit udp any any eq 1604
 permit tcp any any range 2512 2513
 permit udp any any range 2512 2513
 remark pcoip - PCoIP
 permit tcp any any eq 4172
 permit udp any any eq 4172
 permit tcp any any eq 5172
 permit udp any any eq 5172
 remark timbuktu - Timbuktu
 permit tcp any any eq 407
 permit udp any any eq 407
 remark xwindows - XWindows
 permit tcp any any range 6000 6003
 remark vnc - VNC
 permit tcp any any eq 5800
 permit udp any any eq 5800
 permit tcp any any range 5900 5901
 permit udp any any range 5900 5901
exit
ip access-list extended APIC_EM-SIGNALING-ACL
 remark h323 - H.323
 permit tcp any any eq 1300
 permit udp any any eq 1300
 permit tcp any any range 1718 1720
```

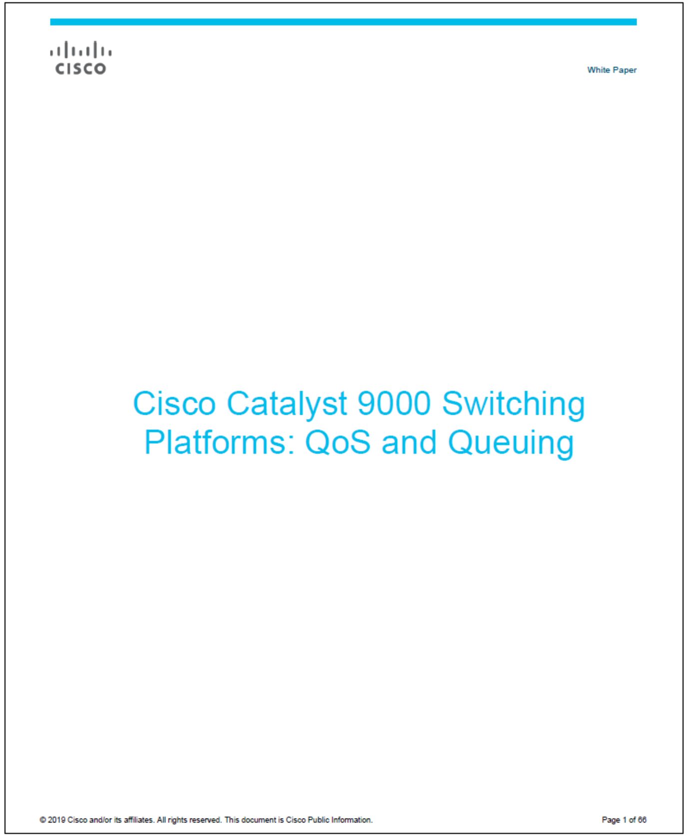
Intent-Based Application Policy





Recommended Reading
Cisco Catalyst 9000 Switching Platforms: QoS and Queuing

https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9000/white-paper-c11-742388.pdf


White Paper

Cisco Catalyst 9000 Switching Platforms: QoS and Queuing

© 2019 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public Information. Page 1 of 66

Campus QoS Design 4.0—In-Depth

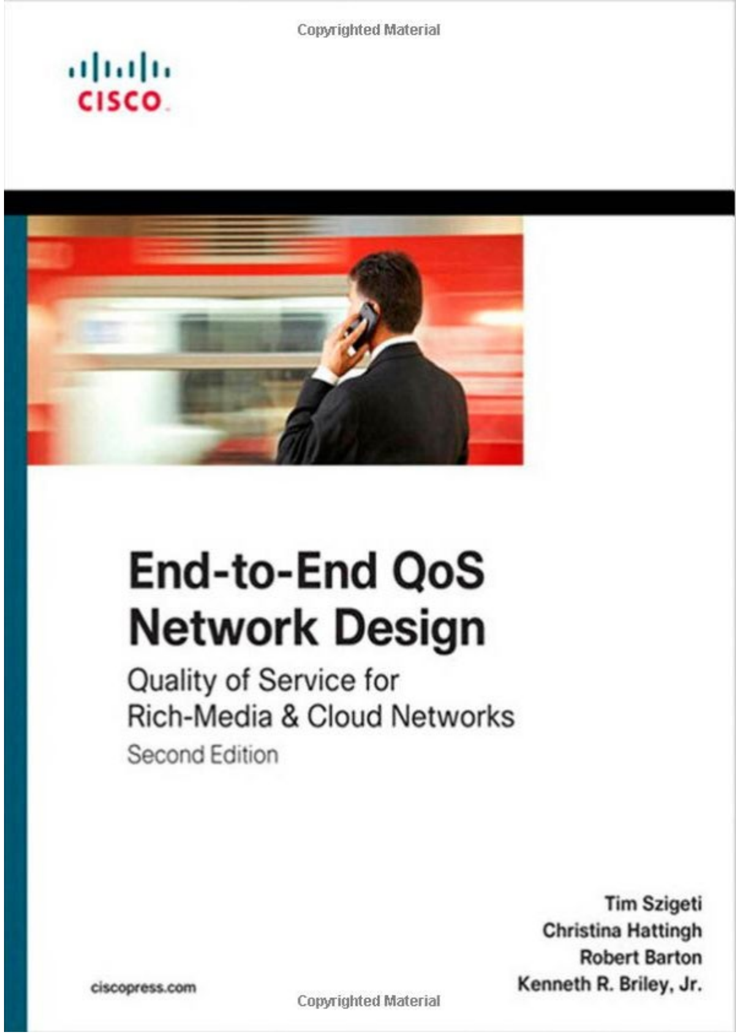
Comprehensive Design Chapters

- Enterprise Quality of Service Design 4.0
  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html
- Campus QoS Design 4.0
  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html
- WLAN QoS Design (BYOD CVD)
  http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/BYOD_AVC.html

Recommended Reading
End-to-End QoS (v2)

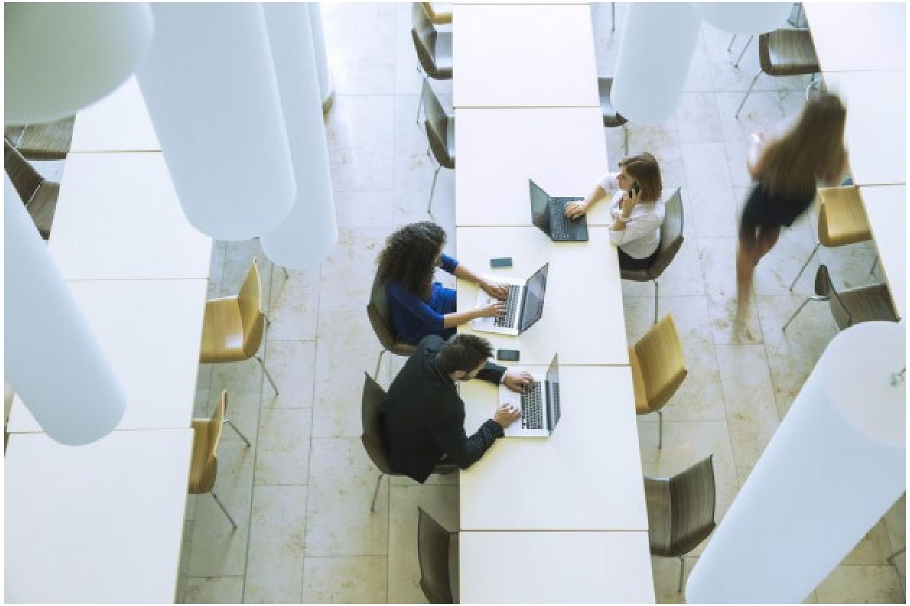
- Release Date: Jan 2014
- Page Count: 1040
- Comprehensive QoS design guidance for PINs and platforms:
  - Campus Catalyst 3750/4500/6500
  - WLAN WLC 5508 / Catalyst 3850 NGWC
  - Data Center Nexus 1000V/2000/5500/7000
  - WAN & Branch Cisco ASR 1000 / ISR G2
  - MPLS VPN Cisco ASR 9000 / CRS-3
  - IPSec VPNs Cisco ISR G2
- ISBN: 1-58714-369-0

http://www.amazon.com/End---End-QoS-Network-Design/dp/1587143690/



Recommended Reading
APIC-EM EasyQoS Solution Design Guide

https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Dec2017/APIC-EM-EasyQoS-DesignGuide-Dec2017.pdf



Cisco EasyQoS Solution Design Guide
APIC-EM Release 1.6

December, 2017

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco campus

Walk-in self-paced labs

Meet the engineer 1:1 meetings

Related sessions

Thank you

You make **possible**

Appendix: A
Catalyst 6500-E / 6800 Queuing Models

Catalyst 6500-E / 6807-XL with Sup2T/6T

Ingress & Egress Queueing Models

- Ingress Queue Structures

1Q8T	CoS to Queue Mapping	CoS-based Tail-Drop
2Q4T	CoS to Queue Mapping	CoS-based Tail-Drop
2Q8T	CoS to Queue Mapping	CoS-based Tail-Drop
8Q4T	DSCP to Queue Mapping	DSCP-based WRED
8Q8T	CoS to Queue Mapping	CoS-based WRED
1P7Q2T	DSCP to Queue Mapping	DSCP-based WRED

- Ingress & Egress Queue Structures

*2P6Q4T	DSCP to Queue Mapping	DSCP-based WRED

- Egress Queue Structures

1P3Q8T	CoS to Queue Mapping	Cos-based WRED
1P3Q4T	CoS to Queue Mapping	CoS-based WRED
1P7Q4T	DSCP to Queue Mapping	DSCP-based WRED*
1P7Q8T	CoS to Queue Mapping	CoS-based WRED

* 1P7Q4T can be implementing as an alternate ingress queueing structure to 2P6Q4T

1Q8T – Ingress Queueing CoS to Queue Mapping CoS-based Tail-Drop

1Q8T Ingress Queueing Linecards

- WS-X6704-10GE with CFC
- WS-X6724-SFP with CFC
- WS-X6748-SFP and WS-X6748-GE-TX with CFC

Catalyst 6500-E/6807-XL with Sup2T/6T

1Q8T Ingress Queuing Models—CoS-to-Queue Mapping w/ COS-based Tail-Drop

Application-Class	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	CoS 5
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	CoS 4
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	CoS 3
Transactional Data	AF2	CoS 2
Network Management	CS2	CoS 2
Bulk Data	AF1	CoS 1
Scavenger	CS1	CoS 1
Best Effort	DF	CoS 0

1Q8T	
CoS 7	Q1T8–100%
CoS 6	Q1T7–95%
CoS 5	Q1T6–90%
CoS 4	Q1T5–85%
CoS 3	Q1T4–80%
CoS 2	Q1T3–75%
CoS 0	Q1T2–70%
CoS 1	Q1T1–65%

All noted thresholds are tail-drop thresholds

Catalyst 6500-E/6807-XL—1Q8T Ingress Model

```
policy-map type lan-queuing APIC_EM-QUEUING-1Q8T-IN
 class class-default
  queue-limit cos 7 percent 100
  queue-limit cos 6 percent 95
  queue-limit cos 5 percent 90
  queue-limit cos 4 percent 85
  queue-limit cos 3 percent 80
  queue-limit cos 2 percent 75
  queue-limit cos 0 percent 70
  queue-limit cos 1 percent 65
```

```
Interface GigabitEthernet1/1
 service-policy type lan-queuing input APIC_EM-QUEUING-1Q8T-IN
```

Un-configured CoS values default to threshold 8 which is 100%. May not need to configure the CoS 7 value, as this should default to 100%. However, it is shown here for completeness.

Recommend to explicitly configure it.

2Q4T - Ingress Queueing
CoS to Queue Mapping
CoS-based Tail-Drop

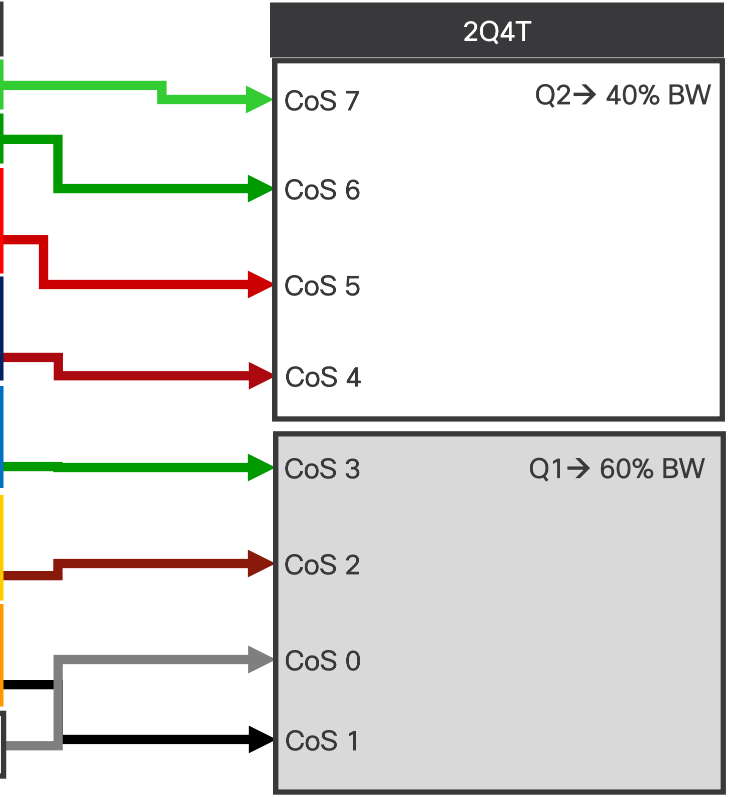
2Q4T Ingress Queueing Linecards

- VS-S2T-10G and VS-S2T-10G-XL with Gigabit Ethernet ports enabled
- Applies to all ports on the Supervisor 2T

Catalyst 6500-E/6807-XL with Sup2T

2Q4T Ingress Queuing Models—CoS-to-Queue Mapping

Application-Class	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	
Transactional Data	AF2	CoS 2
Network Management	CS2	
Bulk Data	AF1	CoS 1
Scavenger	CS1	
Best Effort	DF	CoS 0



Catalyst 6500-E/6807-XL with Sup2T

2Q4T Ingress Queuing Models—CoS-to-Queue Mapping w/ CoS-based Tail-Drop

Application-Class	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	CoS 5
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	CoS 4
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	CoS 3
Transactional Data	AF2	CoS 2
Network Management	CS2	CoS 2
Bulk Data	AF1	CoS 1
Scavenger	CS1	CoS 1
Best Effort	DF	CoS 0

2Q4T	Threshold
CoS 7	Q2T4–100%
CoS 6	Q2T3–95%
CoS 5	Q2T2–90%
CoS 4	Q2T1–85%
CoS 3	Q1T4–100%
CoS 2	Q1T3–95%
Cos 0	Q1T2–90%
CoS1	Q1T1–85%

Q2→ 40% BW

Q1→ 60% BW

All noted thresholds are tail-drop thresholds

Catalyst 6500-E/6807-XL–2Q4T Ingress Model

```
class-map type lan-queuing match-all APIC_EM-Q2-2Q4T-QUEUE
 match cos 7 6 5 4

policy-map type lan-queuing APIC_EM-QUEUING-2Q4T-IN
 class APIC_EM-Q2-2Q4T-QUEUE
  bandwidth percent 40
  queue-limit cos 7 percent 100
  queue-limit cos 6 percent 95
  queue-limit cos 5 percent 90
  queue-limit cos 4 percent 85
 class class-default
  queue-limit cos 3 percent 100
  queue-limit cos 2 percent 95
  queue-limit cos 0 percent 90
  queue-limit cos 1 percent 85
```

```
interface GigabitEthernet1/3/1
 service-policy type lan-queuing input APIC_EM-QUEUING-2Q4T-IN
interface TenGigabitEthernet1/3/4
 service-policy type lan-queuing input APIC_EM-QUEUING-2Q4T-IN
```

Un-configured CoS values default to threshold 8 which is 100%. May not need to configure the CoS 7 or CoS 3 values, as this should default to 100%, but is shown here for completeness.

Recommend explicitly configuring thresholds however.

2Q8T - Ingress Queueing
CoS to Queue Mapping
CoS-based Tail-Drop

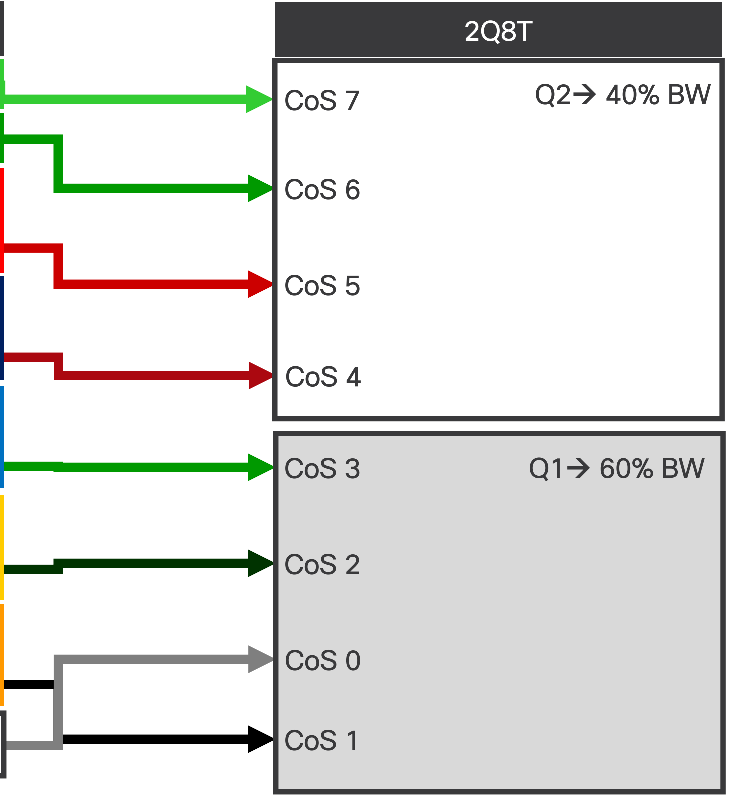
2Q8T Ingress Queueing Linecards

- WS-X6724-SFP with DFC4/DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL)
- WS-X6748-SFP and WS-X6748-GE-TX with DFC4/DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL)
- WS-X6824-SFP-2T and WS-X6824-SFP-2TXL
- WS-X6848-SFP-2T, WS-X6848-SFP-2TXL, WS-X6848-TX-2T and WS-X6848-TX-2TXL

Cisco Catalyst 6500-E/6807-XL with Sup2T

2Q8T Ingress Queuing Models—CoS-to-Queue Mapping

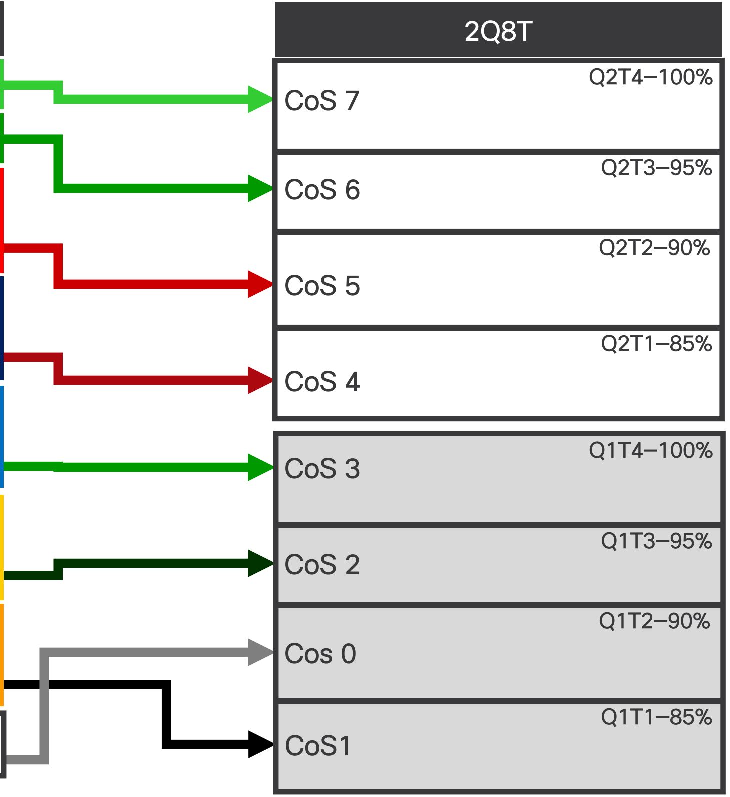
Application-Class	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	
Transactional Data	AF2	CoS 2
Network Management	CS2	
Bulk Data	AF1	CoS 1
Scavenger	CS1	
Best Effort	DF	CoS 0



Cisco Catalyst 6500-E/6807-XL with Sup2T

2Q8T Ingress Queuing Models—CoS-to-Queue Mapping w/ CoS-based Tail-Drop

Application-Class	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	
Transactional Data	AF2	CoS 2
Network Management	CS2	
Bulk Data	AF1	CoS 1
Scavenger	CS1	
Best Effort	DF	CoS 0



Q2→ 40% BW

Q1→ 60% BW

All noted thresholds are tail-drop thresholds

Catalyst 6500-E/6807-XL—2Q8T Ingress Model

```
class-map type lan-queuing match-all APIC_EM-Q2-2Q8T-QUEUE
 match cos 7 6 5 4

policy-map type lan-queuing APIC_EM-QUEUING-2Q8T-IN
 class APIC_EM-Q2-2Q8T-QUEUE
  bandwidth percent 40
  queue-limit cos 7 percent 100
  queue-limit cos 6 percent 95
  queue-limit cos 5 percent 90
  queue-limit cos 4 percent 85
 class class-default
  queue-limit cos 3 percent 100
  queue-limit cos 2 percent 95
  queue-limit cos 0 percent 90
  queue-limit cos 1 percent 85
```

```
interface GigabitEthernet1/3/2
 service-policy type lan-queuing input APIC_EM-QUEUING-2Q8T-IN
```

Un-configured CoS values default to threshold 8 which is 100%. May not need to configure the CoS 7 or CoS 3 values, as this should default to 100%.

Recommend explicitly configuring thresholds

8Q4T – Ingress Queueing DSCP to Queue Mapping DSCP-based WRED

8Q4T Ingress Queueing Linecards

- VS-S2T-10G, VS-S2T-10G-XL with Gigabit Ethernet ports disabled
- WS-X6908-10G-2T, WS-X6908-10G-2TXL
- WS-X6816-10T-2T, WS-X6816-10T-2TXL, WS-X6816-10G-2T, WS-X6816-10G-2TXL in performance mode
- WS-X6716-10G-3C, WS-X6716-10G-3CXL, WS-X6716-10T-3C, WS-X6716-10T-3CXL with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-E, WS-F6k-DFC4-EXL) in performance mode)

How to Disable or Display the State of GigabitEthernet Interfaces on the Sup2T

```
o23-6500-1(config)#platform qos 10g-only
```

Global command disables GigabitEthernet interfaces on the Sup2T.

```
o23-6500-1#show platform qos module 3
   QoS is enabled globally
   Port QoS is enabled globally
   QoS serial policing mode enabled globally
    Distributed Policing is Disabled
    Secondary PUPs are enabled
 QoS Trust state is DSCP on the following interface:
EO0/2 Gi1/1 Gi1/2 Gi1/3 Gi1/4 Gi1/5 Gi1/6 Gi1/7 Gi1/8 Gi1/9
Gi1/10 Gi1/11 Gi1/12 Gi1/13 Gi1/14 Gi1/15 Gi1/16 Gi1/17 Gi1/18 Gi1/19
Gi1/20 Gi1/21 Gi1/22 Gi1/23 Gi1/24 Gi1/25 Gi1/26 Gi1/27 Gi1/28 Gi1/29
Gi1/30 Gi1/31 Gi1/32 Gi1/33 Gi1/34 Gi1/35 Gi1/36 Gi1/37 Gi1/38 Gi1/39
Gi1/40 Gi1/41 Gi1/42 Gi1/43 Gi1/44 Gi1/45 Gi1/46 Gi1/47 Gi1/48 Te2/1
Te2/2 Te2/3 Te2/4 Te2/5 Te2/6 Te2/7 Te2/8 Gi3/1 Gi3/2 Gi3/3
Te3/4 Te3/5 Te5/1 Te5/2 Te5/3 Te5/4 Te5/5 Te5/6 Te5/7 Te5/8
Te5/9 Te5/10 Te5/11 Te5/12 Te5/13 Te5/14 Te5/15 Te5/16 Te6/1 Te6/2
Te6/3 Te6/4 CPP CPP.1 Vl1
   QoS 10g-only mode supported: Yes [Current mode: Off]
   Global Policy-map: ingress[]
…
```

Exec-level command to show whether the GigabitEthernet interfaces on the Sup2T are enabled or disabled

GigabitEthernet interfaces on the Sup2T are currently enabled

How to Enable or Display Performance Mode on Linecards

```
o23-6500-1(config)#no hw-module slot 5 oversubscription port-group 4
```

Global command enables performance mode on a port group of a linecard

```
o23-6500-1#show hw-module slot 5
oversubscription
port-group        oversubscription-mode
1                 enabled
2                 enabled
3                 enabled
4                 disabled
```

Exec-level command to show whether the oversubscription is enabled or disabled (performance mode) per port group of a linecard

Cisco Catalyst 6500-E/6807-XL with Sup2T

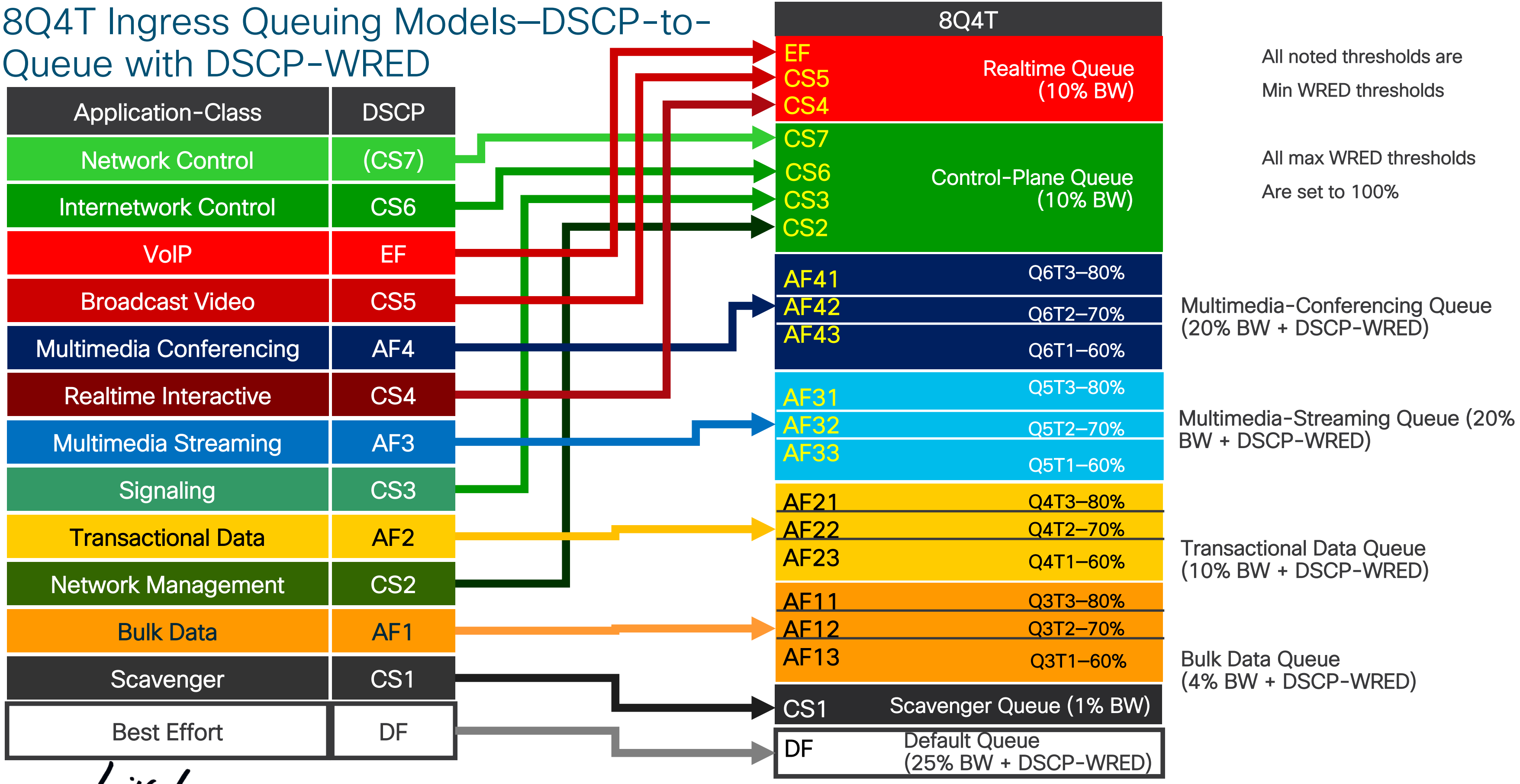
8Q4T Ingress Queuing Models—DSCP-to-Queue Mapping

Application-Class	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

8Q4T	
EF CS5 CS4	Realtime Queue (10% BW)
CS7 CS6 CS3 CS2	Control Queue (10% BW)
AF4	Multimedia-Conferencing Queue (20% BW + DSCP-WRED)
AF3	Multimedia-Streaming Queue (20% BW + DSCP-WRED)
AF2	Transactional Data Queue (10% BW + DSCP-WRED)
AF1	Bulk Data Queue (4% BW + DSCP-WRED)
CS1	Scavenger Queue (1% BW)
DF	Default Queue (25% BW + DSCP-WRED)

Cisco Catalyst 6500-E/6807-XL with Sup2T

8Q4T Ingress Queuing Models–DSCP-to-Queue with DSCP-WRED



Catalyst 6500-E/6807-XL –8Q4T Ingress Model

```
class-map type lan-queuing match-all APIC_EM-REALTIME-8Q4T-QUEUE
 match dscp cs4 cs5 ef
class-map type lan-queuing match-all APIC_EM-CONTROL-8Q4T-QUEUE
 match dscp cs2 cs3 cs6 cs7
class-map type lan-queuing match-all APIC_EM-MM_CONF-8Q4T-QUEUE
 match dscp af41 af42 af43
class-map type lan-queuing match-all APIC_EM-MM_STREAM-8Q4T-QUEUE
 match dscp af31 af32 af33
class-map type lan-queuing match-all APIC_EM-TRANS_DATA-8Q4T-QUEUE
 match  dscp af21  af22  af23
class-map type lan-queuing match-all APIC_EM-BULK_DATA-8Q4T-QUEUE
 match  dscp af11  af12  af13
class-map type lan-queuing match-all APIC_EM-SCAVENGER-8Q4T-QUEUE
 match dscp cs1
```


Catalyst 6500-E/6807-XL –8Q4T Ingress Model

```
policy-map type lan-queuing APIC_EM-QUEUEING-8Q4T-IN
 class APIC_EM-REALTIME-8Q4T-QUEUE
  bandwidth percent 10
 class APIC_EM-CONTROL-8Q4T-QUEUE
  bandwidth percent 10
 class APIC_EM-MM_CONF-8Q4T-QUEUE
  bandwidth percent 20
  random-detect dscp-based
  random-detect dscp af41 percent 80 100
  random-detect dscp af42 percent 70 100
  random-detect dscp af43 percent 60 100
 class APIC_EM-MM_STREAM-8Q4T-QUEUE
  bandwidth percent 20
  random-detect dscp-based
  random-detect dscp af31 percent 80 100
  random-detect dscp af32 percent 70 100
  random-detect dscp af33 percent 60 100
```


Catalyst 6500-E/6807-XL –8Q4T Ingress Model

```
[continued]
class APIC_EM-TRANS_DATA-8Q4T-QUEUE
  bandwidth percent 10
  random-detect dscp-based
  random-detect dscp af21 percent 80 100
  random-detect dscp af22 percent 70 100
  random-detect dscp af23 percent 60 100
 class APIC_EM-BULK_DATA-8Q4T-QUEUE
  bandwidth percent 4
  random-detect dscp-based
  random-detect dscp af11 percent 80 100
  random-detect dscp af12 percent 70 100
  random-detect dscp af13 percent 60 100
 class APIC_EM-SCAVENGER-8Q4T-QUEUE
  bandwidth percent 1
 class class-default
  random-detect dscp-based
  random-detect dscp default percent 80 100
```

```
interface TenGigabitEthernet1/3/4
 service-policy type lan-queuing input APIC_EM-QUEUEING-8Q4T-IN
```

8Q8T – Ingress Queueing CoS to Queue Mapping CoS-based Tail-Drop

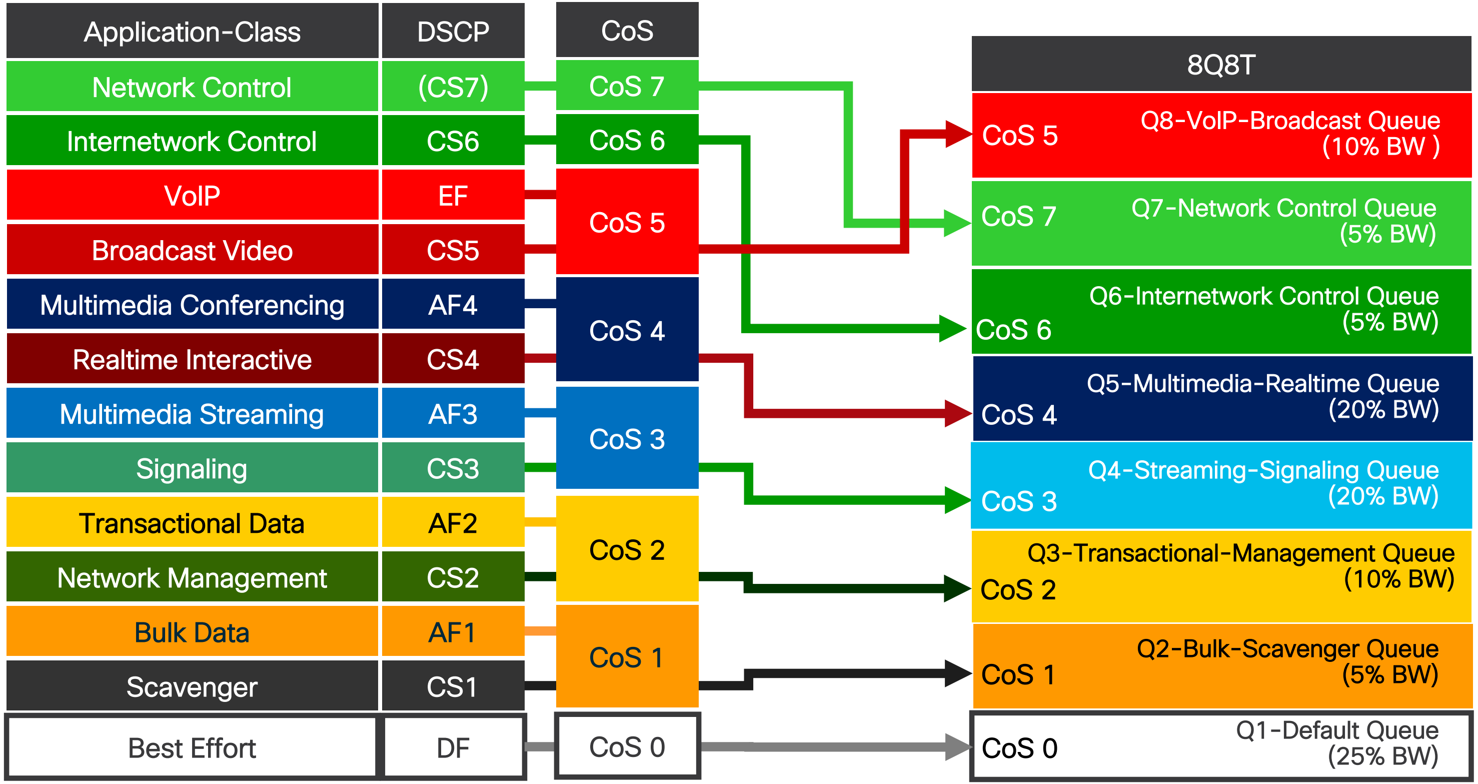
8Q8T Ingress Queueing Linecards

WS-X6704-10GE supported with a DFC4/DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL)

```
o23-6500-1#show module
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1   48  CEF720 48 port 10/100/1000mb Ethernet  WS-X6748-GE-TX     SAL10478SWP
  2    8  DCEF2T 8 port 10GE                     WS-X6908-10G       SAL172682AK
  3    5  Supervisor Engine 2T 10GE w/ CTS (Acti VS-SUP2T-10G       SAL1702WNR0
  5   16  CEF720 16 port 10GE                    WS-X6716-10GE      SAL1228WYB7
  6    4  CEF720 4 port 10-Gigabit Ethernet      WS-X6704-10GE      SAL15013XBH

…

Mod  Sub-Module                  Model              Serial       Hw     Status
---- --------------------------- ------------------ ----------- ------- -------
  1  Centralized Forwarding Card WS-F6700-CFC       SAD074308C9  1.1    Ok
  2  Distributed Forwarding Card WS-F6K-DFC4-E      SAL17152T2R  1.2    Ok
  3  Policy Feature Card 4       VS-F6K-PFC4        SAL1638N3R3  1.2    Ok
  3  CPU Daughterboard           VS-F6K-MSFC5       SAL1702WNG1  1.5    Ok
  5  Distributed Forwarding Card WS-F6K-DFC4-E      SAL1541SQHX  1.1    Ok
  6  Centralized Forwarding Card WS-F6700-CFC       SAL1518CRZ3  4.1    PwrDown
```

Cisco Catalyst 6500-E/6807-XL with Sup2T

8Q8T Ingress Queuing Models—CoS-to-Queue Mapping CoS-based WRED



Catalyst 6500-E/6807-XL –8Q8T Ingress Model

```
class-map type lan-queuing match-all APIC_EM-Q8-8Q8T-QUEUE
 match cos 7
Class-map type lan-queuing match-all APIC_EM-Q7-8Q8T-QUEUE
 match cos 6
class-map type lan-queuing match-all APIC_EM-Q6-8Q8T-QUEUE
 match cos 5
class-map type lan-queuing match-all APIC_EM-Q5-8Q8T-QUEUE
 match cos 4
class-map type lan-queuing match-all APIC_EM-Q4-8Q8T-QUEUE
 match cos 3
class-map type lan-queuing match-all APIC_EM-Q3-8Q8T-QUEUE
 match  cos 2
class-map type lan-queuing match-all APIC_EM-Q2-8Q8T-QUEUE
 match  cos 1
```


Catalyst 6500-E/6807-XL –8Q8T Ingress Model

```
policy-map type lan-queuing APIC_EM-QUEUEING-8Q8T-IN
 class APIC_EM-Q8-8Q8T-QUEUE
  bandwidth percent 10
 class APIC_EM-Q7-8Q8T-QUEUE
  bandwidth percent 5
 class APIC_EM-Q6-8Q8T-QUEUE
  bandwidth percent 5
 class APIC_EM-Q5-8Q8T-QUEUE
  bandwidth percent 20
 class APIC_EM-Q4-8Q8T-QUEUE
  bandwidth percent 20
 class APIC_EM-Q3-8Q8T-QUEUE
  bandwidth percent 10
 class APIC_EM-Q2-8Q8T-QUEUE
  bandwidth percent 5
 class class-default
```

```
interface TenGigabitEthernet1/3/4
service-policy type lan-queuing input APIC_EM-QUEUEING-8Q8T-IN
```

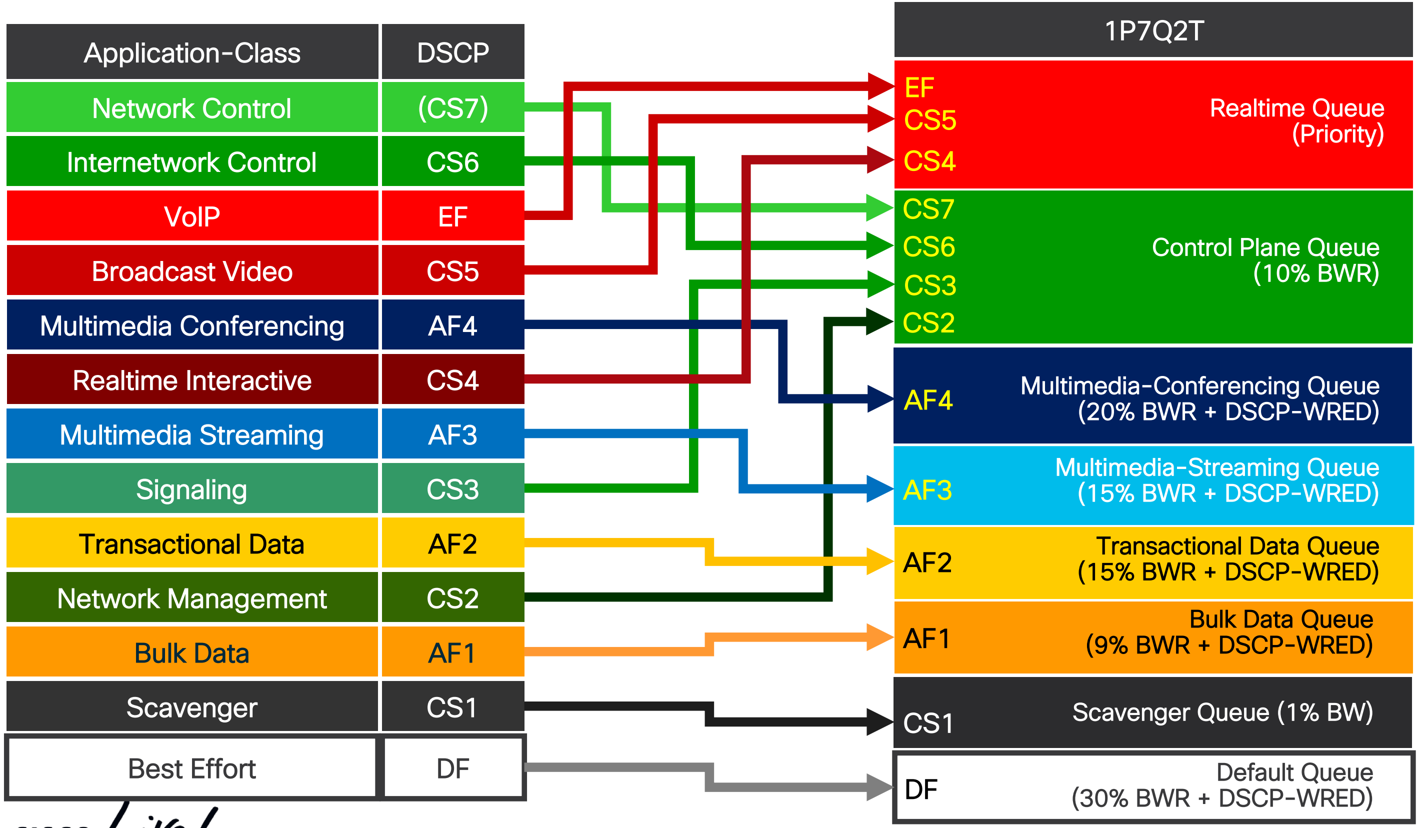

1P7Q2T - Ingress Queueing DSCP to Queue Mapping DSCP-based WRED

1P7Q2T Ingress Queueing Linecards

- WS-X6716-10G-3C, WS-X6716-10G-3CXL, WS-X6716-10T-3C, WS-X6716-10T-3CXL with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-E, WS-F6k-DFC4-EXL) in oversubscription mode
- WS-X6816-10T-2T, WS-X6816-10T-2TXL, WS-X6816-10G-2T, WS-X6816-10G-2TXL in oversubscription mode

Cisco Catalyst 6500-E/6807-XL with Sup2T

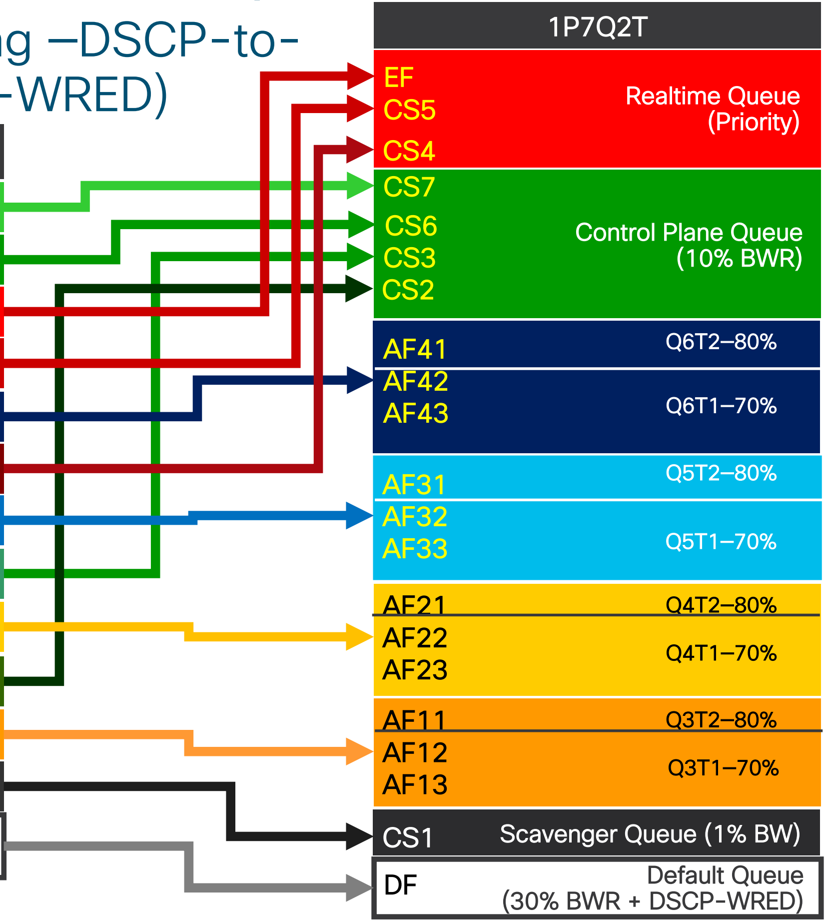
1P7Q2T Ingress Queuing Models–DSCP-to-Queue Mapping



Cisco Catalyst 6500-E/6807-XL with Sup2T

1P7Q2T Ingress Queuing –DSCP-to-Queue Mapping (DSCP-WRED)

Application-Class	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF



All noted thresholds are Min WRED thresholds

All max WRED thresholds Are set to 100%

Multimedia-Conferencing Queue (20% BWR + DSCP-WRED)

Multimedia-Streaming Queue (15% BWR + DSCP-WRED)

Transactional Data Queue (15% BWR + DSCP-WRED)

Bulk Data Queue (9% BWR + DSCP-WRED)

Cisco Catalyst 6500-E/6807-XL - 1P7Q2T Ingress Model

```
class-map type lan-queuing match-all APIC_EM-REALTIME-1P7Q2T-QUEUE
 match dscp cs4 cs5 ef
class-map type lan-queuing match-all APIC_EM-CONTROL-1P7Q2T-QUEUE
 match dscp cs2 cs3 cs6 cs7
class-map type lan-queuing match-all APIC_EM-MM_CONF-1P7Q2T-QUEUE
 match dscp af41 af42 af43
class-map type lan-queuing match-all APIC_EM-MM_STREAM-1P7Q2T-QUEUE
 match dscp af31 af32 af33
class-map type lan-queuing match-all APIC_EM-TRANS_DATA-1P7Q2T-QUEU
 match  dscp af21  af22  af23
class-map type lan-queuing match-all APIC_EM-BULK_DATA-1P7Q2T-QUEUE
 match  dscp af11  af12  af13
class-map type lan-queuing match-all APIC_EM-SCAVENGER-1P7Q2T-QUEUE
 match dscp cs1
```

Catalyst 6500-E/6807-XL –1P7Q2T Ingress Model

```
policy-map type lan-queuing APIC_EM-QUEUEING-1P7Q2T-IN
 class APIC_EM-REALTIME-1P7Q2T-QUEUE
  priority
 class APIC_EM-CONTROL-1P7Q2T-QUEUE
  bandwidth remaining percent 10
class APIC_EM-MM_CONF-1P7Q2T-QUEUE
  bandwidth remaining percent 20
class APIC_EM-MM_STREAM-1P7Q2T-QUEUE
  bandwidth remaining percent 15
```

Catalyst 6500-E/6807-XL - 1P7Q2T Ingress Model

```
[continued]
class APIC_EM-TRANS_DATA-1P7Q2T-QUEU
  bandwidth remaining percent 15
class APIC_EM-BULK_DATA-1P7Q2T-QUEUE
  bandwidth remaining percent 9
class APIC_EM-SCAVENGER-1P7Q2T-QUEUE
  bandwidth remaining percent 1
 class class-default
```

```
interface TenGigabitEthernet1/3/4
service-policy type lan-queuing input APIC_EM-QUEUEING-1P7Q2T-IN
```

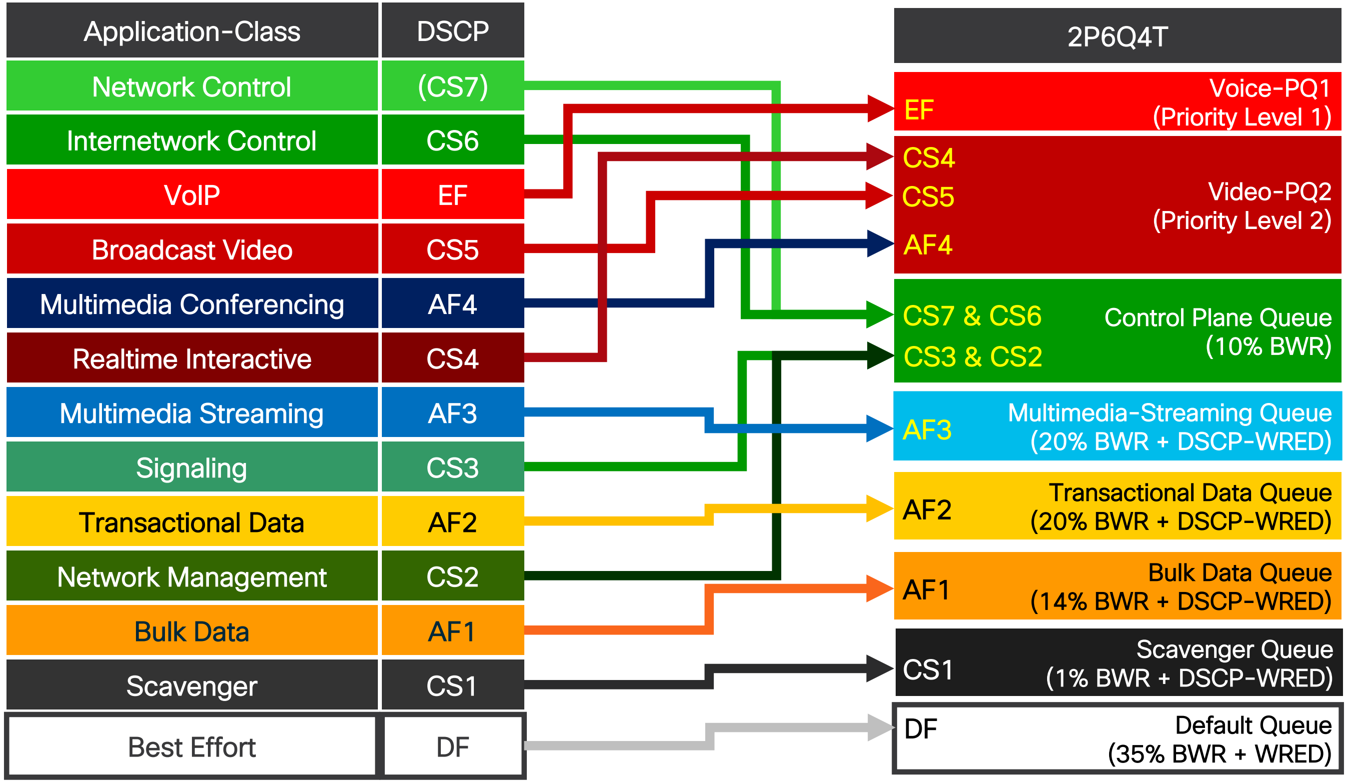
2P6Q4T Ingress & Egress Queueing
DSCP to Queue Mapping
DSCP-based WRED

2P6Q4T Ingress Queueing Linecards

- WS-X6904-40G-2T and WS-X6904-40G-2TXL
- C6800-8P10G, C6800-8P10G-XL
- C6800-16P10G, C6800-16P10G-XL
- C6800-32P10G, C6800-32P10G-XL

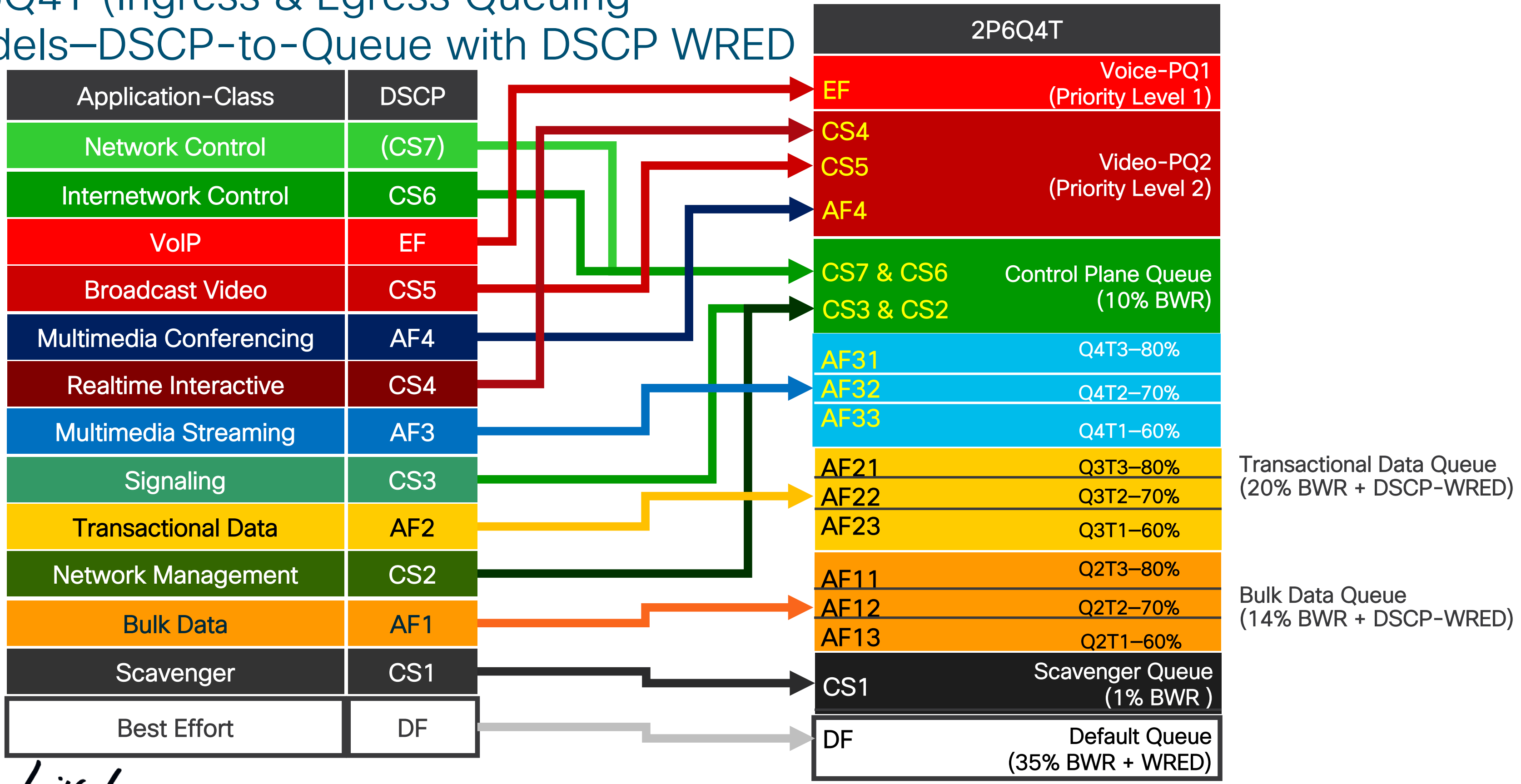
Cisco Catalyst 6500-E/6807-XL with Sup2T

2P6Q4T (Ingress & Egress Queuing Models–DSCP-to-Queue)



Cisco Catalyst 6500-E/6807-XL with Sup2T

2P6Q4T (Ingress & Egress Queuing Models–DSCP-to-Queue with DSCP WRED



Cisco Catalyst 6500-E/6807-XL—2P6Q4T Model

Part 1 of 3—Common Ingress & Egress Queuing Class-Maps

```
class-map type lan-queuing match-all APIC_EM-VOICE-2P6Q4T-PQ1
 match dscp ef
class-map type lan-queuing match-all APIC_EM-VIDEO-2P6Q4T-PQ2
 match dscp cs4 cs5 af41 af42 af43
class-map type lan-queuing match-all APIC_EM-CONTROL-2P6Q4T-QUEUE
 match dscp cs2 cs3 cs6 cs7
class-map type lan-queuing match-all APIC_EM-MM_STREAM-2P6Q4T-QUEUE
 match dscp af31 af32 af33
class-map type lan-queuing match-all APIC_EM-TRANS_DATA-2P6Q4T-QUEUE
 match dscp af21 af22 af23
class-map type lan-queuing match-all APIC_EM-BULK_DATA-2P6Q4T-QUEUE
 match dscp af11 af12 af13
class-map type lan-queuing match-all APIC_EM-SCAVENGER-2P6Q4T-QUEUE
 match dscp cs1
```


Cisco Catalyst 6500-E/6807-XL—2P6Q4T Model

Part 2 of 3—2P6Q4T Queuing Policy-Map

```
policy-map type lan-queuing APIC_EM-QUEUING-2P6Q4T
 class APIC_EM-VOICE-2P6Q4T-PQ1
  priority level 1
 class APIC_EM-VIDEO-2P6Q4T-PQ2
  priority level 2
 class APIC_EM-CONTROL-2P6Q4T-QUEUE
  bandwidth remaining percent 10
 class APIC_EM-MM_STREAM-2P6Q4T-QUEUE
  bandwidth remaining percent 20
  random-detect dscp-based
  random-detect dscp af31 percent 80 100
  random-detect dscp af32 percent 70 100
  random-detect dscp af33 percent 60 100
 class APIC_EM-TRANS_DATA-2P6Q4T-QUEUE
  bandwidth remaining percent 20
  random-detect dscp-based
  random-detect dscp af21 percent 80 100
  random-detect dscp af22 percent 70 100
  random-detect dscp af23 percent 60 100
```

Cisco Catalyst 6500-E/6807-XL–2P6Q4T Model

Part 3 of 3–2P6Q4T Queuing Policy-Map (continued)

```
[continued]
class APIC_EM-BULK_DATA-2P6Q4T-QUEUE
  bandwidth remaining percent 14
  random-detect dscp-based
  random-detect dscp af11 percent 80 100
  random-detect dscp af12 percent 70 100
  random-detect dscp af13 percent 60 100
class APIC_EM-SCAVENGER-2P6Q4T-QUEUE
  bandwidth remaining percent 1
class class-default
  random-detect dscp-based
  random-detect dscp default percent 80 100
```

```
interface TenGigabitEthernet1/1/13
 service-policy type lan-queuing input APIC_EM-QUEUEING-2P6Q4T
 service-policy type lan-queuing output APIC_EM-QUEUEING-2P6Q4T
```

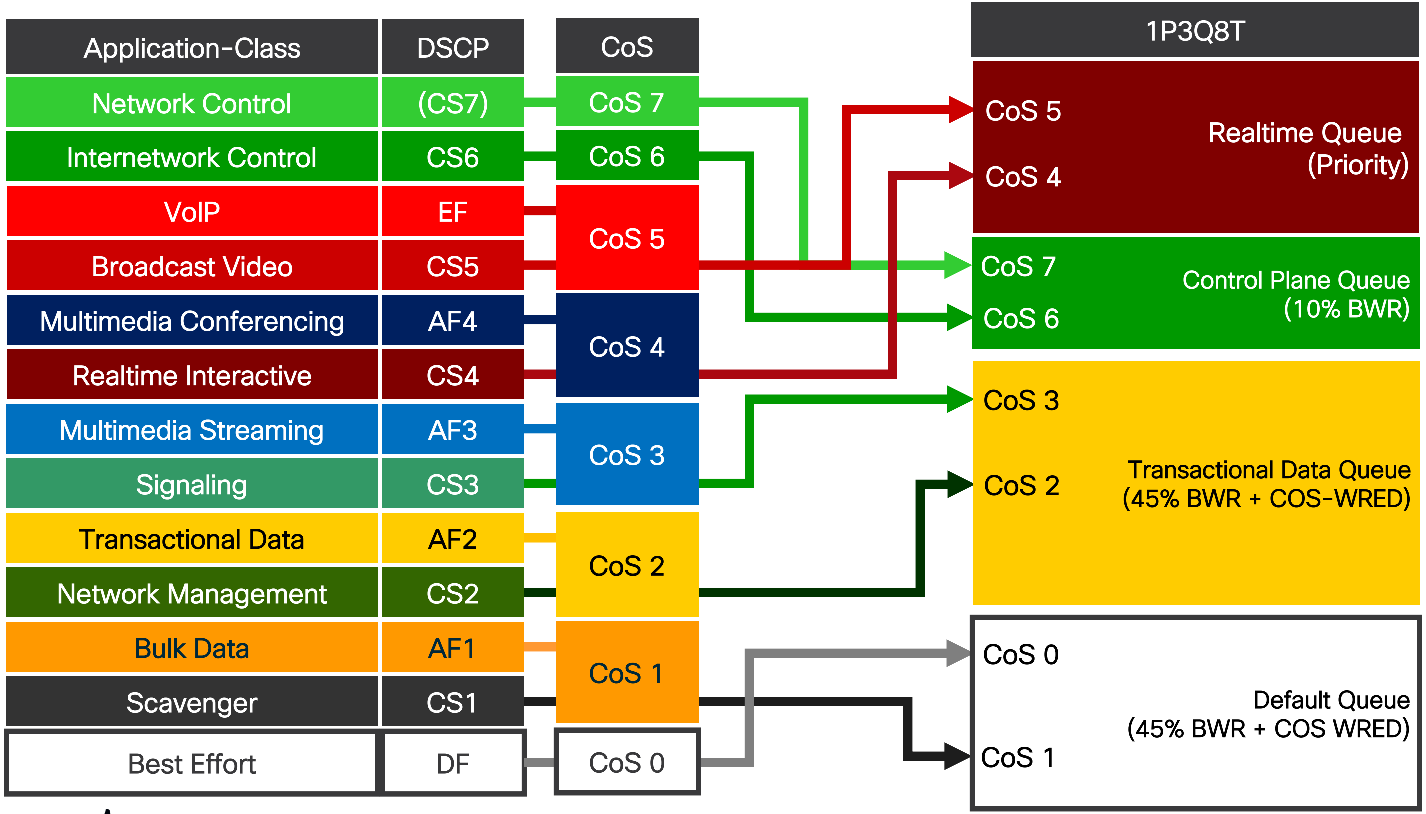
1P3Q8T - Egress Queueing
CoS to Queue Mapping
CoS-based Tail-Drop

1P3Q8T Egress Queueing Linecards

- WS-X6724-SFP, WS-X6748-SFP and WS-X6748-GE-TX with CFC
- WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL)
- WS-X6824-SFP-2T and WS-X6824-SFP-2TXL
- WS-X6848-SFP-2T, WS-X6848-SFP-2TXL, WS-X6848-TX-2T and WS-X6848-TX-2TXL

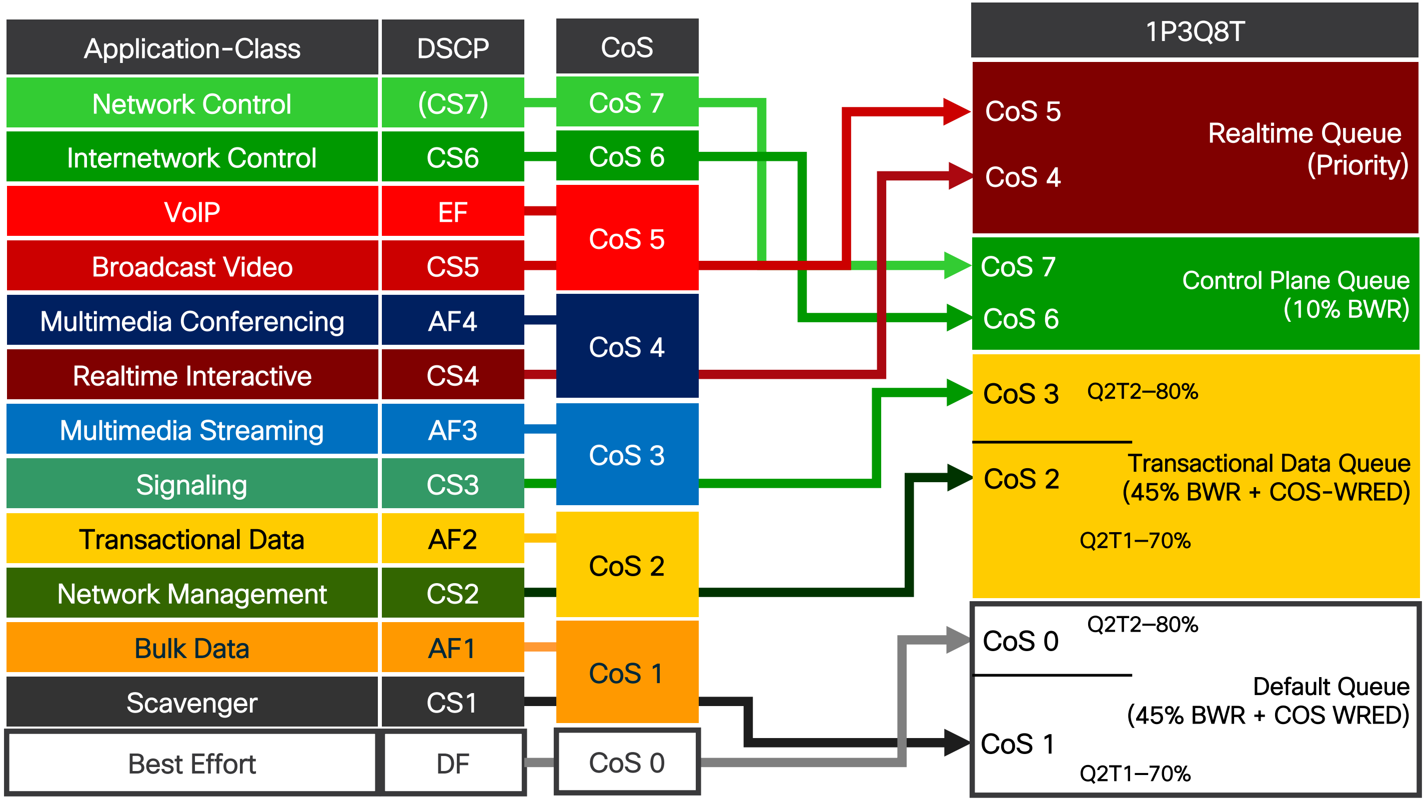
Cisco Catalyst 6500-E/6807-XL with Sup2T

1P3Q8T Egress Queuing Models—CoS-to-Queue Mapping



Cisco Catalyst 6500-E/6807-XL with Sup2T

1P3Q8T Egress Queuing Models—CoS-to-Queue Mapping with CoS-WRED



All noted thresholds are Min WRED thresholds

All max WRED thresholds Are set to 100%

Catalyst 6500-E/6807-XL—1P3Q8T Egress Model

```
class-map type lan-queuing match-all APIC_EM-REALTIME-1P3Q8T-QUEUE
 match cos 4 5
class-map type lan-queuing match-all APIC_EM-CONTROL-1P3Q8T-QUEUE
 match cos 6 7
class-map type lan-queuing match-all APIC_EM-TRANS_DATA-1P3Q8T-QUEUE
 match cos 2 3
```

Cisco Catalyst 6500-E/6807-XL –1P3Q8T Egress Model

```
policy-map type lan-queuing APIC_EM-QUEUING-1P3Q8T-OUT
 class APIC_EM-REALTIME-1P3Q8T-QUEUE
  priority
 class APIC_EM-CONTROL-1P3Q8T-QUEUE
  bandwidth remaining percent 5
 class APIC_EM-TRANS_DATA-1P3Q8T-QUEUE
  bandwidth remaining percent 45
  random-detect cos-based
  random-detect cos 3 percent 80 100
  random-detect cos 2 percent 70 100
 class class-default
  random-detect cos-based
  random-detect cos 0 percent 80 100
  random-detect cos 1 percent 70 100
```

```
interface GigabitEthernet1/3/2
 service-policy type lan-queuing output APIC_EM-QUEUING-1P3Q8T-OUT
```

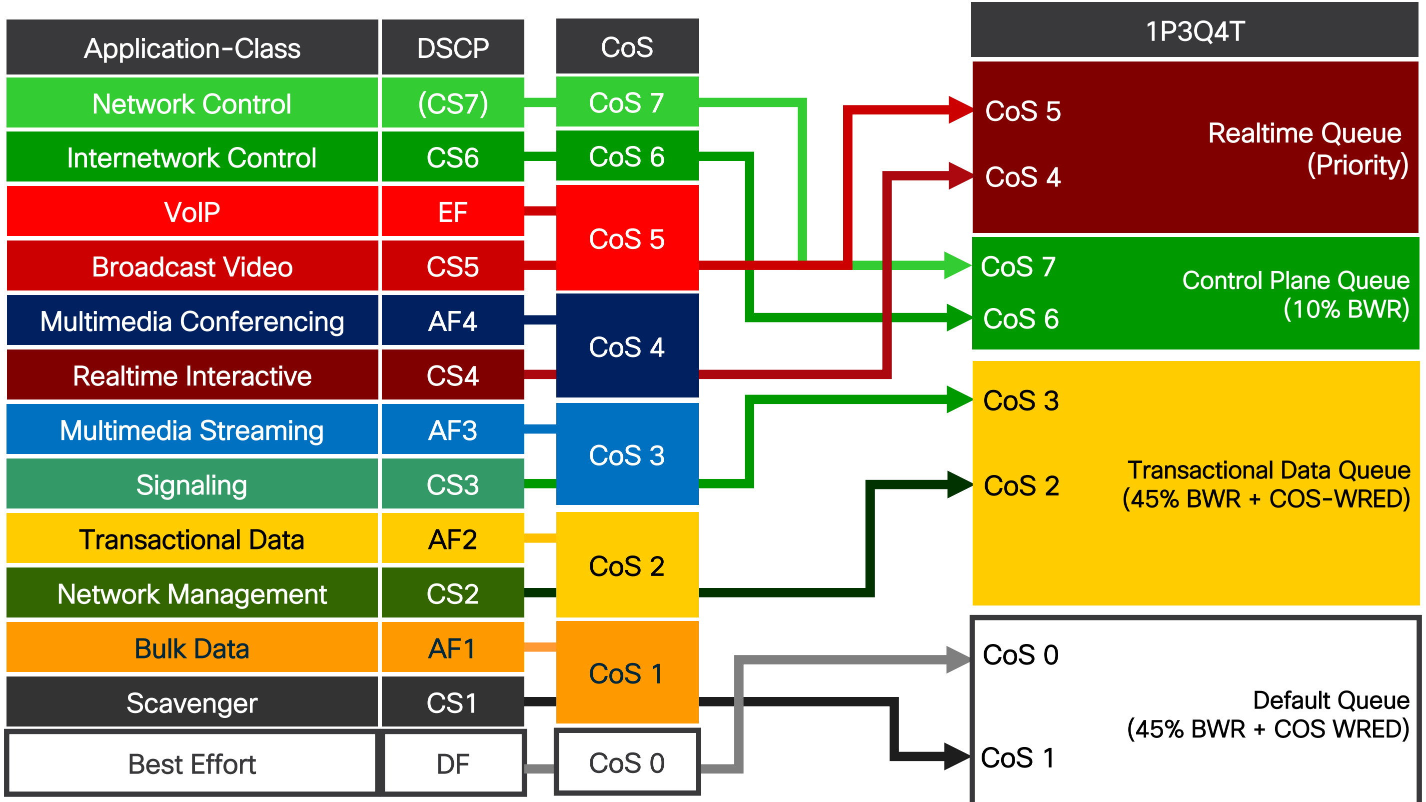
1P3Q4T – Egress Queueing CoS to Queue Mapping CoS-based Tail-Drop

1P3Q4T Egress Queueing Linecards

- VS-S2T-10G and VS-S2T-10G-XL with Gigabit Ethernet ports enabled

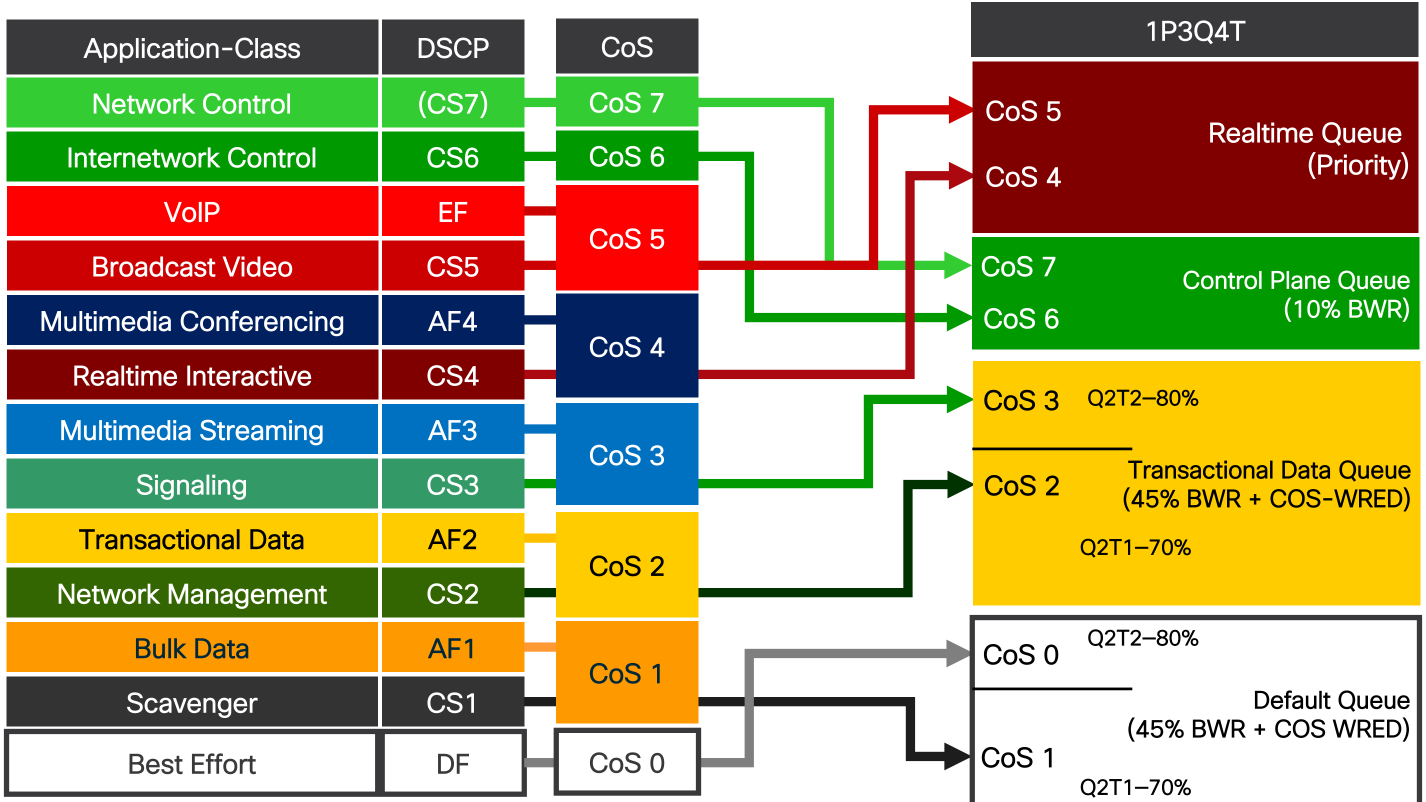
Cisco Catalyst 6500-E/6807-XL with Sup2T

1P3Q4T Egress Queuing Models–CoS-to-Queue Mapping



Cisco Catalyst 6500-E/6807-XL with Sup2T

1P3Q4T Egress Queuing Models—CoS-to-Queue Mapping with CoS WRED



All noted thresholds are Min WRED thresholds

All max WRED thresholds Are set to 100%

Catalyst 6500-E/6807-XL –1P3Q4T Egress Model

```
class-map type lan-queuing match-all APIC_EM-REALTIME-1P3Q4T-QUEUE
 match cos 4 5
class-map type lan-queuing match-all APIC_EM-CONTROL-1P3Q4T-QUEUE
 match cos 6 7
class-map type lan-queuing match-all APIC_EM-TRANS_DATA-1P3Q4T-QUEUE
 match cos 2 3
```

Catalyst 6500-E/6807-XL –1P3Q4T Egress Model

```
policy-map type lan-queuing APIC_EM-QUEUING-1P3Q4T-OUT
 class APIC_EM-REALTIME-1P3Q4T-QUEUE
  priority
 class APIC_EM-CONTROL-1P3Q4T-QUEUE
  bandwidth remaining percent 5
 class APIC_EM-TRANS_DATA-1P3Q4T-QUEUE
  bandwidth remaining percent 45
  random-detect cos-based
  random-detect cos 3 percent 80 100
  random-detect cos 2 percent 70 100
 class class-default
  random-detect cos-based
  random-detect cos 0 percent 80 100
  random-detect cos 1 percent 70 100
```

```
interface GigabitEthernet1/3/1
  service-policy type lan-queuing output APIC_EM-QUEUING-1P3Q4T-OUT
interface TenGigabitEthernet1/3/4
  service-policy type lan-queuing output APIC_EM-QUEUING-1P3Q4T-OUT
```

1P7Q4T –Egress Queueing DSCP to Queue Mapping DSCP-based WRED

1P7Q4T Egress Queueing Linecards

- WS-X6716-10G-3C, WS-X6716-10G-3CXL, WS-X6716-10T-3C, WS-X6716-10T-3CXL with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-E, WS-F6k-DFC4-EXL) in performance or oversubscription mode
- WS-X6816-10T-2T, WS-X6816-10T-2TXL, WS-X6816-10G-2T, WS-X6816-10G-2TXL in performance or oversubscription mode
- WS-X6908-10G-2T and WS-X6908-10G-2TXL

Cisco Catalyst 6500-E/6807-XL with Sup2T

1P7Q4T Egress Queuing Models—DSCP-to-Queue Mapping

Application-Class	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

1P7Q4T	
EF CS5 CS4	Realtime Queue (Priority)
CS7 CS6 CS3 CS2	Control Plane Queue (10% BWR)
AF4	Multimedia-Conferencing Queue (20% BWR + DSCP-WRED)
AF3	Multimedia-Streaming Queue (15% BWR + DSCP-WRED)
AF2	Transactional Data Queue (15% BWR + DSCP-WRED)
AF1	Bulk Data Queue (9% BWR + DSCP-WRED)
CS1	Scavenger Queue (1% BW)
DF	Default Queue (30% BWR + DSCP-WRED)

Cisco Catalyst 6500-E/6807-XL with Sup2T

1P7Q4T Egress Queuing Models—DSCP-to-Queue with DSCP-WRED

Application-Class	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

1P7Q4T

DSCP	Queue / Threshold
EF, CS5, CS4	Realtime Queue (Priority)
CS7, CS6, CS3, CS2	Control Queue (10% BWR)
AF41	Q6T3–80%
AF42	Q6T2–70%
AF43	Q6T1–60%
AF31	Q5T3–80%
AF32	Q5T2–70%
AF33	Q5T1–60%
AF21	Q4T3–80%
AF22	Q4T2–70%
AF23	Q4T1–60%
AF11	Q3T3–80%
AF12	Q3T2–70%
AF13	Q3T1–60%
CS1	Scavenger Queue (1% BWR)
DF	Default Queue (30% BWR + DSCP-WRED)

Multimedia-Conferencing Queue (20% BWR + DSCP-WRED)

Multimedia-Streaming Queue (15% BWR + DSCP-WRED)

Transactional Data Queue (15% BWR + DSCP-WRED)

Bulk Data Queue (9% BWR + DSCP-WRED)

All noted thresholds are Min WRED thresholds

All max WRED thresholds Are set to 100%

Catalyst 6500-E/6807-XL –1P7Q4T Egress Model

```
class-map type lan-queuing match-all APIC_EM-REALTIME-1P7Q4T-QUEUE
 match dscp cs4 cs5 ef
class-map type lan-queuing match-all APIC_EM-CONTROL-1P7Q4T-QUEUE
 match dscp cs2 cs3 cs6 cs7
class-map type lan-queuing match-all APIC_EM-MM_CONF-1P7Q4T-QUEUE
 match dscp af41 af42 af43
class-map type lan-queuing match-all APIC_EM-MM_STREAM-1P7Q4T-QUEUE
 match dscp af31 af32 af33
class-map type lan-queuing match-all APIC_EM_TRANS_DATA-1P7Q4T-QUEUE
 match  dscp af21  af22  af23
class-map type lan-queuing match-all APIC_EM_BULK_DATA-1P7Q4T-QUEUE
 match  dscp af11  af12  af13
class-map type lan-queuing match-all APIC_EM_SCAVENGER-1P7Q4T-QUEUE
 match dscp cs1
```


Cisco Catalyst 6500-E/6807-XL –1P7Q4T Egress Model

```
policy-map type lan-queuing APIC_EM-QUEUING-1P7Q4T-OUT
 class APIC_EM-REALTIME-1P7Q4T-QUEUE
  priority
 class APIC_EM-CONTROL-1P7Q4T-QUEUE
  bandwidth remaining percent 10
class APIC_EM-MM_CONF-1P7Q4T-QUEUE
  bandwidth remaining percent 20
  random-detect dscp-based
  random-detect dscp af41 percent 80 100
  random-detect dscp af42 percent 70 100
  random-detect dscp af42 percent 60 100
 class APIC_EM-MM_STREAM-1P7Q4T-QUEUE
  bandwidth remaining percent 15
  random-detect dscp-based
  random-detect dscp af31 percent 80 100
  random-detect dscp af32 percent 70 100
  random-detect dscp af33 percent 60 100
```


Cisco Catalyst 6500-E/6807-XL –1P7Q4T Egress Model

```
[continued]
class APIC_EM_TRANS_DATA-1P7Q4T-QUEUE
  bandwidth remaining percent 15
  random-detect dscp-based
  random-detect dscp af21 percent 80 100
  random-detect dscp af22 percent 70 100
  random-detect dscp af23 percent 60 100
class APIC_EM_BULK_DATA-1P7Q4T-QUEUE
  bandwidth remaining percent 9
  random-detect dscp-based
  random-detect dscp af11 percent 80 100
  random-detect dscp af12 percent 70 100
  random-detect dscp af13 percent 60 100
class APIC_EM_SCAVENGER-1P7Q4T-QUEUE
  bandwidth remaining percent 1
 class class-default
  random-detect dscp-based
  random-detect dscp default percent 80 100
```

```
interface TenGigabitEthernet1/3/4
 service-policy type lan-queuing output APIC_EM-QUEUING-1P7Q4T-OUT
```

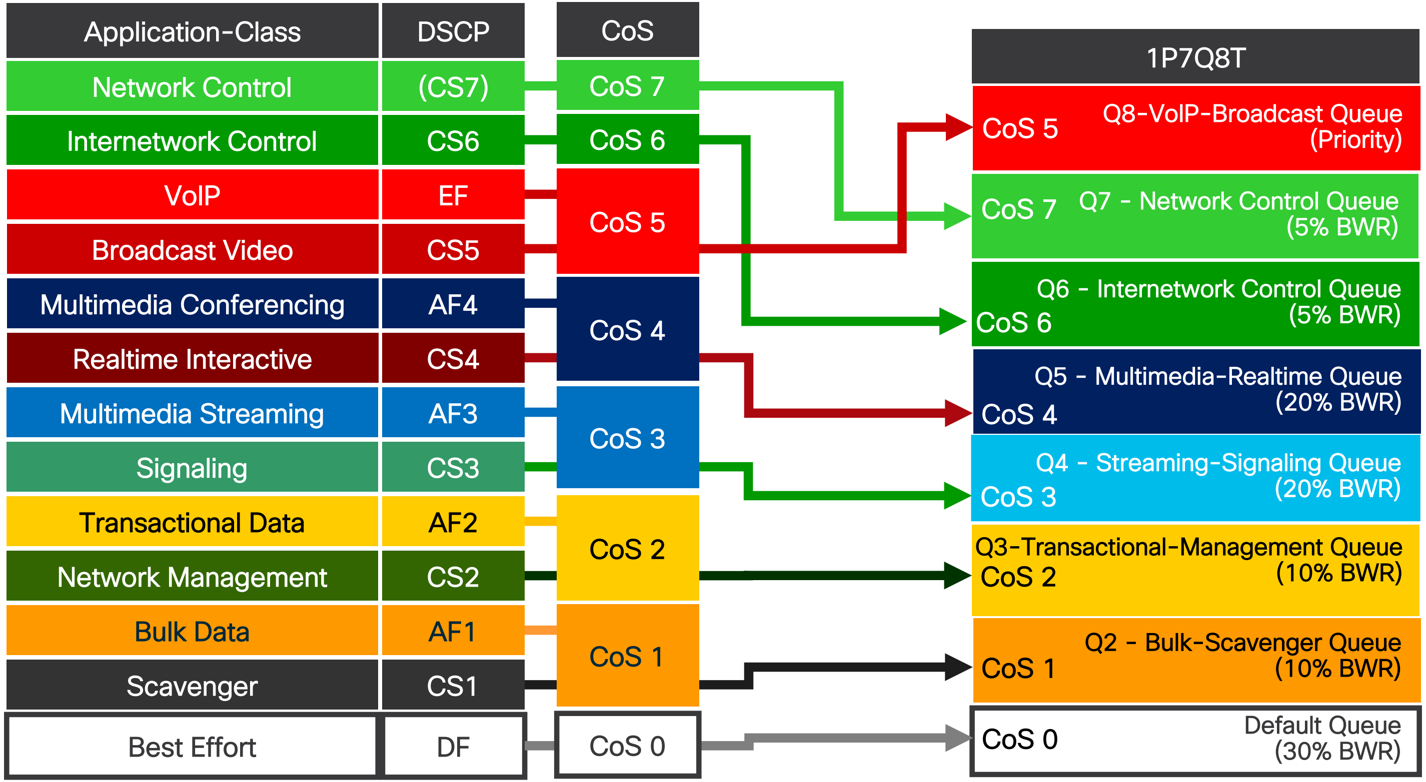

1P7Q8T - Egress Queueing CoS to Queue Mapping CoS-based Tail-Drop

1P7Q8T Egress Queueing Linecards

- WS-X6704-10GE with CFC
- WS-X6704-10GE with a DFC4 or DFC4XL upgrade (WS-F6k-DFC4-A, WS-F6k-DFC4-AXL)

Cisco Catalyst 6500-E/6807-XL with Sup2T

1P7Q8T Egress Queuing Models—CoS-to-Queue Mapping CoS-based WRED



Catalyst 6500-E/6807-XL –1P7Q8T Egress Model

```
class-map type lan-queuing match-all APIC_EM-Q8-1P7Q8T-QUEUE
 match cos 7
class-map type lan-queuing match-all APIC_EM-Q7-1P7Q8T-QUEUE
 match cos 6
class-map type lan-queuing match-all APIC_EM-Q6-1P7Q8T-QUEUE
 match cos 5
class-map type lan-queuing match-all APIC_EM-Q5-1P7Q8T-QUEUE
 match cos 4
class-map type lan-queuing match-all APIC_EM-Q4-1P7Q8T-QUEUE
 match cos 3
class-map type lan-queuing match-all APIC_EM-Q3-1P7Q8T-QUEUE
 match  cos 2
class-map type lan-queuing match-all APIC_EM-Q2-1P7Q8T-QUEUE
 match  cos 1
```


Catalyst 6500-E/6807-XL –1P7Q8T Egress Model

```
policy-map type lan-queuing APIC_EM-QUEUING-1P7Q8T-OUT
 class APIC_EM-Q8-1P7Q8T-QUEUE
  priority
 class APIC_EM-Q7-1P7Q8T-QUEUE
  bandwidth remaining percent 5
 class APIC_EM-Q6-1P7Q8T-QUEUE
  bandwidth remaining percent 5
 class APIC_EM-Q5-1P7Q8T-QUEUE
  bandwidth remaining percent 20
 class APIC_EM-Q4-1P7Q8T-QUEUE
  bandwidth remaining percent 20
 class APIC_EM-Q3-1P7Q8T-QUEUE
  bandwidth remaining percent 10
 class APIC_EM-Q2-1P7Q8T-QUEUE
  bandwidth remaining percent 10
 class class-default
```

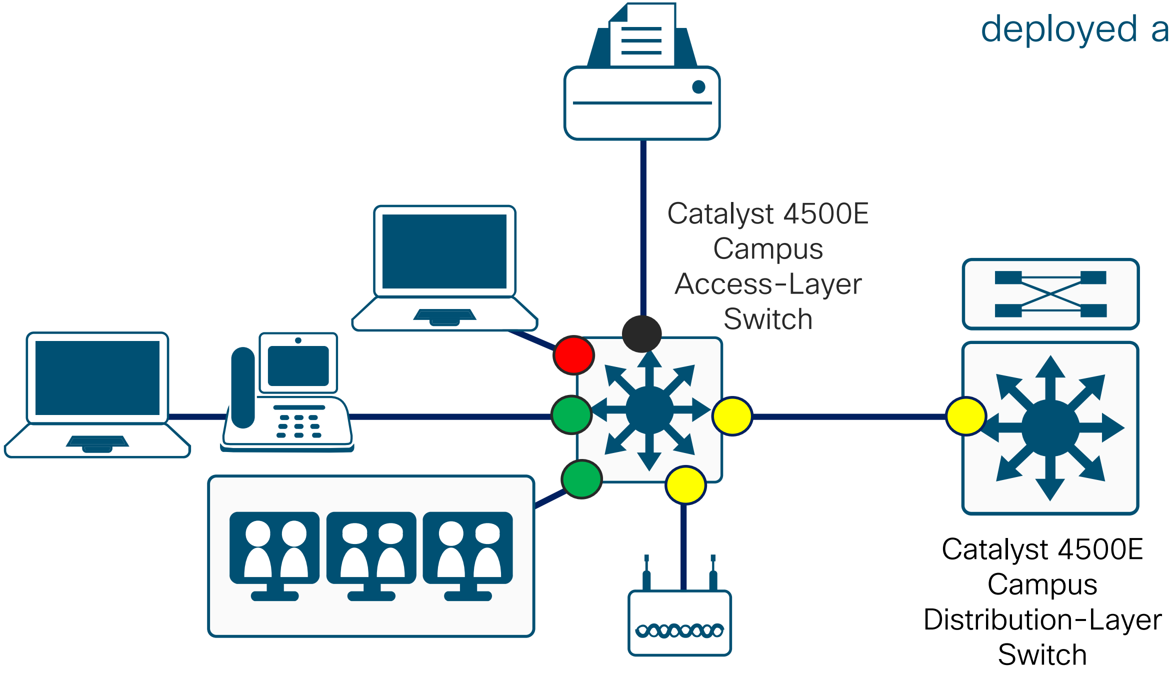
```
interface TenGigabitEthernet1/3/4
 service-policy type lan-queuing output APIC_EM-QUEUING-1P7Q8T-OUT
```

Appendix B: Cisco Catalyst 4500E QoS Design

Catalyst 4500E

QoS Roles in the Campus

The primary role of the Catalyst 4500E Series switch is as a distribution-layer switch. However, it is also sometimes deployed as an access-layer switch.



- No Trust + Ingress Queuing + Egress Queuing
- Trust DSCP + Ingress Queuing + Egress Queuing
- Conditional Trust + Ingress Queuing + Egress Queuing
- Classification/Marking + [Optional Policing] + Ingress Queuing + Egress Queuing

Catalyst 4500E
QoS Design Steps (Access-Layer Switch)

1. Configure Ingress QoS Model(s):
   - ❑ Trust DSCP / CoS Model (Default)*
   - ❑ Conditional Trust Model
   - ❑ Service Policy Models
2. Configure Egress Queuing

* Note: Catalyst 4500E uses MQC QoS, which trusts by default. Therefore no explicit policy is required for DSCP trust.

Catalyst 4500E

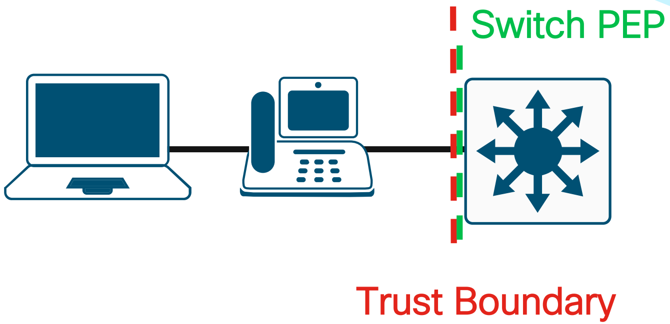
Conditional Trust Example

Catalyst 4500E supports both **match-all** (logical AND) and **match-any** (logical OR) operators

Conditional trust command (**trust device**) must be prefaced by **qos** on the Catalyst 4500E

```
class-map match-all VOICE
 match cos 5
class-map match-all SIGNALING
 match cos 3
!
policy-map CISCO-IPPHONE
 class VOICE
  set dscp ef
 class SIGNALING
  set dscp cs3
 class class-default
  set dscp default
```

```
interface GigabitEthernet 3/1
 qos trust device cisco-phone
 service-policy input CISCO-IPPHONE
```



Catalyst 4500E

Classification Options

- ACL-based classification: **match access-group** *ACL_NAME*
  - Syntax is identical to Catalyst 2960-X / 3560-X / 3750-X ACL-based classification & marking examples
- Application Visibility and Control with Domain Name System-Authoritative Source (AVC with DNS-AS) classification (IOS 15.2(5)E / IOS XE 3.9.0E and Higher) **match protocol attribute**
  - Supervisor Engines 9-E, 8-E, 8L-E, 7-E, 7L-E with IP Base and IP Services
  - Note: The Catalyst 4500E does NOT support NBAR2

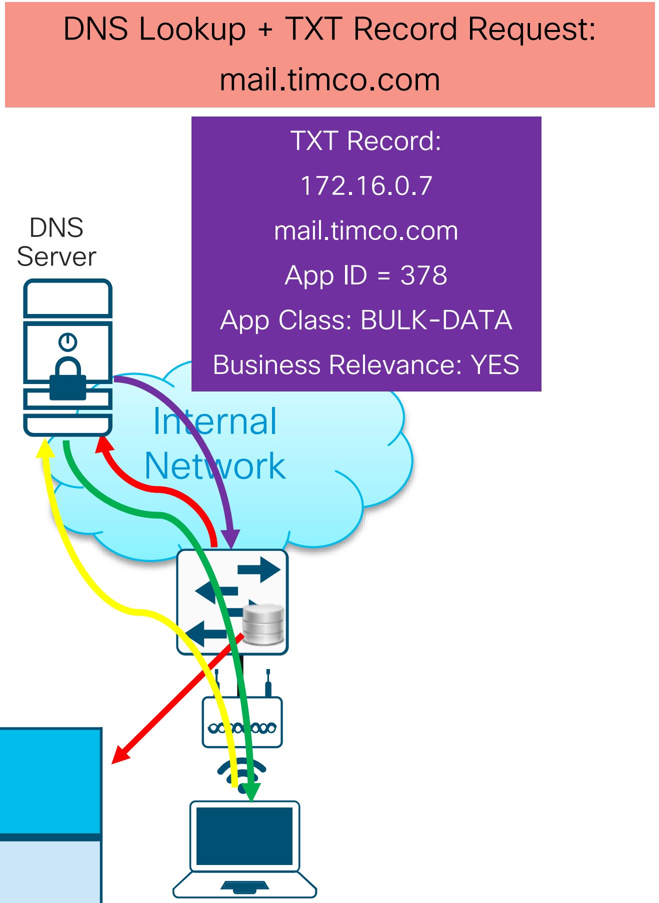
DNS-Authoritative Source (DNS-AS)

What is DNS-AS?

- Application visibility end-to-end in the network
- Light-weight application detection process
- A scalable means of identifying encrypted & cloud applications
- An efficient means to distribute application metadata
- No client software requirement
- Simplified end-to-end policy enforcement

DNS-AS Operation

1) Client requests a DNS Lookup
2) Access Switch examines the DNS request
3) Internal DNS Server returns a DNS response (A-Record)
4) Access Switch requests application metadata information by generating *its own* DNS query
5) Internal DNS Server returns application metadata (A-Record + TXT Record)
6) Access Switch maintains a Binding Table of application metadata



IP Address	PTR	App-ID	App-Class	Business-Relevance
172.16.0.7	mail.timco.com	378	Bulk Data	YES

cisco Live!

Catalyst 4500E

AVC with DNS-AS Classification & Marking Policy Example

```
!
avc dns-as client enable
!
avc dns-as client trusted-domains
domain ^.*f1.*$
domain ^.*cisco.*$
domain *.toocoolforyou.net
domain *.sontowski.de
domain *.pension-solutions.de
domain *.bav-spezialist.de
domain *.sontowski-immobilien.de
domain *.pegasus-cp.de
domain *.via-vorsorge.de
domain *.blackberry.net
domain *.eu.blackberry.net
domain *.evorsorge.de
domain *.dns-as.org
domain *.nbar2web.org
domain *.f1-consult.com
domain *.f1-consult.de
domain *.f1-online.net
domain *.f1v4.net
domain *.f1v6.net
```

Enables DNS-AS

Identifies domains from which metadata may be received and trusted for policy-purposes

Configures basic DNS lookup-info

```
ip domain round-robin
ip domain-list toocoolforyou.net
ip domain-lookup source-interface Loopback0
ip domain-name toocoolforyou.net
ip name-server 192.168.167.244
ip name-server 192.168.168.244
```

IOS 15.2(5)E

IOS XE 3.9.0E and Higher

Catalyst 4500E AVC with DNS-AS Classification & Marking Example

```
class-map match-all VOICE
   match protocol attribute traffic-class voip-telephony
   match protocol attribute business-relevance business-relevant
class-map match-all BROADCAST-VIDEO
   match protocol attribute traffic-class broadcast-video
   match protocol attribute business-relevance business-relevant
class-map match-all REAL-TIME-INTERACTIVE
   match protocol attribute traffic-class real-time-interactive
   match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-CONFERENCING
   match protocol attribute traffic-class multimedia-conferencing
   match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA-STREAMING
   match protocol attribute traffic-class multimedia-streaming
   match protocol attribute business-relevance business-relevant
 class-map match-all SIGNALING
   match protocol attribute traffic-class signaling
   match protocol attribute business-relevance business-relevant
class-map match-all NETWORK-CONTROL
   match protocol attribute traffic-class network-control
   match protocol attribute business-relevance business-relevant
class-map match-all NETWORK-MANAGEMENT
   match protocol attribute traffic-class ops-admin-mgmt
   match protocol attribute business-relevance business-relevant
class-map match-all TRANSACTIONAL-DATA
   match protocol attribute traffic-class transactional-data
   match protocol attribute business-relevance business-relevant
class-map match-all BULK-DATA
   match protocol attribute traffic-class bulk-data
   match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER
   match protocol attribute business-relevance business-irrelevant
```

IOS 15.2(5)E
IOS XE 3.9.0E
and Higher

```
policy-map MARKING
 class VOICE
  set dscp ef
 class BROADCAST-VIDEO
  set dscp cs5
 class REAL-TIME-INTERACTIVE
  set dscp cs4
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class MULTIMEDIA-STREAMING
  set dscp af31
 class SIGNALING
  set dscp cs3
 class NETWORK-CONTROL
  set dscp cs6
 class NETWORK-MANAGEMENT
  set dscp cs2
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
```

Same ‘Holy Grail’ classification policy as on other router/switch platforms

Catalyst 4500E

Marking & Policing Policy Example

```
policy-map MARKING&POLICING
 class VOIP
  police 128k bc 8000
   conform-action set-dscp-transmit ef
   exceed-action drop
 class SIGNALING
  police 32k bc 8000
   conform-action set-dscp-transmit cs3
   exceed-action drop
 class MULTIMEDIA-CONFERENCING
  police 5m bc 8000
   conform-action set-dscp-transmit af41
   exceed-action set-dscp-transmit af42
 class TRANSACTIONAL-DATA
  police 10m bc 8000
   conform-action set-dscp-transmit af21
   exceed-action set-dscp-transmit af22
```

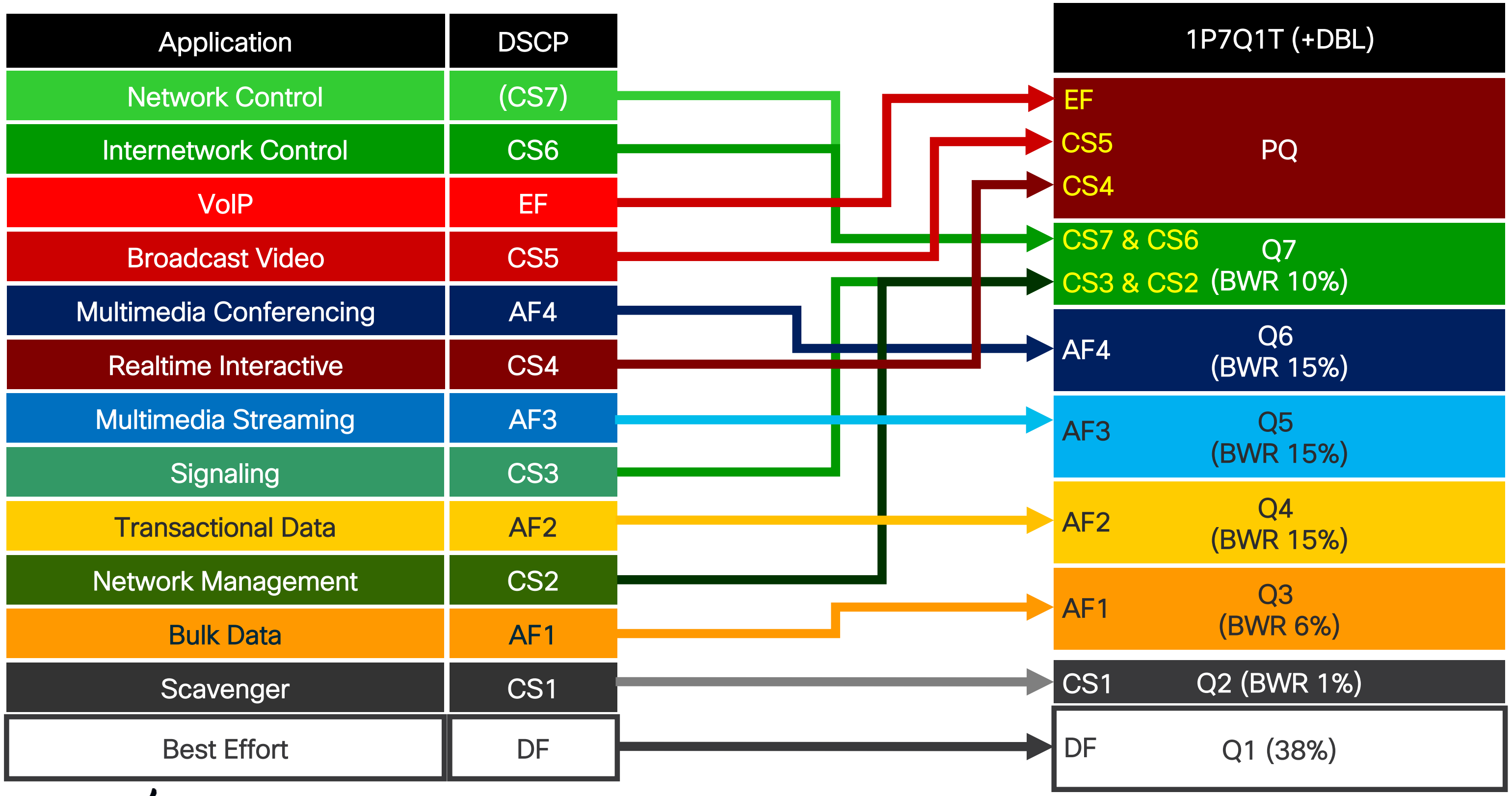
```
class BULK-DATA
  police 10m bc 8000
   conform-action set-dscp-transmit af11
   exceed-action set-dscp-transmit af12
 class SCAVENGER
  police 10m bc 8000
   conform-action set-dscp-transmit cs1
   exceed-action drop
 class class-default
  police 10m bc 8000
   conform-action set-dscp-transmit default
   exceed-action set-dscp-transmit cs1
```

```
interface GigabitEthernet 3/1
 service-policy input MARKING&POLICING
```

Marking / remarking is configured as part of the policing action (i.e. no table-map or markdown-map is referenced)

Catalyst 4500E

1P7Q1T+Dynamic Buffer Limiting (DBL) Egress Queuing Model



BWR = Bandwidth Remaining

Catalyst 4500E

1P7Q1T+DBL Egress Queuing Config

```
class-map match-all PRIORITY-QUEUE
 match dscp cs4 cs5 ef
class-map match-all CONTROL-MGMT-QUEUE
 match dscp cs7 cs6 cs3 cs2
class-map match-all MULTIMEDIA-CONFERENCING-QUEUE
 match dscp af41 af42 af43
class-map match-all MULTIMEDIA-STREAMING-QUEUE
 match dscp af31 af32 af33
class-map match-all TRANSACTIONAL-DATA-QUEUE
 match dscp af21 af22 af23
class-map match-all BULK-DATA-QUEUE
 match dscp af11 af12 af13
class-map match-all SCAVENGER-QUEUE
 match dscp cs1
```

Enables the PQ

If PQ is enabled then **bandwidth remaining** must be used

```
policy-map 1P7Q1T
 class PRIORITY-QUEUE
  priority
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 15
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 15
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 15
  dbl
 class BULK-DATA-QUEUE
  bandwidth remaining percent 6
  dbl
 class SCAVENGER-QUEUE
  bandwidth remaining percent 1
 class class-default
  bandwidth remaining percent 38
  dbl
```

DBL can be enabled on a per-class basis, but should not be enabled on the PQ or Control traffic queues. Enabling DBL on UDP-based queues and/or Scavenger queue is optional.

```
service-policy output 1P7Q1T
```

Catalyst 4500E Campus QoS Design At-A-Glance

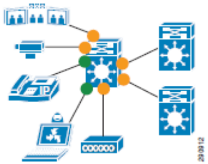
Cisco Catalyst 4500E (Supervisor 6-E / 7-E / 8-E) QoS Design

At-A-Glance

Role in Campus Network

The Cisco Catalyst 4500 series switches with Supervisor 6-E/7-E are well-suited to the role of access- or distribution-layer switches in campus networks. As such, these switches may connect directly to a variety of endpoints, as well as to distribution-layer and/or core-layer switches, as shown in Figure 1.

Figure 1 Cisco Catalyst 4500 Series Switch with Supervisor 6-E/7-E/8-E in a Campus Network



QoS Design Steps

There are only two main steps to configure QoS on a Cisco Catalyst 4500 series switch with Supervisor 6-E/7-E:

1. Configure Ingress QoS Model(s):
   – Trust DSCP Model
   – Conditional Trust Model
   – Service Policy Models
2. Configure Egress Queuing

Step 1: Configure Ingress QoS Model(s)

The three most utilized ingress QoS models for campus networks are:

- Trust DSCP Model
- Conditional Trust Model
- Service Policy Models

Combinations of these ingress QoS models may be used at the same time.

Trust DSCP Model

By default all interfaces trust DSCP; as such, no explicit configuration is required to enable this model.

In the default trust DSCP state, the interface statically accepts and preserves the Layer 3 DSCP markings of all incoming packets. This model is suitable for interfaces connecting to endpoints that can mark DSCP values and are administratively controlled (such as WLAN controllers) as well as for any uplinks to distribution layer switches. Switch ports that should trust DSCP are shown as yellow circles in Figure 1.

Conditional Trust Model

The Conditional Trust model configures the interface to dynamically accept markings from endpoints that have met a specific condition, such as a successful CDP negotiation (switch ports set to conditional trust are shown as green circles in Figure 1).

This model is suitable for switch ports connecting to:

• Cisco IP phones—**trust device cisco-phone**

• Cisco TelePresence Systems—**trust device cts**

• Cisco IP Video Surveillance cameras—**trust device ip-camera**

• Cisco Digital Media Players—**trust device media-player**

This model is also suitable for PCs and untrusted devices, since the ports connecting to such devices will remain in their default untrusted state.

Service Policy Models

There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC policies to implement classification, marking, and/or policing policies. These policies are constructed with:

• class-maps which identify the flows using packet markings or by access-lists or other criteria

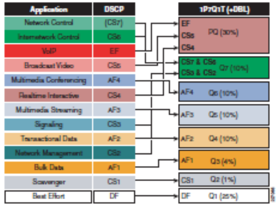
• policy-maps which specify policy actions to be taken on a class-by-class basis

• service-policy statements which apply a specific policy-map to an interface(s) and specify direction

Step 2: Configure Egress Queuing

The egress queuing model for the Catalyst 4500 with Supervisor 6-E/7-E/8-E is shown in Figure 2.

Figure 2 Cisco Catalyst 4500 Supervisor 6-E / 7-E / 8-E Egress Queuing Model



EtherChannel QoS

Ingress QoS policies on the Cisco Catalyst 4500 Supervisor 6-E/7-E/8-E are configured on the logical Port-Channel interface (but typically these are simply to enable DSCP trust—which requires no explicit configuration), while egress QoS policies (such as the service-policy-statement to enable egress queuing) are configured on the physical port-member interfaces.

Cisco Validated Design (CVD)

The Cisco Validated Design for Cisco Catalyst 4500 with Supervisor 6-E/7-E/8-E in the role of an access switch in a campus network is presented on the reverse.

Campus Cisco Catalyst 4500 Supervisor 6-E/7-E QoS Design — At-A-Glance

Step 1: Configure Ingress QoS Model:

Trust DSCP Model:

```
<no configuration/default state>
```

Conditional Trust Model:

```
class-map match-all VOICE
 match cos 5
class-map match-all SIGNALING
 match cos 3

policy-map CISCO-IPPHONE
 class VOICE
  set dscp ef
 class SIGNALING
  set dscp cs3
 class class-default
  set dscp default

qos trust device cisco-phone
service-policy input CISCO-IPPHONE
```

Service Policy Models:

```
[class-maps omitted for brevity]
policy-map MARKING-POLICY
 class VOIP
  set dscp ef
 class MULTIMEDIA-CONFERENCING
  set dscp af41
 class SIGNALING
  set dscp cs3
 class TRANSACTIONAL-DATA
  set dscp af21
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default

service-policy input MARKING-POLICY
```

Step 2: Egress Queuing Configuration

```
class-map match-any PRIORITY-QUEUE
 match dscp ef
 match dscp cs5
 match dscp cs4
class-map match-any CONTROL-MGMT-QUEUE
 match dscp cs7
 match dscp cs6
 match dscp cs3
 match dscp cs2
class-map match-all MULTIMEDIA-CONFERENCING-QUEUE
 match dscp af41 af42 af43
class-map match-all MULTIMEDIA-STREAMING-QUEUE
 match dscp af31 af32 af33
class-map match-all TRANSACTIONAL-DATA-QUEUE
 match dscp af21 af22 af23
class-map match-all BULK-DATA-QUEUE
 match dscp af11 af12 af13
class-map match-all SCAVENGER-QUEUE
 match dscp cs1

policy-map EGRESS-QUEUING
 class PRIORITY-QUEUE
  priority
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 10
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 10
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 10
  dbl
 class BULK-DATA-QUEUE
  bandwidth remaining percent 4
  dbl
 class SCAVENGER-QUEUE
  bandwidth remaining percent 1
 class class-default
  bandwidth remaining percent 25
  dbl

service-policy output EGRESS-QUEUING
```

Assigns VoIP (EF) Broadcast Video (CS5) and Realtime Interactive (CS4) to the PRIORITY-QUEUE

Assigns Network Control (CS7), Internetwork Control (CS6), Signaling (CS3) and Management (CS2) to the CONTROL-MGMT-QUEUE

Assigns AF4 to the MULTIMEDIA-CONFERENCING-QUEUE

Assigns AF3 to the MULTIMEDIA-STREAMING-QUEUE

Assigns AF2 to the TRANSACTIONAL-DATA-QUEUE

Assigns AF1 to the BULK-DATA-QUEUE

Assigns CS1 to the SCAVENGER-QUEUE

PRIORITY-QUEUE gets strict priority servicing (All other queues get percentages of bandwidth *remaining* after the PQ has been fully serviced)

CONTROL-MGMT-QUEUE gets 10% of remaining bandwidth

MM-CONF-QUEUE gets 10% of remaining bandwidth

MM-STREAMING-QUEUE gets 10% of remaining bandwidth

TRANS-DATA-QUEUE gets 10% of remaining bandwidth and Dynamic Buffer Limiting

BULK-DATA-QUEUE gets 4% of remaining bandwidth and Dynamic Buffer Limiting

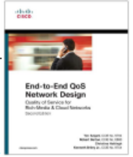
SCAVENGER-QUEUE is limited to 1% of remaining bandwidth

Default (Best-Effort) queue 25% of remaining bandwidth and Dynamic Buffer Limiting

Applies EGRESS-QUEUEING policy to interface

Note: Highlighted commands are interface specific; otherwise these are global.

For more details, see Campus QoS Design 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html
And the Cisco Press Book: **End-to-End QoS Network Design** (Second Edition)-Chapter 15



Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

DNS-AS At-A-Glance

Cisco Domain Name System-Authoritative Source (DNS-AS)

At-A-Glance

The Role of DNS-AS

An increasing number of applications are being encrypted, which limits the effectiveness of deep-packet inspection technologies. Additionally, many applications are multiplexing their media streams, making these increasingly difficult to distinguish and treat differently.

Providing application metadata can address both of these challenges and enhance the utility of network QoS, security, performance routing and other policies.

The challenge thus becomes how to distribute such application metadata. For instance, if applications running on devices were to communicate such metadata to the network, this would require a phenomenal amount of cross-platform software development and maintenance.

However, DNS is not only a trusted source of information (as it is centrally administered, either by an enterprise or by a service provider), but is also flexible and extensible. As such, it may be used as an "authoritative source" of application metadata.

Thus, DNS-AS can provide the following value to enterprise networks:

- accurately classify encrypted applications
- identify thousands of applications (e.g. by leveraging OpenAppID)
- provide layer 7 visibility to network devices that have no deep-packet inspection capabilities
- reduce configuration complexity on network devices for classification
- require no software updates to endpoint devices, applications or operating systems

Consider two main DNS-AS use-cases:

- identifying *internal* applications
- identifying *external* applications

Identifying Internal Applications

As internal DNS servers are centrally administered by the enterprise IT department, these may be modified to include custom DNS TXT records that reflect application metadata, such as:

- application name
- application ID
- RFC 4594 traffic classification
- Business relevance, etc.

With this application metadata in place in the local DNS server database, then - for example - a network access switch with no deep-packet inspection capabilities can leverage DNS-AS to correctly classify and apply QoS (and other types of policies) to any internal application.

The DNS-AS operational steps to identify *internal* applications are:

1) A client requests a DNS Lookup, as shown in Figure 1.
2) The access switch intercepts and clones the DNS request.
3) The internal DNS Server returns a DNS response (A-Record).
4) The access switch requests application metadata information (via a TXT record), as shown in Figure 2.
5) The internal DNS Server returns a TXT Record with application metadata information.
6) The access switch maintains a Binding Table of application metadata.

At this point, the access switch can apply QoS policies or security or routing or other types policies to the flow.

Figure 1 DNS-AS Identification of Internal Applications- Steps 1 to 3

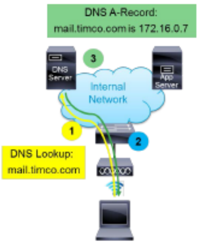
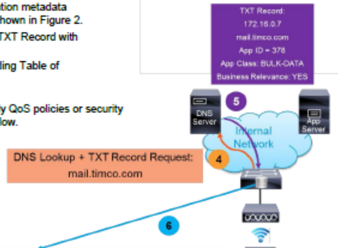


Figure 2 DNS-AS Identification of Internal Applications- Steps 4 to 6



IP Address	PTR	App-ID	App-Class	Business-Relevance
172.16.0.7	mail.timco.com	378	Bulk Data	YES

Identifying External Applications

A few additional steps are required when identifying external applications that have no application metadata in their DNS records. In this model, the internet edge router plays a key role as a DNS-AS Proxy.

The DNS-AS operational steps to identify *external* applications are:

1) A client requests a DNS Lookup, as shown in Figure 3.
2) The access switch intercepts and clones the DNS request.
3) The external DNS Server returns a DNS response (A-Record).
4) The access switch requests application metadata information (via a TXT record).
5) The external DNS Server has no TXT Record with application metadata.
6) The internet edge router notices the request for a TXT Record without response and:

   A) On the first flow:

   The internet edge router uses NBAR2 to perform deep-packet inspection to identify the flow and makes an entry in its local Binding Table.

   B) On subsequent flows:

   The internet edge router responds (as a DNS-Proxy) to the request for application metadata (by inserting a TXT Record into the DNS response from the external DNS server).

7) The access switch maintains a Binding Table of application metadata.

Figure 3 DNS-AS Identification of External Applications- Steps 1 to 5

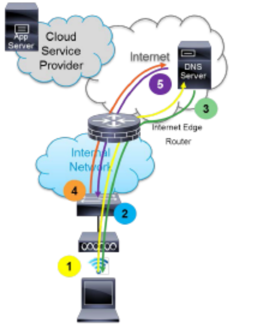
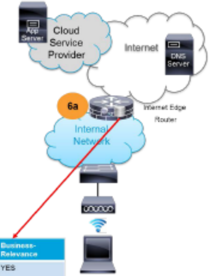
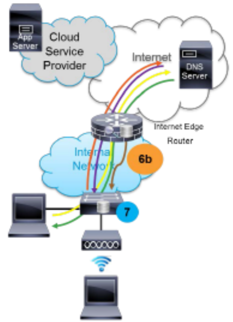


Figure 4 DNS-AS Identification of External Applications- Step 6a



IP Address	PTR	App-ID	App-Class	Business-Relevance
172.99.120.37	app.cloudco.com	3789	Transactional Data	YES

Figure 4 DNS-AS Identification of External Applications- Steps 6 and 7

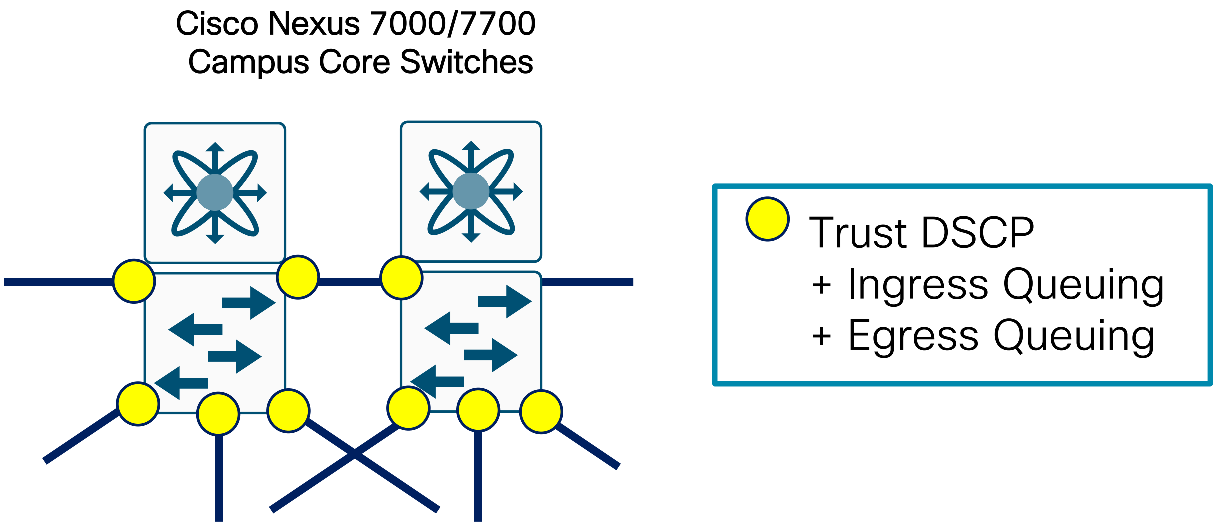


Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

Appendix B: Cisco Nexus 7000/7700 QoS Design

Cisco Nexus 7000/7700

QoS Roles in the Campus Core



Cisco Nexus 7000/7700

QoS Design Steps

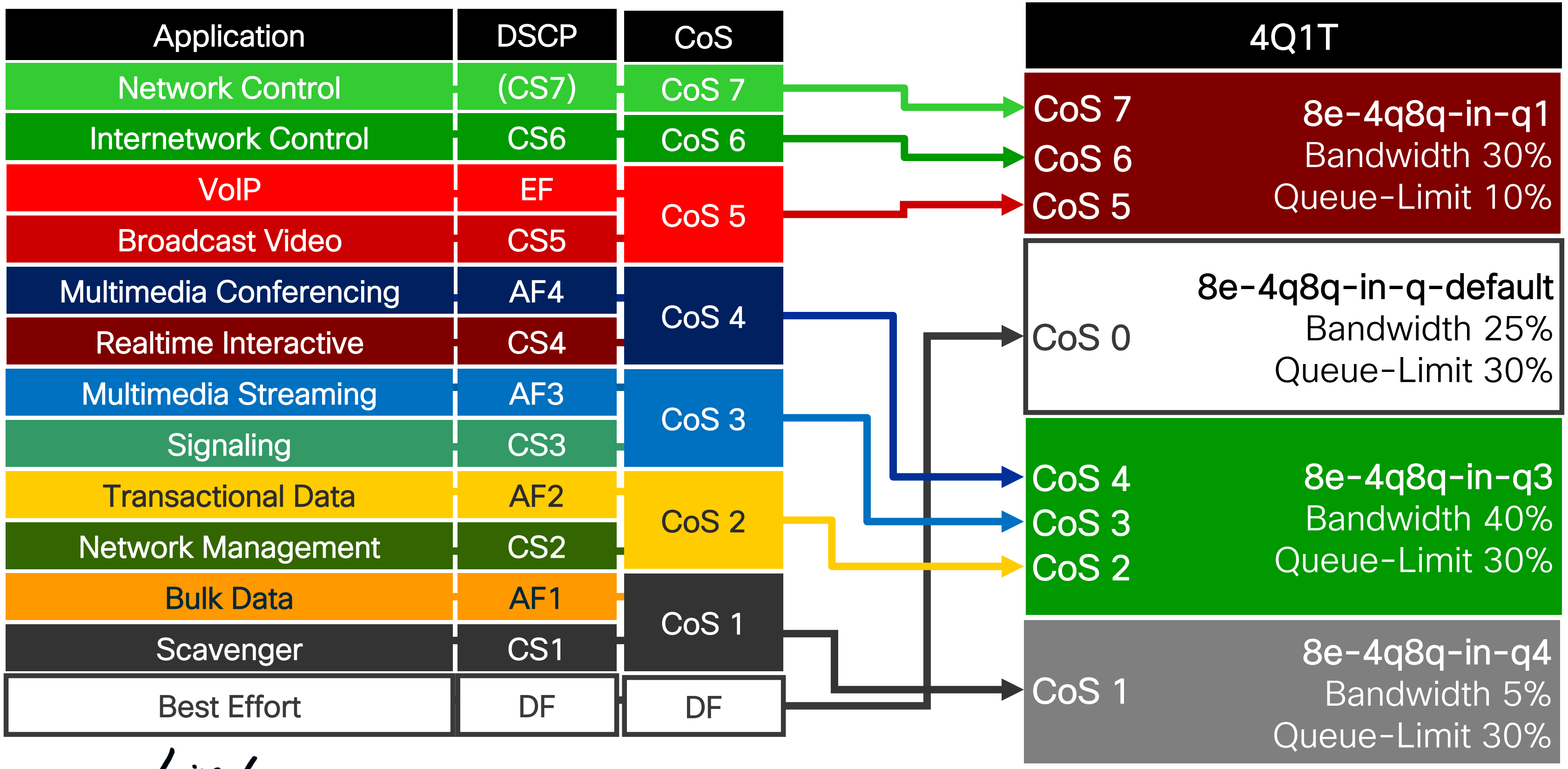
1. Configure System QoS (F-Series Modules)
2. Configure Ingress Queuing
3. Configure Egress Queuing
4. Configure CoS-Queue and Bandwidth Ratios for Fabric QoS (Nexus 7000 with M2 Modules)

NX-OS trusts by default. Therefore no explicit policy is required for DSCP trust

Nexus 7700 with F2E, F3, and M3

Cisco Nexus 7700 (F2E, F3, M3 Modules)

4Q1T Ingress Queuing (CoS-to-Queue) Model



cisco Live!

Cisco Nexus 7700 (F2E, F3, M3 Modules)

4Q1T Ingress Queuing (DSCP-to-Queue) Model

Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

4Q1T

DSCP	Queue
CS7 CS6 EF CS5 CS4	8e-4q8q-in-q1 Bandwidth 30% Queue-Limit 10%
DF	8e-4q8q-in-q-default Bandwidth 25% Queue-Limit 30%
AF4 AF3 CS3 AF2 CS2	8e-4q8q-in-q3 Bandwidth 40% Queue-Limit 30%
AF1 CS1	8e-4q8q-in-q4 Bandwidth 5% Queue-Limit 30%

Nexus 7700 with F2E, F3, and M3 Series QoS Design Steps

Specify the System Network-QoS Policy

```
N7706-1(config)# system qos
DC-7010-2(config-sys-qos)# service-policy type network-qos default-nq-8e-4q8q-policy
```

Verification:

```
N7706-1# show policy-map system

  Type network-qos policy-maps
  ============================
  policy-map type network-qos default-nq-8e-4q8q-policy template 8e-4q8q
    class type network-qos c-nq-8e-4q8q
      match cos 0-7
      congestion-control tail-drop threshold burst-optimized
      mtu 1500
 …
  Service-policy input:    default-8e-4q8q-in-policy
 …
  Service-policy output:    default-8e-4q8q-out-policy
 …
```


Cisco Nexus 7700 (F2E, F3, M3 Modules)

Part 1 of 2: 4Q1T-Ingress Queuing Class-Maps

```
class-map type queuing match-any 8e-4q8q-in-q1
  match cos 5-7
  no match dscp 40-63
  match dscp 32, 40, 46, 48, 56
class-map type queuing match-any 8e-4q8q-in-q3
  match cos 2-4
  match dscp 16, 18, 20, 22
  match dscp 24, 26, 28, 30
  match dscp 34, 36, 38
class-map type queuing match-any 8e-4q8q-in-q4
  match cos 1
  match dscp 8, 10, 12, 14
class-map type queuing match-any 8e-4q8q-in-q-default
  match cos 0
```

Undesired default DSCP-to-Ingress Queue mappings need to be explicitly removed

Similar to C3PL, NX-OS allows for multiple types of QoS policies:

- **type qos** for classification, marking and policing
- **type queuing** for ingress and egress queuing

NX-OS has (non-configurable) system-defined names for queuing class-maps

Cisco Nexus 7700 (F2E, F3, M3 Modules)

Part 2 of 2: 4Q1T-Ingress Queuing Policy-Map

```
policy-map type queuing CAMPUS-F3-4Q1T-INGRESS
  class type queuing 8e-4q8q-in-q1
    bandwidth percent 30
    queue-limit percent 10
 class type queuing 8e-4q8q-in-q-default
    bandwidth percent 25
    queue-limit percent 30
  class type queuing 8e-4q8q-in-q3
    bandwidth percent 40
    queue-limit percent 30
  class type queuing 8e-4q8q-in-q4
    bandwidth percent 5
    queue-limit percent 30
```

```
interface Ethernet 1/1-24
 service-policy type queuing input CAMPUS-F3-4Q1T-INGRESS
```

Used for Data Center Bridging Exchange (DCBX) to advertise QoS capabilities to any DCB-peers

Q2 is the Default Queue

Allocates buffers to queues

Cisco Nexus 7700 (F2E, F3, M3 Modules)

1P7Q1T Egress Queuing (CoS-to-Queue) Model

Application	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	CoS 5
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	CoS 4
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	CoS 3
Transactional Data	AF2	CoS 2
Network Management	CS2	CoS 2
Bulk Data	AF1	CoS 1
Scavenger	CS1	CoS 1
Best Effort	DF	DF

1P7Q1T	
CoS 7 CoS 6 CoS 5	8e-4q8q-out-q1 PQ-Shaped to 30%
CoS 4 CoS 3 CoS 2	8e-4q8q-out-q2 BWR 55%
CoS 1	8e-4q8q-out-q3 BWR 10%
	8e-4q8q-out-q4 BWR 1%
	8e-4q8q-out-q5 BWR 1%
	8e-4q8q-out-q6 BWR 1%
	8e-4q8q-out-q7 BWR 1%
CoS 0	8e-4q8q-out-q-default BWR 31%

Cisco Nexus 7700 (F2E, F3, M3 Modules)

Part 1 of 2: 1P7Q1T Egress Queuing Class-Maps

```
class-map type queuing match-any 8e-4q8q-out-q1
 no match cos 0-7
 match cos 5-7
class-map type queuing match-any 8e-4q8q-out-q2
 no match cos 0-7
 match cos 2-4
class-map type queuing match-any 8e-4q8q-out-q3
 no match cos 0-7
 match cos 1
```

Note: Modifies the default CoS-to-Queue mappings

Cisco Nexus 7700 (F2E, F3, M3 Modules)

Part 2 of 2: 1P7Q1T Egress Queuing Policy-Map

```
policy-map type queuing APIC_EM-1P7Q1T-OUT
  class type queuing 8e-4q8q-out-q1
    priority level 1
    shape average percent 30
  class type queuing 8e-4q8q-out-q2
    bandwidth remaining percent 55
  class type queuing 8e-4q8q-out-q3
    bandwidth remaining percent 10
  class type queuing 8e-4q8q-out-q4
    bandwidth remaining percent 1
  class type queuing 8e-4q8q-out-q5
    bandwidth remaining percent 1
  class type queuing 8e-4q8q-out-q6
    bandwidth remaining percent 1
  class type queuing 8e-4q8q-out-q7
    bandwidth remaining percent 1
  class type queuing 8e-4q8q-out-q-default
    bandwidth remaining percent 31
```

```
interface Ethernet 1/1-24
 service-policy type queuing output CAMPUS-F3-1P3Q1T-EGRESS
```

Note: Indicates the Priority Queue

Note: Queue-Limits are not supported in egress direction

Cisco Nexus 7700 QoS Design At-A-Glance

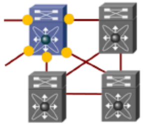
Cisco Nexus 7700 (F3 Module) Campus QoS Design

At-A-Glance

Role in Campus Network

The Cisco Nexus series switches with F3 modules are suited to the role of a core-layer switch in campus networks. As such, these switches typically connect directly to other switches or routers, as shown in Figure 1.

Figure 1 Cisco Nexus 7700 (F3 Module) Switches in a Campus Network



QoS Design Steps

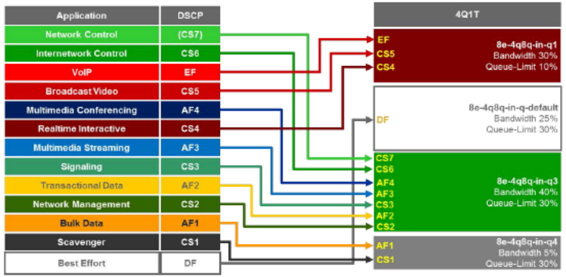
There are two main steps to configure QoS on Cisco Nexus 7700 series switches with F3 modules:

1. Configure Ingress Queuing
2. Configure Egress Queuing

Step 1: Configure Ingress Queuing

The 4Q1T ingress queuing model for the Cisco Nexus 7700 with F3 modules is shown in Figure 2.

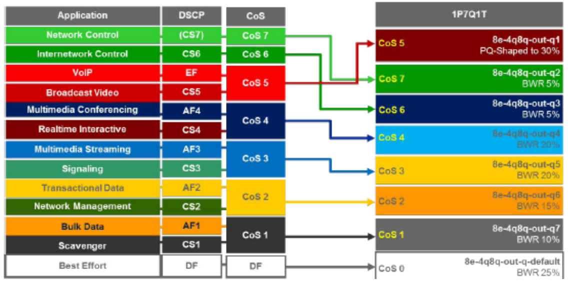
Figure 2 Nexus 7700 F3 (4Q1T) Ingress Queuing Model



Step 2: Configure Egress Queuing

The (CoS-Based) 1P7Q1T egress queuing model for the Cisco Nexus 7700 with F3 module is shown in Figure 3.

Figure 3 Nexus 7700 F3 (CoS-Based 1P7Q1T) Egress Queuing Model



Cisco Validated Design (CVD)

The Cisco Validated Design for Cisco Nexus 7700 series switches with F3 modules in the role of a core-layer switch in a campus network is presented on the reverse.

Step 1: Configure 4Q1T Ingress Queuing Policies

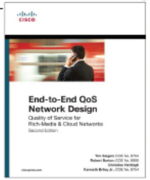
```
class-map type queuing match-any 8e-4q8q-in-q1
  match cos 5
  no match dscp 40-63
  match dscp 32, 40, 46
class-map type queuing match-any 8e-4q8q-in-q3
  match cos 2-4, 6-7
  match dscp 16, 18, 20, 22
  match dscp 24, 26, 28, 30
  match dscp 34, 36, 38
  match dscp 48, 56
class-map type queuing match-any 8e-4q8q-in-q4
  match cos 1
  match dscp 8, 10, 12, 14
class-map type queuing match-any 8e-4q8q-in-q-default
  match cos 0

policy-map type queuing CAMPUS-F3-4Q1T-INGRESS
  class type queuing 8e-4q8q-in-q1
    bandwidth percent 30
    queue-limit percent 10
 class type queuing 8e-4q8q-in-q-default
    bandwidth percent 25
    queue-limit percent 30
  class type queuing 8e-4q8q-in-q3
    bandwidth percent 40
    queue-limit percent 30
  class type queuing 8e-4q8q-in-q4
    bandwidth percent 5
    queue-limit percent 30


service-policy type queuing input CAMPUS-F3-4Q1T-INGRESS
```

Note: Highlighted commands are interface specific; otherwise these are global.

Step 2 Configure (CoS-Based) 1P7Q1T Egress Queuing Policies

```
class-map type queuing match-any 8e-4q8q-out-q1
 match cos 5
class-map type queuing match-any 8e-4q8q-out-q2
 match cos 7
class-map type queuing match-any 8e-4q8q-out-q3
 match cos 6
class-map type queuing match-any 8e-4q8q-out-q4
 match cos 4
class-map type queuing match-any 8e-4q8q-out-q5
 match cos 3
class-map type queuing match-any 8e-4q8q-out-q6
 match cos 2
class-map type queuing match-any 8e-4q8q-out-q7
 match cos 1

policy-map type queuing CAMPUS-F3-1P7Q1T-EGRESS
  class type queuing 8e-4q8q-out-q1
    priority level 1
    shape average percent 30
  class type queuing 8e-4q8q-out-q2
    bandwidth remaining percent 5
  class type queuing 8e-4q8q-out-q3
    bandwidth remaining percent 5
  class type queuing 8e-4q8q-out-q4
    bandwidth remaining percent 20
  class type queuing 8e-4q8q-out-q5
    bandwidth remaining percent 20
  class type queuing 8e-4q8q-out-q6
    bandwidth remaining percent 15
  class type queuing 8e-4q8q-out-q7
    bandwidth remaining percent 10
  class type queuing 8e-4q8q-out-q-default
    bandwidth remaining percent 25

service-policy type queuing output CAMPUS-F3-1P7Q1T-EGRESS
```

For more details on Cisco Nexus 7000 QoS design, see the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 25



Uploaded to the BRKCRS-2501 Campus QoS Design Simplified - Webex Teams Space

Nexus 7000 with F2, F2E, and F3

Cisco Nexus 7000 (F-Series)

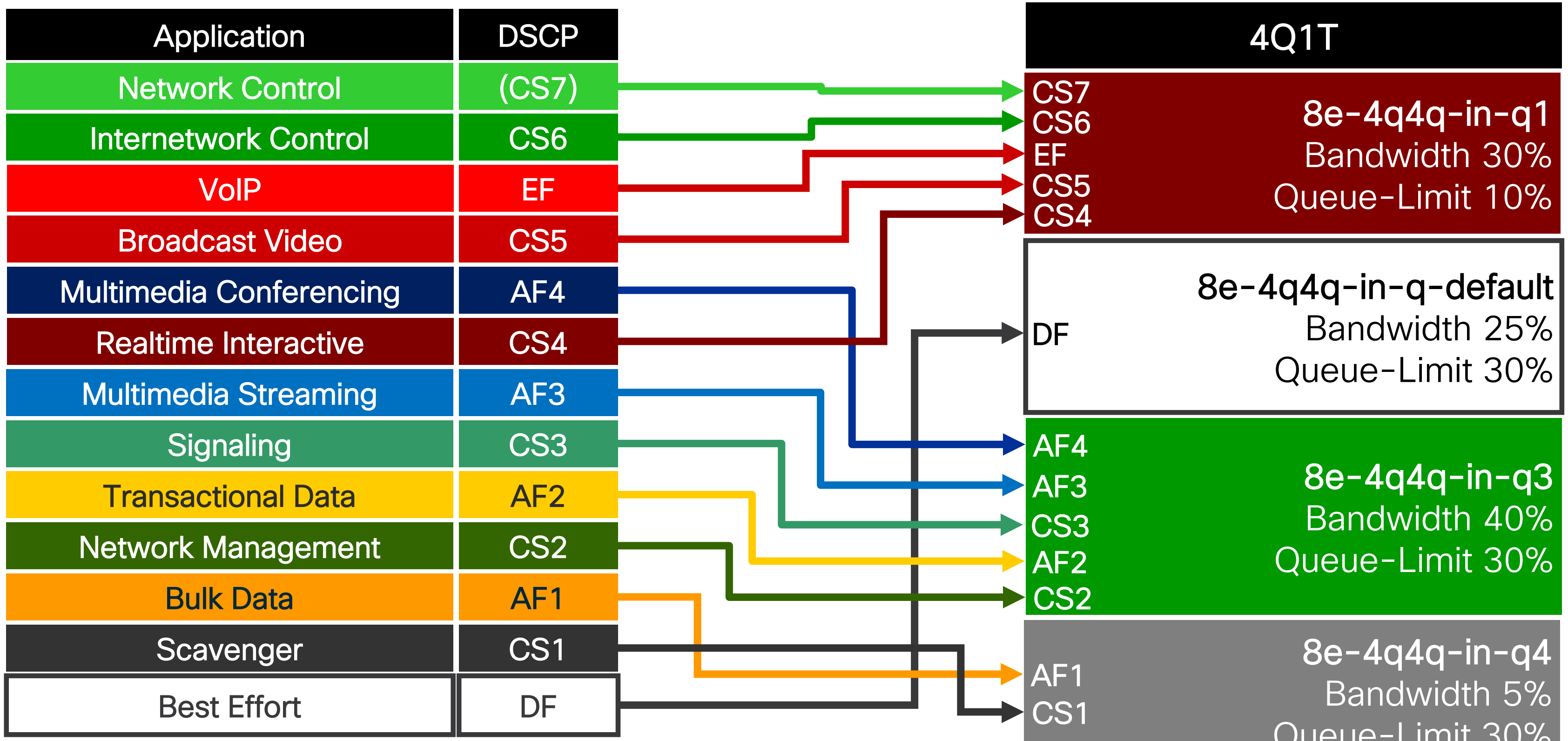
4Q1T Ingress Queuing (CoS-to-Queue) Model

Application	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	
Transactional Data	AF2	CoS 2
Network Management	CS2	
Bulk Data	AF1	CoS 1
Scavenger	CS1	
Best Effort	DF	DF

4Q1T	
CoS 7 CoS 6 CoS 5	8e-4q4q-in-q1 Bandwidth 30% Queue-Limit 10%
CoS 0	8e-4q4q-in-q-default Bandwidth 25% Queue-Limit 30%
CoS 4 CoS 3 CoS 2	8e-4q4q-in-q3 Bandwidth 40% Queue-Limit 30%
CoS 1	8e-4q4q-in-q4 Bandwidth 5% Queue-Limit 30%

Cisco Nexus 7000 (F-Series)

4Q1T Ingress Queuing (DSCP-to-Queue) Model



Nexus 7000 with F2, F2E, and F3 Series QoS Design Steps

Step 1: Specify the System Network-QoS Policy

```
DC-7010-2(config)# system qos
DC-7010-2(config-sys-qos)# service-policy type network-qos default-nq-8e-4q4q-policy
```

Verification:

```
DC-7010-2# show policy-map system

  Type network-qos policy-maps
  ============================
  policy-map type network-qos default-nq-8e-4q4q-policy template 8e-4q4q
    class type network-qos c-nq-8e-4q4q
      match cos 0-7
      congestion-control tail-drop
      mtu 1500
 …
  Service-policy input:   default-8e-4q4q-in-policy
 …
  Service-policy output:   default-8e-4q4q-out-policy
 …
```


Nexus 7000 with F2, F2E, and F3 Series QoS Design Steps

Step 2: Configure Ingress Queuing Class-Maps (1 of 2)

```
hardware qos dscp-to-queue ingress module-type all
```

From NX-OS 6.2.2 on

```
class-map type queuing match-any 4q1t-8e-4q4q-in-q1
 no match dscp 0-63
 no match cos 0-7

class-map type queuing match-any 4q1t-8e-4q4q-in-q3
 no match dscp 0-63
 no match cos 0-7

class-map type queuing match-any 4q1t-8e-4q4q-in-q4
 no match dscp 0-63
 no match cos 0-7
```

Recommended to remove all currently mapped marking (default or otherwise) values to prevent errors during deployment from all classes except class-default (where removing markings is not permitted)

Nexus 7000 with F2, F2E, and F3 Series QoS Design Steps

Step 2: Configure Ingress Queuing Class-Maps (2 of 2)

```
class-map type queuing match-any 4q1t-8e-4q4q-in-q1
 match cos 5-7
 match dscp 32, 40, 46, 48, 56
!
class-map type queuing match-any 4q1t-8e-4q4q-in-q3
 match cos 2-4
 match dscp 16, 18, 20, 22, 24, 26, 28, 30, 34, 36, 38
!
class-map type queuing match-any 4q1t-8e-4q4q-in-q4
 match cos 1
 match dscp 8, 10, 12, 14
```

All non-standard DSCP values have been implicitly mapped to the default-queue in previous slide.

Nexus 7000 with F2, F2E, and F3 Series QoS Design Steps

Step 3: Create and Apply the Ingress Queuing Policy-Map

```
policy-map type queuing APIC_EM-8e-4q4q-in
  class type queuing 4q1t-8e-4q4q-in-q1
    queue-limit percent 10
    bandwidth percent 30
  class type queuing 4q1t-8e-4q4q-in-q-default
    queue-limit percent 30
    bandwidth percent 25
  class type queuing 4q1t-8e-4q4q-in-q3
    queue-limit percent 30
    bandwidth percent 40
  class type queuing 4q1t-8e-4q4q-in-q4
    queue-limit percent 30
    bandwidth percent 5
```

New policy may be created

```
interface Ethernet x/x-x
 service-policy type queuing input APIC_EM-8e-4q4q-in
```

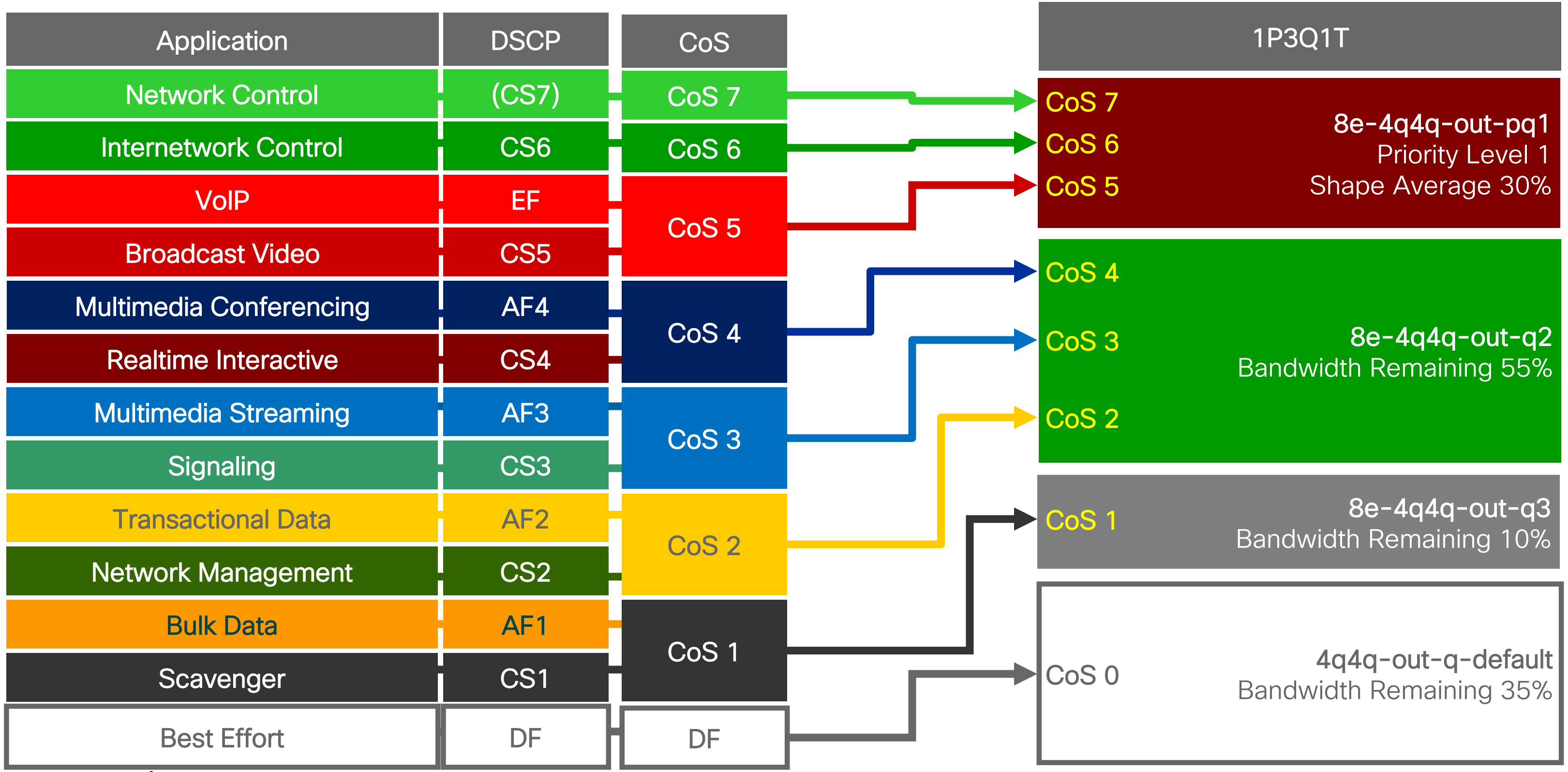
Queuing policy is applied to physical interfaces

```
interface Port-Channel xxx
 service-policy type queuing input APIC_EM-8e-4q4q-in
```

For interfaces which are part of a EtherChannel, the ingress queuing policy is applied to the logical port-channel interface.

Cisco Nexus 7000 (F-Series)

Egress Queuing Model (1P3Q1T) – CoS-to-Queue Mapping



Nexus 7000 with F2, F2E, and F3 Series QoS Design Steps

Step 4: Configure Egress Queuing Class-Maps

```
class-map type queuing match-any 1p3q1t-8e-4q4q-out-pq1
 no match cos 0-7
class-map type queuing match-any 1p3q1t-8e-4q4q-out-q2
 no match cos 0-7
class-map type queuing match-any 1p3q1t-8e-4q4q-out-q3
 no match cos 0-7
!
class-map type queuing match-any 1p3q1t-8e-4q4q-out-pq1
 match cos 5-7
class-map type queuing match-any 1p3q1t-8e-4q4q-out-q2
 match cos 2-4
class-map type queuing match-any 1p3q1t-8e-4q4q-out-q3
 match cos 1
```

Reset all CoS values to the default queue

CoS 0 is implicitly mapped to the default queue based on the above configuration

Nexus 7000 with F2, F2E, and F3 Series QoS Design Steps

Step 5: Create and Apply the Egress Queuing Policy-Map

```
policy-map type queuing APIC_EM-8e-4q4q-out
  class type queuing 1p3q1t-8e-4q4q-out-pq1
    priority level 1
    shape average percent 30
  class type queuing 1p3q1t-8e-4q4q-out-q3
    bandwidth remaining percent 10
  class type queuing 1p3q1t-8e-4q4q-out-q2
    bandwidth remaining percent 55
  class type queuing 1p3q1t-8e-4q4q-out-q-default
    bandwidth remaining percent 35
```

New policy may be created

```
interface Ethernet 1/1-24
 service-policy type queuing output APIC_EM-8e-4q4q-out
```

Queuing policy is applied to physical interfaces

```
interface Port-Channel xxx
 service-policy type queuing input APIC_EM-8e-4q4q-out
```

For interfaces which are part of a EtherChannel, the ingress queuing policy is applied to the logical port-channel interface.

Nexus 7000 with M2 Modules

Cisco Nexus 7000 (M2 Module)

Ingress Queuing Model (8Q2T) – CoS-to-Queue Mapping

Application	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	CoS 5
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	CoS 4
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	CoS 3
Transactional Data	AF2	CoS 2
Network Management	CS2	CoS 2
Bulk Data	AF1	CoS 1
Scavenger	CS1	CoS 1
Best Effort	DF	DF

8Q2T	
CoS 7 CoS 6 CoS 5	8q2t-in-q1 BW 30% / QL 10%
CoS 4 CoS 3 CoS 2	8q2t-in-q2 BW 40% / QL 30%
CoS 1	8q2t-in-q3 BW 5% / QL 30%
	8q2t-in-q4 BW 1% / QL 1%
	8q2t-in-q5 BW 1% / QL1%
	8q2t-in-q6 BW 1% / QL1%
	8q2t-in-q7 BW 1% / QL 1%
CoS 0	8q2t-in-q-default BW 21% / QL 26%

These queues are unused due to only 4 queues in fabric QoS

Cisco Nexus 7000 (M2 Module)

Ingress Queuing Model (8Q2T) – DSCP-to-Queue Mapping

Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signaling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

8Q2T	
CS7, CS6, EF, CS5, CS4	8q2t-in-q1 BW 30% / QL 10%
AF4, AF3, CS3, AF2, CS2	8q2t-in-q2 BW 40% / QL 30% + DSCP-WRED
AF1, CS1	8q2t-in-q3 BW 5% / QL 30% + DSCP-WRED
	8q2t-in-q4 BW 1% / QL 1%
	8q2t-in-q5 BW 1% / QL1%
	8q2t-in-q6 BW 1% / QL1%
	8q2t-in-q7 BW 1% / QL 1%
DF	8q2t-in-q-default BW 21% / QL 26% + DSCP-WRED

These queues are unused due to only 4 queues in fabric QoS

Nexus 7000 (M2)–Ingress Queuing Design

Part 1 of 4: 8Q2T-Ingress Queuing (CoS-to-Queue & DSCP-to-Queue)

Enables DSCP-to-Queue Mapping (ingress only)

```
hardware qos dscp-to-queue ingress module-type all
```

From NX-OS 6.2.2 on

Class-maps will have default/non-default CoS and/or DSCP values to them. These can be reset with “no match” commands. This results in all CoS and DSCP values mapped to the default queue

NX-OS provides system-defined class-map names (which cannot be renamed)

```
class-map type queuing match-any 8q2t-in-q1
 no match dscp 0-63
 no match cos 0-7
class-map type queuing match-any 8q2t-in-q2
 no match dscp 0-63
 no match cos 0-7
class-map type queuing match-any 8q2t-in-q3
 no match dscp 0-63
 no match cos 0-7
class-map type queuing match-any 8q2t-in-q4
 no match dscp 0-63
 no match cos 0-7
class-map type queuing match-any 8q2t-in-q5
 no match dscp 0-63
 no match cos 0-7
class-map type queuing match-any 8q2t-in-q6
 no match dscp 0-63
 no match cos 0-7
class-map type queuing match-any 8q2t-in-q7
 no match dscp 0-63
 no match cos 0-7
```


Nexus 7000 (M2)–Ingress Queuing Design

Part 1 of 4: 8Q2T-Ingress Queuing (CoS-to-Queue & DSCP-to-Queue)

```
class-map type queuing match-any 8q2t-in-q1
  match cos 5-7
  match dscp 32, 40, 46, 48, 56

class-map type queuing match-any 8q2t-in-q2
  match cos 2-4
  match dscp 16, 18, 20, 22, 24
  match dscp 26, 28, 30, 34, 36, 38

class-map type queuing match-any 8q2t-in-q3
  match cos 1
  match dscp 8, 10, 12, 14
```


Nexus 7000 (M2)–Ingress Queuing Design

Part 2 of 4: 8Q2T-Ingress Queuing Policy-Map with DSCP-Based WRED

```
policy-map type queuing APIC_EM-QUEUING-8Q2T-IN
  class type queuing 8q2t-in-q1
    bandwidth percent 30
    queue-limit percent 10
  class type queuing 8q2t-in-q2
    bandwidth percent 40
    queue-limit percent 30
    random-detect dscp-based
AF4x random-detect dscp 34,36,38 minimum-threshold percent 80 maximum-threshold percent 100
AF3x random-detect dscp 26,28,30 minimum-threshold percent 80 maximum-threshold percent 100
AF2x random-detect dscp 18,20,22 minimum-threshold percent 80 maximum-threshold percent 100
…
```

DSCP-based WRED not enabled for Q1

AF4x, AF3x, and AF2x traffic set for WRED min threshold of 80% and max threshold of 100%
CS3 and CS2 traffic implicitly set for WRED min and max threshold of 100%

Nexus 7000 (M2)–Ingress Queuing Design

Part 4 of 4: 8Q2T-Ingress Queuing Policy-Map with DSCP-Based WRED

```
 [continued]
  class type queuing 8q2t-in-q3
    bandwidth percent 5
    queue-limit percent 30
    random-detect dscp-based
AF1x random-detect dscp 10,12,14 minimum-threshold percent 80 maximum-threshold percent 100
CS1  random-detect dscp 8 minimum-threshold percent 80 maximum-threshold percent 100
  class type queuing 8q2t-in-q4
    bandwidth percent 1
    queue-limit percent 1
  class type queuing 8q2t-in-q5
    bandwidth percent 1
    queue-limit percent 1
  class type queuing 8q2t-in-q6
    bandwidth percent 1
    queue-limit percent 1
 …
```

AF1x and CS1 traffic set for WRED min threshold of 80% and max threshold of 100%

Nexus 7000 (M2)–Ingress Queuing Design

Part 4 of 4: 8Q2T-Ingress Queuing Policy-Map with DSCP-Based WRED

```
[continued]
  class type queuing 8q2t-in-q7
    bandwidth percent 1
    queue-limit percent 1
  class type queuing 8q2t-in-q-default
    bandwidth percent 21
    queue-limit percent 26
    random-detect dscp-based
    random-detect dscp 0 minimum-threshold percent 80 maximum-threshold percent 100
```

Default

Default traffic set for WRED min threshold of 80% and max threshold of 100%
All non-standard DSCP values implicitly set to min and max thresholds of 100%.

```
interface Ethernet x/x-x
 service-policy type queuing input APIC_EM-QUEUING-8Q2T-IN
```

Queuing policy is applied to physical interfaces

```
interface Port-Channel xxx
 service-policy type queuing input APIC_EM-QUEUING-8Q2T-IN
```

For interfaces which are part of a EtherChannel, the ingress queuing policy is applied to the logical port-channel interface.

Cisco Nexus 7000 (M2 Module)

1P7Q4T Egress Queuing (CoS-to-Queue) Model

Application	DSCP	CoS
Network Control	(CS7)	CoS 7
Internetwork Control	CS6	CoS 6
VoIP	EF	CoS 5
Broadcast Video	CS5	CoS 5
Multimedia Conferencing	AF4	CoS 4
Realtime Interactive	CS4	CoS 4
Multimedia Streaming	AF3	CoS 3
Signaling	CS3	CoS 3
Transactional Data	AF2	CoS 2
Network Management	CS2	CoS 2
Bulk Data	AF1	CoS 1
Scavenger	CS1	CoS 1
Best Effort	DF	DF

1P7Q1T	
CoS 7 CoS 6 CoS 5	8e-4q8q-out-q1 PQ-Shaped to 30%
CoS 4 CoS 3 CoS 2	8e-4q8q-out-q2 BWR 55%
CoS 1	8e-4q8q-out-q3 BWR 10%
	8e-4q8q-out-q4 BWR 1%
	8e-4q8q-out-q5 BWR 1%
	8e-4q8q-out-q6 BWR 1%
	8e-4q8q-out-q7 BWR 1%
CoS 0	8e-4q8q-out-q-default BWR 31%

Nexus 7000 (M2)–Egress Queuing Design

Part 1 of 4: 1P7Q4T-Egress Queuing Class-Maps (CoS-to-Queue)

```
class-map type queuing match-any 1p7q4t-out-pq1
  no match cos 0-7
class-map type queuing match-any 1p7q4t-out-q2
  no match cos 0-7
class-map type queuing match-any 1p7q4t-out-q3
  no match cos 0-7
class-map type queuing match-any 1p7q4t-out-q4
  no match cos 0-7
class-map type queuing match-any 1p7q4t-out-q5
  no match cos 0-7
class-map type queuing match-any 1p7q4t-out-q6
  no match cos 0-7
class-map type queuing match-any 1p7q4t-out-q7
  no match cos 0-7
```

All CoS values implicitly mapped to the default-queue.

Nexus 7000 (M2)–Egress Queuing Design

Part 2 of 4: 1P7Q4T-Egress Queuing Class-Maps (CoS-to-Queue)

```
class-map type queuing match-any 1p7q4t-out-pq1
  match cos 5-7
class-map type queuing match-any 1p7q4t-out-q2
 match cos 2-4
class-map type queuing match-any 1p7q4t-out-q3
 match cos 1
```

CoS 0 implicitly mapped to the default-queue still.

Nexus 7000 (M2)–Egress Queuing Design

Part 3 of 4: 1P7Q4T-Egress Queuing Policy-Map with CoS-Based WRED

```
policy-map type queuing APIC_EM-QUEUING-1P7Q4T-OUT
  class type queuing 1p7q4t-out-pq1
    priority
    shape average percent 30
    queue-limit percent 10
  class type queuing 1p7q4t-out-q2
    bandwidth remaining percent 55
    queue-limit percent 30
    random-detect cos-based
    random-detect cos 4 minimum-threshold percent 80 maximum-threshold percent 100
    random-detect cos 3 minimum-threshold percent 80 maximum-threshold percent 100
    random-detect cos 2 minimum-threshold percent 80 maximum-threshold percent 100
  class type queuing 1p7q4t-out-q3
    bandwidth remaining percent 10
    queue-limit percent 30
    random-detect cos-based
    random-detect cos 1 minimum-threshold percent 80 maximum-threshold percent 100
…
```

Nexus 7000 (M2)—Egress Queuing Design

Part 4 of 4: 1P7Q4T-Egress Queuing Policy-Map with CoS-Based WRED

```
 class type queuing 1p7q4t-out-q4
    bandwidth remaining percent 1
    queue-limit percent 1
 class type queuing 1p7q4t-out-q5
    bandwidth remaining percent 1
    queue-limit percent 1
  class type queuing 1p7q4t-out-q6
    bandwidth remaining percent 1
    queue-limit percent 1
  class type queuing 1p7q4t-out-q7
    bandwidth remaining percent 1
    queue-limit percent 1
  class type queuing 1p7q4t-out-q-default
    bandwidth remaining percent 31
    queue-limit percent 26
    random-detect cos-based
    random-detect cos 0 minimum-threshold percent 80 maximum-threshold percent 100
```

```
interface Ethernet x/x-x
 service-policy type queuing output APIC_EM-QUEUING-1P7Q4T-OUT
```

```
interface Port-Channel xxx
 service-policy type queuing output APIC_EM-QUEUING-1P7Q4T-OUT
```

Queuing policy is applied to physical interfaces

For interfaces which are part of a EtherChannel, the egress queuing policy is applied to the logical port-channel interface

Configure CoS-Queue and Bandwidth Ratios for Fabric QoS

Step1: Clone System-Defined Policies

```
qos copy policy-map type queuing system-in-policy prefix APIC_EM-
qos copy policy-map type queuing system-out-policy prefix APIC_EM-
```


Configure CoS-Queue and Bandwidth Ratios for Fabric QoS

Step 2: Configuring Cos2q Fabric Mapping

```
class-map type queuing system-pq1
 match cos 5, 6, 7
class-map type queuing system-q2
 match cos 2, 3, 4
class-map type queuing system-q3
 match cos 1
class-map type queuing system-q-default
 match cos 0
```

Configure CoS-Queue and Bandwidth Ratios for Fabric QoS

Step 3: Configuring Ingress Buffer Policy

```
policy-map type queuing APIC_EM-system-in-policy
  class type queuing system-pq1
  class type queuing system-q2
  class type queuing system-q3
  class type queuing system-q-default
    queue-limit default
```


Configure CoS-Queue and Bandwidth Ratios for Fabric QoS

Step 4: Configuring Egress Queue Bandwidth Allocation

```
policy-map type queuing APIC_EM-system-out-policy
  class type queuing system-pq1
    priority level 1
  class type queuing system-q3
    bandwidth remaining percent 10
  class type queuing system-q-default
    bandwidth remaining percent 35
  class type queuing system-q2
    bandwidth remaining percent 55
```

Note that order is important, since bandwidth remaining cannot exceed 100%, and there are system-defined default values already in place.

Configure CoS-Queue and Bandwidth Ratios for Fabric QoS

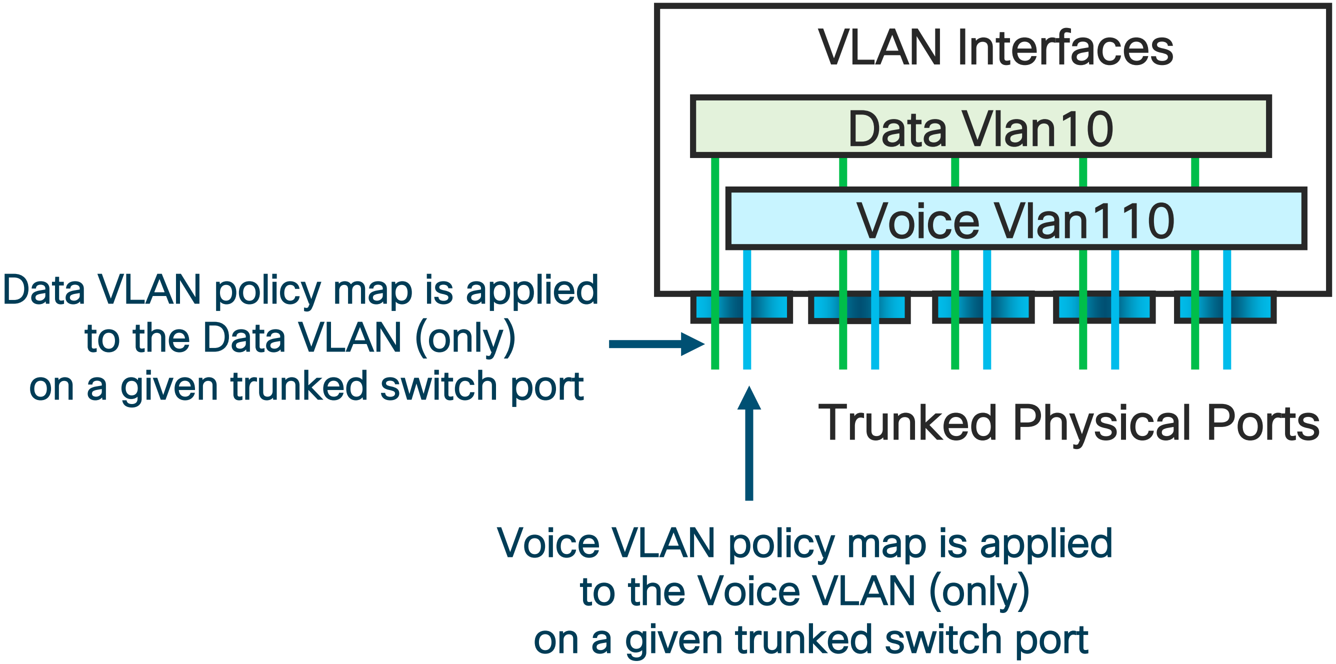
Step1: Configuring the New User-defined Policies on the Fabric

```
system fabric
  service-policy type queuing input APIC_EM-system-in-policy
  service-policy type queuing output APIC_EM-system-out-policy
```


Appendix C: Per-Port / Per-VLAN QoS

Campus QoS Design Considerations

Per-Port/Per-VLAN QoS



Catalyst 9000 / 3850 / 3650

Per-Port/Per-VLAN Policy

```
class-map VVLAN
 match vlan 110
class-map DVLAN
 match vlan 10
```

Individual (trunked) VLANs are matched by the **match vlan** command

```
policy-map VLAN-POLICERS
 class VVLAN
  police 192000 conform-action transmit  exceed-action drop
 class DVLAN
  police 50000000 conform-action transmit  exceed-action drop
```

Policers are applied on a Per-VLAN basis

```
interface GigabitEthernet 1/0/1
 service-policy input VLAN-POLICERS
```

Per-VLAN policers are then applied on a Per-Port basis

Catalyst 4500

Per-Port/Per-VLAN QoS Policy Example

```
interface range GigabitEthernet 2/1-48
 qos trust device cisco-phone
 vlan 10
  service-policy input DVLAN-POLICERS
 vlan 110
  service-policy input VVLAN-POLICERS
```

Per-Port/Per-VLAN policies can be applied to a specific VLAN on a trunked interface via an interface-VLAN configuration mode

Appendix D: AutoQoS Configurations - Catalyst 3750-X / 3560-X / 2960-X

Auto QoS - Catalyst 3750-X / 3560-X / 2960-X

- Auto QoS is a macro which provisions a pre-defined ingress classification & marking policy and an egress (and/or ingress) queueing policy
- Eleven forms of the interface-level Auto QoS command ("auto qos voip trust" and "auto qos trust" generate the same configuration)
  - auto qos voip {cisco-phone | cisco-softphone | trust}
  - auto qos video {cts | ip-camera | media-player}
  - auto qos classify [police]
  - auto qos trust [cos | dscp]
- To remove Auto QoS on an interface (run another macro to remove Auto QoS) preface the command with a "no" (i.e. no auto qos voip cisco-phone)
  - It is not recommended to modify the configuration provisioned by the Auto QoS commands because it may affect the ability of the switch to remove the configuration on the interface or globally when removing Auto QoS

Auto QoS Versions and Compact

- Two versions of Auto QoS configurations are supported on older MLS QoS platforms
  - The older version is deprecated, and not recommended to be used
- The global command "auto qos srnd4" must be configured to use the current version of Auto QoS on Catalyst 3750-X / 3560-X / 2960-X platforms.

```
auto qos srnd4
```

This must be configured in the global configuration of the switch in order to enable the current version of Auto QoS

- For all switches, the global configuration-level command "auto qos global compact" resets all generated global configuration commands for Auto QoS
  - All global configuration-level QoS commands are hidden. They do not show up in the configuration with a "show running-configuration" command

```
auto qos global compact
```

Only indication within the global running configuration that Auto QoS global configurations have been generated

Egress Queuing Policy for All Auto QoS Commands

Egress Queuing & Map Commands Generated

Same for all “auto qos” commands

```
mls qos map cos-dscp 0 8 16 24 32 46 48 56
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
mls qos srr-queue output dscp-map queue 1 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue output dscp-map queue 1 threshold 3 46 47
mls qos srr-queue output dscp-map queue 2 threshold 1 16 17 18 19 20 21 22 23
mls qos srr-queue output dscp-map queue 2 threshold 1 26 27 28 29 30 31 34 35
mls qos srr-queue output dscp-map queue 2 threshold 1 36 37 38 39
mls qos srr-queue output dscp-map queue 2 threshold 2 24
mls qos srr-queue output dscp-map queue 2 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue output dscp-map queue 2 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue output dscp-map queue 3 threshold 3 0 1 2 3 4 5 6 7
mls qos srr-queue output dscp-map queue 4 threshold 1 8 9 11 13 15
mls qos srr-queue output dscp-map queue 4 threshold 2 10 12 14
mls qos queue-set output 1 threshold 1 100 100 50 200
mls qos queue-set output 1 threshold 2 125 125 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 150 50 200
mls qos queue-set output 1 buffers 15 25 40 20
mls qos
```

CoS-to-DSCP map

CoS to egress queue / threshold mapping

DSCP to egress queue / threshold mapping

WTD thresholds and buffer allocation for queues

Globally enables QoS

Ingress Queuing & Map Commands Generated

Same for all "auto qos" commands

```
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input threshold 1 80 90
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input cos-map queue 1 threshold 2 3
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
mls qos srr-queue input cos-map queue 2 threshold 1 4
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 49 50 51 52 53 54 55
mls qos srr-queue input dscp-map queue 1 threshold 3 56 57 58 59 60 61 62 63
mls qos srr-queue input dscp-map queue 2 threshold 3 32 33 40 41 42 43 44 45
mls qos srr-queue input dscp-map queue 2 threshold 3 46 47
```

Bandwidth ratio between Q1 and Q2 after BW allocation for the PQ (Q2)

WTD thresholds for the non-priority queue (Q2)

Bandwidth reserved for the priority queue (Q2)

CoS to ingress queue / threshold mapping

DSCP to egress queue / threshold mapping

Generated for platforms that support ingress queuing

auto qos voip cisco-phone

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos voip cisco-phone

ACL definition

```
ip access-list extended AUTOQOS-ACL-DEFAULT
 permit ip any any
```

Class-map definition

```
class-map match-all AUTOQOS_VOIP_DATA_CLASS
 match ip dscp ef
class-map match-all AUTOQOS_VOIP_VIDEO_CLASS
 match ip dscp af41
class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
 match ip dscp cs3
class-map match-all AUTOQOS_DEFAULT_CLASS
 match access-group name AUTOQOS-ACL-DEFAULT
```

Table-map definition for policer mark-down

```
mls qos map policed-dscp  0 10 18 24 46 to 8
```

Policy-map definition

```
policy-map AUTOQOS-SRND4-CISCOPHONE-POLICY
 class AUTOQOS_VOIP_DATA_CLASS
  set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_VOIP_VIDEO_CLASS
  set dscp af41
  police 10000000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_VOIP_SIGNAL_CLASS
  set dscp cs3
  police 32000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_DEFAULT_CLASS
  set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
```


Interface-Level Configuration Commands Generated

auto qos voip cisco-phone

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernet1/0/1
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cisco-phone
 mls qos trust cos
 auto qos voip cisco-phone
 service-policy input AUTOQOS-SRND4-CISCOPHONE-POLICY
```

This is the only command to enable “auto qos voip cisco-phone” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernet1/0/1
 auto qos voip cisco-phone
```

When the "auto qos global compact" command is enabled the "auto qos voip cisco-phone" command is the only command that appears in the interface-level configuration.

auto qos voip cisco-softphone

Ingress Classification & Marking Policy – Global Configuration Commands Generated (1 of 2)

auto qos voip cisco-softphone

ACL definitions

```
ip access-list extended AUTOQOS-ACL-DEFAULT
 permit ip any any
ip access-list extended AUTOQOS-ACL-MULTIENHANCED-CONF
 permit udp any any range 16384 32767
ip access-list extended AUTOQOS-ACL-SCAVANGER
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999
ip access-list extended AUTOQOS-ACL-SIGNALING
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061
```

```
ip access-list extended AUTOQOS-ACL-BULK-DATA
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3
ip access-list extended AUTOQOS-ACL-TRANSACTIONAL-DATA
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
```

Next page for class-map and policy-map definitions

Ingress Classification & Marking Policy – Global Configuration Commands Generated (2 of 2)

auto qos voip cisco-softphone

Class-map definition

```
class-map match-all AUTOQOS_VOIP_VIDEO_CLASS
 match ip dscp af41
class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
 match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
class-map match-all AUTOQOS_VOIP_DATA_CLASS
 match ip dscp ef
class-map match-all AUTOQOS_DEFAULT_CLASS
 match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_TRANSACTION_CLASS
 match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
class-map match-all AUTOQOS_VOIP_SIGNAL_CLASS
 match ip dscp cs3
class-map match-all AUTOQOS_SIGNALING_CLASS
 match access-group name AUTOQOS-ACL-SIGNALING
class-map match-all AUTOQOS_BULK_DATA_CLASS
 match access-group name AUTOQOS-ACL-BULK-DATA
class-map match-all AUTOQOS_SCAVANGER_CLASS
 match access-group name AUTOQOS-ACL-SCAVANGER
```

Policy-map definition

```
policy-map AUTOQOS-SRND4-SOFTPHONE-POLICY
 class AUTOQOS_VOIP_DATA_CLASS
  set dscp ef
  police 128000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_MULTIENHANCED_CONF_CLASS
  set dscp af41
  police 5000000 8000 exceed-action drop
 class AUTOQOS_BULK_DATA_CLASS
  set dscp af11
  police 10000000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_TRANSACTION_CLASS
  set dscp af21
  police 10000000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_SCAVANGER_CLASS
  set dscp cs1
  police 10000000 8000 exceed-action drop
 class AUTOQOS_SIGNALING_CLASS
  set dscp cs3
  police 32000 8000 exceed-action drop
 class AUTOQOS_DEFAULT_CLASS
  set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
```

Table-map definition for policer mark-down

```
mls qos map policed-dscp  0 10 18 24 46 to 8
```

Interface-Level Configuration Commands Generated

auto qos voip cisco-softphone

Interface-level configuration without "auto qos global compact" configured

```
interface GigabitEthernet1/0/2
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 auto qos voip cisco-softphone
 service-policy input AUTOQOS-SRND4-SOFTPHONE-POLICY
```

This is the only command to enable "auto qos voip cisco-softphone" at the interface-level and to generate all global commands. All other commands are generated.

Note that conditional trust is not enabled with "auto qos voip cisco-softphone"

Interface-level configuration with "auto qos global compact" configured

```
interface GigabitEthernet1/0/2
 auto qos voip cisco-softphone
```

When the "auto qos global compact" command is enabled the "auto qos voip cisco-softphone" command is the only command that appears in the interface-level configuration.

auto qos video cts

Interface-Level Configuration Commands Generated

auto qos video cts

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernet1/0/3
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device cts
 mls qos trust dscp
 auto qos video cts
```

This is the only command to enable “auto qos video cts” at the interface-level and to generate all global commands. All other commands are generated.

Note that there is no service-policy. Conditional trust is enabled, and the interface trusts DSCP markings.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernet1/0/3
 auto qos video cts
```

When the "auto qos global compact" command is enabled the "auto qos video cts" command is the only command that appears in the interface-level configuration.

auto qos video ip-camera

Interface-Level Configuration Commands Generated

auto qos video ip-camera

Interface-level configuration without "auto qos global compact" configured

```
interface GigabitEthernet1/0/4
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device ip-camera
 mls qos trust dscp
 auto qos video ip-camera
```

This is the only command to enable "auto qos video ip-camera" at the interface-level and to generate all global commands. All other commands are generated.

Note that there is no service-policy. Conditional trust is enabled, and the interface trusts DSCP markings.

Interface-level configuration with "auto qos global compact" configured

```
interface GigabitEthernet1/0/4
 auto qos video ip-camera
```

When the "auto qos global compact" command is enabled the "auto qos video ip-camera" command is the only command that appears in the interface-level configuration.

auto qos video media-player

Interface-Level Configuration Commands Generated

auto qos video media-player

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernet1/0/5
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust device media-player
 mls qos trust dscp
 auto qos video media-player
```

This is the only command to enable “auto qos video media-player” at the interface-level and to generate all global commands. All other commands are generated.

Note that there is no service-policy. Conditional trust is enabled, and the interface trusts DSCP markings.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernet1/0/5
 auto qos video media-player
```

When the "auto qos global compact" command is enabled the "auto qos video media-player" command is the only command that appears in the interface-level configuration.

auto qos classify

Ingress Classification & Marking Policy – Global Configuration Commands Generated (1 of 2)

auto qos classify

ACL definitions

```
ip access-list extended AUTOQOS-ACL-DEFAULT
 permit ip any any
ip access-list extended AUTOQOS-ACL-MULTIENHANCED-CONF
 permit udp any any range 16384 32767
ip access-list extended AUTOQOS-ACL-SCAVANGER
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999
ip access-list extended AUTOQOS-ACL-SIGNALING
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061
```

```
ip access-list extended AUTOQOS-ACL-BULK-DATA
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3
ip access-list extended AUTOQOS-ACL-TRANSACTIONAL-DATA
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
```

Next page for class-map & policy-map definitions

Ingress Classification & Marking Policy – Global Configuration Commands Generated (2 of 2)

auto qos classify

Class-map definitions

```
class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
 match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
class-map match-all AUTOQOS_DEFAULT_CLASS
 match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_TRANSACTION_CLASS
 match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
class-map match-all AUTOQOS_SIGNALING_CLASS
 match access-group name AUTOQOS-ACL-SIGNALING
class-map match-all AUTOQOS_BULK_DATA_CLASS
 match access-group name AUTOQOS-ACL-BULK-DATA
class-map match-all AUTOQOS_SCAVANGER_CLASS
 match access-group name AUTOQOS-ACL-SCAVANGER
```

Policy-map definition

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICY
 class AUTOQOS_MULTIENHANCED_CONF_CLASS
  set dscp af41
 class AUTOQOS_BULK_DATA_CLASS
  set dscp af11
 class AUTOQOS_TRANSACTION_CLASS
  set dscp af21
 class AUTOQOS_SCAVANGER_CLASS
  set dscp cs1
 class AUTOQOS_SIGNALING_CLASS
  set dscp cs3
 class AUTOQOS_DEFAULT_CLASS
  set dscp default
```


Interface-Level Configuration Commands Generated

auto qos classify

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernet1/0/7
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 auto qos classify
 service-policy input AUTOQOS-SRND4-CLASSIFY-POLICY
```

This is the only command to enable “auto qos classify” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernet1/0/7
 auto qos classify
```

When the "auto qos global compact" command is enabled the "auto qos classify" command is the only command that appears in the interface-level configuration.

auto qos classify police

Ingress Classification & Marking Policy – Global Configuration Commands Generated (1 of 2)

auto qos classify police

ACL definitions

```
ip access-list extended AUTOQOS-ACL-DEFAULT
 permit ip any any
ip access-list extended AUTOQOS-ACL-MULTIENHANCED-CONF
 permit udp any any range 16384 32767
ip access-list extended AUTOQOS-ACL-SCAVANGER
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999
ip access-list extended AUTOQOS-ACL-SIGNALING
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061
```

```
ip access-list extended AUTOQOS-ACL-BULK-DATA
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3
ip access-list extended AUTOQOS-ACL-TRANSACTIONAL-DATA
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
```

Next page for class-map & policy-map definitions

Ingress Classification & Marking Policy – Global Configuration Commands Generated (2 of 2)

auto qos classify police

Class-map definitions

```
class-map match-all AUTOQOS_MULTIENHANCED_CONF_CLASS
 match access-group name AUTOQOS-ACL-MULTIENHANCED-CONF
class-map match-all AUTOQOS_DEFAULT_CLASS
 match access-group name AUTOQOS-ACL-DEFAULT
class-map match-all AUTOQOS_TRANSACTION_CLASS
 match access-group name AUTOQOS-ACL-TRANSACTIONAL-DATA
class-map match-all AUTOQOS_SIGNALING_CLASS
 match access-group name AUTOQOS-ACL-SIGNALING
class-map match-all AUTOQOS_BULK_DATA_CLASS
 match access-group name AUTOQOS-ACL-BULK-DATA
class-map match-all AUTOQOS_SCAVANGER_CLASS
 match access-group name AUTOQOS-ACL-SCAVANGER
```

Policy-map definition

```
policy-map AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
 class AUTOQOS_MULTIENHANCED_CONF_CLASS
  set dscp af41
  police 5000000 8000 exceed-action drop
 class AUTOQOS_BULK_DATA_CLASS
  set dscp af11
  police 10000000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_TRANSACTION_CLASS
  set dscp af21
  police 10000000 8000 exceed-action policed-dscp-transmit
 class AUTOQOS_SCAVANGER_CLASS
  set dscp cs1
  police 10000000 8000 exceed-action drop
 class AUTOQOS_SIGNALING_CLASS
  set dscp cs3
  police 32000 8000 exceed-action drop
 class AUTOQOS_DEFAULT_CLASS
  set dscp default
  police 10000000 8000 exceed-action policed-dscp-transmit
```

Interface-Level Configuration Commands Generated

auto qos classify police

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernet1/0/8
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 auto qos classify police
 service-policy input AUTOQOS-SRND4-CLASSIFY-POLICE-POLICY
```

This is the only command to enable “auto qos classify police” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernet1/0/8
 auto qos classify police
```

When the "auto qos global compact" command is enabled the "auto qos classify police" command is the only command that appears in the interface-level configuration.

auto qos trust and auto qos voip trust

Interface-Level Configuration Commands Generated

auto qos trust

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernet1/0/9
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust cos
 auto qos trust
```

This is the only command to enable “auto qos trust” at the interface-level and to generate all global commands. All other commands are generated.

Note that there is no service-policy. Conditional trust is enabled, and the interface trusts CoS markings.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernet1/0/9
 auto qos trust
```

When the "auto qos global compact" command is enabled the "auto qos trust" command is the only command that appears in the interface-level configuration.

auto qos trust cos

Interface-Level Configuration Commands Generated

auto qos trust cos

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernet1/0/11
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust cos
 auto qos trust cos
```

This is the only command to enable “auto qos trust cos” at the interface-level and to generate all global commands. All other commands are generated.

Note that there is no service-policy. Conditional trust is enabled, and the interface trusts CoS markings.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernet1/0/11
 auto qos trust cos
```

When the "auto qos global compact" command is enabled the "auto qos trust cos" command is the only command that appears in the interface-level configuration.

auto qos trust dscp

Interface-Level Configuration Commands Generated

auto qos trust dscp

Interface-level configuration without "auto qos global compact" configured

```
interface GigabitEthernet1/0/10
 srr-queue bandwidth share 1 30 35 5
 priority-queue out
 mls qos trust dscp
 auto qos trust dscp
```

This is the only command to enable "auto qos trust dscp" at the interface-level and to generate all global commands. All other commands are generated.

Note that there is no service-policy. Conditional trust is enabled, and the interface trusts DSCP markings.

Interface-level configuration with "auto qos global compact" configured

```
interface GigabitEthernet1/0/10
 auto qos trust dscp
```

When the "auto qos global compact" command is enabled the "auto qos trust dscp" command is the only command that appears in the interface-level configuration.

Appendix E: AutoQoS Configurations - Catalyst 9000 / 3850 / 3650

Auto QoS – Catalyst 9000 / 3850 / 3650 (Wired)

- Auto QoS is a macro which provisions a pre-defined ingress classification & marking policy and an egress (and/or ingress) queueing policy
- Eleven forms of the interface-level Auto QoS command ("auto qos voip trust" and "auto qos trust" generate the same configuration)
  - auto qos voip {cisco-phone | cisco-softphone | trust}
  - auto qos video {cts | ip-camera | media-player}
  - auto qos classify [police]
  - auto qos trust [cos | dscp]
- To remove Auto QoS on an interface (run another macro to remove Auto QoS) preface the command with a "no" (i.e. no auto qos voip cisco-phone)
  - It is not recommended to modify the configuration provisioned by the Auto QoS commands because it may affect the ability of the switch to remove the configuration on the interface or globally when removing Auto QoS

Hiding Auto QoS Generated Configuration

- The global configuration-level command "auto qos global compact" resets all generated global configuration commands for Auto QoS
- All global configuration-level commands are hidden (other than the "auto qos global compact" command). They do not show up in the configuration with a "show running-configuration" command

```
auto qos global compact
```

Only indication within the global running configuration that Auto QoS global configurations have been generated

- When auto qos global compact is enabled and auto qos is enabled on an interface, only the command which enabled auto qos on the interface appears within the configuration.
  - Service policies which are generated and applied to the interface are also hidden

```
interface GigabitEthernet1/0/15
 auto qos voip cisco-phone
```

Only indication within the interface-level running configuration that Auto QoS interface-level configurations have been generated

Egress Queuing Policy for All Auto QoS Commands

Egress Queuing Policy – Global Configuration Commands Generated

Same for all “auto qos” commands

Class-map definition

```
class-map match-any AutoQos-4.0-Output-Priority-Queue
  match  dscp cs4  cs5  ef
  match cos  5
class-map match-any AutoQos-4.0-Output-Control-Mgmt-Queue
  match  dscp cs2 cs3  cs6  cs7
  match cos  3
class-map match-any AutoQos-4.0-Output-Multimedia-Conf-Queue
  match  dscp af41  af42  af43
  match cos  4
class-map match-any AutoQos-4.0-Output-Trans-Data-Queue
  match  dscp af21  af22  af23
  match cos  2
class-map match-any AutoQos-4.0-Output-Bulk-Data-Queue
  match  dscp af11  af12  af13
  match cos  1
class-map match-any AutoQos-4.0-Output-Scavenger-Queue
  match  dscp cs1
class-map match-any AutoQos-4.0-Output-Multimedia-Strm-Queue
  match  dscp af31  af32  af33
```

Policy-map definition

```
policy-map AutoQos-4.0-Output-Policy
 class AutoQos-4.0-Output-Priority-Queue
    priority level 1 percent 30
 class AutoQos-4.0-Output-Control-Mgmt-Queue
    bandwidth remaining percent 10
    queue-limit dscp  cs2 percent 80
    queue-limit dscp  cs3 percent 90
    queue-limit dscp  cs6 percent 100
    queue-limit dscp  cs7 percent 100
    queue-buffers ratio 10
 class AutoQos-4.0-Output-Multimedia-Conf-Queue
    bandwidth remaining percent 10
    queue-buffers ratio 10
 class AutoQos-4.0-Output-Trans-Data-Queue
    bandwidth remaining percent 10
    queue-buffers ratio 10
 class AutoQos-4.0-Output-Bulk-Data-Queue
    bandwidth remaining percent 4
    queue-buffers ratio 10
 class AutoQos-4.0-Output-Scavenger-Queue
    bandwidth remaining percent 1
    queue-buffers ratio 10
 class AutoQos-4.0-Output-Multimedia-Strm-Queue
    bandwidth remaining percent 10
    queue-buffers ratio 10
 class class-default
    bandwidth remaining percent 25
    queue-buffers ratio 25
```


auto qos voip cisco-phone

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos voip cisco-phone

ACL definition

```
ip access-list extended AutoQos-4.0-Acl-Default
 permit ip any any
```

Class-map definition

```
class-map match-any AutoQos-4.0-Voip-Data-CiscoPhone-Class
  match cos 5
class-map match-any AutoQos-4.0-Voip-Signal-CiscoPhone-Class
  match cos 3
class-map match-any AutoQos-4.0-Default-Class
  match access-group name AutoQos-4.0-Acl-Default
```

Policy-map definition

```
policy-map AutoQos-4.0-CiscoPhone-Input-Policy
 class AutoQos-4.0-Voip-Data-CiscoPhone-Class
   set dscp ef
    police cir 128000 bc 8000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
 class AutoQos-4.0-Voip-Signal-CiscoPhone-Class
   set dscp cs3
    police cir 32000 bc 8000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
 class AutoQos-4.0-Default-Class
   set dscp default
```

Table-map definition for policer mark-down

```
table-map policed-dscp
 map from  0 to 8
 map from  10 to 8
 map from  18 to 8
 map from  24 to 8
 map from  46 to 8
 default copy
```

Interface-Level Configuration Commands Generated

auto qos voip cisco-phone

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 trust device cisco-phone
 auto qos voip cisco-phone
 service-policy input AutoQos-4.0-CiscoPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos voip cisco-phone” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos voip cisco-phone
```

When the "auto qos global compact" command is enabled the "auto qos voip cisco-phone" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos voip
cisco-softphone

Ingress Classification & Marking Policy – Global Configuration Commands Generated (1 of 3)

auto qos voip cisco-softphone

ACL definitions

```
ip access-list extended AutoQos-4.0-Acl-MultiEnhanced-Conf
 permit udp any any range 16384 32767
 permit tcp any any range 50000 59999

ip access-list extended AutoQos-4.0-Acl-Scavanger
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999

ip access-list extended AutoQos-4.0-Acl-Signaling
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061

ip access-list extended AutoQos-4.0-Acl-Default
 permit ip any any
```

```
ip access-list extended AutoQos-4.0-Acl-Bulk-Data
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3

ip access-list extended AutoQos-4.0-Acl-Transactional-Data
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
 permit tcp any any eq 1527
 permit tcp any any eq 6200
 permit tcp any any eq 3389
 permit tcp any any eq 5985
 permit tcp any any eq 8080
```

Next page for class-map definitions

Ingress Classification & Marking Policy – Global Configuration Commands Generated (2 of 3)

auto qos voip cisco-softphone

Class-map definition

```
class-map match-any AutoQos-4.0-Voip-Data-Class
  match dscp ef
  match cos 5
class-map match-any AutoQos-4.0-Voip-Signal-Class
  match dscp cs3
  match cos 3
class-map match-any AutoQos-4.0-Multimedia-Conf-Class
  match access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
class-map match-any AutoQos-4.0-Bulk-Data-Class
  match access-group name AutoQos-4.0-Acl-Bulk-Data
class-map match-any AutoQos-4.0-Transaction-Class
  match access-group name AutoQos-4.0-Acl-Transactional-Data
class-map match-any AutoQos-4.0-Scavanger-Class
  match access-group name AutoQos-4.0-Acl-Scavanger
class-map match-any AutoQos-4.0-Signaling-Class
  match access-group name AutoQos-4.0-Acl-Signaling
class-map match-any AutoQos-4.0-Default-Class
  match access-group name AutoQos-4.0-Acl-Default
```

Table-map definition
for policer mark-down

```
table-map policed-dscp
 map from  0 to 8
 map from  10 to 8
 map from  18 to 8
 map from  24 to 8
 map from  46 to 8
 default copy
```

Next page for policy-map definition

Ingress Classification & Marking Policy – Global Configuration Commands Generated (3 of 3)

auto qos voip cisco-softphone

Policy-map definition

```
policy-map AutoQos-4.0-CiscoSoftPhone-Input-Policy
 class AutoQos-4.0-Voip-Data-Class
   set dscp ef
    police cir 128000 bc 8000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
 class AutoQos-4.0-Voip-Signal-Class
   set dscp cs3
    police cir 32000 bc 8000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
 class AutoQos-4.0-Multimedia-Conf-Class
   set dscp af41
    police cir 5000000
      conform-action transmit
      exceed-action drop
 class AutoQos-4.0-Bulk-Data-Class
   set dscp af11
    police cir 10000000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
[continued]
```

```
class AutoQos-4.0-Transaction-Class
   set dscp af21
    police cir 10000000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
class AutoQos-4.0-Scavanger-Class
   set dscp cs1
    police cir 10000000
      conform-action transmit
      exceed-action drop
 class AutoQos-4.0-Signaling-Class
   set dscp cs3
    police cir 32000 bc 8000
      conform-action transmit
      exceed-action drop
 class AutoQos-4.0-Default-Class
   set dscp default
    police cir 10000000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
```


Interface-Level Configuration Commands Generated

auto qos voip cisco-softphone

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos voip cisco-softphone
 service-policy input AutoQos-4.0-CiscoSoftPhone-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos voip cisco-softphone” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos voip cisco-softphone
```

When the "auto qos global compact" command is enabled the "auto qos voip cisco-softphone" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos video cts

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos video cts

Policy-map definition

```
policy-map AutoQos-4.0-Trust-Cos-Input-Policy
 class class-default
   set cos cos table AutoQos-4.0-Trust-Cos-Table
```

Table-map definition for trust CoS

```
Table Map AutoQos-4.0-Trust-Cos-Table
 default copy
```


Interface-Level Configuration Commands Generated

auto qos video cts

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 trust device cts
 auto qos video cts
 service-policy input AutoQos-4.0-Trust-Cos-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos video cts” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
auto qos video cts
```

When the "auto qos global compact" command is enabled the "auto qos video cts" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos video ip-camera

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos video ip-camera

Policy-map definition

```
policy-map AutoQos-4.0-Trust-Dscp-Input-Policy
 class class-default
  set cos cos table AutoQos-4.0-Trust-Dscp-Table
```

Table-map definition for trust CoS

```
Table Map AutoQos-4.0-Trust-Dscp-Table
 default copy
```

Interface-Level Configuration Commands Generated

auto qos video ip-camera

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 trust device ip-camera
 auto qos video ip-camera
 service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos video ip-camera” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
auto qos video ip-camera
```

When the "auto qos global compact" command is enabled the "auto qos video ip-camera" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos video media-player

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos video media-player

Table-map definition for trust CoS

```
Table Map AutoQos-4.0-Trust-Dscp-Table
 default copy
```

Policy-map definition

```
policy-map AutoQos-4.0-Trust-Dscp-Input-Policy
 class class-default
  set cos cos table AutoQos-4.0-Trust-Dscp-Table
```

Interface-Level Configuration Commands Generated

auto qos video media-player

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 trust device media-player
 auto qos video media-player
 service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos video media-player” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
auto qos video media-player
```

When the "auto qos global compact" command is enabled the "auto qos video media-player" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos classify

Ingress Classification & Marking Policy – Global Configuration Commands Generated (1 of 2)

auto qos classify

ACL definitions

```
ip access-list extended AutoQos-4.0-Acl-MultiEnhanced-Conf
 permit udp any any range 16384 32767
 permit tcp any any range 50000 59999

ip access-list extended AutoQos-4.0-Acl-Scavanger
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999

ip access-list extended AutoQos-4.0-Acl-Signaling
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061

ip access-list extended AutoQos-4.0-Acl-Default
 permit ip any any
```

```
ip access-list extended AutoQos-4.0-Acl-Bulk-Data
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3

ip access-list extended AutoQos-4.0-Acl-Transactional-Data
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
 permit tcp any any eq 1527
 permit tcp any any eq 6200
 permit tcp any any eq 3389
 permit tcp any any eq 5985
 permit tcp any any eq 8080
```

Next page for class-map & policy-map definitions

Ingress Classification & Marking Policy – Global Configuration Commands Generated (2 of 2)

auto qos classify

Class-map definitions

```
class-map match-any AutoQos-4.0-Multimedia-Conf-Class
 match access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
class-map match-any AutoQos-4.0-Bulk-Data-Class
 match access-group name AutoQos-4.0-Acl-Bulk-Data
class-map match-any AutoQos-4.0-Transaction-Class
 match access-group name AutoQos-4.0-Acl-Transactional-Data
Class-map match-any AutoQos-4.0-Scavanger-Class
 match access-group name AutoQos-4.0-Acl-Scavanger
class-map match-any AutoQos-4.0-Signaling-Class
 match access-group name AutoQos-4.0-Acl-Signaling
class-map match-any AutoQos-4.0-Default-Class
 match access-group name AutoQos-4.0-Acl-Default
```

Policy-map definition

```
policy-map AutoQos-4.0-Classify-Input-Policy
 class AutoQos-4.0-Multimedia-Conf-Class
  set dscp af41
 class AutoQos-4.0-Bulk-Data-Class
  set dscp af11
 class AutoQos-4.0-Transaction-Class
  set dscp af21
 class AutoQos-4.0-Scavanger-Class
  set dscp cs1
 class AutoQos-4.0-Signaling-Class
  set dscp cs3
 class AutoQos-4.0-Default-Class
  set dscp default
```


Interface-Level Configuration Commands Generated

auto qos classify

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos classify
 service-policy input AutoQos-4.0-Classify-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos classify” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos classify
```

When the "auto qos global compact" command is enabled the "auto qos classify" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos classify police

Ingress Classification & Marking Policy – Global Configuration Commands Generated (1 of 3)

auto qos classify police

ACL definitions

```
ip access-list extended AutoQos-4.0-Acl-MultiEnhanced-Conf
 permit udp any any range 16384 32767
 permit tcp any any range 50000 59999

ip access-list extended AutoQos-4.0-Acl-Scavanger
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999

ip access-list extended AutoQos-4.0-Acl-Signaling
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061

ip access-list extended AutoQos-4.0-Acl-Default
 permit ip any any
```

```
ip access-list extended AutoQos-4.0-Acl-Bulk-Data
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3

ip access-list extended AutoQos-4.0-Acl-Transactional-Data
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
 permit tcp any any eq 1527
 permit tcp any any eq 6200
 permit tcp any any eq 3389
 permit tcp any any eq 5985
 permit tcp any any eq 8080
```

Next page for class-map & policy-map definitions

Ingress Classification & Marking Policy – Global Configuration Commands Generated (2 of 3)

auto qos classify police

Class-map definitions

```
class-map match-any AutoQos-4.0-Multimedia-Conf-Class
  match access-group name AutoQos-4.0-Acl-MultiEnhanced-Conf
class-map match-any AutoQos-4.0-Bulk-Data-Class
  match access-group name AutoQos-4.0-Acl-Bulk-Data
class-map match-any AutoQos-4.0-Transaction-Class
  match access-group name AutoQos-4.0-Acl-Transactional-Data
class-map match-any AutoQos-4.0-Scavanger-Class
  match access-group name AutoQos-4.0-Acl-Scavanger
class-map match-any AutoQos-4.0-Signaling-Class
  match access-group name AutoQos-4.0-Acl-Signaling
class-map match-any AutoQos-4.0-Default-Class
  match access-group name AutoQos-4.0-Acl-Default
```

Table-map definition for policer mark-down

```
table-map policed-dscp
 map from  0 to 8
 map from  10 to 8
 map from  18 to 8
 map from  24 to 8
 map from  46 to 8
 default copy
```

Next page for policy-map definition

Ingress Classification & Marking Policy – Global Configuration Commands Generated (3 of 3)

auto qos classify police

Policy-map definition

```
policy-map AutoQos-4.0-Classify-Police-Input-Policy
 class AutoQos-4.0-Multimedia-Conf-Class
   set dscp af41
    police cir 5000000
      conform-action transmit
      exceed-action drop
 class AutoQos-4.0-Bulk-Data-Class
   set dscp af11
    police cir 10000000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
 class AutoQos-4.0-Transaction-Class
   set dscp af21
    police cir 10000000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
```

```
[Continued]
class AutoQos-4.0-Scavanger-Class
   set dscp cs1
    police cir 10000000
      conform-action transmit
      exceed-action drop
 class AutoQos-4.0-Signaling-Class
   set dscp cs3
    police cir 32000 bc 8000
      conform-action transmit
      exceed-action drop
 class AutoQos-4.0-Default-Class
   set dscp default
    police cir 10000000
      conform-action transmit
      exceed-action set-dscp-transmit dscp table policed-dscp
```


Interface-Level Configuration Commands Generated

auto qos classify police

Interface-level configuration without "auto qos global compact" configured

```
interface GigabitEthernetx/x/x
 auto qos classify police
 service-policy input AutoQos-4.0-Classify-Police-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable "auto qos classify police" at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with "auto qos global compact" configured

```
interface GigabitEthernetx/x/x
 auto qos classify police
```

When the "auto qos global compact" command is enabled the "auto qos classify police" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos trust and auto qos voip trust

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos trust

Policy-map definition

```
policy-map AutoQos-4.0-Trust-Cos-Input-Policy
 class class-default
   set cos cos table AutoQos-4.0-Trust-Cos-Table
```

Table-map definition for trust CoS

```
Table Map AutoQos-4.0-Trust-Cos-Table
 default copy
```

Interface-Level Configuration Commands Generated

auto qos trust

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos trust
 service-policy input AutoQos-4.0-Trust-Cos-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos trust” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
auto qos trust
```

When the "auto qos global compact" command is enabled the "auto qos trust" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos trust cos

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos trust cos

Policy-map definition

```
policy-map AutoQos-4.0-Trust-Cos-Input-Policy
 class class-default
  set cos cos table AutoQos-4.0-Trust-Cos-Table
```

Table-map definition for trust CoS

```
Table Map AutoQos-4.0-Trust-Cos-Table
 default copy
```

Interface-Level Configuration Commands Generated

auto qos trust cos

Interface-level configuration without "auto qos global compact" configured

```
interface GigabitEthernetx/x/x
 auto qos trust cos
 service-policy input AutoQos-4.0-Trust-Cos-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable "auto qos trust cos" at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with "auto qos global compact" configured

```
interface GigabitEthernetx/x/x
 auto qos trust cos
```

When the "auto qos global compact" command is enabled the "auto qos trust cos" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

auto qos trust dscp

Ingress Classification & Marking Policy – Global Configuration Commands Generated

auto qos trust dscp

Policy-map definition

```
policy-map AutoQos-4.0-Trust-Dscp-Input-Policy
 class class-default
   set dscp dscp table AutoQos-4.0-Trust-Dscp-Table
```

Table-map definition for trust dscp

```
Table Map AutoQos-4.0-Trust-Dscp-Table
 default copy
```


Interface-Level Configuration Commands Generated

auto qos trust dscp

Interface-level configuration without “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos trust dscp
 service-policy input AutoQos-4.0-Trust-Dscp-Input-Policy
 service-policy output AutoQos-4.0-Output-Policy
```

This is the only command to enable “auto qos trust dscp” at the interface-level and to generate all global commands. All other commands are generated.

Interface-level configuration with “auto qos global compact” configured

```
interface GigabitEthernetx/x/x
 auto qos trust dscp
```

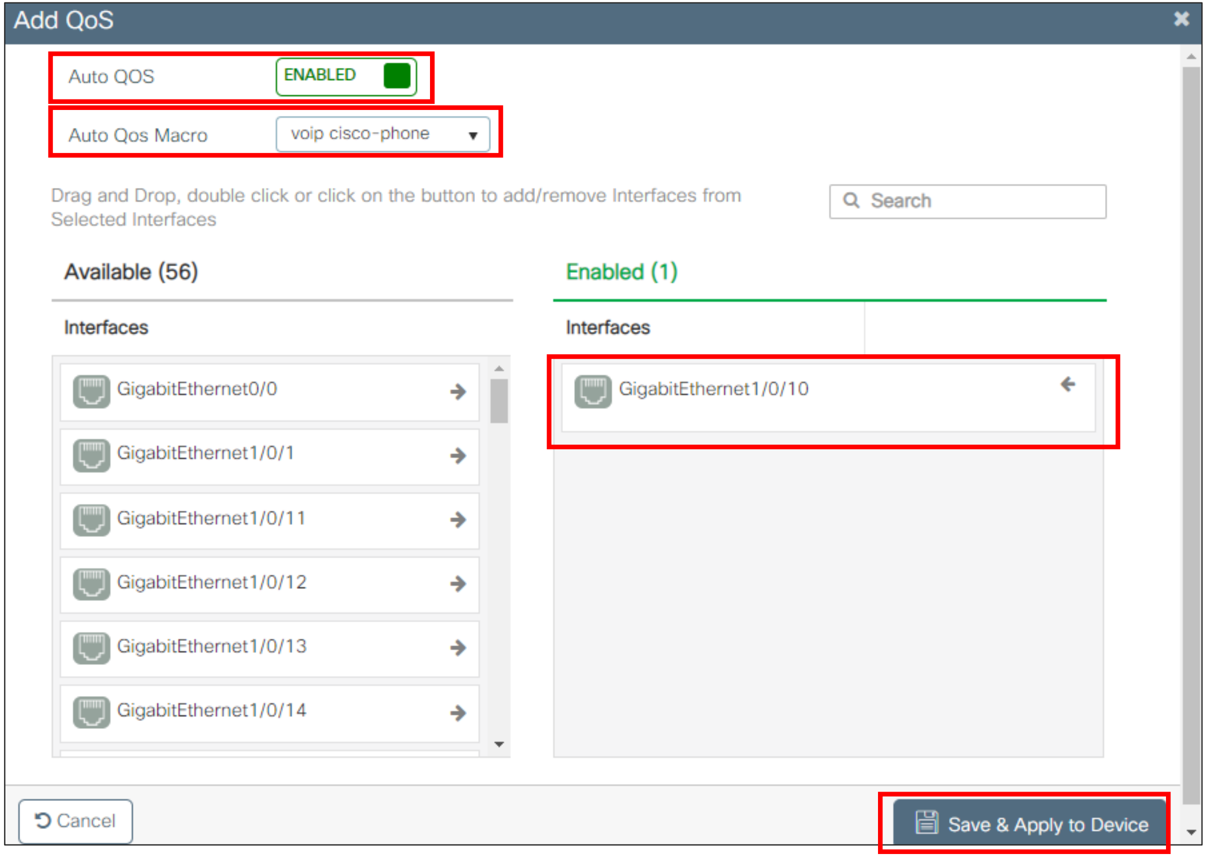
When the "auto qos global compact" command is enabled the "auto qos trust dscp" command is the only command that appears in the interface-level configuration. No global commands appear in the configuration.

Appendix F: Catalyst 9000 QoS via the Web UI

QoS Policy via the Catalyst 9000 Series Web UI

Auto QoS

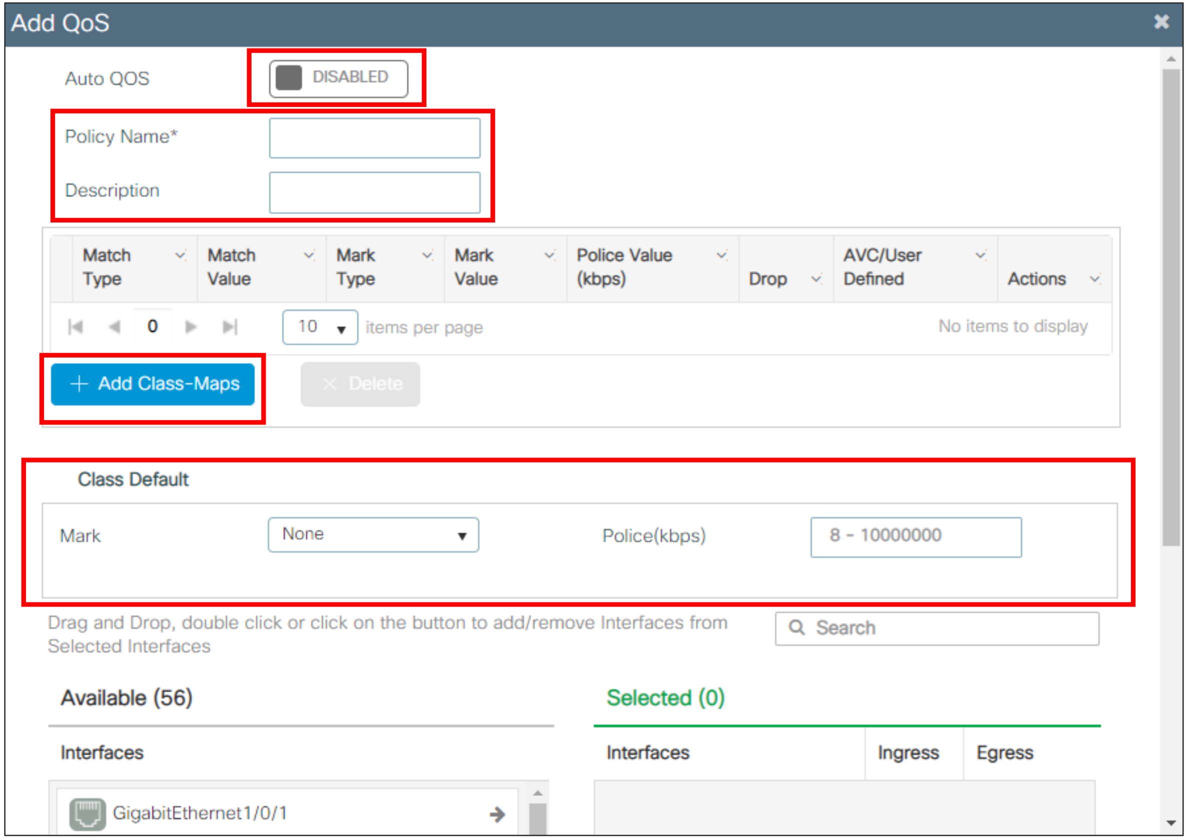
- Navigate to **Configuration > Services > QoS**
- Click **+Add** to add a new policy
- Enable Auto QoS
- From the drop-down menu select one of the eleven Auto QoS macros
- Select one or more interfaces to apply the Auto QoS macro by clicking on the → arrow
- Click Save & Apply to Device



QoS Policy via the Catalyst 9000 Series Web UI

Custom Policy

- Navigate to **Configuration > Services > QoS**
- Click **+Add** to add a new policy
- Disable Auto QoS
- Configure a Policy Name (policy-map) and a Description
- Click **+Add Class-Maps** to add one or more class-maps
- Two choices for class-maps:
  - AVC – NBAR-based
  - User-Defined – DSCP or ACL
- Determine the behavior of the Class Default traffic-class

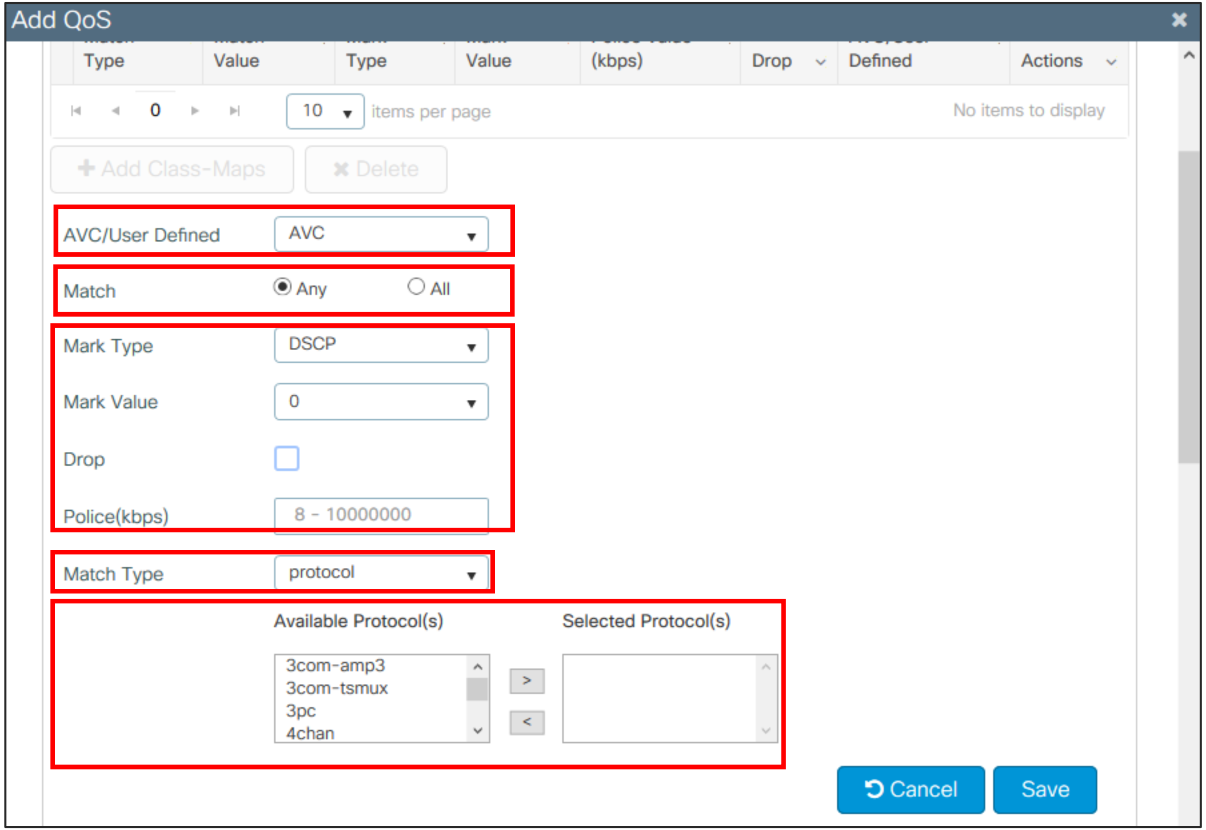


cisco Live!

QoS Policy via the Catalyst 9000 Series Web UI

Add Class-Map –AVC

- From the drop-down menu select AVC
- Select Match Any (logical OR) or Match All (logical AND)
- Currently supported match types for AVC class-maps
  - Protocol, Category, Subcategory, or Application-group
- Select up to 16 protocols from the menu and click > to apply them to the class-map
- Configure the action(s)
  - Drop
  - Mark (DSCP or CoS)
  - Police (specify the rate) – no markdown

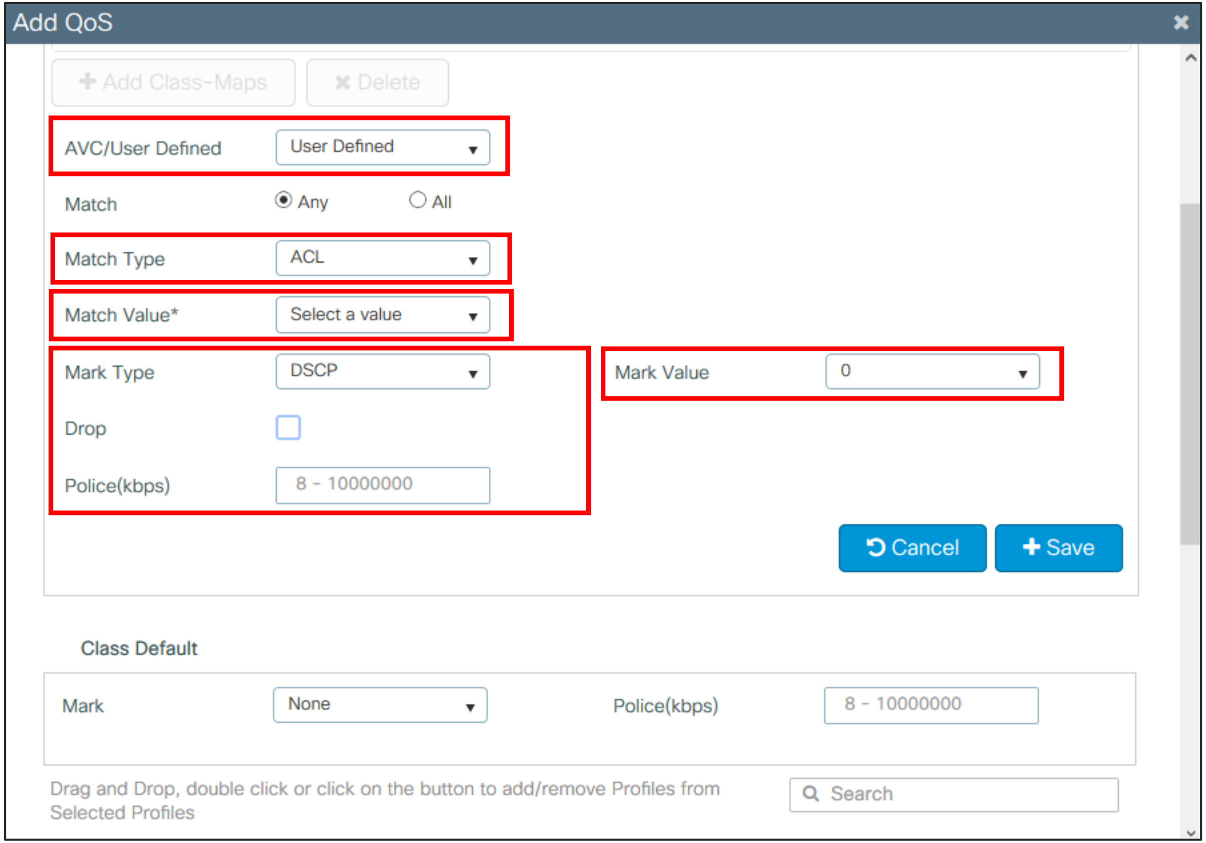


CISCO Live!

QoS Policy via the Catalyst 9000 Series Web UI

Add Class-Map – User Defined (non AVC)

- From the drop-down menu select **User Defined**
- Currently supported match types for User Defined class-maps
  - DSCP, CoS, or ACL
- For match type of ACL, select the ACL from the drop-down list under Match Value
  - You must configure the ACL via CLI
- Configure the action(s)
  - Drop
  - Mark (DSCP or CoS)
  - Police (specify the rate) – no markdown

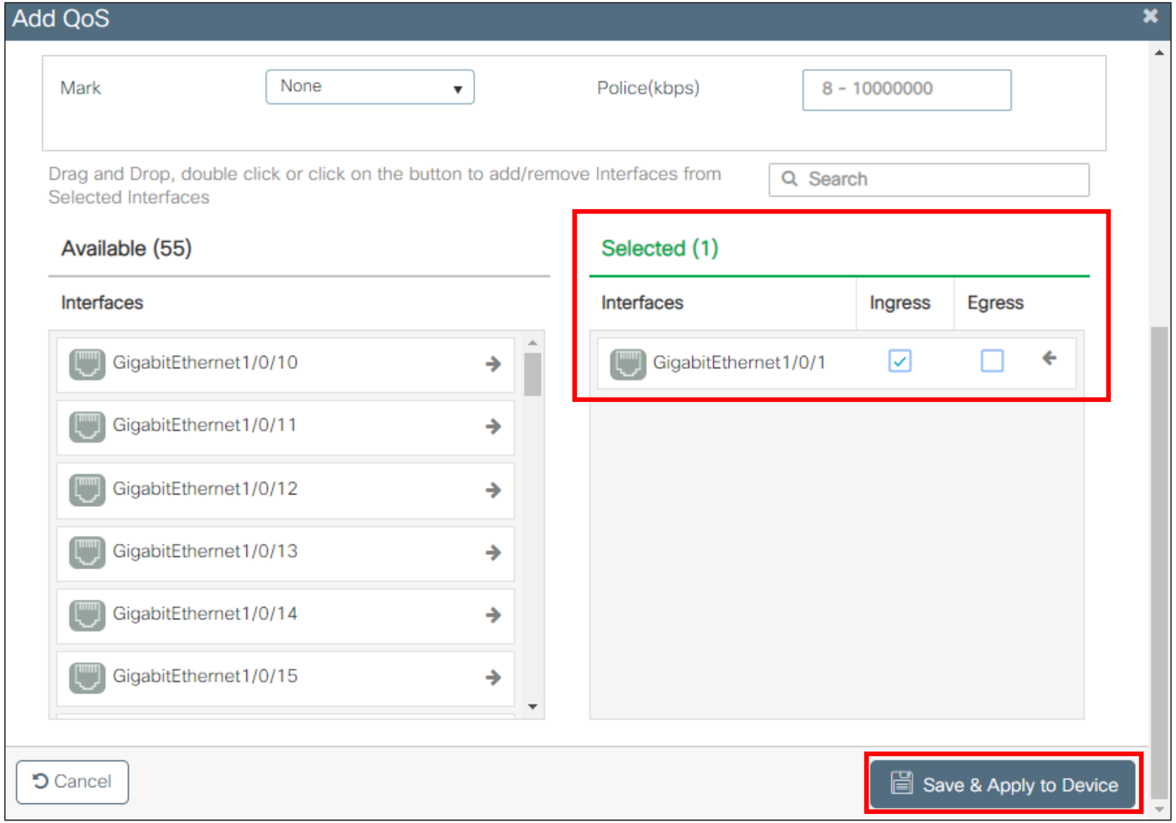


cisco Live!

QoS Policy via the Catalyst 9000 Series Web UI

Custom Policy – Applying the Service-Policy to Interfaces

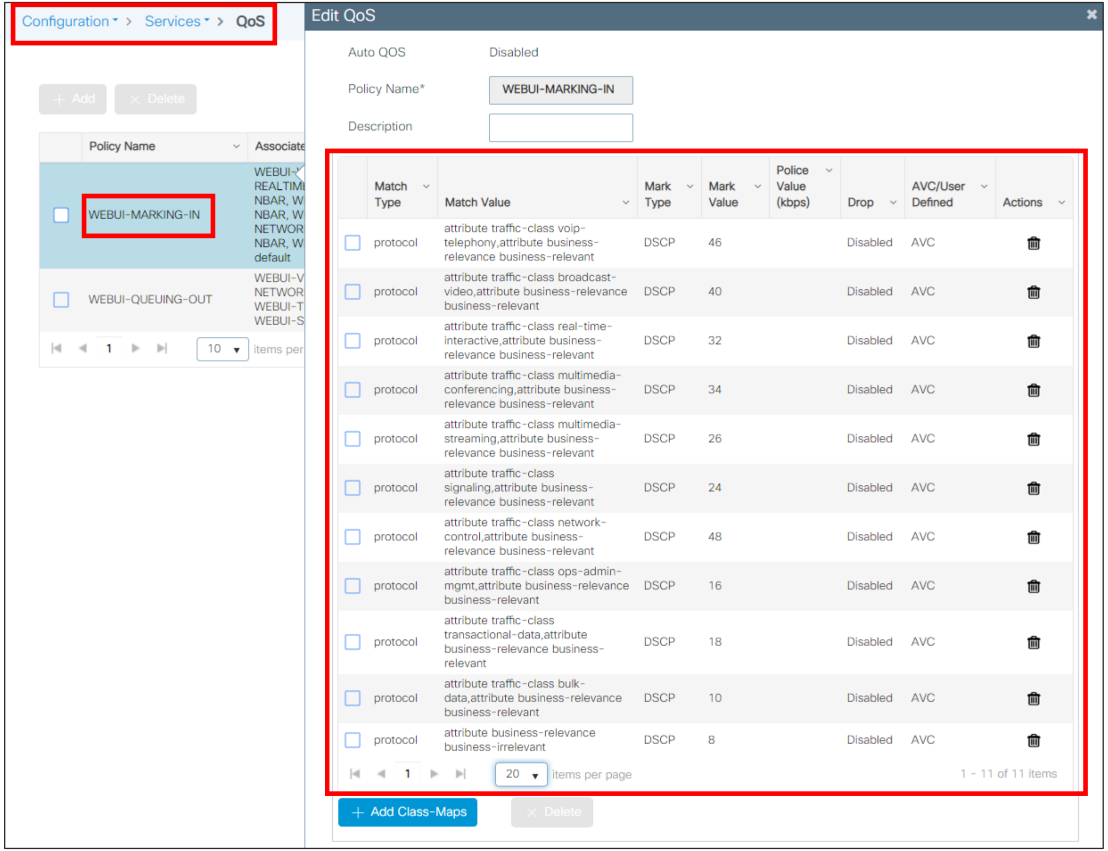
- Click the → arrow next the interface or interfaces to which you wish to apply this QoS Policy
- Select the direction (Ingress for an ingress classification & marking policy)
- Click the **Save & Apply to Device** button



QoS Policy via the Catalyst 9000 Series Web UI

WEBUI-MARKING-IN Policy

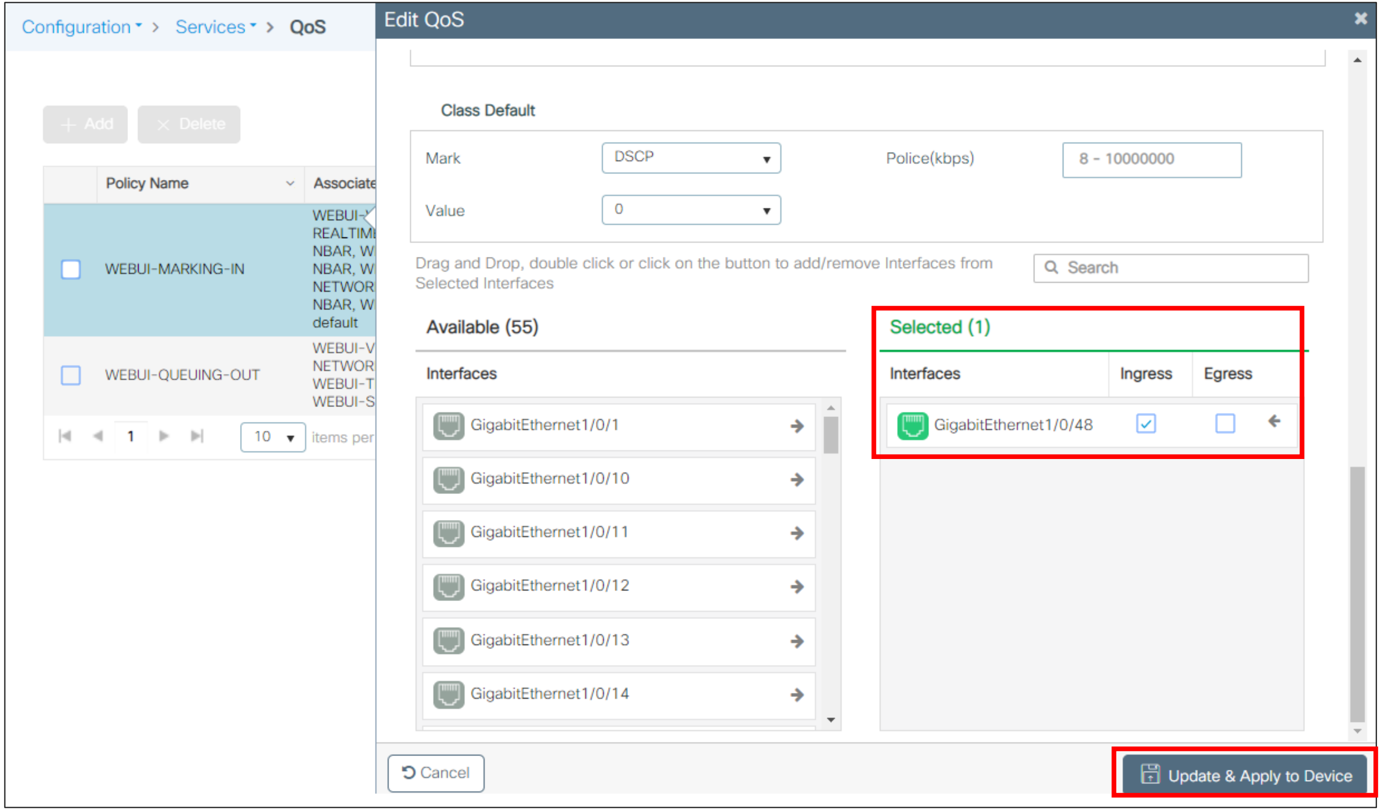
- Pre-configured AVC / NBAR2-based ingress classification & marking policy which appears when you enable AVC via the Web UI
  - Switch must have necessary Cisco DNA Center licensing for AVC / NBAR2
- Navigate to **Configuration > Services > QoS**
- Click on WEBUI-MARKING-IN to expose the side panel
- Implements the Cisco RFC 4594-based 12-class QoS model using “match protocol attribute traffic-class” and “match protocol attribute business-relevance”



QoS Policy via the Catalyst 9000 Series Web UI

WEBUI-MARKING-IN Policy (continued)

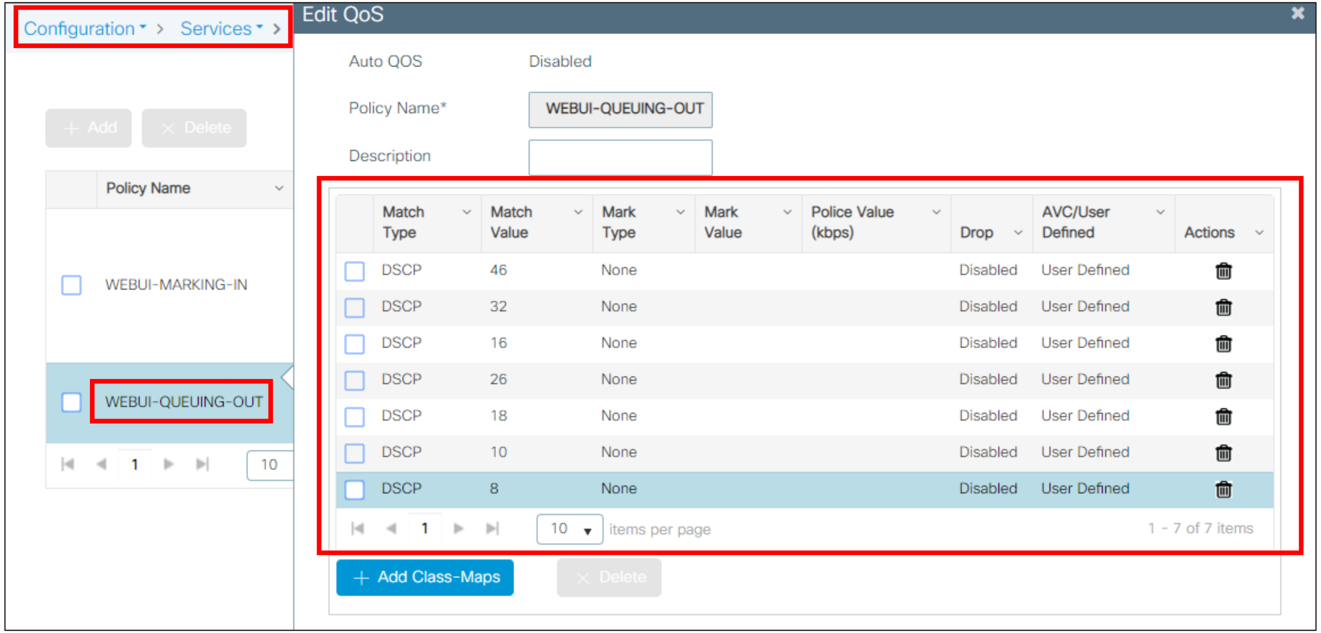
- Select one or more interfaces to apply the Auto QoS macro by clicking on the → arrow
- Select the direction (Ingress for an ingress classification & marking policy)
- Click **Save & Apply to Device**
- You don't have the ability to change the business-relevance or traffic-class of an individual application from within the Web UI. You will need to use Cisco DNA Center for intent-based QoS policy or configure this via the CLI



QoS Policy via the Catalyst 9000 Series Web UI

WEBUI-QUEUING-OUT Policy

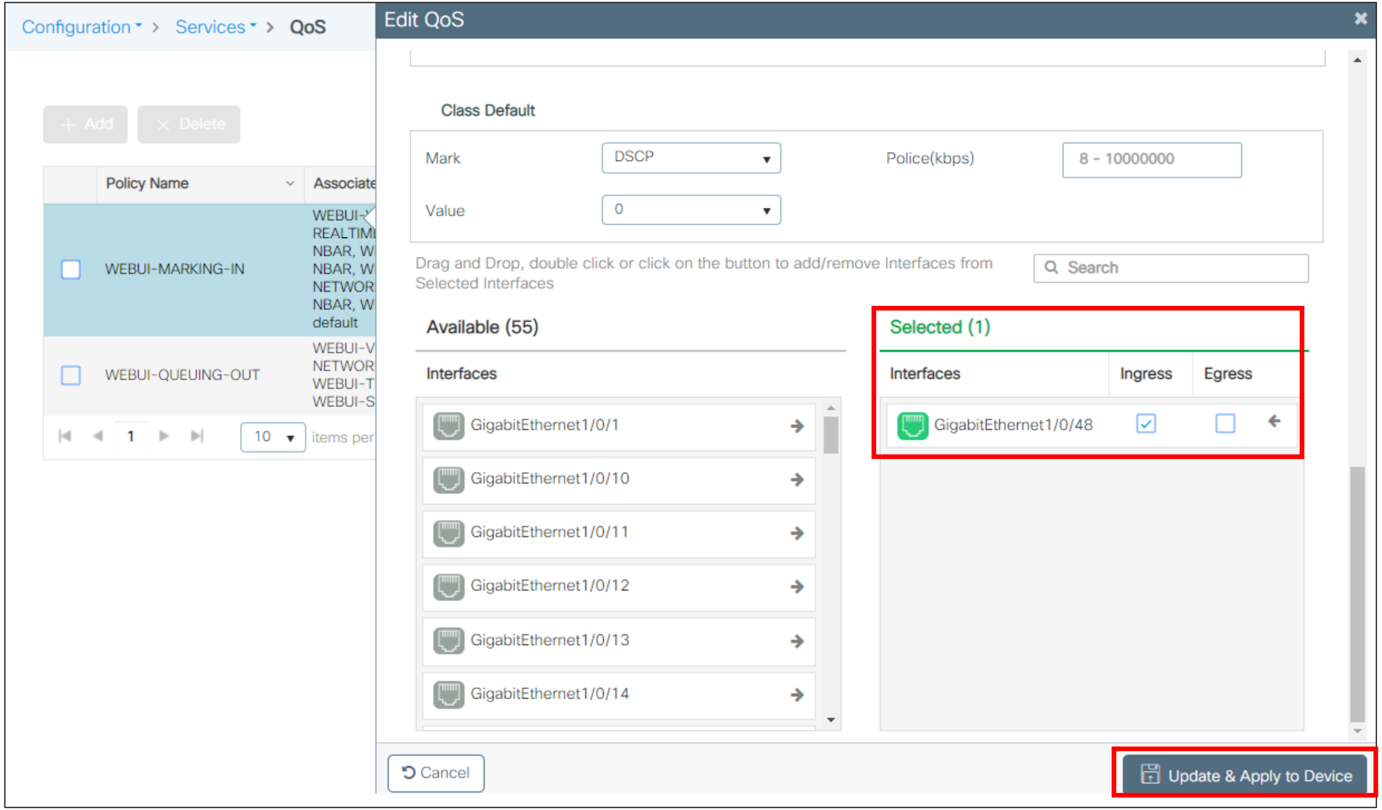
- Pre-configured egress queuing policy which appears when you enable AVC via the Web UI
- Navigate to **Configuration > Services > QoS**
- Click on WEBUI-QUEUING-OUT to expose the side panel
- Implements a 2P6Q3T egress queuing policy with Cisco best-practice recommendations



QoS Policy via the Catalyst 9000 Series Web UI

WEBUI-MARKING-IN Policy (continued)

- Select one or more interfaces to apply the Auto QoS macro by clicking on the → arrow
- Select the direction (Ingress for an ingress classification & marking policy)
- Click **Save & Apply to Device**
- You don't have the ability to change the business-relevance or traffic-class of an individual application from within the Web UI. You will need to use Cisco DNA Center for intent-based QoS policy or configure this via the CLI



QoS Policy via the Catalyst 9000 Series Web UI

WEBUI-QUEUING-OUT Policy-Map

```
policy-map WEBUI-QUEUING-OUT
 class WEBUI-VOICE-DSCP
  priority level 1 percent 1
  queue-buffers ratio 5
 class WEBUI-BROADCAST_VIDEO-DSCP
  priority level 2 percent 30
  queue-buffers ratio 5
 class WEBUI-NETWORK_CONTROL-DSCP
  bandwidth remaining percent 10
  queue-buffers ratio 5
 class WEBUI-MULTIMEDIA_STREAMING-DSCP
  bandwidth remaining percent 20
  queue-buffers ratio 10
  queue-limit dscp af33 percent 80
  queue-limit dscp af32 percent 90
  queue-limit dscp af31 percent 100
…
```

Two priority queues

Implements separate Bulk-Data and Scavenger queues

```
[continued]
 class WEBUI-TRANSACTIONAL_DATA-DSCP
  bandwidth remaining percent 20
  queue-buffers ratio 10
  queue-limit dscp af23 percent 80
  queue-limit dscp af22 percent 90
  queue-limit dscp af21 percent 100
 class WEBUI-BULK_DATA-DSCP
  bandwidth remaining percent 14
  queue-buffers ratio 20
  queue-limit dscp af13 percent 80
  queue-limit dscp af12 percent 90
  queue-limit dscp af11 percent 100
 class WEBUI-SCAVENGER-DSCP
  bandwidth remaining percent 1
  queue-buffers ratio 5
 class class-default
  bandwidth remaining percent 35
  queue-buffers ratio 40
```

Allocates buffers to all queues

Enables DSCP-based WTD and tunes tail-drop percentages to align to AF PHBs

Configures bandwidth remaining for non-priority queues

QoS Policy via the Catalyst 9000 Series Web UI

WEBUI-QUEUING-OUT Class-Maps

```
class-map match-any WEBUI-VOICE-DSCP
 match dscp ef
class-map match-any WEBUI-BROADCAST_VIDEO-DSCP
 match dscp cs4
 match dscp af41
 match dscp af42
 match dscp af43
 match dscp cs5
class-map match-any WEBUI-MULTIMEDIA_STREAMING-DSCP
 match dscp af31
 match dscp af32
 match dscp af33
class-map match-any WEBUI-NETWORK_CONTROL-DSC
 match dscp cs2
 match dscp cs3
 match dscp cs6
 match dscp cs7
…
```

```
[continued]
class-map match-any WEBUI-TRANSACTIONAL_DATA-DSCP
 match dscp af21
 match dscp af22
 match dscp af23
class-map match-any WEBUI-BULK_DATA-DSCP
 match dscp af11
 match dscp af12
 match dscp af13
class-map match-any WEBUI-SCAVENGER-DSCP
 match dscp cs1
```


Backup: Catalyst 9800 Auto QoS Configurations

Wireless Ingress Policy – Global Configuration Commands Generated

Auto Qos Mode Enterprise

Class-map definitions

```
class-map match-any AutoQos-4.0-wlan-Voip-Data-Class
 match dscp ef
class-map match-any AutoQos-4.0-wlan-Voip-Signal-Class
 match protocol skinny
 match protocol cisco-jabber-control
 match protocol sip
 match protocol sip-tls
class-map match-any AutoQos-4.0-wlan-Multimedia-Conf-Class
 match protocol cisco-phone-video
 match protocol cisco-jabber-video
 match protocol ms-lync-video
 match protocol webex-media
class-map match-any AutoQos-4.0-wlan-Transaction-Class
 match protocol cisco-jabber-im
 match protocol ms-office-web-apps
 match protocol salesforce
 match protocol sap
class-map match-any AutoQos-4.0-wlan-Bulk-Data-Class
 match protocol ftp
 match protocol ftp-data
 match protocol ftps-data
 match protocol cifs
```

```
class-map match-any AutoQos-4.0-wlan-Scavanger-Class
 match protocol netflix
 match protocol youtube
 match protocol skype
 match protocol bittorrent
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
 class AutoQos-4.0-wlan-Voip-Data-Class
  set dscp ef
 class AutoQos-4.0-wlan-Voip-Signal-Class
  set dscp cs3
 class AutoQos-4.0-wlan-Multimedia-Conf-Class
  set dscp af41
 class AutoQos-4.0-wlan-Transaction-Class
  set dscp af21
 class AutoQos-4.0-wlan-Bulk-Data-Class
  set dscp af11
 class AutoQos-4.0-wlan-Scavanger-Class
  set dscp cs1
 class class-default
  set dscp default
```

Wireless Egress Policy – Global Configuration Commands Generated

Auto QoS Mode Enterprise

Class-map definitions

```
class-map match-any AutoQos-4.0-RT1-Class
 match dscp ef
 match dscp cs6
class-map match-any AutoQos-4.0-RT2-Class
 match dscp cs4
 match dscp cs3
 match dscp af41
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-ET-SSID-Output-Policy
 class AutoQos-4.0-RT1-Class
  set dscp ef
 class AutoQos-4.0-RT2-Class
  set dscp af31
 class class-default
```

Wireless Policy Profile Configuration Commands Generated

Auto QoS Mode Enterprise

Wireless policy profile definition

```
wireless profile policy default-policy-profile
 autoqos mode enterprise-avc
 description "default policy profile"
 service-policy input AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
 service-policy output AutoQos-4.0-wlan-ET-SSID-Output-Policy
 no shutdown
```

Ingress and egress service-policies applied to the wireless default-policy-profile.

Egress Port-level Queuing Policy – Commands Generated

Auto Qos Mode Enterprise

ACL definition

```
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
```

Class-map definitions

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
```

Interface definition

```
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
```

Wireless Ingress & Egress Policy Global Configuration Commands Generated

Auto Qos Mode Enterprise

Ingress policy-map definition

```
policy-map AutoQos-4.0-wlan-GT-SSID-Input-Policy
 class class-default
  set dscp default
```

All traffic set to best effort

Egress policy-map definition

```
policy-map AutoQos-4.0-wlan-GT-SSID-Output-Policy
 class class-default
  set dscp default
```

Wireless policy profile definition

```
wireless profile policy default-policy-profile
 autoqos mode guest
 description "default policy profile"
 service-policy input AutoQos-4.0-wlan-GT-SSID-Input-Policy
 service-policy output AutoQos-4.0-wlan-GT-SSID-Output-Policy
 no shutdown
```

Ingress and egress service-policies applied to the wireless default-policy-profile.

Egress Port-level Queuing Policy – Commands Generated

Auto Qos Mode Enterprise

ACL definition

```
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
```

Class-map definitions

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
```

Interface definition

```
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
```

Appendix G: Catalyst 9800 Auto QoS Configurations

Catalyst 9800 Auto QoS Configuration

Mode	BSSID Ingress	BSSID Egress	Port Egress	Radio
Voice	platinum-up	platinum	N/A	ACM on
Guest	AutoQos-4.0-wlan-GT-SSID-Input-Policy	AutoQoS-4.0-wlan-GT-SSID-Output-Policy	Auto-QoS-4.0-wlan-Port-Output-Policy	
Fastlane	N/A	N/A	N/A	Fastlane EDCA
Enterprise	AutoQoS-4.0-wlan-ET-SSID-Input-AVC-Policy	AutoQoS-4.0-wlan-ET-SSID-Output-Policy	Auto-QoS-4.0-wlan-Port-Output-Policy	

Auto QoS Mode Enterprise

Wireless Ingress Policy – Global Configuration Commands Generated

Auto Qos Mode Enterprise

Class-map definitions

```
class-map match-any AutoQos-4.0-wlan-Voip-Data-Class
 match dscp ef
class-map match-any AutoQos-4.0-wlan-Voip-Signal-Class
 match protocol skinny
 match protocol cisco-jabber-control
 match protocol sip
 match protocol sip-tls
class-map match-any AutoQos-4.0-wlan-Multimedia-Conf-Class
 match protocol cisco-phone-video
 match protocol cisco-jabber-video
 match protocol ms-lync-video
 match protocol webex-media
class-map match-any AutoQos-4.0-wlan-Transaction-Class
 match protocol cisco-jabber-im
 match protocol ms-office-web-apps
 match protocol salesforce
 match protocol sap
class-map match-any AutoQos-4.0-wlan-Bulk-Data-Class
 match protocol ftp
 match protocol ftp-data
 match protocol ftps-data
 match protocol cifs
```

```
class-map match-any AutoQos-4.0-wlan-Scavanger-Class
 match protocol netflix
 match protocol youtube
 match protocol skype
 match protocol bittorrent
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
 class AutoQos-4.0-wlan-Voip-Data-Class
  set dscp ef
 class AutoQos-4.0-wlan-Voip-Signal-Class
  set dscp cs3
 class AutoQos-4.0-wlan-Multimedia-Conf-Class
  set dscp af41
 class AutoQos-4.0-wlan-Transaction-Class
  set dscp af21
 class AutoQos-4.0-wlan-Bulk-Data-Class
  set dscp af11
 class AutoQos-4.0-wlan-Scavanger-Class
  set dscp cs1
 class class-default
  set dscp default
```


Wireless Egress Policy – Global Configuration Commands Generated

Auto QoS Mode Enterprise

Class-map definitions

```
class-map match-any AutoQos-4.0-RT1-Class
 match dscp ef
 match dscp cs6
class-map match-any AutoQos-4.0-RT2-Class
 match dscp cs4
 match dscp cs3
 match dscp af41
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-ET-SSID-Output-Policy
 class AutoQos-4.0-RT1-Class
  set dscp ef
 class AutoQos-4.0-RT2-Class
  set dscp af31
 class class-default
```


Wireless Policy Profile Configuration Commands Generated

Auto QoS Mode Enterprise

Wireless policy profile definition

```
wireless profile policy default-policy-profile
 autoqos mode enterprise-avc
 description "default policy profile"
 service-policy input AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
 service-policy output AutoQos-4.0-wlan-ET-SSID-Output-Policy
 no shutdown
```

Ingress and egress service-policies applied to the wireless default-policy-profile.

Egress Port-level Queuing Policy – Commands Generated

Auto Qos Mode Enterprise

ACL definition

```
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
```

Class-map definitions

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
```

Interface definition

```
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
```

Auto QoS Mode Guest

Wireless Ingress & Egress Policy Global Configuration Commands Generated

Auto Qos Mode Enterprise

Ingress policy-map definition

```
policy-map AutoQos-4.0-wlan-GT-SSID-Input-Policy
 class class-default
  set dscp default
```

All traffic set to best effort

Egress policy-map definition

```
policy-map AutoQos-4.0-wlan-GT-SSID-Output-Policy
 class class-default
  set dscp default
```

Wireless policy profile definition

```
wireless profile policy default-policy-profile
 autoqos mode guest
 description "default policy profile"
 service-policy input AutoQos-4.0-wlan-GT-SSID-Input-Policy
 service-policy output AutoQos-4.0-wlan-GT-SSID-Output-Policy
 no shutdown
```

Ingress and egress service-policies applied to the wireless default-policy-profile.

Egress Port-level Queuing Policy – Commands Generated

Auto Qos Mode Enterprise

ACL definition

```
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
```

Class-map definitions

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
```

Interface definition

```
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
```

Policy-map definition

```
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
```


Appendix H: Catalyst 9000 Series / 3850 / 3650 Hierarchical QoS

Catalyst 9000 / 3850 / 3650

Hierarchical QoS Policies–Queuing within Shaped Rate Example

```
policy-map 50MBPS-SHAPER
 class class-default
  shape average 50000000
  service-policy 2P6Q3T
interface GigabitEthernet 1/0/1
 service-policy output 50MBPS-SHAPER
```

Defines the sub-line rate (CIR)

Provides back-pressure to the system to engage the (previously-defined) queuing policy, so that packets are properly prioritized within the sub-line rate

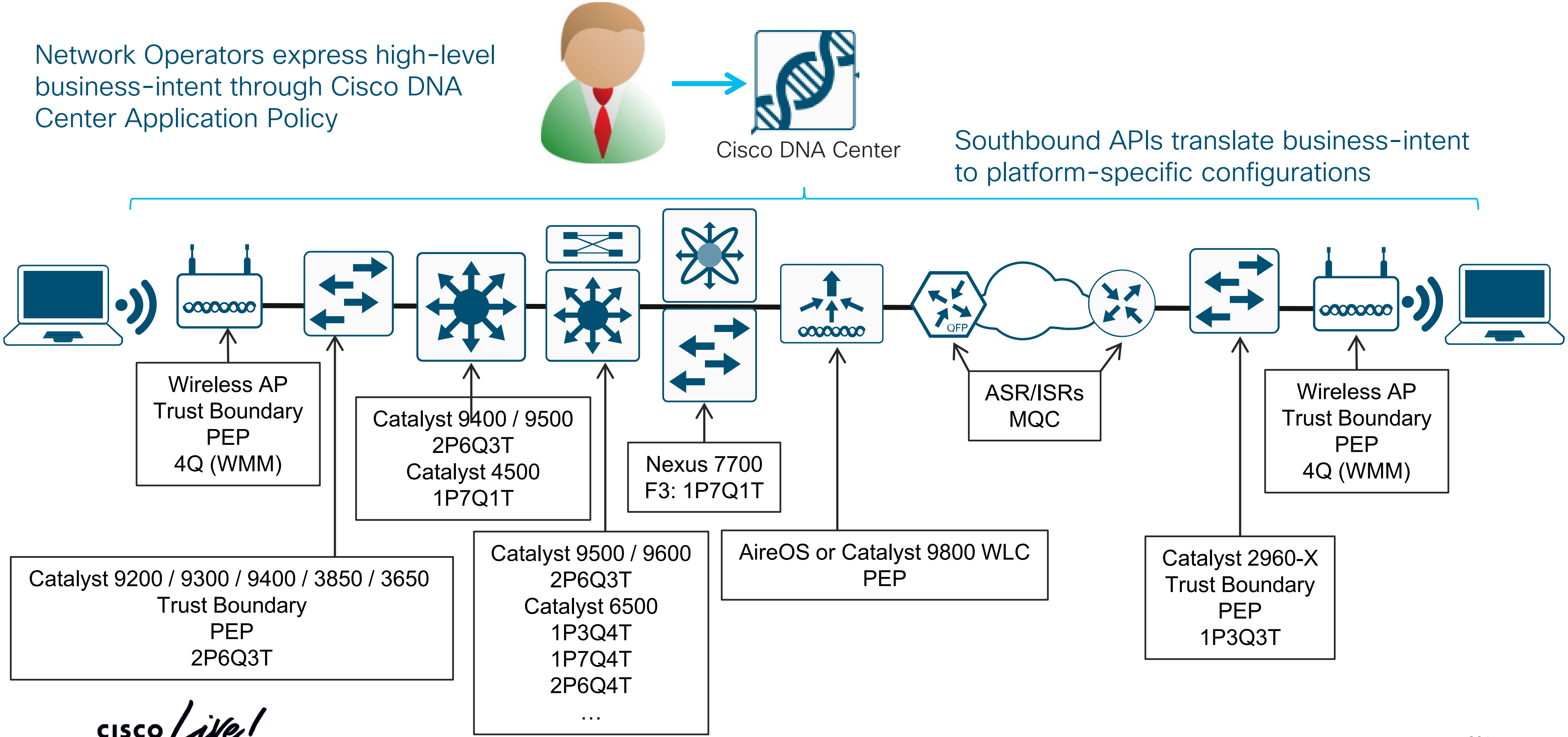
Only the Hierarchical Shaping policy is attached to the interface(s)

Appendix I: Cisco DNA Center Application Policy & Application Assurance

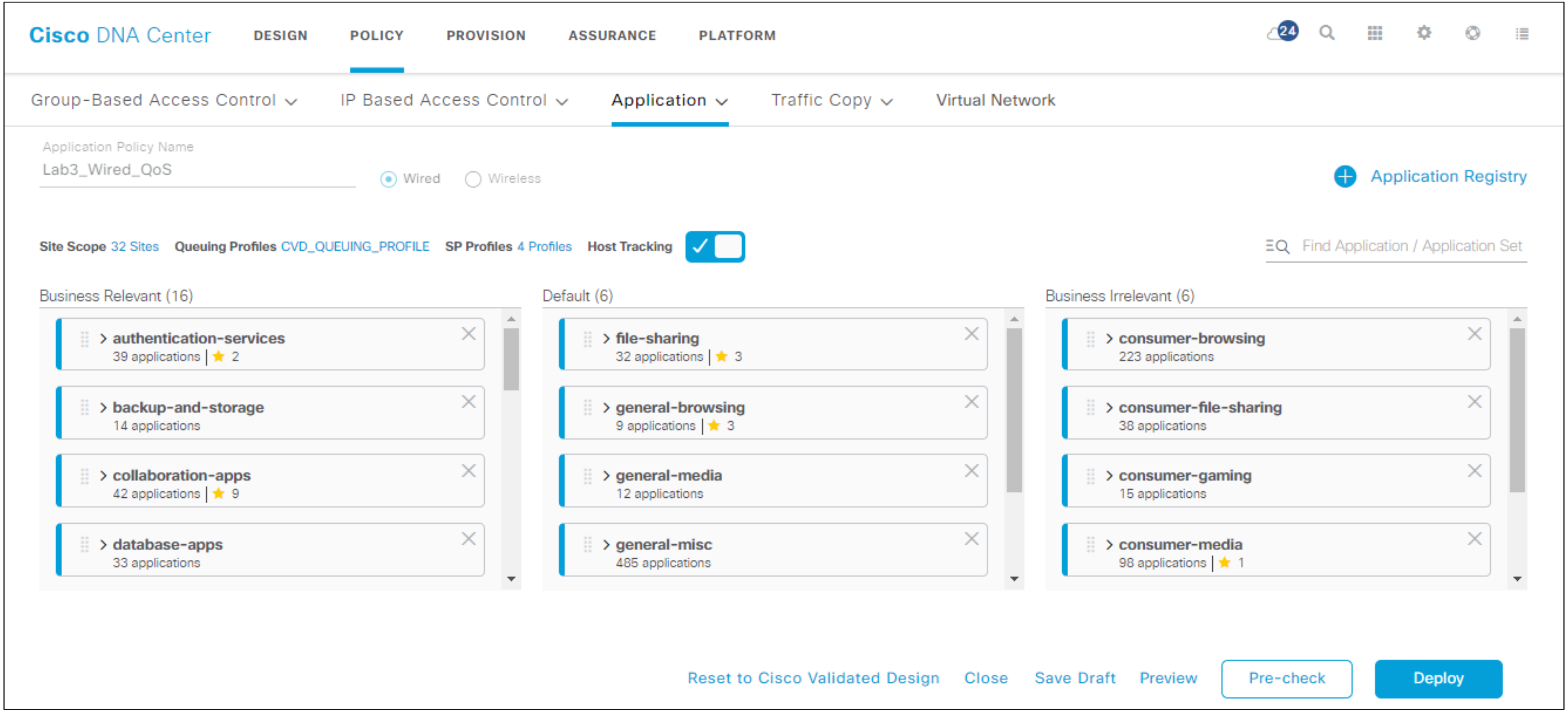
Cisco DNA Center Application Policy

Network Operators express high-level business-intent through Cisco DNA Center Application Policy

Southbound APIs translate business-intent to platform-specific configurations



Cisco DNA Center Application Policy



cisco Live!

Cisco DNA Assurance – Application Health

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Dashboards ⌄ Insights And Trends ⌄ Manage ⌄

Application Health

Dec 6, 2019 11:45 AM

24 Hours: Dec 05, 11:50 am – Dec 06, 11:53 am Actions ⌄

Application (10)

As of Dec 6, 2019 12:08 pm

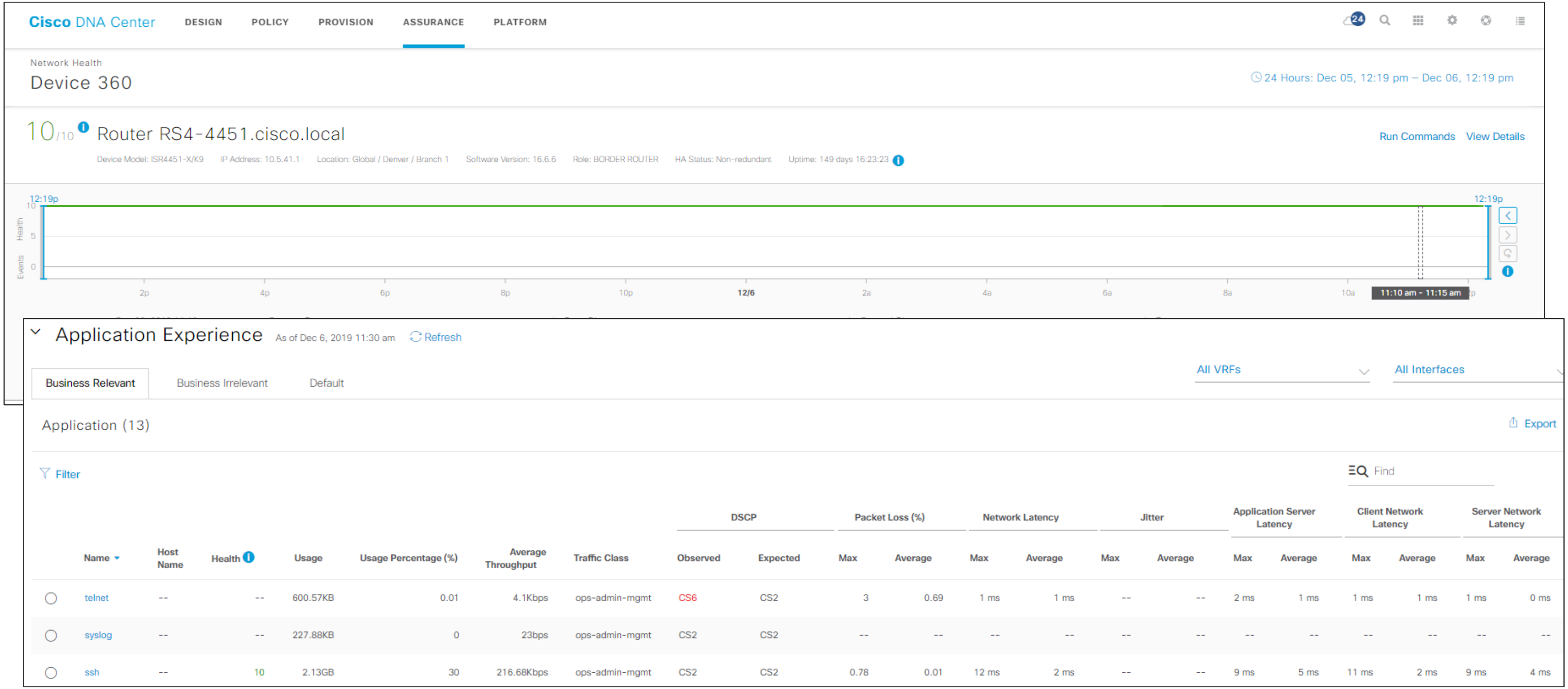
LATEST TREND

TYPE All | Business Relevant | Business Irrelevant | Default   HEALTH All | Poor | Fair | Good | Unknown

Filter   Export

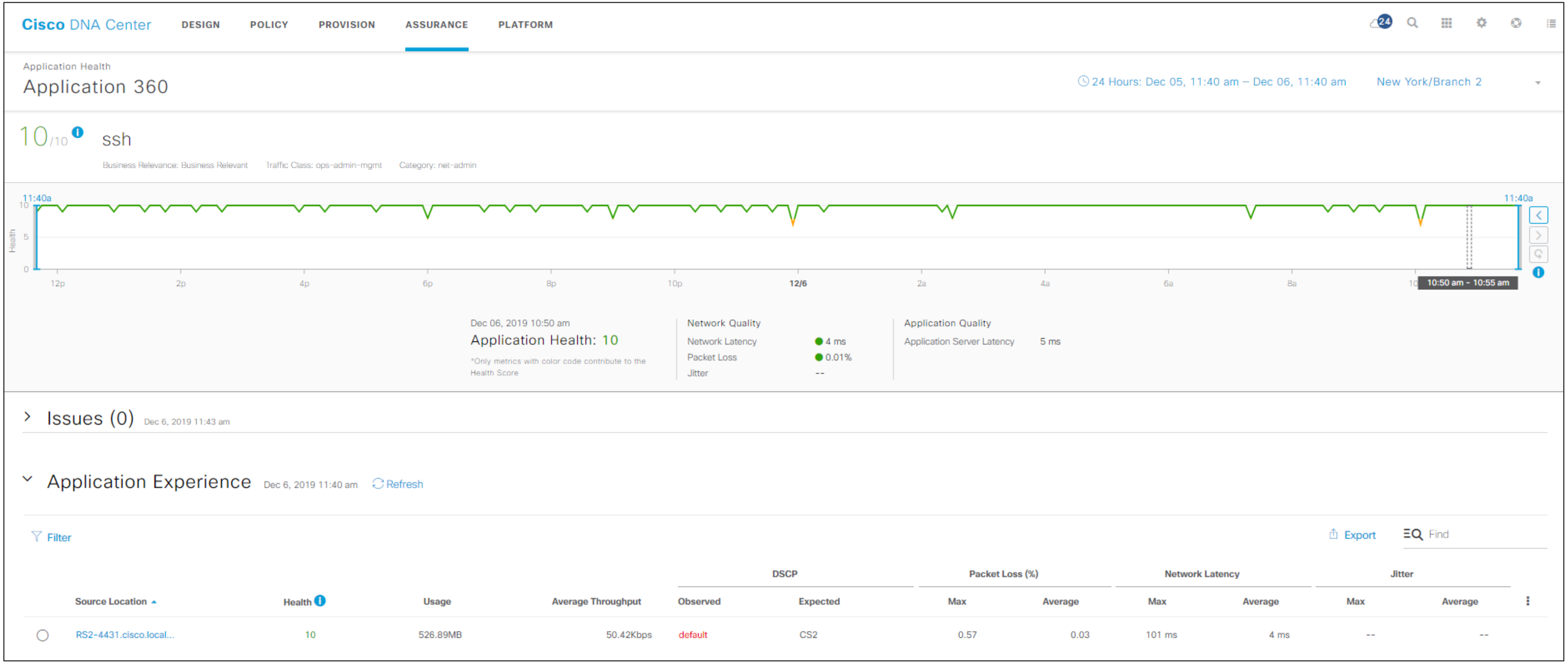
Name	Health	Business Relevance	Traffic Class	Usage	Average Throughput	Packet Loss (%)	Network Latency	Jitter	Application Server Latency	Client Network Latency	Server Network Latency
ssh	10	Business Relevant	ops-admin-mgmt	3.96MB	55.31Kbps	0	3 ms	--	6 ms	6 ms	9 ms
snmp	--	Business Relevant	ops-admin-mgmt	2.13MB	29.84Kbps	--	--	--	--	--	--
ipfix	--	Business Relevant	ops-admin-mgmt	636.34KB	8.69Kbps	--	--	--	--	--	--
radius	--	Business Relevant	ops-admin-mgmt	54.27KB	741bps	--	--	--	--	--	--
cisco-ip-sla	--	Business Relevant	multimedia-conferencing	29.22KB	399bps	--	--	--	--	--	--
telepresence-control	5	Business Relevant	signaling	17.9KB	244bps	14	1 ms	--	2 ms	1 ms	0 ms
db-service	--	Business Relevant	transactional-data	7.05KB	96bps	--	--	--	--	--	--
syslog	--	Business Relevant	ops-admin-mgmt	6.21KB	85bps	--	--	--	--	--	--

Device 360—Application Experience (ISR Router)

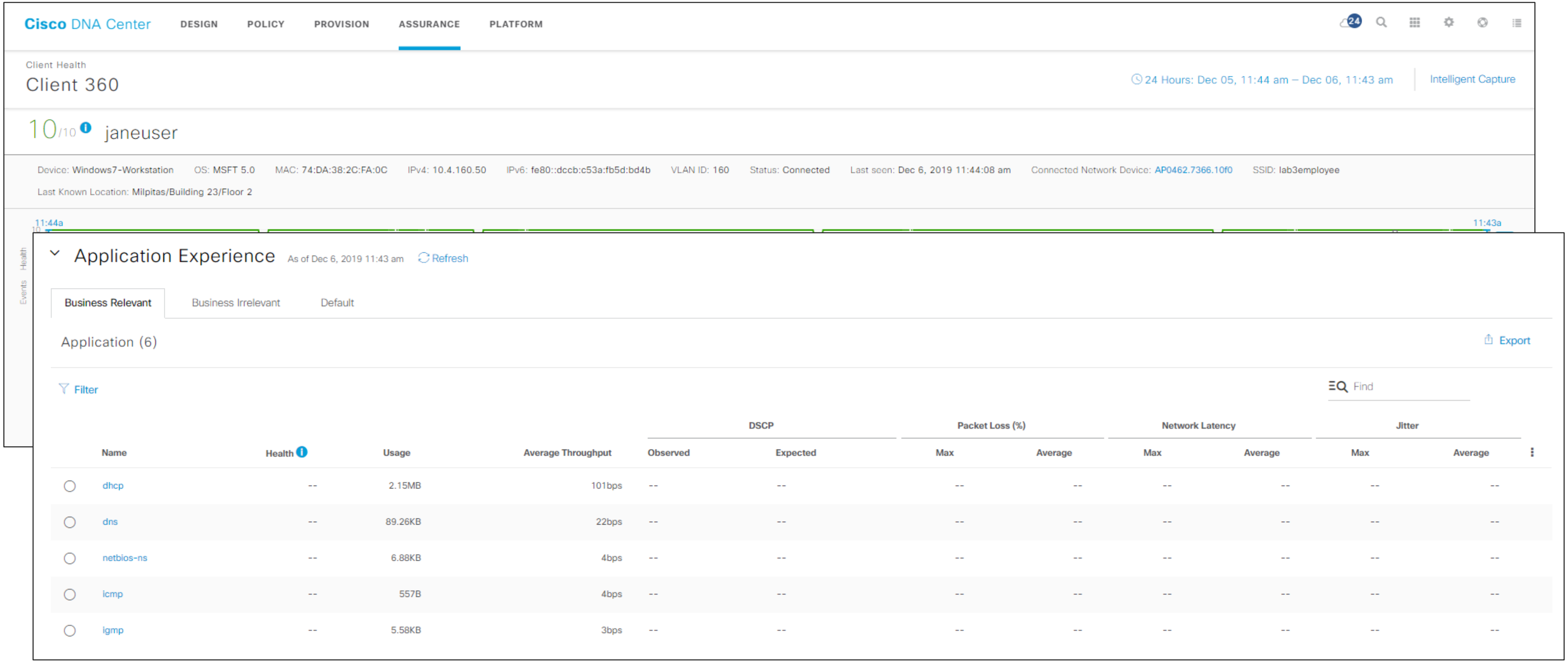


Name	Host Name	Health	Usage	Usage Percentage (%)	Average Throughput	Traffic Class	DSCP Observed	DSCP Expected	Packet Loss (%) Max	Packet Loss (%) Average	Network Latency Max	Network Latency Average	Jitter Max	Jitter Average	Application Server Latency Max	Application Server Latency Average	Client Network Latency Max	Client Network Latency Average	Server Network Latency Max	Server Network Latency Average
telnet	--	--	600.57KB	0.01	4.1Kbps	ops-admin-mgmt	CS6	CS2	3	0.69	1 ms	1 ms	--	--	2 ms	1 ms	1 ms	1 ms	1 ms	0 ms
syslog	--	--	227.88KB	0	23bps	ops-admin-mgmt	CS2	CS2	--	--	--	--	--	--	--	--	--	--	--	--
ssh	--	10	2.13GB	30	216.68Kbps	ops-admin-mgmt	CS2	CS2	0.78	0.01	12 ms	2 ms	--	--	9 ms	5 ms	11 ms	2 ms	9 ms	4 ms

Application 360—SSH



Client 360 – Application Experience



Name	Health	Usage	Average Throughput	DSCP Observed	DSCP Expected	Packet Loss (%) Max	Packet Loss (%) Average	Network Latency Max	Network Latency Average	Jitter Max	Jitter Average
dhcp	--	2.15MB	101bps	--	--	--	--	--	--	--	--
dns	--	89.26KB	22bps	--	--	--	--	--	--	--	--
netbios-ns	--	6.88KB	4bps	--	--	--	--	--	--	--	--
icmp	--	557B	4bps	--	--	--	--	--	--	--	--
igmp	--	5.58KB	3bps	--	--	--	--	--	--	--	--

Calculating Jitter and Loss for RTP Apps

Jitter is calculated by comparing the timestamps of RTP packets with subsequent sequence numbers

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|V=2|P|X|  CC   |M|     PT      |       sequence number         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           timestamp                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           synchronization source (SSRC) identifier            |
+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
|            contributing source (CSRC) identifiers             |
|                             ....                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

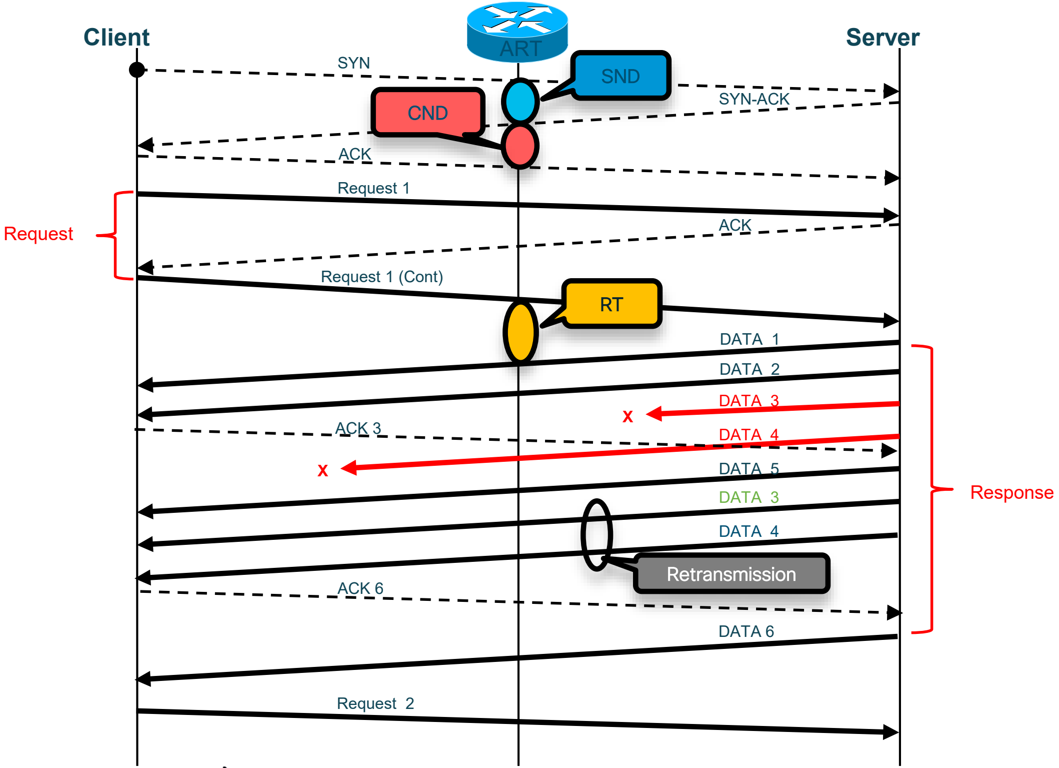
Gaps in subsequent RTP packet sequence numbers identifies lost packets

RTP Header Format

https://tools.ietf.org/html/rfc3550#section-5.1

Calculating Latency and Loss for TCP Apps

Application Response Time (ART)



SND = Server Network Delay

CND = Client Network Delay

Network Delay (ND)	ND = (CND + SND) /2
Response Time (RT)	t(First response pkt) – t(Last request pkt)
Application Delay (AD)	AD = RT – SND
Packet Loss	Loss ≈ Retransmissions (95%+ accuracy)

Complete your online session survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on ciscolive.com/emea.

Cisco Live sessions will be available for viewing on demand after the event at ciscolive.com.

Continue your education

Demos in the Cisco Showcase

Walk-In Labs

Meet the Engineer 1:1 meetings

Related sessions

Thank you

You make **possible**