

---

# EasyQoS 1.6 Documentation

*Release latest*

Feb 21, 2018



---

## Table of Contents

---

<b>1</b>	<b>APIC-EM Release 1.6, December, 2017</b>	<b>1</b>
1.1	Chapter 1: Solution Overview . . . . .	2
1.2	Chapter 2: Strategic QoS Policy . . . . .	5
1.3	Chapter 3: Tactical QoS Policy . . . . .	10
1.4	Chapter 4: APIC-EM and the EasyQoS Application . . . . .	13
1.5	Chapter 5: EasyQoS Monitoring (Beta) . . . . .	52
1.6	Chapter 6: WAN and Branch Static QoS Design . . . . .	58
1.7	Chapter 7: Service Provider Managed-Service WAN QoS Design . . . . .	86
1.8	Chapter 8: Campus LAN Static QoS Design . . . . .	114
1.9	Chapter 9: Catalyst and Nexus Switch Platform Queuing Design . . . . .	131
1.10	Chapter 10: WLAN QoS Design . . . . .	252
1.11	Chapter 11: Dynamic QoS Design . . . . .	266
1.12	Additional Resources . . . . .	274
1.13	Style Sheet . . . . .	275



# CHAPTER 1

---

APIC-EM Release 1.6, December, 2017

---



## 1.1 Chapter 1: Solution Overview

### 1.1.1 Customer Challenges

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

---

**Note:** The clients's actual public key length is not collected. Stealhwatcg displays the key reported by the ciphdr suite.

---

Virtually all businesses are looking to increase the productivity of their employees through the effective and innovative use of collaborative applications, regardless of the hardware-platforms these applications run on (PCs, laptops, tablets, smartphones, etc.), the physical or geographical location of the collaborating employees, or the types of media they wish to share on-demand. However, enabling and providing seamless Quality of Experience (QoE) around such services has traditionally placed challenging demands on network operators, to the point where the foremost barrier to enabling QoS/QoE for collaborative applications is the not technical abilities of the infrastructure. Instead, it is the intrinsic complexity of enabling these features across disparate devices in a comprehensive, yet cohesive, manner.

In order for QoS to be effective, it needs to be deployed end-to-end, the same way a chain needs to be deployed end-to-end between a source and a target in order to have utility. Every link in the chain must have a cohesive, compatible QoS policy in order to achieve an end-to-end service level. However, it is the platform-by-platform variations in customizing, optimizing, and tuning that present the biggest barrier to QoS/QoE deployments.

Enter the network controller. The network controller helps by simplifying and abstracting platform-specific complexity from the network operator. Specifically, the network controller is programmed with all the link-specific information and Cisco best-practice knowledge so as to construct optimal end-to-end QoS "chains." An operator does not need to know the hardware or software queuing structures of the underlying infrastructure, nor do they need to know the QoS implications of interconnecting wired and wireless networks, nor do they need to know how the applications are to be recognized, despite the fact that an increasing number of these are encrypted. All the operator needs to know is which applications are important to his/her business. End-to-end provisioning is done in minutes (vs. months), leveraging industry standards and Cisco Validated Designs (CVDs).

### 1.1.2 Solution Description

Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) is Cisco's enterprise Software-Defined Networking (SDN) controller. APIC-EM provides the automation functionality within Cisco's new enterprise architecture, called the *Digital Network Architecture (DNA)*. A high level overview of the architecture is shown in the following figure.

1. High-Level Overview of the Cisco Digital Network Architecture

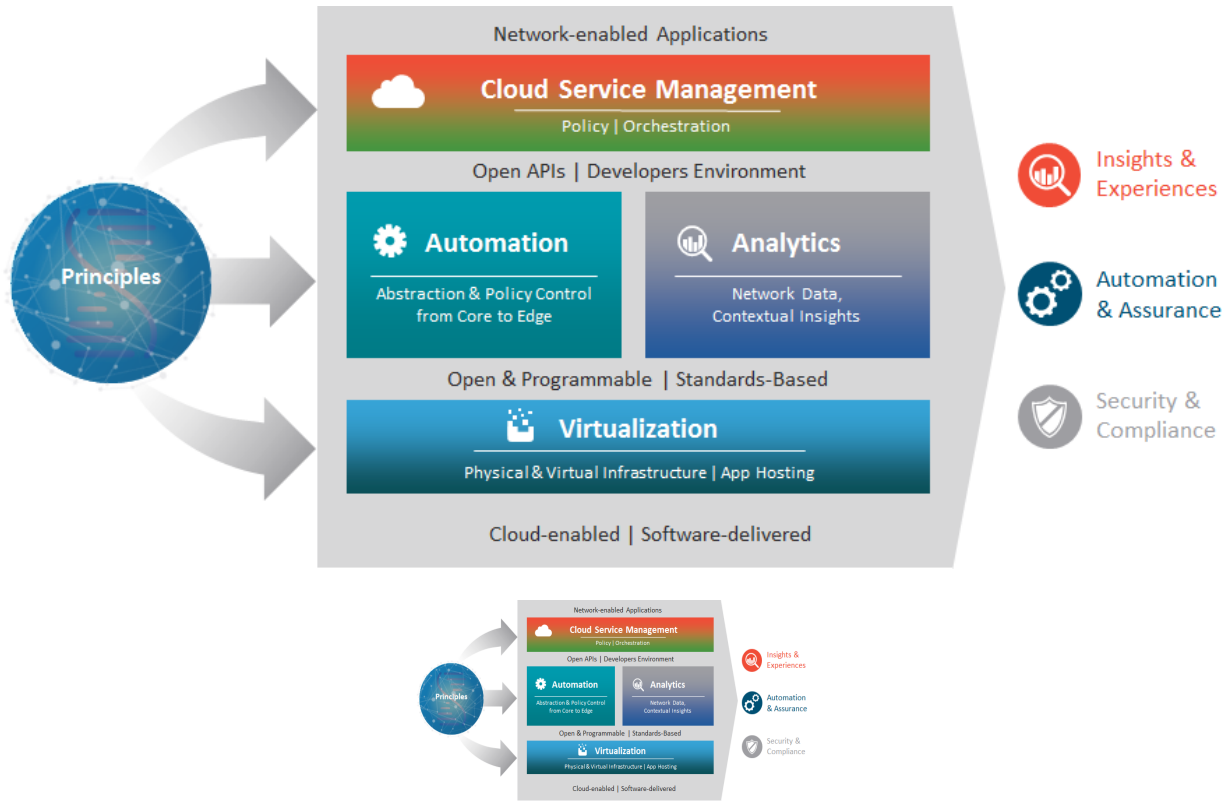


Fig. 1.1: figure are like images but with a caption

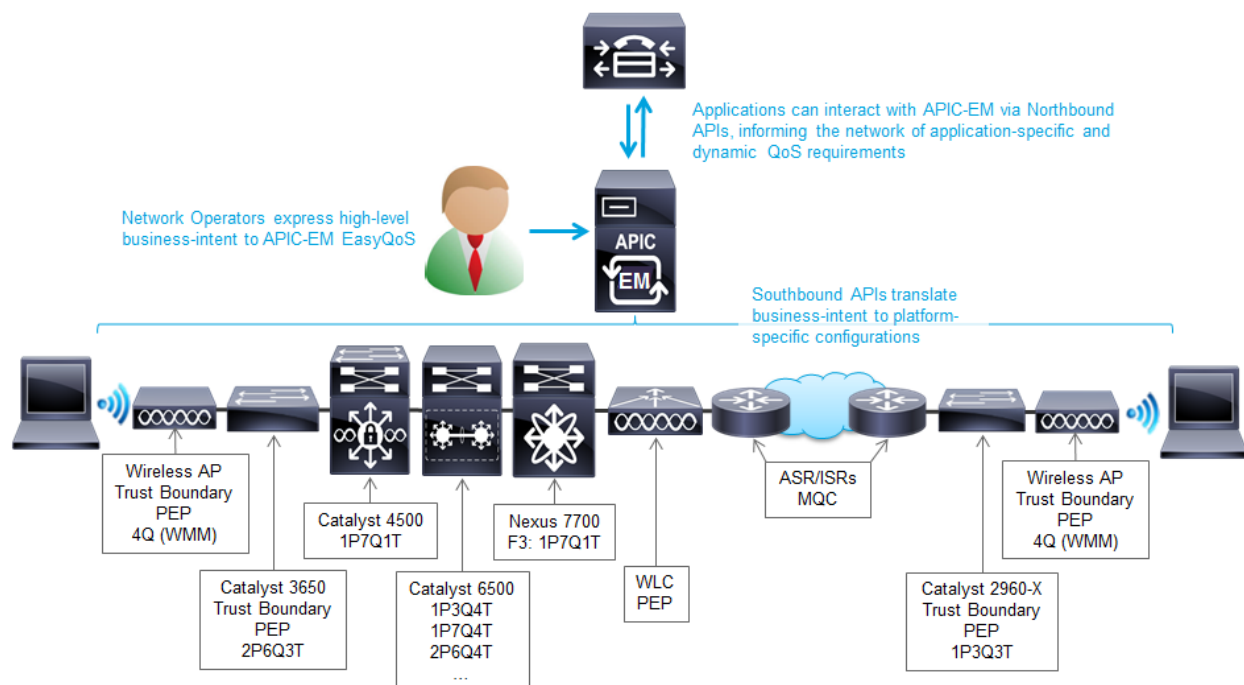
EasyQoS is an application that runs on top of APIC-EM. Hence, it is an integral part of the overall DNA architecture. The EasyQoS solution abstracts QoS policy by using a declarative model as opposed to an imperative model. A *declarative model* focuses on the intent or WHAT is to be accomplished, without describing HOW it is to be accomplished. For example, a network operator may express that an application such as Cisco Jabber is business-relevant—meaning that it is to be treated with the appropriate service—but he/she does not specify the details of how the QoS/QoE policies are to be configured in order to achieve this intent.

In contrast, an *imperative model* focuses on the execution of the intent (describing in detail HOW the objective is to be realized). For example, an imperative policy may include assigning Cisco Jabber to a hardware priority queue with a given bandwidth allocation percentage on a specific network switch interface.

Using a declarative model for policy-expression, rather than an imperative model, frees the network operator from having to spend extensive time-consuming cycles to deploy QoS policies. With a network controller, changes can be made in minutes, rather than months, resulting in agile networks that are tightly-aligned with evolving business requirements.

The following figure provides an overview of how the solution works.

#### 1. High-Level Overview of the EasyQoS Solution



In the center of the figure is the APIC-EM controller with the EasyQoS application running on top of it. Network operators express their business intent directly through a web-based graphical user interface (GUI). EasyQoS then translates this business intent into platform specific configurations that are provisioned via southbound Application Programming Interfaces (APIs) onto groups of network infrastructure devices (referred to as policy scopes), based upon the application-level business intent. This functionality is referred to as *Static QoS* within this document.

Not only can a network controller simplify QoS/QoE deployments and accelerate these like never before, but it can also deliver completely new functionality in the form of application-integration. Traditionally applications have been separate and at arms-length from the network infrastructure, often with dedicated yet distinct teams of IT personnel to administer each. However, the role of the network isn't primarily to forward packets but rather to interconnect users via applications. As such, the network controller can play a crucial new role as the broker or intermediary between applications and the network. In order to do so, it has to understand the languages of each, which it does via two main types of APIs:

- Northbound API (NB API)/Northbound Interface (NBI): this interface allows for applications to communicate with the network controller, informing it of network policy requirements in real-time. Northbound APIs are commonly deployed with Representational State Transfer (REST) models.
- Southbound API (SB API)/Southbound Interface (SBI): this interface allows for the controller to communicate to individual network devices to configure the application policy-requirements. Southbound APIs include NETCONF/YANG models, as well as more traditional methods such as command line interface (CLI) and Simple Network Management Protocol (SNMP).

Specific to the context of QoE for collaboration, the network controller can receive information from the call-manager of the collaborative application—such as Cisco Unified Communications Manager (CUCM) for Cisco Jabber or Cisco WebEx or Cisco Spark—via the Northbound APIs, in order to inform it of any voice and/or video calls that are proceeding on the network, providing it with the details of these flows. With this information, the controller can then quickly deploy QoS end-to-end across the enterprise for these voice and video calls, via the Southbound APIs. This functionality is referred to as *Dynamic QoS* within this document.

In summary the following is the business value of the EasyQoS solution:

- The EasyQoS solution provides end-to-end orchestration of QoS in the Enterprise network.

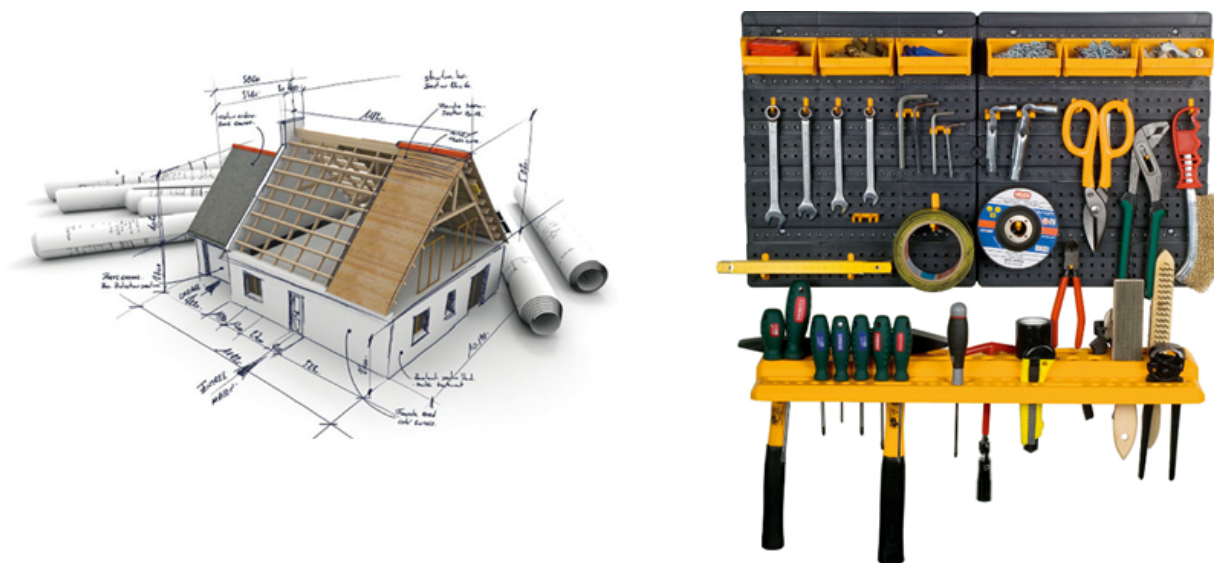


- The EasyQoS solution makes QoS policy simple and easy to deploy with an operator expressing business relevance for applications and the controller doing the rest under the hood.
- The EasyQoS solution works for both greenfield and brownfield deployments.
- The EasyQoS solution provides a declarative model that is business-intent driven, while abstracting away the platform/media/capability details.

## 1.2 Chapter 2: Strategic QoS Policy

Over the past several years there has been an evolution in how Cisco approaches the deployment of QoS within organizations—revolving around the concept of policy abstraction. Traditionally when approaching QoS, the discussion quickly turns toward the tools that are used to implement QoS within the network infrastructure. The higher level conversation regarding the overall purpose for implementing QoS—that is, what you want to build with QoS—was often skipped. The challenge is to step back and see the bigger picture of how QoS connects to the business requirement first, before jumping in with the tools, as illustrated in the figure below.

### 1. What Do You Consider First?



### 1.2.1 Where to Start?

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 or all of the following:

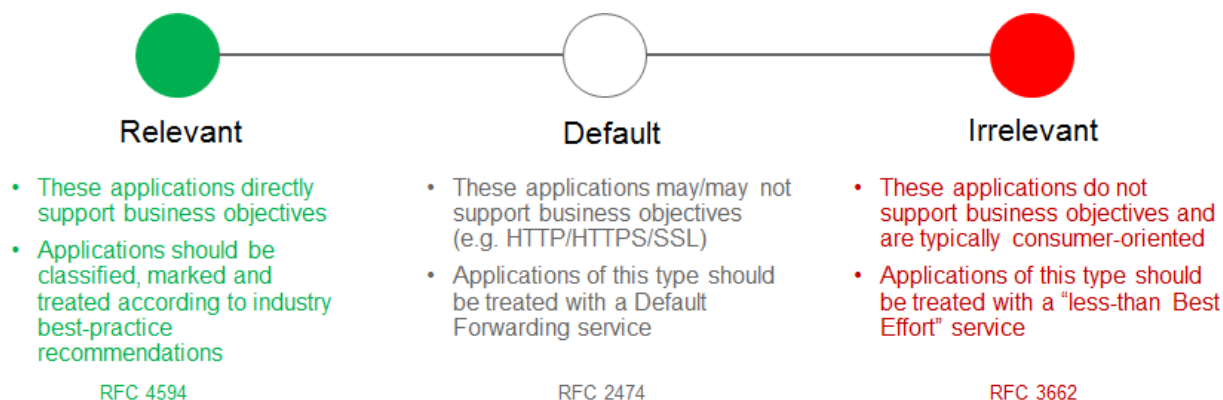
- Guaranteeing voice quality meets enterprise standards
- Ensuring a high QoE for video
- Increasing user productivity by increasing network responsiveness for interactive applications
- Managing applications that are “bandwidth hogs”
- Identifying and de-prioritizing consumer applications
- Improving network availability
- Hardening the network infrastructure

## 1.2.2 Determining Application Business-Relevancy

With these goals in mind, network architects can clearly identify which applications are relevant to their business and which are not. There are three main states of business-relevance:

- **Business-Relevant**—these applications are known to contribute to business objectives of the organization and may include voice, multimedia applications, collaborative applications, database applications, email applications, file/content transfer applications, backup applications, etc., as well as control plane, signaling, and network management protocols.
- **Default**—these applications may or may not contribute to business objectives. For example, HTTP/HTTPS at times may be used for work or for personal reasons. As such, it may not always be possible to assign a static business-relevant designation to such applications (especially not without deeper packet inspection capabilities, which are not always available on all platforms).
- **Business-Irrelevant**—these applications are known to have no contribution to business-objectives and are often personal or entertainment-oriented in nature. Such applications may include video-on-demand (for example, Netflix, Hulu, YouTube, etc.), gaming traffic, peer-to-peer file-sharing applications, personal communication apps (for example, Skype, FaceTime, etc.) and other applications.

### 1. Determining Application Business Relevance



The 1300+ applications in Cisco's Network Based Application Recognition (NBAR) library have already been pre-programmed according to their most commonly-deployed level of business-relevance. This saves an operator from having to exhaustively go down a lengthy list and configure business-relevance one application at a time. However, the operator can override the default setting for business-relevance of any given application.

## 1.2.3 Mapping Business-Relevance to QoS Treatments




### Cisco's RFC 4594-Based Strategic QoS Model

After 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 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 the following figure.

### 1. Cisco (RFC 4594-Based) QoS Recommendations

	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

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.

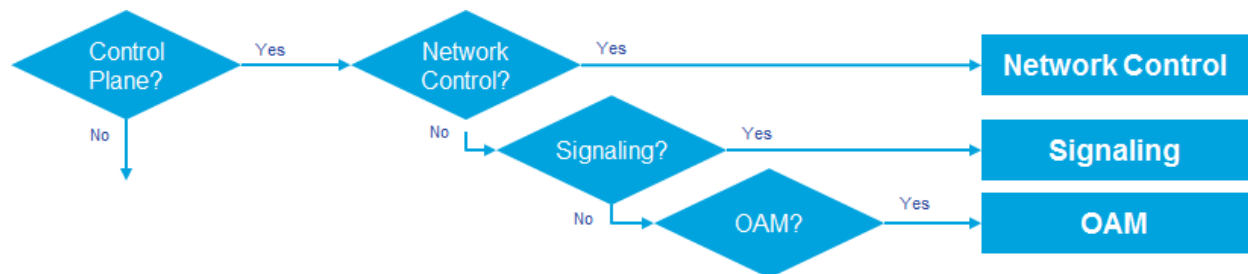
### QoS treatment for Business-Relevant Applications

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 subdivided further, as shown in the following figure.

#### 1. 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. Weighted Random Early Detection (WRED) should not be enabled on this class, because 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, because 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, because OAM traffic should not be dropped. Example traffic includes SSH, SNMP, Syslog, etc.

Provisioning for voice is relatively straightforward, as shown in the following figure.

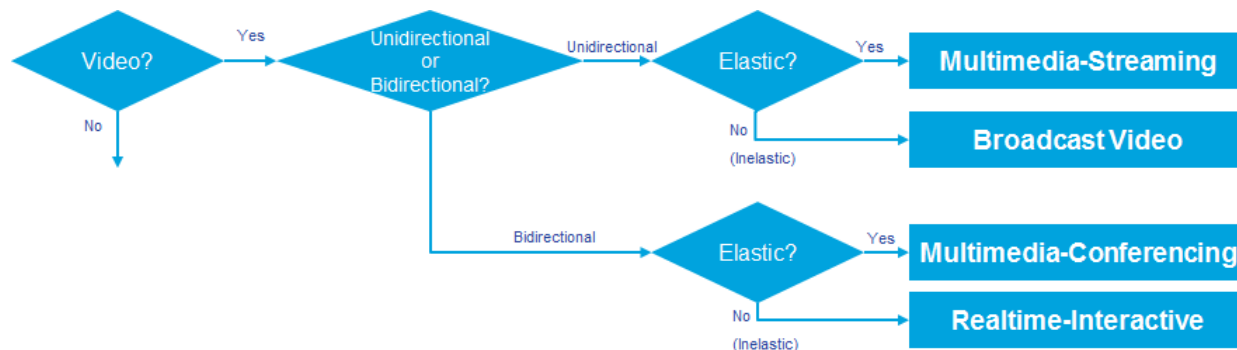
#### 1. Voice Traffic Class



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, such as Cisco Jabber, WebEx, and Spark.

Video—This traffic class may have unique QoS requirements depending on the type of video, as illustrated in the following figure.

#### 1. Video Traffic-classes



To determine the optimal traffic classification for a video application, two key questions need to be answered:

- 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 requirements—are configured not to use these.

With these two questions answered, video applications may be assigned to their respective traffic-classes, including the following.

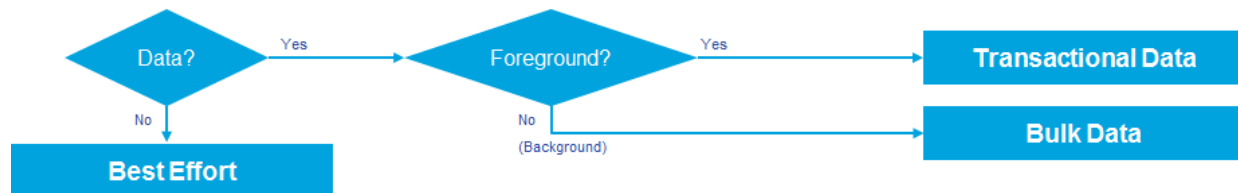
Broadcast Video—This traffic class is intended for broadcast TV, live events, video surveillance flows, and similar inelastic streaming video flows. Traffic in this class should be marked CS5 and may be provisioned with an EF PHB; as such, admission to this class should be controlled. Example traffic includes live Cisco Enterprise TV 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 subcomponents 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 Differentiated Services Code Point-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 VoD streams, ELearning videos, etc.

#### 1. Data Traffic-classes



When it comes to data applications, there is really only one key question to answer (as illustrated in the figure above): 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 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-based 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 applications, Customer Relationship Management 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-based WRED enabled. This traffic class may be subject to policing and re-marking. Example applications include: email, backup operations, FTP/SFTP transfers, video and content distribution, etc.

With all business-relevant applications assigned to their respective traffic-classes, only two types of traffic-classes are left to be provisioned—Default and Scavenger traffic-classes.

### QoS Treatment for Default-Business Relevance Applications

**Best Effort**—This traffic class is the default class. The vast majority of applications will continue to default to this Best-Effort service class. As such, the 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. It is recommended that you enable WRED on this class.

## **QoS Treatment for Business-Irrelevant Applications**

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.

Applications within the Scavenger traffic class 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, which is the first to starve should network congestion occur. Example traffic includes Netflix, YouTube, Xbox Live/360 Movies, iTunes, BitTorrent, etc.

## **1.3 Chapter 3: Tactical QoS Policy**

### **1.3.1 Translating QoS Strategy into Tactical Designs**

To meet the demands of today’s media-rich networks, administrators should articulate a QoS strategy that reflects their business intent. This strategy details which applications are business relevant and which applications are not business relevant, as well as how these applications are to be marked and treated over the IP network. Furthermore, this QoS strategy is end-to-end and is not constrained by any technical or administrative limitation.

While defining such an unconstrained QoS strategy is an important part of the deployment process, when it comes to practical deployment, various technical constraints have to be taken into account, including the following:

- Hardware constraints
- Software constraints
- Media capability constraints
- Bandwidth constraints
- Service provider constraints

Thus the goal of tactical QoS design is to adapt the QoS strategy to the maximum of each platform’s capabilities, subject to all relevant constraints.

The following are additional recommendations to keep in mind during the tactical design phase:

- Only enable QoS features if these directly contribute to expressing the QoS strategy on the given platform.
- Leverage QoS design best-practices to generate platform specific configurations that reflect the QoS strategy with maximum fidelity.

### **1.3.2 QoS Design Best Practices**

The following sections discuss generic best practices for QoS design.

#### **Hardware vs. Software QoS Design**

Some Cisco routers, such as Cisco Integrated Services Routers (ISRs), perform QoS in software, which places incremental loads on the CPU. The actual incremental load depends on the numerous factors, including: the complexity and functionality of the policy, the volume and composition of the traffic, the speed of the interface, the speed of the CPU, the memory of the router, etc. On the other hand, other devices (such as Cisco Catalyst switches) often perform QoS in dedicated hardware—Application Specific Integrated Circuits (ASICs). As such, these switches can perform even the most complex QoS policy on maximum traffic loads at line rates on GE/10GE/40GE/100GE interfaces—all without



any marginal CPU tax. Thus, whenever a choice exists, Cisco recommends implementing QoS policies in devices that perform QoS operations in hardware—rather than software—as this will result in more efficient utilization of network infrastructure resources.

For example, suppose an administrator has the option of deploying classification and marking policies in a branch network in either a Catalyst switch (in hardware) or at the LAN-edge interface of an ISR router (in software). Because a choice exists as to where the policy should be deployed, it would be more efficient to classify and mark within the Catalyst switch.

However, there may be cases where such a choice doesn't exist. Continuing the example: there may be a business need to perform deep-packet inspection on branch-originated traffic (which may not be supported on the particular Catalyst switch model deployed at the branch), and as such the administrator would then have to apply the required classification and marking policies on the ISR router.

### **Classification and Marking Best Practices**

When classifying and marking traffic, a recommended design best practice is to classify and mark applications as close to their sources as technically and administratively feasible. This principle promotes end-to-end differentiated services and PHBs.

In general, it is not recommended that you trust markings that can be set by end users on their PCs or other similar devices because end users can easily abuse provisioned QoS policies if permitted to mark their own traffic. For example, if an EF PHB has been provisioned over the network, a PC user can easily configure all their traffic to be marked to EF, thus hijacking network priority queues to service their non-real-time traffic. Such abuse could easily ruin the service quality of real-time applications throughout the enterprise. On the other hand, if enterprise controls are in place to centrally administer PC QoS markings, then it may be an acceptable design option to trust them.

Following this rule, it is further recommended that you use DSCP markings whenever possible, because these Layer 3 IP-header markings are end-to-end, more granular, and more extensible than Layer 2 markings. For example, IEEE 802.1p, IEEE 802.1le (now part of the IEEE 802.11 standard) and MPLS EXP only support three bits (values 0-7) for marking. Therefore, only up to eight classes of traffic can be supported with these marking schemes and inter-class relative priority (such as RFC 2597 Assured Forwarding drop preference markdown) is not supported. On the other hand, Layer 3 DSCP markings allow for up to 64 distinct classes of traffic.

As the line between enterprises and service providers continues to blur and the need for interoperability and complementary QoS markings is critical, you should follow standards-based DSCP PHB markings to ensure interoperability and future expansion.

### **Policing and Remarking Best Practices**

There is little reason to forward unwanted traffic only to police and drop it at a downstream node. Therefore, it is recommended that you police traffic flows as close to their sources as possible.

Whenever supported, markdown should be done according to standards-based rules, such as RFC 2597, the Assured Forwarding PHB. For example, excess traffic marked to AFx1 should be marked down to AFx2 (or AFx3 whenever dual-rate policing—such as defined in RFC 2698—is supported). Following such markdowns, congestion management policies, such as DSCP-based WRED, should be configured to drop AFx3 more aggressively than AFx2, which in turn should be dropped more aggressively than AFx1.

### **Congestion Management (Queuing) Best Practices**

Business-critical applications require service guarantees regardless of network conditions. The only way to provide service guarantees is to enable queuing at any and every node that has the potential for congestion.

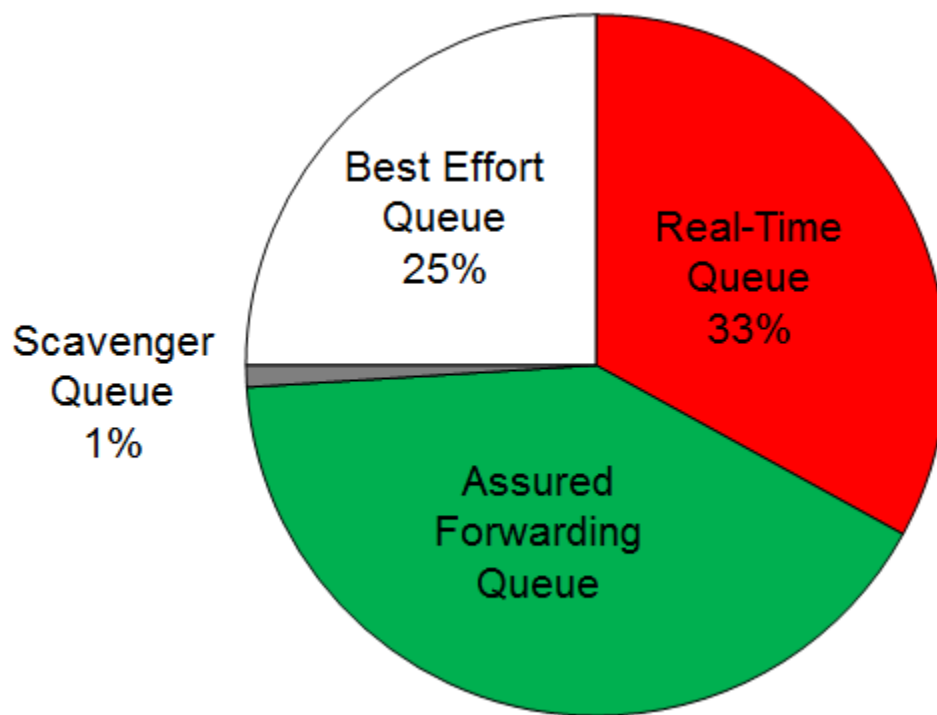
In addition, because each application class has unique service level requirements, optimally each should be assigned a dedicated queue. In such a manner, specific bandwidth allocations and dropping policies can be assigned to each discrete application class to meet its distinctive QoS requirements. Otherwise, if multiple application classes are assigned into a common queuing bucket, the administrator no longer can control if bandwidth resources are being shared among these application classes according to their individual requirements.

At a minimum, however, the following standards-based queuing behaviors should be supported:

- Real-time queue(s)—to support an RFC 3246 Expedite Forwarding service
- Guaranteed-bandwidth queue(s) —to support RFC 2597 Assured Forwarding services
- Default queue—to support an RFC 2474 Default Forwarding service
- Bandwidth—constrained queue-to support an RFC 3662 Scavenger service

Cisco offers design recommendations for each of these types of queues. These queuing best practices are illustrated in the following figure.

#### 1. Queuing Best Practices



#### Real-Time Queue

The Real-Time queue corresponds to the RFC 3246 EF PHB. The amount of bandwidth assigned to the Real-Time queue is usually variable. However, if the majority of bandwidth is provisioned with strict-priority queuing (which is effectively a first-in, first-out queue), the overall effect is a dampening of QoS functionality. Remember the goal of convergence is to enable voice, video, and data applications to transparently coexist on a single network. When real-time applications dominate a link, non-real-time applications fluctuate significantly in their response times, destroying the transparency of the converged network.

Cisco has done extensive testing and has found that a significant decrease in non-real-time application response times occurs when real-time traffic exceeds one-third of link bandwidth capacity. In fact, both testing and customer deployments have shown that a general best queuing practice is to limit the amount of strict priority queuing to 33% of link bandwidth capacity. This strict priority queuing recommendation is a conservative and safe design ratio for merging real-time applications with data applications.



Finally, WRED—or any similar congestion avoidance mechanism—should never be enabled on the strict priority queue. Traffic assigned to this queue is often highly drop sensitive; therefore, early dropping should never be induced on these flows.

#### Assured Forwarding Queue

At least one queue should be provisioned as an Assured Forwarding Queue. Per RFC 2597, up to four queues can be provisioned with this service:

- AF Class 1—AF11, AF12, AF13
- AF Class 2—AF21, AF22, AF23
- AF Class 3—AF31, AF32, AF33
- AF Class 4—AF41, AF42, AF43

These queues should have bandwidth guarantees that correspond with the application class requirements of the traffic assigned to it.

In addition, DSCP-based WRED should be enabled on these queues, such that traffic marked AFx3 is (statistically) dropped sooner and more often than AFx2, which in turn is (statistically) dropped more aggressively than AFx1.

#### Best Effort Queue

The Best Effort Queue is the default treatment for all traffic that has not been explicitly assigned to another queue. Only if an application has been selected for preferential/deferential treatment is it removed from the default class. Because most enterprises have several thousand applications running over their networks, adequate bandwidth must be provisioned for this class as a whole to handle the sheer number and volume of applications that default to it. Therefore, Cisco recommends provisioning at least 25% of link bandwidth for the default Best Effort class.

In addition, it is recommended that you enable WRED on the default class to improve throughput and reduce TCP synchronization. Because all traffic destined to this class is to be marked to the same DSCP value (of 0), there is no “weight” component to the WRED dropping decision, and therefore the congestion algorithm is effectively random early detect.

#### Less-Than-Best-Effort (Scavenger) Queue

Whenever the Scavenger Queue is enabled, it should be assigned a minimal amount of bandwidth, such as 1% (or whatever the minimal bandwidth allocation that the platform supports).

WRED is not required on the Scavenger class queue because traffic assigned to this queue has no implied “good-faith” service guarantee or expectation. Therefore, there is little to gain by adding this feature and it may even be wasteful of router CPU resources.

## 1.4 Chapter 4: APIC-EM and the EasyQoS Application

The Application Policy Infrastructure Controller—Enterprise Module (APIC-EM) is Cisco’s enterprise SDN controller. EasyQoS is one of several applications which run on APIC-EM. The following sections discuss how to access APIC-EM, declaratively express QoS policies within the EasyQoS application, and then deploy those QoS policies to groups of network infrastructure devices.

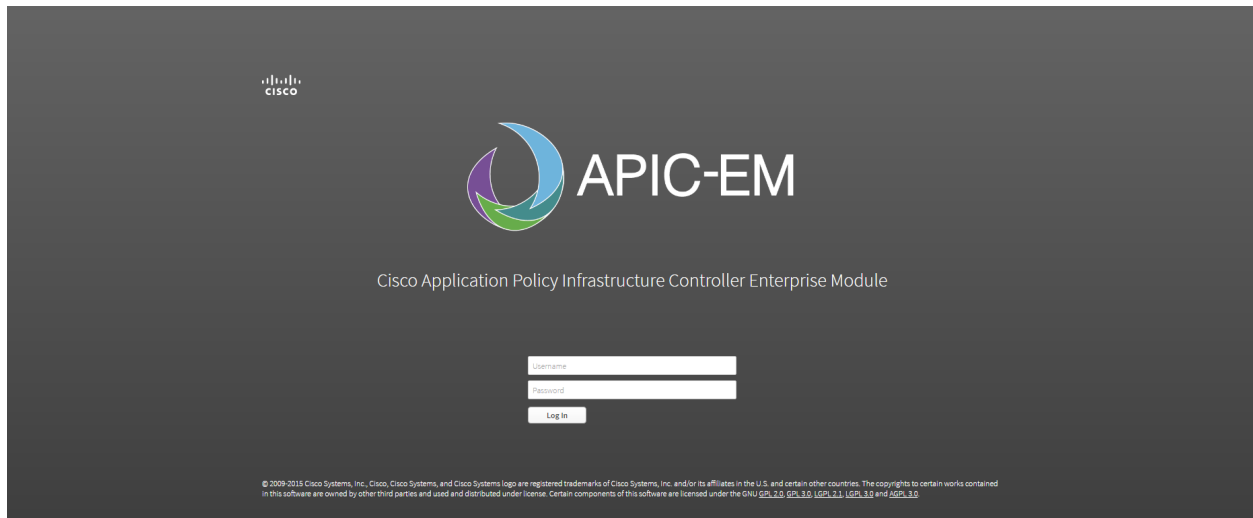
### 1.4.1 Logging Into APIC-EM

APIC-EM provides a web-based GUI for configuring and monitoring the base APIC-EM functionality as well as the applications that reside upon it.

- Note: APIC-EM also includes an extensive set of northbound REST-based APIs for configuring and monitoring APIC-EM functionality and the applications that reside upon it. This version of the APIC-EM EasyQoS Design Guide does not cover the northbound REST-based APIs. Future versions may include a discussion of the northbound APIs.

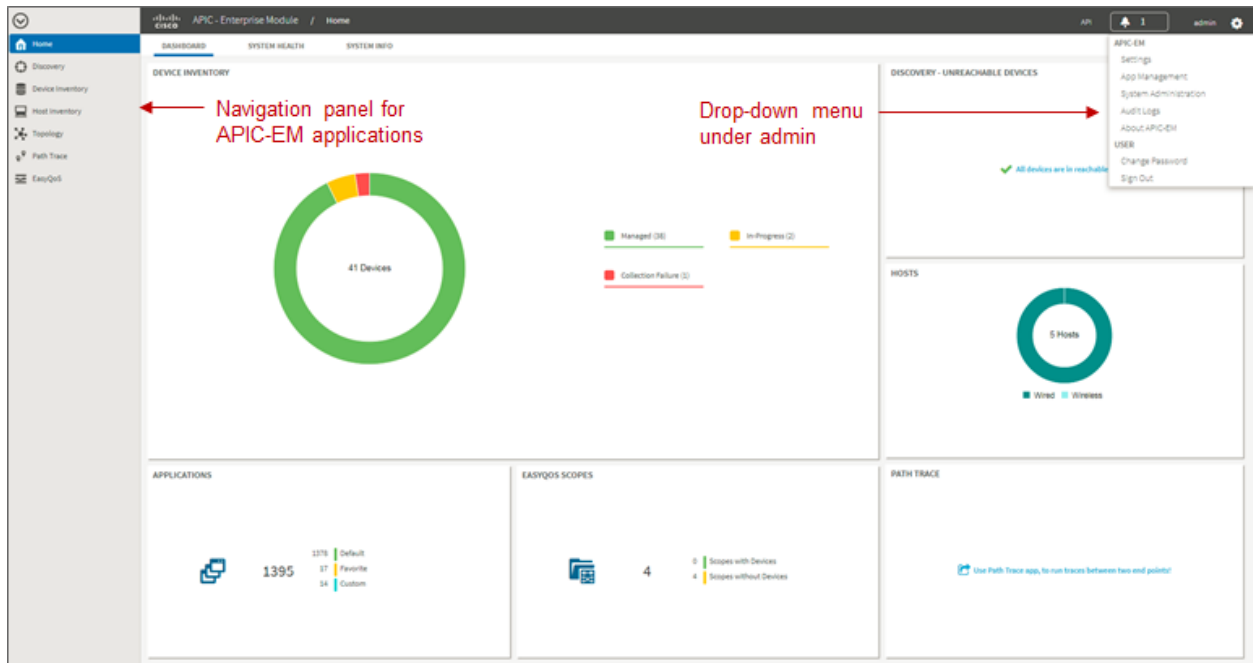
In order to access the APIC-EM login page, the network operator must launch a web browser and open an HTTPS connection to the IP address or fully qualified domain name of the APIC-EM server. An example of the login page is shown in the figure below.

### 1. APIC-EM Login Screen



Upon entering the proper login credentials (username and password) and clicking the Log In button, the network operator will be taken to the APIC-EM Home page, as shown below.

### 1. APIC-EM Home Page



APIC-EM supports both integration with an external AAA server via the RADIUS protocol, as well as an Internal Users database locally administered on the APIC-EM server. Both are accessed from Settings within the drop-down

menu that appears when clicking “admin” in the upper right-hand corner of any APIC-EM page, as shown in the figure above.

The expandable navigation panel on the left-side of any APIC-EM page displays the various applications (or functions) available within APIC-EM. The following four applications (or functions) provided by the APIC-EM controller are not part of the EasyQoS application itself but are discussed within this document, because they provide necessary functionality for the EasyQoS application to operate.

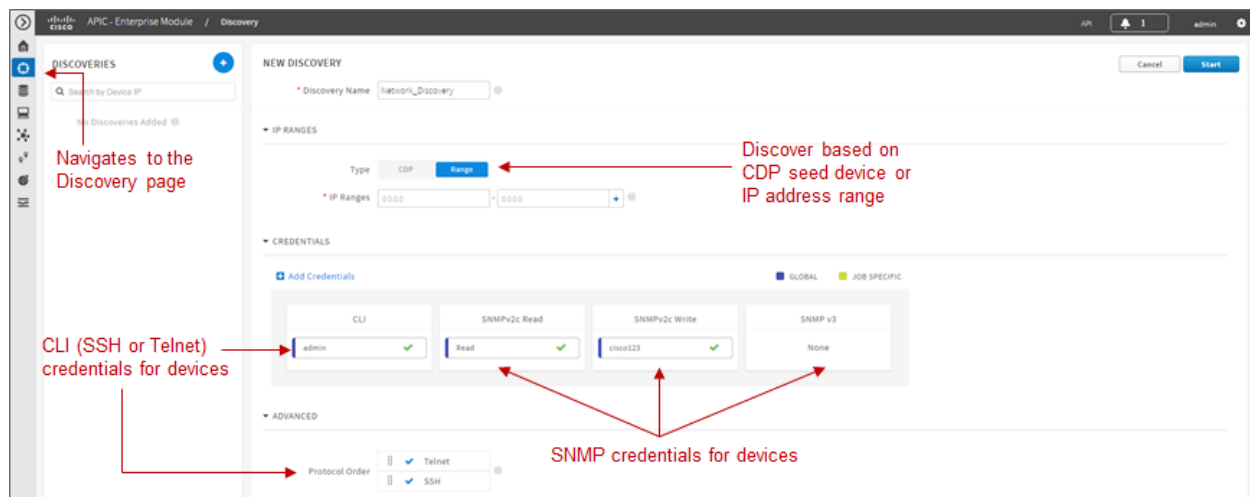
- Network Device Discovery
- Device Inventory
- Host Inventory
- Topology

This document does not discuss the IWAN, Network Plug and Play, Integrity Verification, Remote Troubleshooter, Cisco Active Advisor, or Cisco Wide Area Bonjour applications, because they do not directly provide functionality that is required for the EasyQoS application. The Path Trace application is briefly mentioned at the end of the **\*APIC-EM and the EasyQoS Application\*** chapter.

## 1.4.2 Network Device Discovery

In order to apply QoS Policies to network devices within the EasyQoS application, network devices must first be discovered, added to the APIC-EM device inventory, and managed by APIC-EM. Hence, the network operator must first perform a Discovery in order to discover network devices and place them into the Device Inventory database. Clicking the Discovery icon with the expandable panel on left-side of any APIC-EM page takes the network operator to the Discovery page. An example is shown in the following figure.

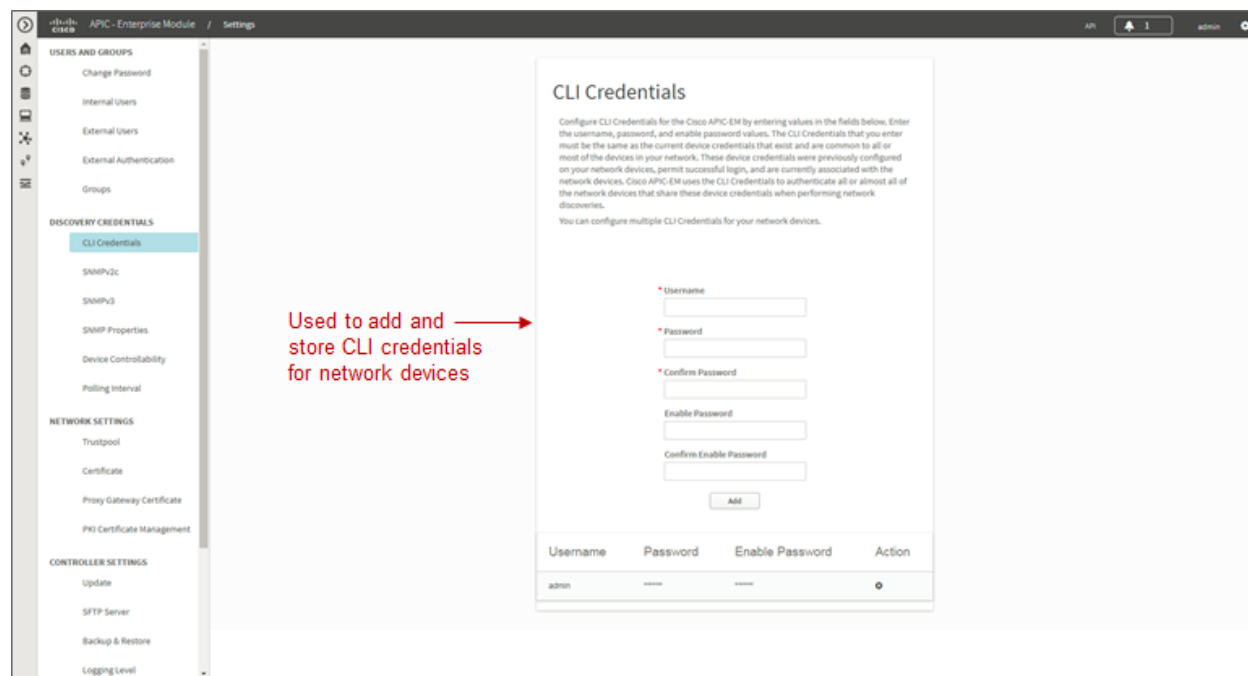
### 1. APIC-EM Discovery Page



The Discovery page allows the network operator to create Discovery jobs based on either a Cisco Discovery Protocol (CDP) seed device or an IP address range. The Discovery process requires SNMP credentials (v2c, or v3) and CLI credentials (SSH or Telnet) to be entered. The network operator must ensure that CLI credentials—including an enable password—have been previously configured on the network device and that the device is network reachable from APIC-EM.

SNMP and CLI credentials for devices can be created and stored via Settings within the drop-down menu that appears when clicking “admin” in the upper right-hand corner of any APIC-EM page. The following screen shot shows an example of where the CLI credentials are configured within APIC-EM.

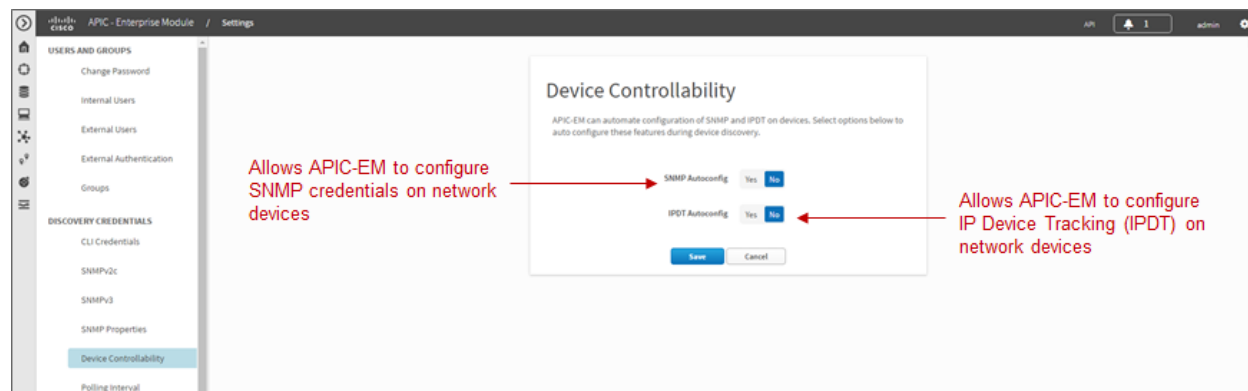
### 1. Adding CLI Credentials to APIC-EM



SNMP credentials can be added similarly. The saved credentials can then be referenced within the Discovery process.

APIC-EM release 1.3 added a Device Controllability feature. This feature allowed APIC-EM to configure the SNMP credentials onto network infrastructure devices—via the CLI interface. APIC-EM release 1.4 extended the Device Controllability feature by allowing APIC-EM to selectively configure both SNMP credentials and/or IP Device Tracking (IPDT) onto network infrastructure devices—via the CLI interface. Both of these functions can save time by not requiring the network operator to manually access each network infrastructure device and configure the SNMP credentials or IPDT. The following figure shows the screen that appears when selecting Device Controllability.

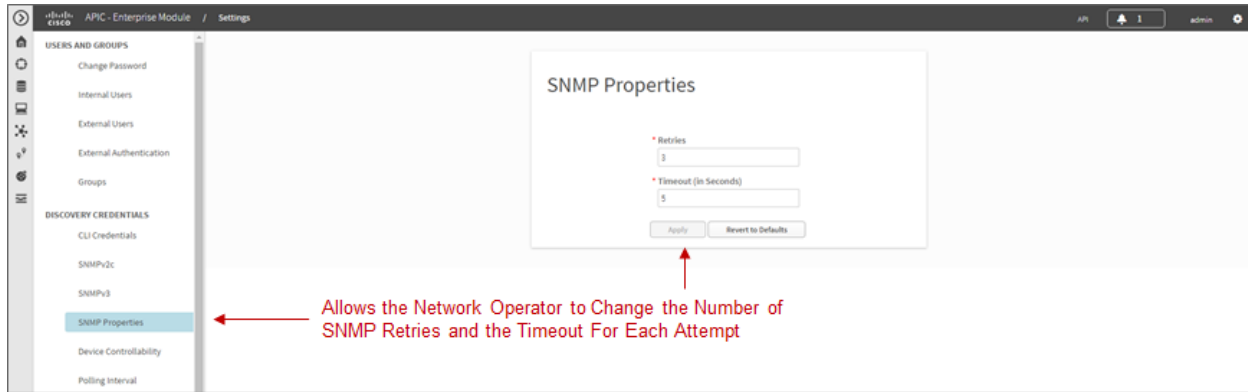
### 1. Device Controllability Feature



If the SNMP Autoconfig functionality within the Device Controllability feature is disabled (which is the default setting), the network operator must ensure that SNMP access is configured on each network device and that each device is SNMP reachable from APIC-EM.

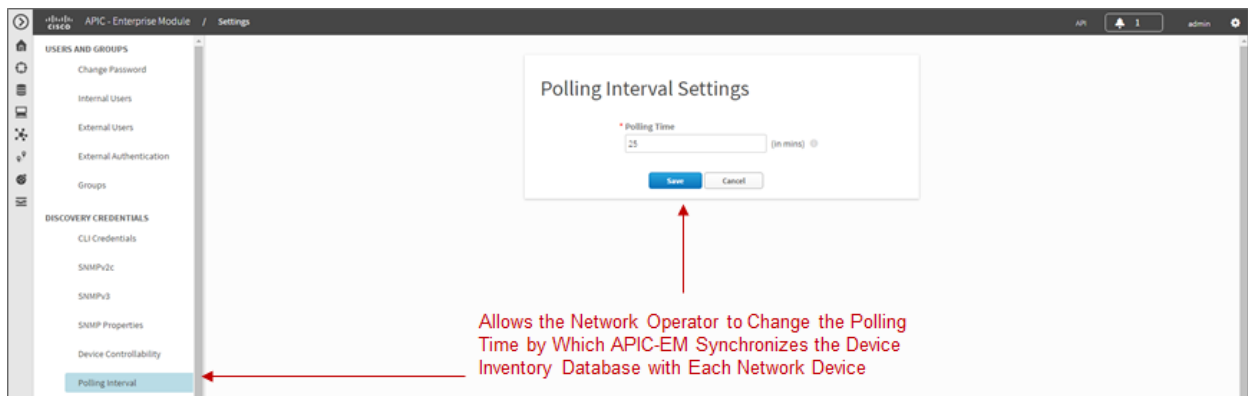
The SNMP Properties page can be used to modify the number of SNMP retries and the timeout between each attempt. The network operator may find it useful to modify the default settings if some network devices occasionally experience SNMP timeouts when APIC-EM attempts to synchronize its Device Inventory database with those devices. An example of the SNMP Properties page is shown below.

### 1. SNMP Properties



APIC-EM release 1.4 and higher allows the polling interval by which APIC-EM synchronizes the Device Inventory database with each network device to be configurable via the Polling Interval Settings page. An example is shown in the figure below.

### 1. Polling Interval



The default setting of 25 minutes is also the minimum polling interval. The polling interval can be extended up once every 24 hours if desired.

## 1.4.3 Device Inventory

Only after network devices have been discovered will those devices be added to the APIC-EM Device Inventory database and managed by APIC-EM. Clicking the Device Inventory icon within the expandable panel on left-side of any APIC-EM page takes the network operator to the Device Inventory page. An example is shown in the following figure.

### 1. APIC-EM Device Inventory Page

Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
AC1-2950-1.cisco.local	10.4.15.6	Reachable	65 days, 19:25:08.08	22 minutes ago	00:25:00	Managed
AC1-2950.cisco.local	10.4.15.7	Reachable	66 days, 0:14:05.53	13 minutes ago	00:25:00	Managed
AC1-2950-1.cisco.local	10.4.15.5	Reachable	66 days, 0:28:31.24	13 minutes ago	00:25:00	Managed
AC1-2950-2.cisco.local	10.4.15.6	Reachable	90 days, 14:13:34.45	21 minutes ago	00:25:00	Managed
AC2-2950.cisco.local	10.4.79.7	Reachable	110 days, 14:50:59.62	19 minutes ago	00:25:00	Managed
AC2-2950.cisco.local	10.4.79.8	Reachable	96 days, 17:28:53.20	22 minutes ago	00:25:00	Managed
AC2-3750.cisco.local	10.4.79.6	Reachable	16 days, 23:00:01.66	15 minutes ago	00:25:00	Managed
AC2-4503.cisco.local	10.4.79.5	Reachable	64 days, 16:15:55.13	6 minutes ago	00:25:00	Managed
AC3-2950.cisco.local	10.4.95.5	Reachable	98 days, 17:51:36.49	21 minutes ago	00:25:00	Managed
AP2100-0398	10.4.0.28	Reachable	N/A	22 minutes ago	N/A	Managed
AP2100-106	10.4.0.21	Reachable	N/A	22 minutes ago	N/A	Managed
AP2800-6454	10.4.0.20	Reachable	N/A	22 minutes ago	N/A	Managed
C3850-1	10.5.20.5	Reachable	65 days, 1:54:56.40	24 minutes ago	00:25:00	Managed
CC-6807-59.cisco.local	10.4.40.49	Reachable	110 days, 14:43:14.50	24 minutes ago	00:25:00	Managed
Cisco_3a532f	10.4.174.24	Reachable	5 days, 17:02:46.00	3 minutes ago	00:25:00	Managed
D1-6840.cisco.local	10.4.40.10	Reachable	110 days, 14:43:36.44	23 minutes ago	00:25:00	Managed
D2-4000-6	10.4.40.66	Reachable	110 days, 14:50:03.80	21 minutes ago	00:25:00	Managed
D3-3850.cisco.local	10.4.40.18	Reachable	100 days, 18:43:18.60	14 minutes ago	00:25:00	Managed
D3-7004-1	10.4.48.1	Reachable	110 days, 14:59:20.45	18 minutes ago	00:25:00	Managed

As mentioned previously, devices must be in a Managed state in order to provision EasyQoS policy. APIC-EM periodically (approximately every 25 minutes by default) synchronizes the Device Inventory database with each network device. However, the polling interval can be modified, as discussed in the **\*Network Device Discovery\*** section. If changes to the configuration of a particular network device have been made either via CLI or via management platforms such as Prime Infrastructure, it is recommended that you wait until APIC-EM has re-synchronized with the device, in order to ensure the configuration changes have been identified by APIC-EM, before applying any changes to QoS policy through EasyQoS. Alternatively, you can manually synchronize an individual device by selecting it within the device inventory and clicking the Resync button within the menu that appears. An example is shown in the figure below.

### 1. Manual Resync of a Network Device

Click the Resync button in order to manually sync the device to the APIC-EM Device Inventory

Device Name	IP Address	Reachability Status	Up Time	Last Updated Time	Poller Time	Last Inventory Collection Status
SS-5520	10.4.174.22	Reachable	122 days, 17:52:02.73	8 minutes ago	00:25:00	Managed
SS-5520-2	10.4.174.21	Reachable	102 days, 20:05:13.59	8 minutes ago	00:25:00	Managed
SS-6504	10.4.40.90	Reachable	122 days, 17:55:46.34	10 minutes ago	00:25:00	Managed
SS-6540	10.4.174.20	Reachable	122 days, 17:48:54.34	8 minutes ago	00:25:00	Managed
WE-6800-59.cisco.local	10.4.40.42	Reachable	122 days, 17:40:05.40	18 minutes ago	00:25:00	Managed
WE-ASR1002X-1	10.4.32.241	Reachable	109 days, 3:10:22.90	a few seconds ago	00:25:00	Managed
WE-ASR1002X-3.cisco.local	10.4.32.10	Reachable	1 day, 6:00:26.99	20 minutes ago	00:25:00	Managed

37 Devices

Check the box next to the device in order to bring up the menu at the top of the screen

The manual resync feature, which is available as of APIC-EM release 1.4 and higher, allows the network operator to set a longer polling interval if desired – yet still re-sync individual devices when necessary. A longer polling interval may ease the amount of processing and therefore lower CPU utilization of APIC-EM for larger deployments, especially when changes to network infrastructure devices occur infrequently.

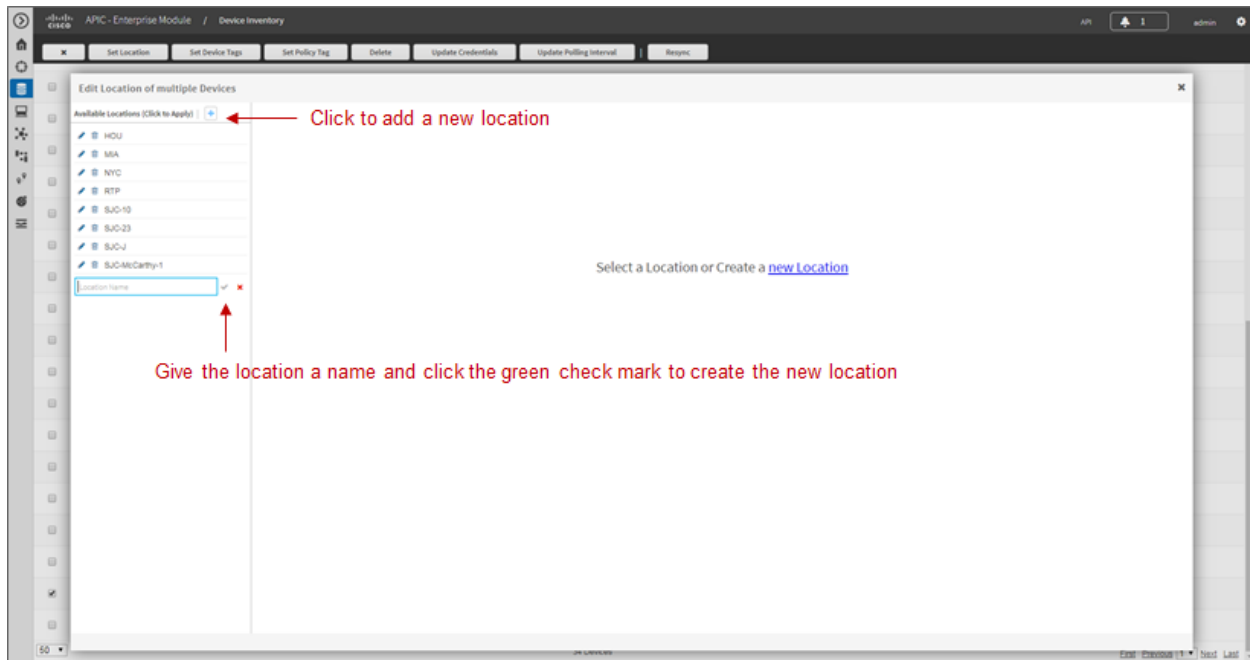
An example of why a device would need to be resynchronized would be adding or changing a WAN service provider profile (SPP) tag manually via the CLI to a Cisco ISR or ASR WAN interface. APIC-EM would have to resync with

the ISR or ASR in order to be aware of the updated WAN SPP tag first, in order to apply the appropriate QoS policy to the WAN interface.

The location feature allows the network operator to assign a geographic location to a device or set of devices. This affects how the network is viewed within the Topology page. For small networks, displaying all devices in the network within a single Topology page may be acceptable. However, as the number of devices grows, the network operator may wish to view devices based upon their geographic location—such as all devices per branch location, per campus location, per campus building, etc.

The network operator can assign a location to a device or group of devices by selecting the device or devices within the Device Inventory page and then clicking the Set Location button, shown in the figure above. This brings up a popup screen, as shown in the figure below.

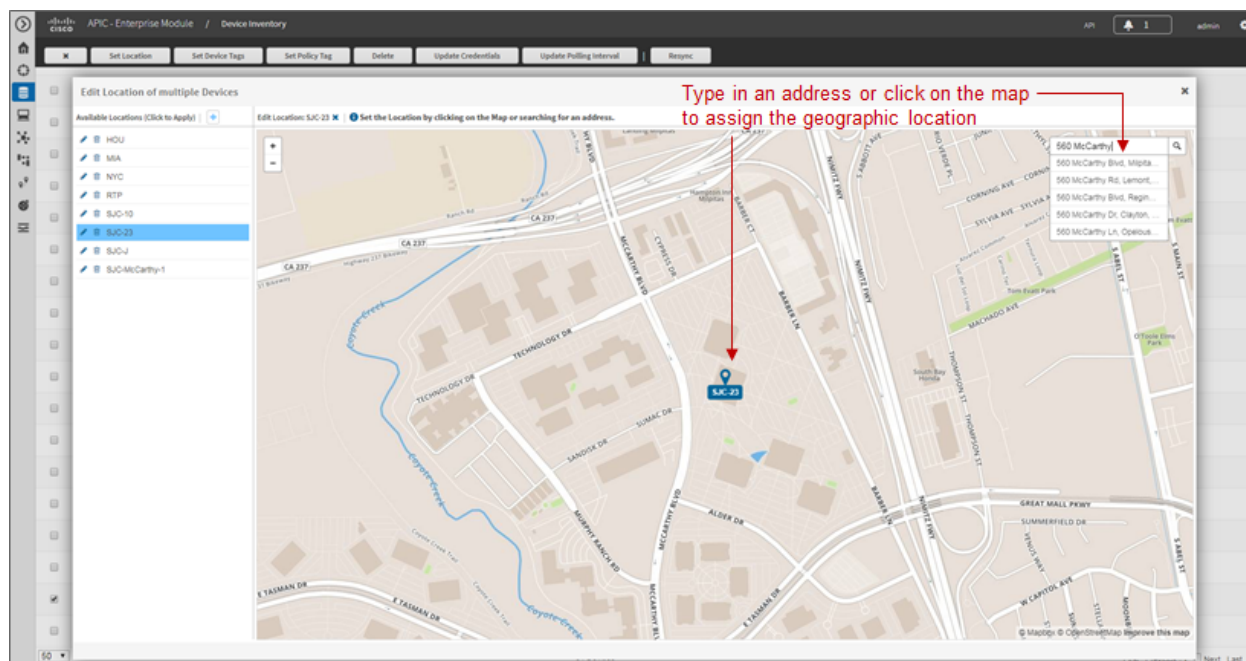
### 1. Location Popup Screen



In order to create a new location, click the blue + adjacent to Available Locations. This will bring up a new blank box field below the existing locations. The network operator must give the new location a name and click the green checkmark to create the location. Location names should not contain blank spaces. When the new location is created, a new screen will appear, prompting the network operator to either type in an address corresponding to the new location or click a geographic location within the displayed map. The network operator can zoom in to a specific geographic location within the map if necessary. An example is shown in the following figure.

### 1. Setting the Address of the New Location





## 1.4.4 Host Inventory

### Cisco Device Endpoints

APIC-EM also discovers certain Cisco hardware device endpoints which are then included within Static and Dynamic QoS policies provisioned to network infrastructure devices. These hardware endpoints include the following:

- Cisco IP phones
- Cisco TelePresence devices
- Cisco video conferencing endpoints
- Cisco video surveillance cameras

APIC-EM makes use of CDP running on Catalyst switches in order to discover these hardware endpoints. EasyQoS uses the IP addresses of the hardware endpoints collected through CDP information, along with the knowledge of which Catalyst switch and switch port the endpoint is connected to—in order to pre-populate access control entries (ACEs) within classification & marking access control lists (ACLs) for Static and Dynamic QoS on switching devices. In order for this functionality to operate, CDP must be enabled on the Catalyst switch ports that connect to hardware endpoint devices. By default CDP is enabled on Cisco Catalyst switch ports.

The Cisco hardware endpoint devices themselves must also support CDP. The CDP information provided by the hardware endpoint must also include its IP address. If the IP address is not included, APIC-EM will not know which switch port to populate with ACE entries.

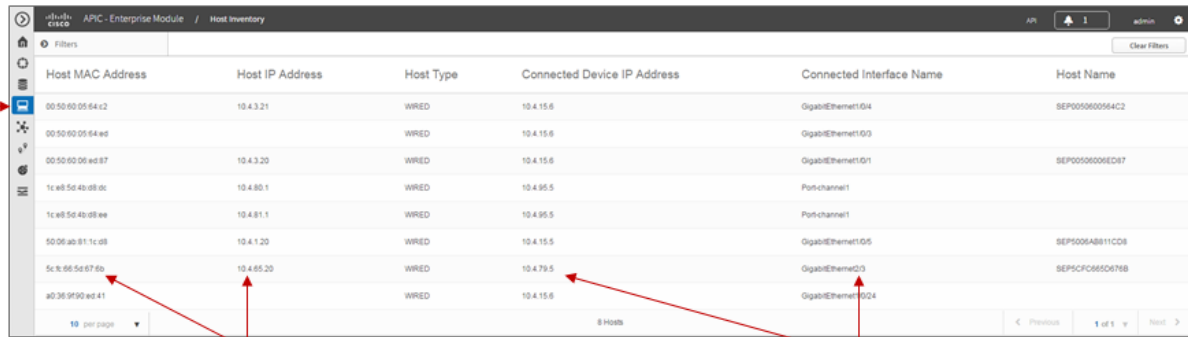
- Note: Older versions of Cisco TelePresence code may not support the sending of IP addresses within CDP when in a VLAN configuration—such as when a Voice VLAN is configured. Such systems may require an upgrade to TC7.3.6, CE8.0.2, or CE8.1.1 or higher in order for these devices to be statically populated within the correct ingress classification & marking ACLs when deploying EasyQoS. Please refer to Cisco defect CSCuy71139 for details.

Discovered Cisco endpoint devices are populated within the Host Inventory database within APIC-EM. These can be displayed by clicking the Host Inventory icon with the expandable panel on left-side of any APIC-EM page. An example of the Host Inventory page is shown in the following figure.



## 1. APIC-EM Host Inventory Page

Navigates to the  
Host Inventory page



The screenshot shows the 'Host Inventory' page in the APIC-EM interface. A red arrow points from the text 'Navigates to the Host Inventory page' to the 'Host Inventory' link in the left sidebar. Another red arrow points from the text 'Identifies the MAC and IP addresses of the device (wired device in this example)' to the first two rows of the table. A third red arrow points from the text 'Identifies the switch and switch port to which the wired device, in this example, is connected' to the 'Connected Device IP Address' and 'Connected Interface Name' columns.

Host MAC Address	Host IP Address	Host Type	Connected Device IP Address	Connected Interface Name	Host Name
00:50:00:05:64:c2	10.4.3.21	WIRED	10.4.15.6	GigabitEthernet1/0/4	SEP0050000564C2
00:50:00:05:64:e8		WIRED	10.4.15.6	GigabitEthernet1/0/3	
00:50:00:06:0d:87	10.4.3.20	WIRED	10.4.15.6	GigabitEthernet1/0/1	SEP005000060D87
1c:9d:5d:4b:08:dc	10.4.80.1	WIRED	10.4.95.5	Port-channel1	
1c:9d:5d:4b:08:ee	10.4.81.1	WIRED	10.4.95.5	Port-channel1	
00:0c:ab:81:1c:08	10.4.1.20	WIRED	10.4.15.5	GigabitEthernet1/0/5	SEP000c00ab811C08
1c:9c:98:5d:67:0a	10.4.85.20	WIRED	10.4.79.5	GigabitEthernet1/0/3	SEP1c9c985d670A
a0:36:9f:90:e0:41		WIRED	10.4.15.6	GigabitEthernet1/0/4	

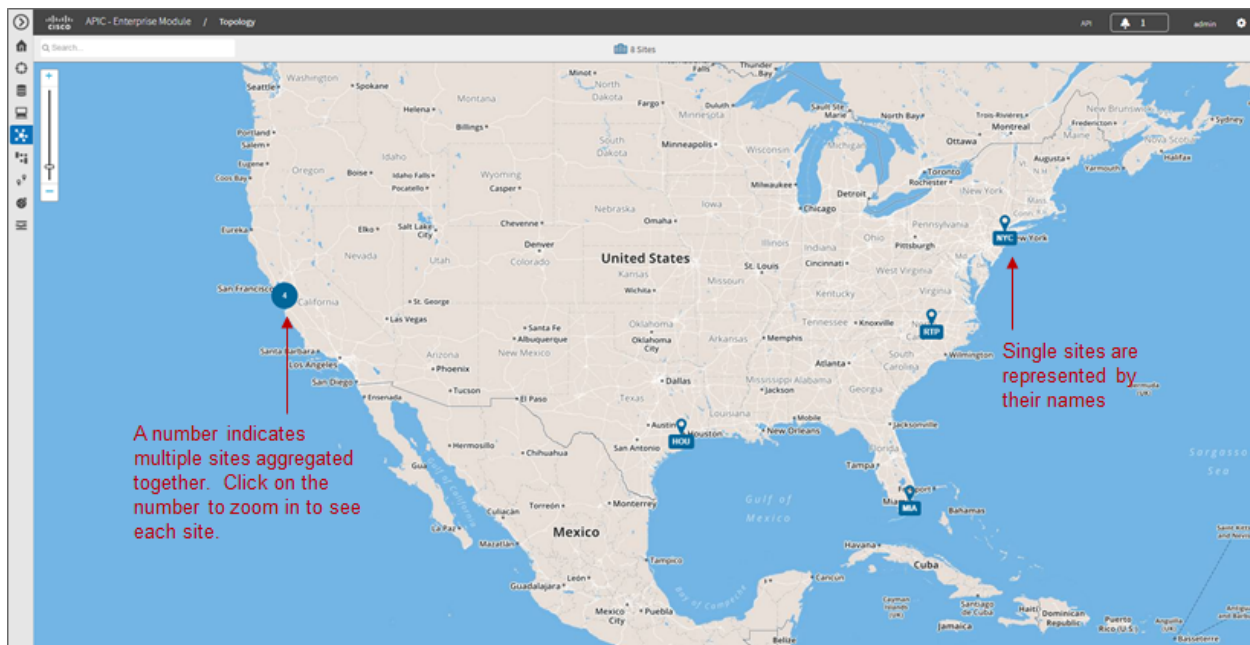
For wired Cisco device endpoints, after the endpoint information is collected, APIC-EM provisions ACE entries into the ACLs configured for Static QoS corresponding to the ingress classification & marking policy deployed across all access-edge ports on the switch to which the device is connected. This is discussed in detail in the **\*Cisco Device Endpoints\*** section of the **\*Campus LAN Static QoS Design\*** chapter. If Dynamic QoS is enabled, EasyQoS will also push ACE entries into the Dynamic ACL policy shells corresponding to the dynamic ingress classification & marking policy for the specific switch port as well. Dynamic QoS is discussed in detail within the **\*Dynamic QoS Design\*** chapter.

There are no equivalent ACE entries generated for wireless devices with the current EasyQoS solution. This is because the AireOS wireless LAN controller (WLC) EasyQoS ingress classification & marking policy uses Cisco Application Visibility and Control (AVC) profiles, rather than Layer 2-4 ACLs.

### 1.4.5 Topology

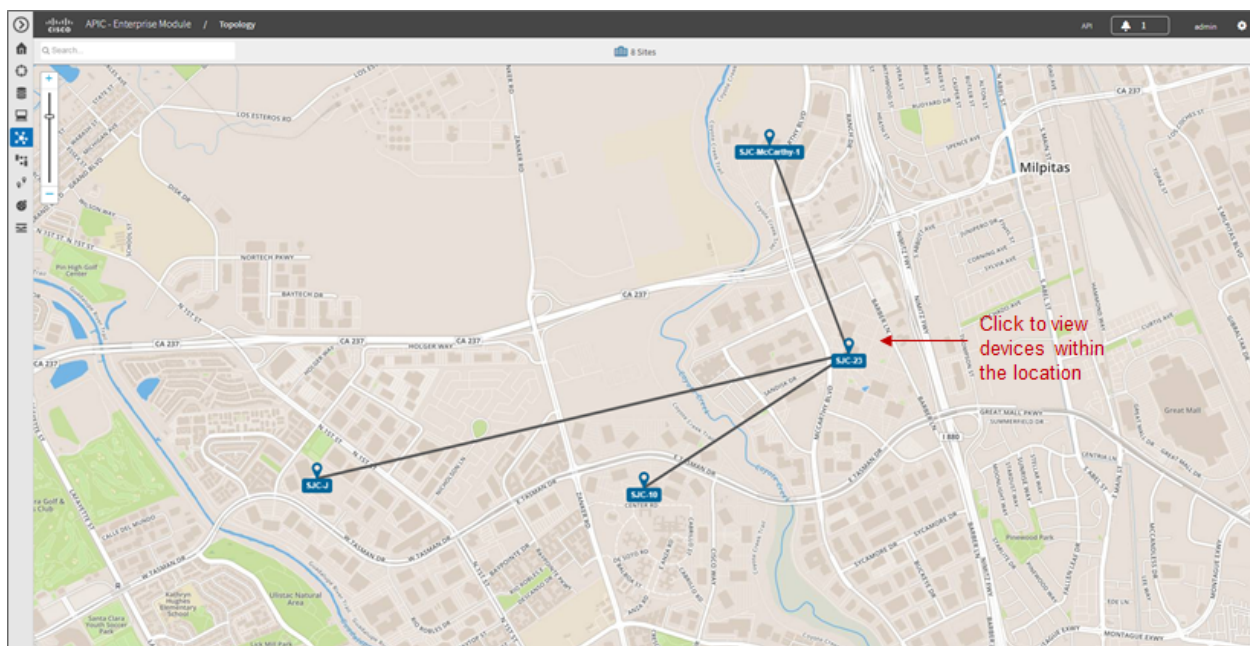
After network infrastructure devices have been discovered, the network operator can view the network via the Topology page. The Topology page is accessed by clicking the Topology icon within the expandable panel on left-side of any APIC-EM page. If devices have been assigned locations, the initial view of the Topology page will be a map, as shown in the following figure.

#### 1. APIC-EM Top-Level Map



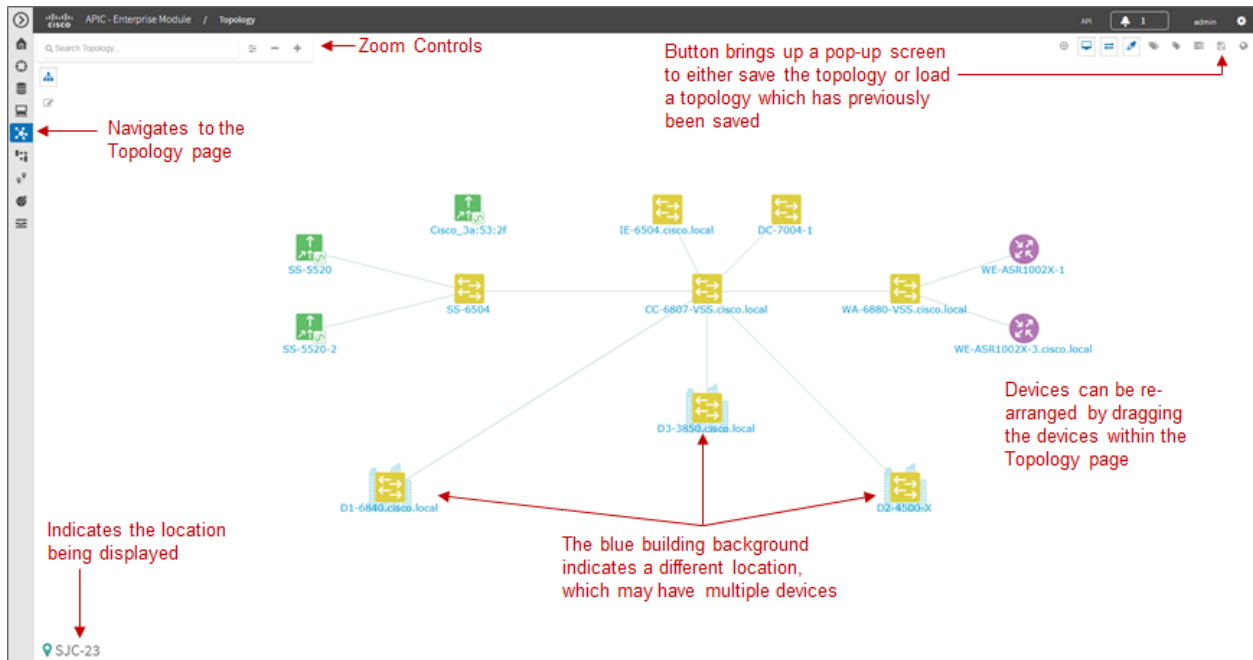
Individual sites are identified by their location names. Locations that are geographically close are aggregated together and represented by a number. Clicking the number will zoom the map in closer to reveal each site, as shown in the following figure.

#### 1. Zooming in to Reveal Aggregated Sites



Finally, by clicking the name of an individual location, the network operator can display the topology of the devices within the site. An example is shown in the following figure.

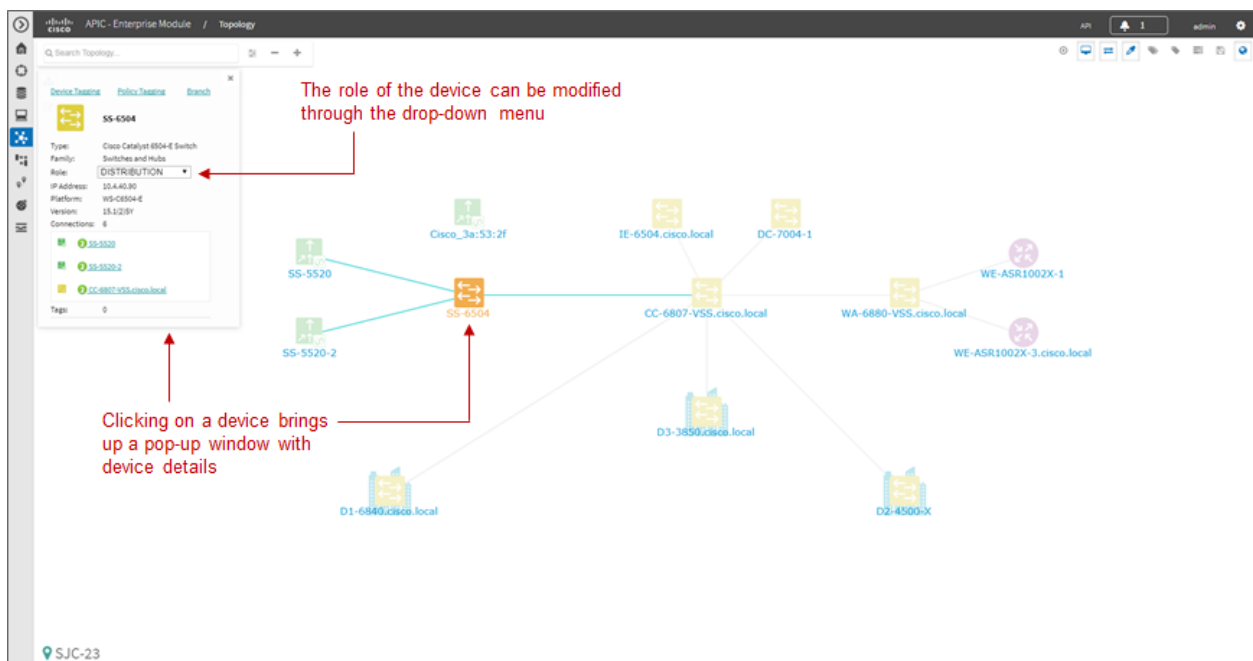
#### 1. Displaying the Topology of Devices within a Location



APIC-EM automatically discovers the relationship between devices and connects them together within the Topology page. Individual devices or groups of devices can be re-positioned by dragging them around within the page and by zooming-in and zooming-out as needed. When the network operator has arranged the devices as desired, he/she can save the layout via the Save or Load Topology icon in the upper right corner of the Topology page. This can be loaded in the future when visiting the Topology page, so that the network operator doesn't have to re-arrange the devices upon every visit to the Topology page.

Clicking a device will bring up a side window with additional detail on the device—including the role of the device within the network—as shown in the figure below.

#### 1. Selecting the Role of a Device from Within the Topology Page



Each discovered network infrastructure device is automatically categorized into one of the following roles:

- Core
- Distribution
- Access
- Border Router
- Unknown

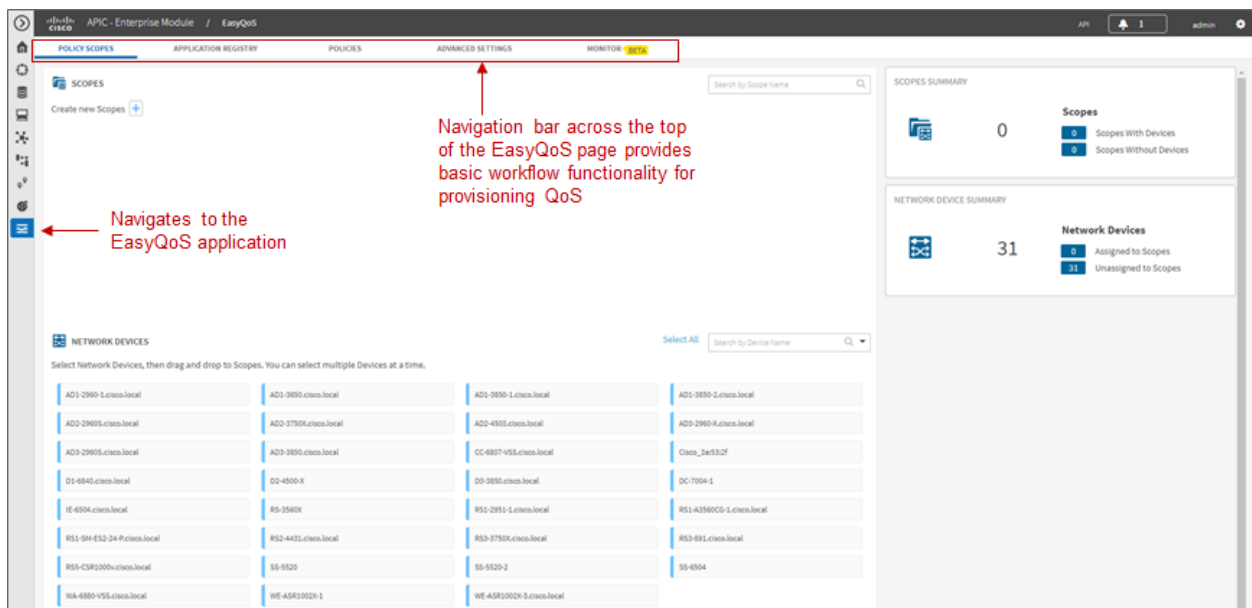
The Core, Distribution, and Access roles apply to Catalyst switches. The Access role also applies to WLC platforms. The Border Router role applies only to Cisco ISRs and ASRs. The network operator should verify that the particular device selected has been characterized with the correct role, in order to ensure the correct QoS policy is applied to the device by the EasyQoS application. This applies primarily to Catalyst switches. If necessary, the network operator can change the role within the side window. The policy applied to Catalyst switches based upon their role is discussed in the *\*Campus LAN Static QoS Design\** chapter.

### 1.4.6 EasyQoS Application

The Discovery, Device Inventory, Host Inventory, and Topology functions discussed in the previous sections are not part of the EasyQoS application. However, they were discussed because the functionality they provide is necessary for the EasyQoS application to operate. This section shifts the discussion to the specific functionality within the EasyQoS application itself.

The EasyQoS application is accessed by clicking the EasyQoS icon within the expandable panel on left-side of any APIC-EM page. An example is shown in the following figure.

#### 1. APIC-EM EasyQoS



As shown in the figure above, the EasyQoS application has several tabs that appear as a bar across the top of the page.

- Policy Scopes
- Application Registry
- Policies
- Advanced Settings
- Monitoring (Beta)

The tabs are intended to roughly guide the network operator through something similar to a basic workflow for deploying QoS policy. Therefore, it is recommended that you access the tabs in order (from left to right) when deploying QoS policy, although the network operator is free to access the tabs in any order. Each of these tabs will be discussed in separate sections.

## Policy Scopes

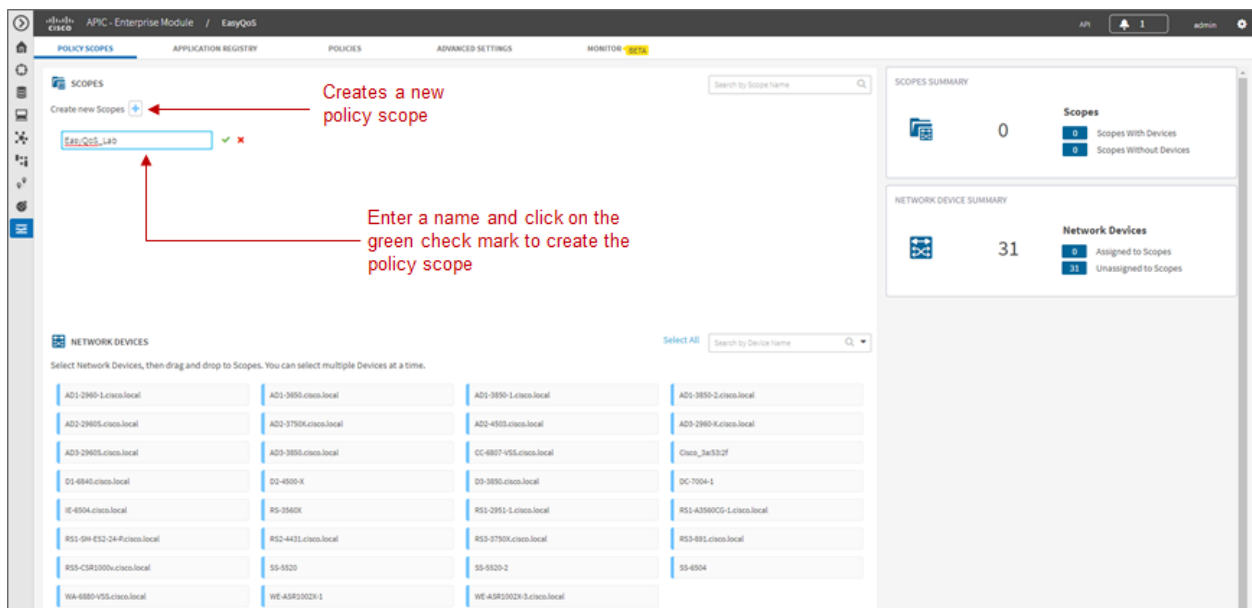
The network operator is by default automatically taken to the first tab—Policy Scopes—when clicking the EasyQoS application icon within the expandable panel on left-side of any APIC-EM page.

The first step to deploying QoS policy through EasyQoS is to create one or more policy scopes. Policy scopes are simply a way of grouping one or more network devices together in order to apply QoS policy to the group all at once, rather than having to individually apply QoS policy to one network device at a time.

The network operator can define a single policy scope for all of the network devices under his/her administrative control. Alternatively, the network operator is free to define multiple policy scopes—each of which contains one or more network devices. Either way, EasyQoS will deploy the appropriate QoS policy to each device, based upon the network topology, the role of the device within the network, and the application-level business intent expressed by the network operator. Up to 2,000 devices can be configured in a single policy scope as of APIC-EM version 1.3 and higher.

In order to create a new policy scope, the network operator can click the + next to Create New Scopes on the upper left side of the Policy Scopes tab. An empty box representing the new policy scope name will appear. The network operator will be prompted to give the new policy scope a name and click the green check mark in order to create it. An example is shown in the following figure.

### 1. Creating a New Policy Scope

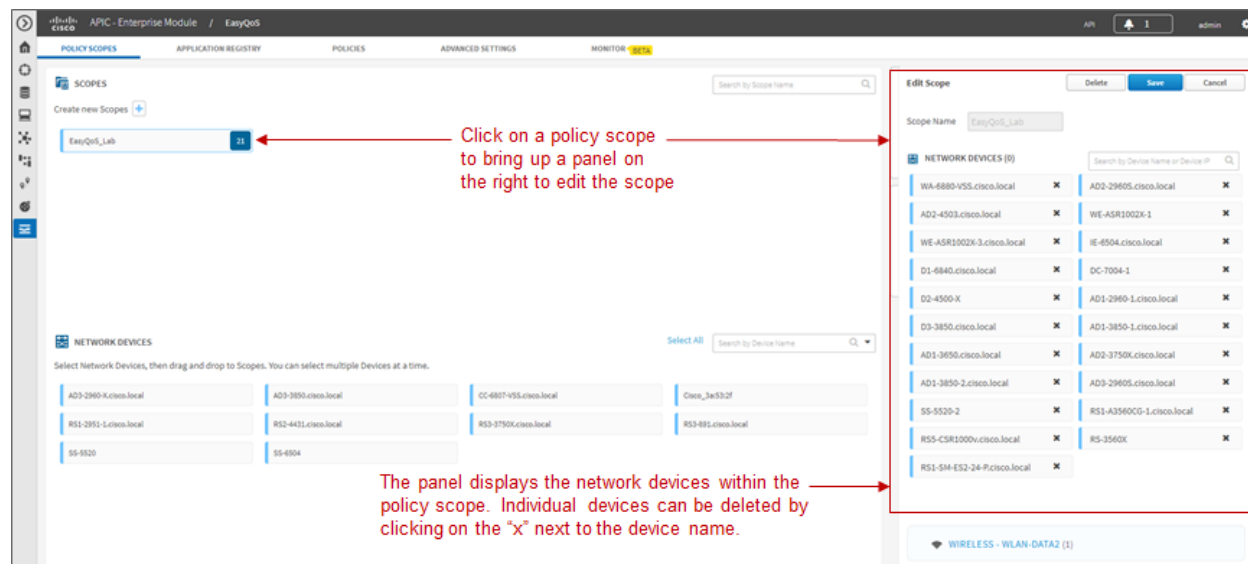


- Note: The Policy Scope name cannot include any blank spaces. Use either an underscore, dash, or single word for the Policy Scope name.

When a new policy scope is created, it contains no network devices. In order to add network devices to a policy scope, the network operator must drag-and-drop one of the available devices within the Network Devices panel into the policy scope. A network device can be a member of only one policy scope at a given time. Only network devices that have been Discovered and added to the Device Inventory of APIC-EM will appear within the Network Devices panel, as shown in the figure above.

After a device has been dragged-and-dropped into a policy scope, it will no longer appear within the Network Devices panel. Instead, it will appear within the right-hand panel within the display when the network operator clicks on the policy scope. An example is shown in the figure below.

### 1. Displaying Network Devices within a Policy Scope



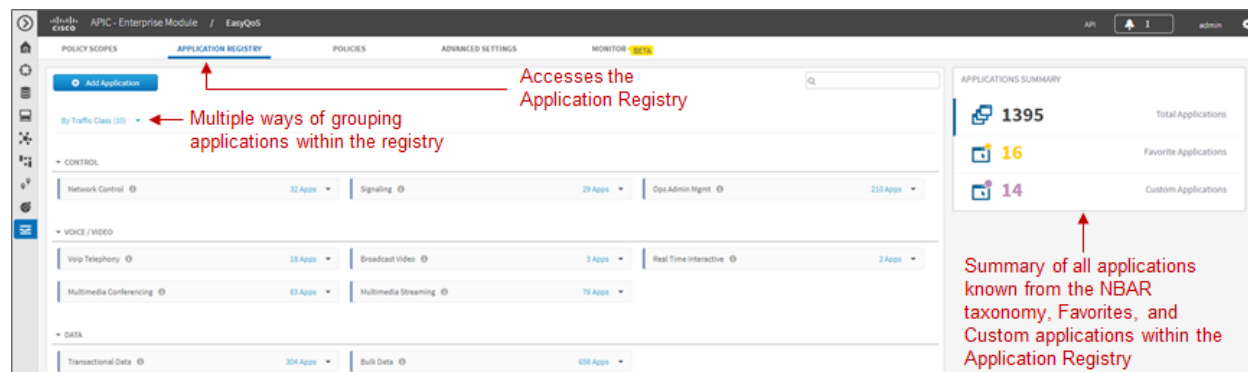
Individual network devices can be deleted from the policy scope by clicking the “x” next to the network device name. The Save button must be clicked in order to save the changes. Devices removed from a policy scope automatically appear again within the Network Devices panel underneath the Scopes panel. The network operator can also delete the entire policy scope by clicking the Delete button.

After the desired number of policy scope(s) are created and the desired network devices have been moved into the policy scope(s), the network operator can click the Application Registry tab.

## Application Registry

The second step in deploying QoS policy through EasyQoS is to access the Application Registry in order to select Favorite applications and to create Custom applications. The Application Registry serves as a common repository of applications known to APIC-EM via the NBAR taxonomy, Favorite applications, and Custom applications. It can be leveraged by various APIC-EM applications such as EasyQoS and IWAN. An example of the Application Registry is shown in the figure below:

### 1. Application Registry





Applications can be grouped in multiple ways when viewing them within the left-panel of the Application Registry as follows:

- **Applications**—This lists all applications (both from the NBAR taxonomy and Custom applications) alphabetically.
- **Application Groups**—This lists all applications based on the NBAR application category attribute to which the applications belong.
- **Traffic Class**—This lists all applications based on the NBAR traffic-class attribute to which the applications belong.

The panel on the right provides a summary of all the 1300+ applications known via the NBAR taxonomy as of NBAR2 Protocol Pack 27.0.0, all Favorite applications, and all Custom applications currently known and/or configured within APIC-EM.

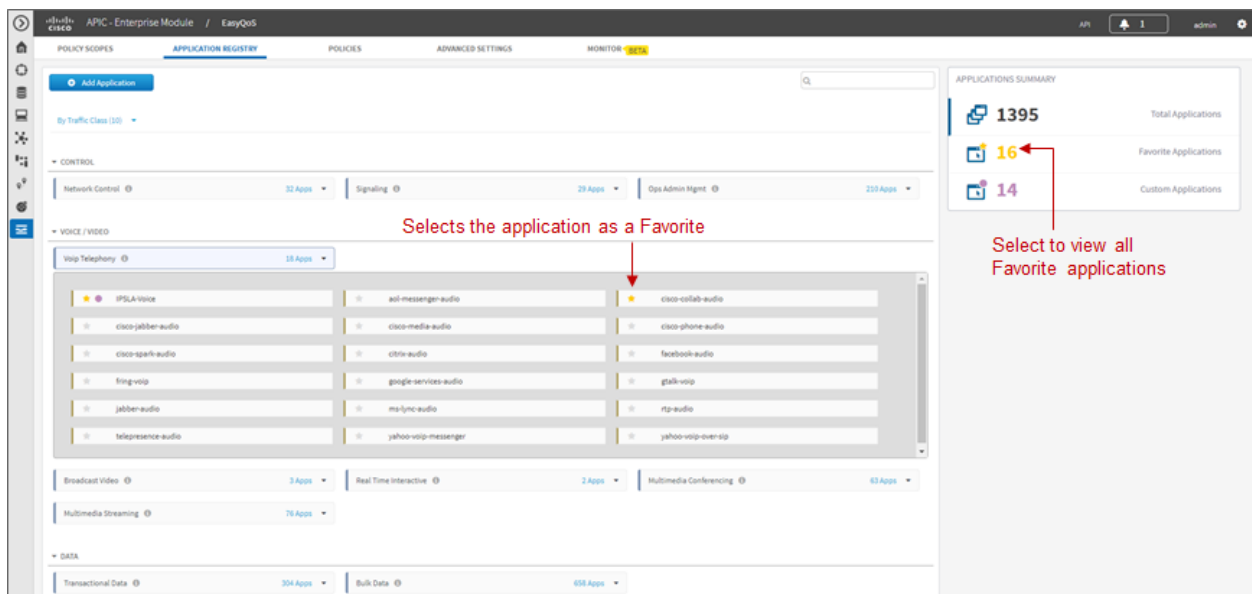
### Favorite Applications

The concept of Favorite Applications has been added to EasyQoS to address the issue that some platforms have limited ability to support applications. For instance, Cisco AireOS WLCs currently can support only 32 applications per AVC profile. Likewise, some older Catalyst switch platforms have limited TCAM space, hence can only support a limited number of ACE entries within the ingress classification & marking ACLs deployed to these devices by EasyQoS.

By selecting an application as a Favorite, the network operator declares a preference for including that application within QoS policies provisioned by EasyQoS, over other applications. When EasyQoS creates QoS policies, it will select applications that have been marked as Favorites for inclusion within the policies before the remainder of the applications within the NBAR taxonomy. Note that by default Custom applications are automatically marked as Favorite applications when they are created.

Applications are selected as Favorites by clicking the star next to the name of the application. Clicking the star causes it to turn yellow, indicating application has been selected as a favorite. An example is shown in the figure below.

#### 1. Selecting Favorite Applications

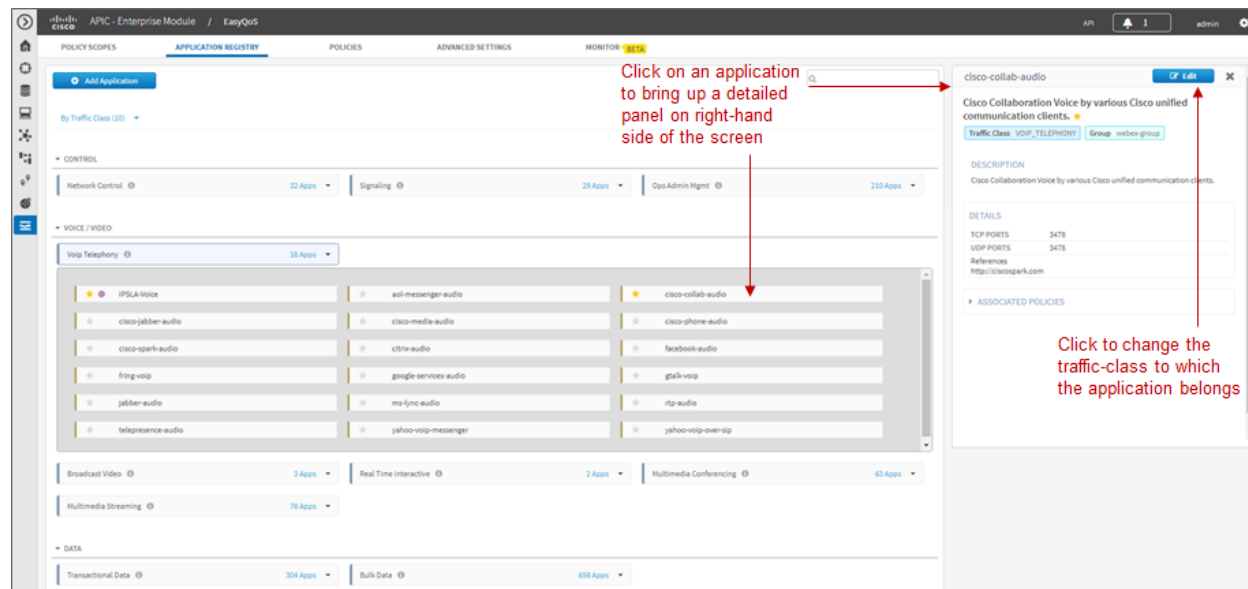


The list of Favorite applications is global to the APIC-EM EasyQoS deployment—meaning that Favorites are the same across all Policy Scopes. The list of Favorite applications can be displayed by clicking Favorite Applications in the panel on the right side of the Application Registry.

Changing the Traffic-Class of an Application

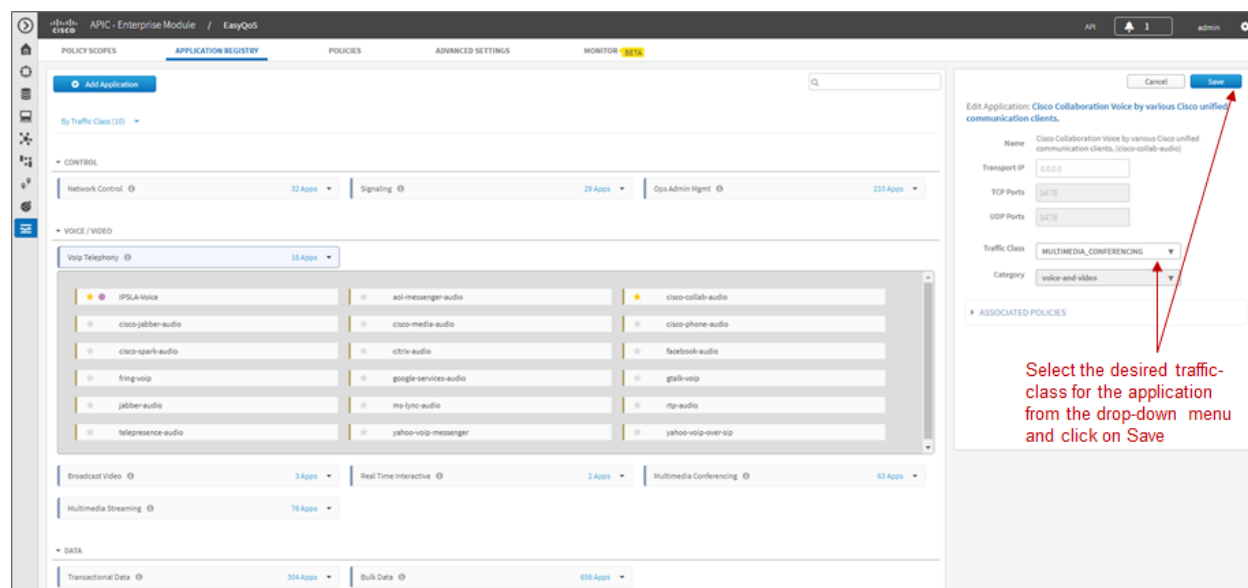
EasyQoS within APIC-EM release 1.5 and higher allows the network operator to change the traffic-class to which an application belongs. By default, all 1300+ applications known to the NBAR2 taxonomy are assigned a traffic-class, based on IETF RFC 4594 guidelines. However, the network operator may sometimes wish to change this. For example it may be desired to put both the audio and video components of a collaboration session into the same traffic-class, rather than have the audio media in the VoIP Telephony traffic-class and the video media in the Multimedia Conferencing traffic class. The network operator can change this by selecting the application within the Application Registry. This will bring up a panel on the right-hand side of screen as shown in the figure below.

### 1. Selecting an Application within the Application Registry



Clicking the Edit button will change the right-hand panel, allowing the network operator to select the desired traffic-class of the application from the drop-down menu. When the network operator is satisfied with the new traffic-class, he/she can click the Save button in the upper right corner of the panel in order to save the changes to the application.

### 1. Changing the Traffic-Class of an Application Example



Changing the traffic-class of an application will modify the EasyQoS ingress classification & marking policy for that particular application. The effects on ASR and ISR router configuration of changing the traffic-class of an application



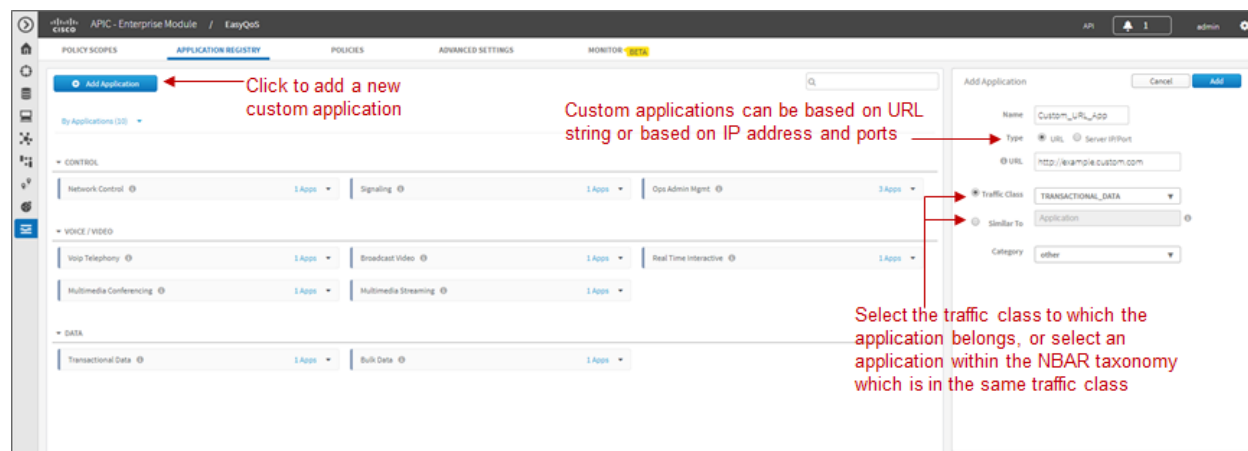
are discussed in the **\*Changing the Traffic-Class of Applications on ASR and ISR Platforms\*** section of the **\*WAN and Branch Static QoS Design\*** chapter. The effects on Catalyst switch configuration are discussed in the **\*Ingress Classification & Marking Policies\*** section of the **\*Campus LAN Static QoS Design\*** chapter.

### Custom Applications

The Application Registry is also where the network operator can create Custom applications. Although AVC/NBAR currently identifies approximately 1300+ applications, organizations sometimes develop their own internal applications, which may not be recognized by AVC/NBAR. In order to identify and provide the proper QoS treatment for these applications across the network infrastructure, the network operator can create a Custom application for each of them.

Custom applications are added by clicking the Add Application button within the Application Registry page. The right-hand panel of the page will change, allowing the network operator to add the application based upon a URL or a Server IP/Port range. An example is shown in the following figure.

#### 1. Custom Application Based on a URL



In the example above, the Custom application is based on a URL. For an EasyQoS Custom application based on a URL, the network operator must provide the following information:

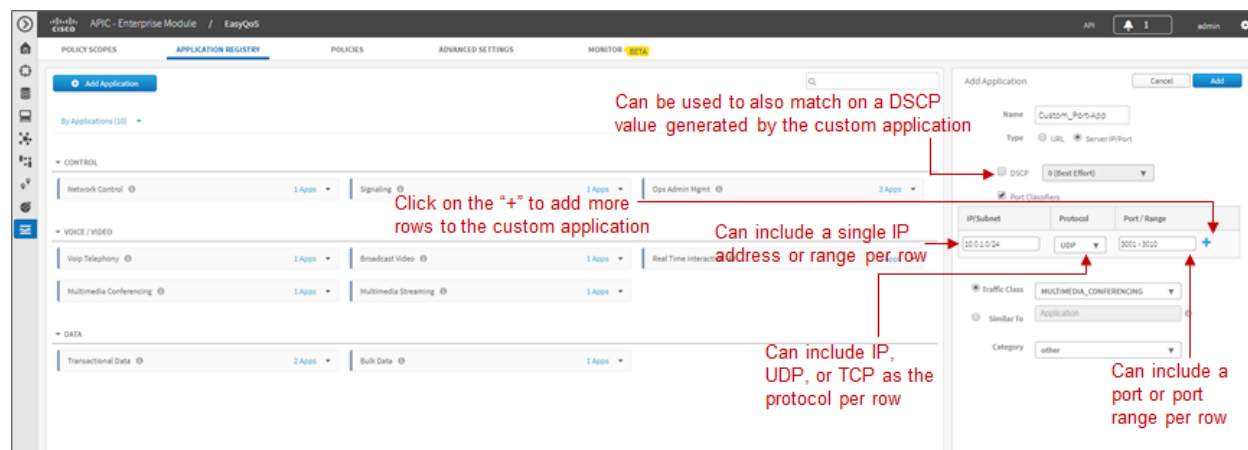
- A name by which APIC-EM will know the application
- The URL string to which the application is matched against within AVC/NBAR policies
- The traffic class to which the application belongs
- Note: EasyQoS within APIC-EM release 1.5 and higher does not do verification of the URL string to ensure it is properly formatted.

If the network operator does not know to which traffic class the Custom application should belong, he/she can simply select the Similar To check box and use the drop-down menu to select one of the applications known to EasyQoS via the NBAR taxonomy that has similar characteristics. By *similar characteristics*, we mean that the NBAR traffic-class and category attributes assigned to that similar application will also be assigned to the Custom application.

Custom applications that are based on URLs are not capable of being deployed on Catalyst switch platforms. They are only deployed onto ISR and ASR platforms that implement policy-maps that contain “match protocol attribute” statements. This is because the traffic-class attribute must be programmed into the Custom application, and the traffic-class attribute requires a “match protocol attribute traffic-class” statement to be configured within the policy-map. An example of the policy configuration for a Custom application that is based on a URL is shown in the **\*Custom Applications on ASR and ISR Platforms\*** section in the **\*WAN and Branch Static QoS Design\*** chapter.

Alternatively, a Custom application can be based upon one or more IP addresses (or address ranges) and one or more IP, TCP, and/or UDP ports (or port ranges). An example using multiple IP addresses and port ranges is shown in the following figure.

## 1. Custom Application Based on Server IP Address and Ports



For an EasyQoS Custom application based on a server IP addresses and ports, the network operator needs to provide the following information:

- A name by which APIC-EM will know the application
- A DSCP value (optional). This field is used to match on a DSCP value generated by the Custom application within the QoS policy generated by EasyQoS.
- Port Classifiers (optional), which include one or more IP addresses or IP address ranges, along with one or more protocols (IP, TCP, UDP, or TCP/UDP), and one or more ports or port ranges.
- The traffic class to which the application belongs

The example in the figure above demonstrates the use of the subnet mask field—set to 24 bits (10.0.1.0/24) in the first row of the Port Classifiers—to include a full subnet as a destination IP address range. Likewise, the range (3000-3010) in the first row of the Port Classifiers shows how to include a range of ports (UDP ports in this example—based on the Protocol setting for the particular row). This IP address or address range as well as port or port range refers to a destination—also referred to as the producer. Additional rows can be added to include more individual IP addresses or IP address ranges, as well as more ports or port ranges to the Custom application.

As with URL-based Custom applications, if the network operator does not know to which traffic class the Custom application should belong, he/she can simply select the Similar To check box and use the drop-down menu to select one of the applications known to EasyQoS via the NBAR taxonomy that has similar characteristics. By *similar characteristics*, we mean that the NBAR traffic-class and category attributes assigned to that similar application will also be assigned to the Custom application.

Custom applications that are based on server (destination) IP addresses and ports are capable of being deployed on both Catalyst switch platforms and ASR or ISR platforms. For Catalyst switch platforms, the server (destination) IP address or address range, ports, and/or DSCP fields are translated into one or more ACEs that are populated within the ACL corresponding to the traffic-class to which the Custom application belongs. An example of this is shown in the **\*Access-Control Lists\*** section in the **\*Campus LAN Static QoS Design\*** chapter.

For more complex applications, a source IP address or address range as well as a source port or port range can be added to the Custom Application. This is referred to as adding a Consumer to the application. Adding a Consumer is discussed in the **\*Policies\*** section below.

## Advanced Settings

With APIC-EM release 1.4, configuration of SP Profiles and Dynamic QoS was moved under the Advanced Settings tab. Additionally, a new feature, Bandwidth (BW) Profiles, was added. APIC-EM release 1.5 renamed Bandwidth Profiles to Queuing Profiles and extended this by allowing the network operator to change the default DSCP marking

of traffic-classes. The following sections discuss Queuing Profiles and SP Profiles. Dynamic QoS is discussed in a separate **\*Dynamic QoS\*** section.

## Queuing Profiles

Queuing Profiles provide a means for the network operator to customize the following:

- The amount of bandwidth allocated for each of the 12 traffic-classes provisioned by EasyQoS
- The DSCP marking to be applied to traffic associated with each of the 12 traffic-classes

EasyQoS includes a default Queuing Profile named CVD\_Queueing\_Profile. Allocation of the bandwidth across the traffic-classes and the DSCP marking associated with each traffic-class within the default Queuing Profile is fixed, as shown in the following figure.

### 1. Default Queuing Profile

Access Queuing Profiles under Advanced Settings

Default Queuing Profile

Click to create a new Queuing Profile to modify BW allocations and DSCP markings

DSCP markings assigned to the traffic classes within the default Queuing Profile cannot be modified

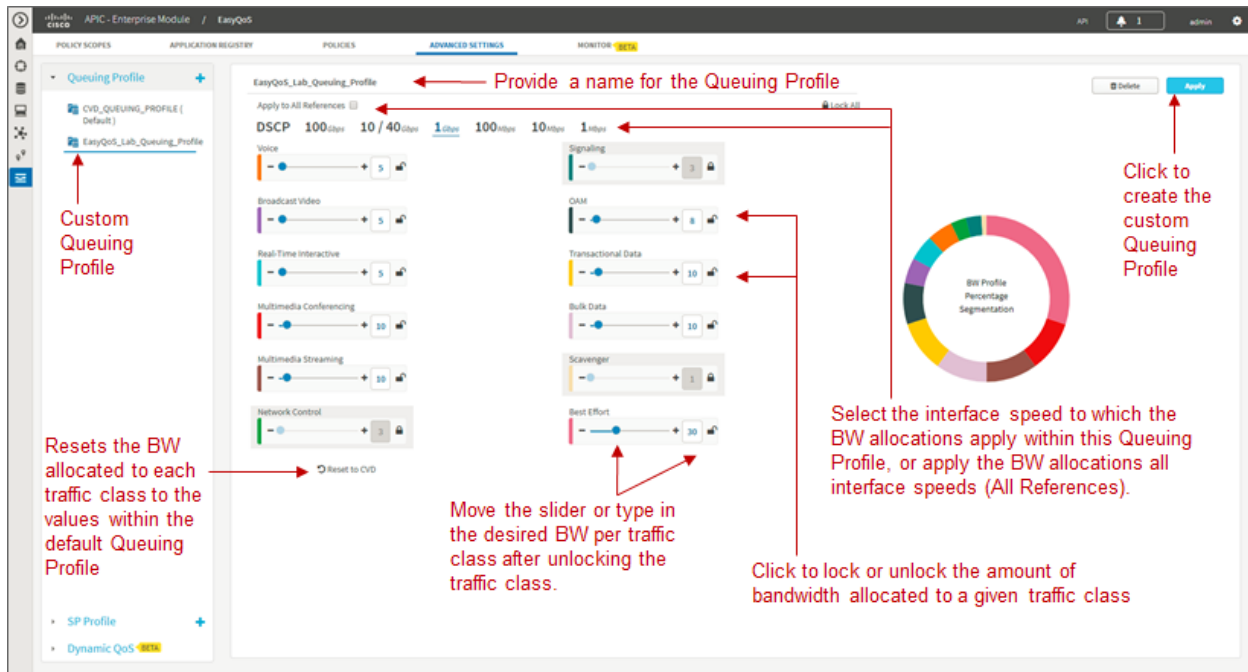
Bandwidth allocations within the default Queuing Profile cannot be modified

Provides a visual view of the BW allocation among the traffic classes

Traffic Class	Bandwidth Allocation (%)	DSCP Marking
Voice	46	46 (EF)
Broadcast Video	40	40 (CS5)
Real-Time Interactive	32	32 (CS4)
Multimedia Conferencing	34	34 (AF4)
Multimedia Streaming	26	26 (AF3)
Network Control	48	48 (CS6)
Signaling	2	24 (CS2)
QAM	2	24 (CS2)
Transactional Data	10	10 (AF2)
Bulk Data	4	10 (AF1)
Scavenger	1	8 (CS1)
Best Effort	25	0 (Best Effort)

In order to modify the bandwidth allocations or DSCP markings, the network operator must create a new custom Queuing Profile by clicking the blue “+” next to Queuing Profile on the left panel of the Advanced Settings screen, as shown in the figure above. This will bring up a new Queuing Profile screen similar to the one in the following figure.

### 1. Creating a Custom Queuing Profile – BW Allocation Example



The network operator must first provide a unique name for the custom Queuing Profile.

### Bandwidth Allocations

Bandwidth allocations for each of the traffic-classes can be set independently for each of the interface speeds shown in the figure above. This is accomplished by highlighting the link speed (100 Gbps, 10/40 Gbps, 1 Gbps, 100 Mbps, 10 Mbps, or 1 Mbps) and adjusting the bandwidth allocations for each traffic-class. For example, the network operator can set bandwidth allocations for 1 Gbps access ports (ports connected to end-user devices) differently from 10 Gbps uplink ports (ports connected to other network infrastructure devices) within the same custom Queuing Profile. For link speeds that are between the values listed, the bandwidth allocations for the next lower link speed apply. Alternatively, the network operator can choose to apply the same bandwidth allocations for each traffic-class to all link speeds by selecting the Apply to all References checkbox.

Each of the 12 traffic-classes in the figure above have a slider that can be used to adjust the bandwidth allocated for the traffic-class. Alternatively, the network operator can simply type in the desired bandwidth in the box adjacent to the slider. The bandwidth allocated for each traffic-class represents the percentage of the total bandwidth. The sum of the bandwidth allocations for all of the traffic-classes must always equal 100 percent.

- Note: As of APIC-EM release 1.6.0, the network operator can change the default 1% bandwidth allocation of the Scavenger traffic-class within a custom Queuing Profile within the EasyQoS GUI. However, changing the bandwidth allocation of the Scavenger traffic-class will have no effect on the actual bandwidth allocation provisioned by EasyQoS to network devices for the Scavenger traffic-class. Further, since the bandwidth allocations within the custom Queuing Profile of the EasyQoS GUI must total 100%, the percentage bandwidth allocations actually provisioned by EasyQoS for the remaining traffic-classes will not match what is shown within the custom Queuing Profile. For further details, refer to Cisco defect CSCvg74117.

In order to adjust the bandwidth allocated to a given traffic-class, the network operator must first ensure the traffic-class is unlocked. The lock icon in each traffic-class locks and unlocks the bandwidth allocation for the traffic-class. Adjusting the bandwidth allocation for one of the unlocked traffic-classes automatically causes the bandwidth in the remaining unlocked traffic-classes to be re-distributed such that the sum of the bandwidth allocation for all traffic-classes is always 100 percent.

One method of specifically setting the bandwidth allocation for all of the traffic-classes would be as follows:

- Unlock all of the traffic-classes

- Select the first traffic-class, set the bandwidth allocation percentage for that traffic class, and lock the traffic-class
- Repeat for the remaining traffic-classes
- The final traffic-class will have the remaining bandwidth percentage not allocated to the other traffic-classes
- Note: The Voice, Broadcast Video, and Real-Time Interactive traffic-classes are considered to be priority traffic within Queuing Profiles. These traffic-classes may be mapped to priority queues on platforms. If the amount of bandwidth allocated to these three traffic-classes exceeds 33%, the network operator will receive a warning indicating that this is not recommended because it could cause bandwidth starvation of non-priority queues.

At any point, the network operator can click the Reset to CVD icon within the screen to reset the bandwidth allocations for the traffic-classes back to their default values.

Bandwidth settings within Queuing Profiles are used to calculate the bandwidth rates used in the commands which configure the various hardware queues in the queuing policies provisioned to each of the supported Catalyst and Nexus switching platforms. Switch platforms typically have only 4 or 8 hardware queues. Bandwidth allocation percentages from the Queuing Profile traffic-classes that are mapped into a specific hardware queue, are summed to obtain the rate configured within the queuing policy. The actual configuration is also dependent upon the specific platform and/or line card. More specifically, the configuration depends upon the number of hardware queues supported by the platform or line card, the number of priority queues supported by the platform or line card, and whether the priority queues are bounded or unbounded. Bounded priority queues have a maximum configured traffic rate (often implemented through a policer), and unbounded priority queues can use as much bandwidth as needed. When priority queues are supported, the bandwidth percentages from the Queuing Profile are adjusted from “bandwidth percentages” to “bandwidth remaining percentages” when configured into policy maps on MQC or C3PL platforms or egress queuing commands on MQC platforms. “Bandwidth remaining percentage” is the amount of bandwidth remaining after accounting for the bandwidth used in priority queues.

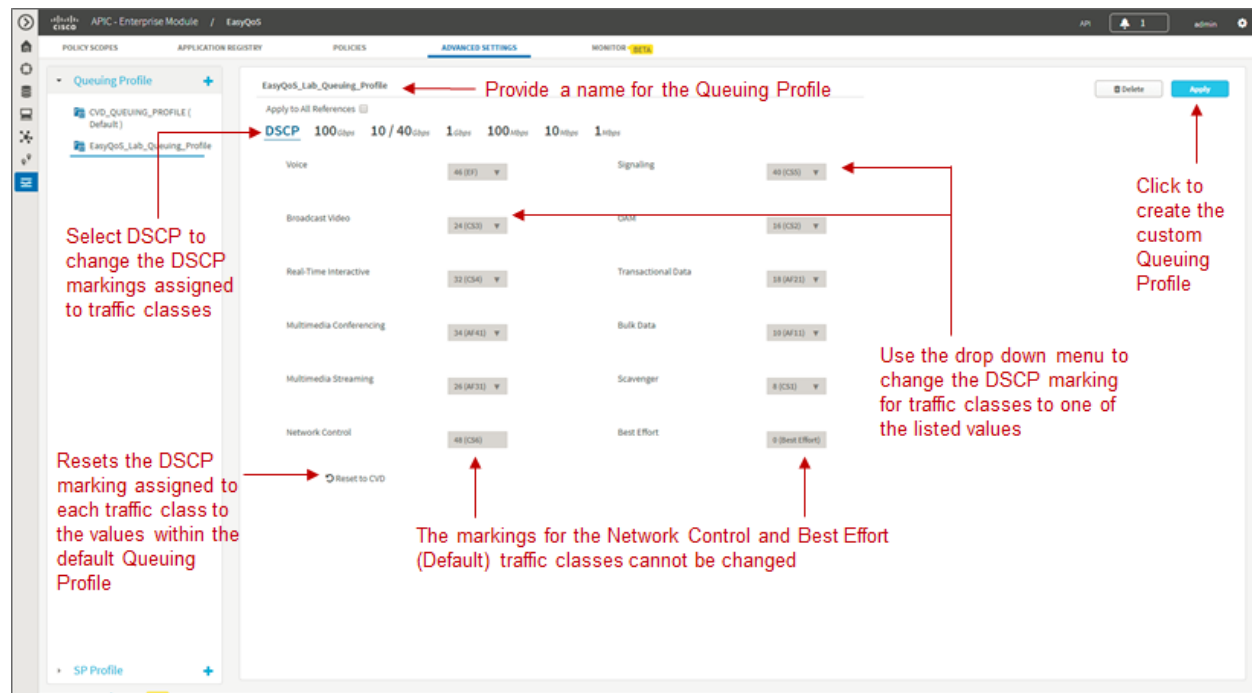
Bandwidth allocation settings within Queuing Profiles are also used to calculate the bandwidth rates used in the commands that configure the various software queues in the egress queuing policy provisioned to ASR and ISR router platforms. Bandwidth allocation settings within Queuing Profiles apply only to ISR and ASR interfaces that are not part of a WAN SP Profile. In other words, they apply only to interfaces which implement the WAN edge queuing policy discussed in the **\*WAN Edge Egress Queuing Policy\*** section in the **\*WAN and Branch Static QoS Design\*** chapter. Because router platforms only implement egress queuing policies, and because these policies are implemented in software, each of the 12 traffic-classes within the Queuing Profile maps to an egress queue (a class-map entry within a policy-map). Because the WAN edge queuing policy implements three low-latency queues (three priority queues), the remaining bandwidth percentages from the bandwidth allocation settings within the Queuing Profile are adjusted from “bandwidth percentages” to “bandwidth remaining percentages” when configured into the policy maps.

### DSCP Markings

- Note: Caution should be used when changing the default DSCP marking of traffic-classes from the Cisco recommended 12-class QoS model. Such changes could result in a less than optimal QoS implementation unless the network operator is highly knowledgeable in QoS design and implementation. This feature is only for customers with advanced knowledge of QoS.

DSCP markings for each traffic-class can be modified by highlighting DSCP instead of one of the link speeds (100 Gbps, 10/40 Gbps, 1 Gbps, 100 Mbps, 10 Mbps, or 1 Mbps), as shown in the figure below.

#### 1. Creating a Custom Queuing Profile – DSCP Markings Example



DSCP markings for the Best Effort (Default) and Network Control traffic-classes cannot be modified. EasyQoS does not provision a class-map entry for Network Control traffic within the ingress classification & marking policy applied to access-layer switches. Network Control traffic is not expected to be seen inbound on a switch port connected to an end-user device. Because no class-map entry exists for Network Control traffic within the ingress classification & marking policy, no policy action, such as setting the DSCP marking of the traffic can be taken. Therefore EasyQoS does not allow modification of the DSCP marking of Network Control traffic. By default, Network Control traffic is considered to be marked with DSCP 48 (CS6).

For the remaining 10 traffic-classes, the network operator can modify the DSCP marking applied to traffic matching the particular traffic-class. This is accomplished through the drop-down menu adjacent to the traffic-class, as shown in the figure above. The drop-down menu will only display DSCP marking values which have not been assigned to another traffic-class already. This is because EasyQoS always deploys a 12-class QoS model. Each of the traffic-classes within the 12-class model must have a policy-action which sets the DSCP value of the matching traffic to a unique value. In other words, EasyQoS will not allow two different traffic-classes within the ingress classification & marking policy-map to have policy-actions which map to the same DSCP value. If the DSCP marking which you wish to assign a traffic-class is already being used by another traffic-class, you must first change the other traffic-class to mark to a different DSCP value. Selectable DSCP values range from 0 to 63, excluding DSCP 0 (Best Effort) and DSCP 48 (CS6).

In the figure above, Broadcast Video traffic has been marked to CS3 and Signaling traffic has been marked to CS5, as specified in IETF RFC 4594, purely as an example of changing traffic-classes, not as a best-practice. Cisco recommends a modification to RFC 4594 in that Signaling traffic is marked to CS3 and Broadcast Video is marked to CS5. The default setting for call signaling within Cisco Unified Communications Manager is set to CS3.

The DSCP markings for each traffic-class are independent of the BW allocations applied to interface speeds. In other words, the DSCP markings are applied to all interface speeds for supported devices within the policy scope. At any point, the network operator can click the Reset to CVD icon within the screen to reset the DSCP markings for the traffic-classes back to their default values, which are the recommended settings for the Cisco RFC 4594-based 12-class QoS model.

When the network operator is satisfied with the bandwidth allocations for each of the interface speeds and the DSCP markings within the custom Queueing Profile, he/she can click the Create button in the upper right side of the screen to create and save the custom Queueing Profile.

### Queuing Profile Support by Platform

Bandwidth allocation selections and DSCP markings within custom Queuing Profiles are not supported by all interfaces and all platforms. The following table summarizes the platform support as of APIC-EM release 1.6.

1. Platform Support for BW Allocation and DSCP Marking Within Custom Queuing Profiles

Platform	BW Allocation	DSCP Marking
Catalyst 6K Series with Sup2T and Catalyst 6880 & 6840 Series	Ingress and Egress queues on line cards/supervisors with a 2P6Q4T queuing structure are supported (BW allocations are modified) by custom BW allocations. All other line cards are not supported by custom BW allocations within Queuing Profiles. Non-supported line cards/supervisors implement EasyQoS default BW allocations within queuing structures.	Custom DSCP markings for traffic-classes are supported (DSCP markings are modified) for line cards/supervisors which support DSCP to queue mapping. These include the following: 2P6Q4T ingress and egress queuing is supported by the following line cards: C6800-8P10G, C6800-8P10G-XL C6800-16P10G, C6800-16P10G-XL C6800-32P10G, C6800-32P10G-XL 8Q4T ingress queuing is supported by the following line cards: VS-S2T-10G, VS-S2T-10G-XL with Gigabit Ethernet ports disabled WS-X6908-10G-2T, WS-X6908-10G-2TXL 1P7Q4T egress queuing is supported by the following line cards: WS-X6908-10G-2T and WS-X6908-10G-2TXL VS-S2T-10G and VS-S2T-10G-XL with Gigabit Ethernet ports disabled For all other line cards and queuing structures the EasyQoS default DSCP markings are implemented for traffic-classes.
Catalyst 6K Series with Sup-720	Custom BW allocations are not supported (BW allocations are not modified). Line cards implement EasyQoS default BW allocations within queuing structures.	Custom DSCP markings for traffic-classes are not supported (DSCP markings are not modified) for any line cards/supervisors. EasyQoS default DSCP markings are implemented for traffic-classes.
Catalyst 3850 and 3650 Series	Custom BW allocations are supported (BW allocations are modified) on the 2P6Q3T egress queuing structures.	Custom DSCP markings for traffic-classes are supported (DSCP markings are modified) for these platforms.
Catalyst 4K Series with Sup-7E, 7LE, 8E, and 8LE and Catalyst 4500-X Series	Custom BW allocations are supported (BW allocations are modified) on the 1P7Q1T egress queuing structures.	Custom DSCP markings for traffic-classes are supported (DSCP markings are modified) for these platforms.
Catalyst 2960-C, 2960-CX, 2960-S, 2960-X, 2060-XR, 3560-C, 3560-CX, 3560-X, and 3750-X Series, as well as the SM-ES2 Series Ether-Switch module	Custom BW allocations are supported (BW allocations are modified) on the 1P3Q3T egress queuing structures. Custom BW allocations are not supported (BW allocations are not modified) on the ingress queuing structures of those platforms which support ingress queuing.	Custom DSCP markings for traffic-classes are not supported (DSCP markings are not modified) for these platforms. EasyQoS default DSCP markings are implemented for traffic-classes.
Nexus 7K Series	Custom BW allocations are not supported (BW allocations are not modified). Modules/supervisors implement EasyQoS default BW allocations within queuing structures.	Custom DSCP markings for traffic-classes are not supported (DSCP markings are not modified) for these platforms. EasyQoS default DSCP markings are implemented for traffic-classes.



Changing the DSCP marking of a traffic-class will modify the EasyQoS egress queuing policy for that particular traffic-class. The effects on ASR and ISR routers of changing the DSCP marking of a traffic-class are discussed in the **\*Changing the DSCP Markings of Traffic-Classes on ASR and ISR Platforms through Custom Queuing Profiles\*** section in the **\*WAN and Branch Static QoS Design\*** chapter. The effects on Catalyst switches are discussed in the **\*Ingress Classification & Marking Policies\*** section of the **\*Campus LAN Static QoS Design\*** chapter. Finally, the effects on wireless LAN controller platforms are discussed in the **\*QoS Trust Boundaries and Policy Enforcement Points\*** section of the **\*WLAN QoS Design\*** chapter.

## SP Profile

The configuration of custom SPPs is an optional step that is dependent upon the following two questions:

- Is a managed-service WAN implemented on any interface of any ISR or ASR router within the scope of the policy to be deployed?
- If there is a managed-service WAN, does the service match one of the four default SP profiles provided by EasyQoS?

The four default SP profiles provided by EasyQoS can be viewed by clicking SP Profile within the Advanced Settings tab and then highlighting one of the four default profiles as shown in the following figure:

### 1. Default SP Profiles Provided by EasyQoS

Four default service provider profiles – 4, 5, 6, and 8 traffic classes

Class Name	DSCP	Priority	%Bandwidth	Admitted Traffic
Voice	EF	✓	10%	voip-telephony
CLASS1 DATA	AF31		44%	multimedia-streaming,real-time-interactive,...
CLASS2 DATA	AF21		25%	bulk-data,ops-admin-mgmt,signaling,transa...
Default	Best Effort		21%	scavenger,best-effort

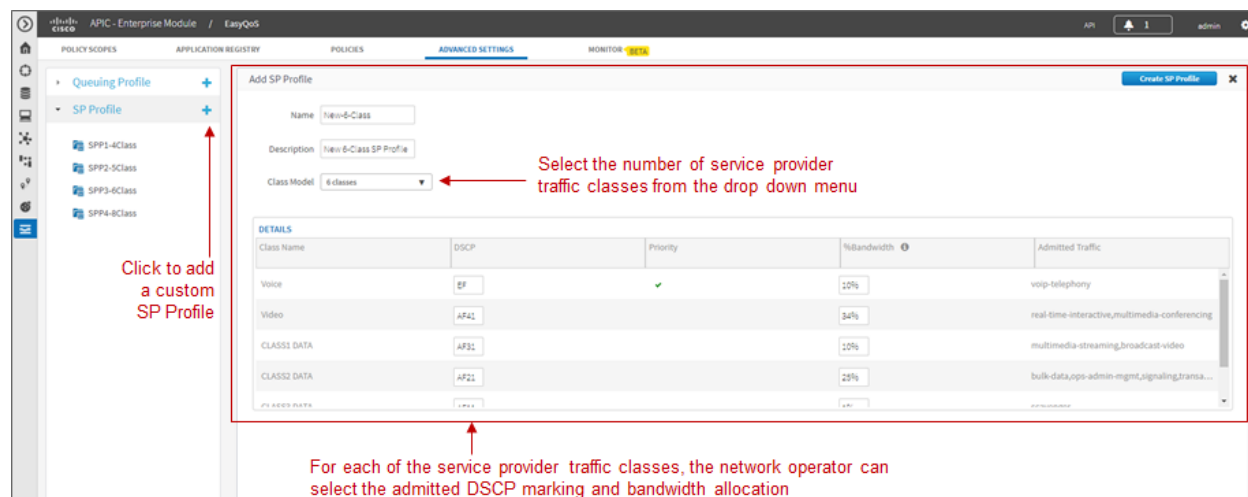
Admitted DSCP marking and bandwidth allocation to each service provider traffic class can be displayed by clicking on one of the profiles

The network operator can view the bandwidth allocations and the admitted DSCP markings for each of the service provider traffic-classes for each of the profiles by simply clicking one of the four default SP profiles.

- Note: If the QoS policy has previously been deployed, and if the selected default SP Profile has been deployed to devices within the policy scope, the devices and interfaces will be displayed within a panel at the bottom of the screen.

If the network operator determines that none of the four default SP profiles matches a managed-service WAN deployed on an interface on any of the devices within the policy scope, he/she can create a custom SP profile by clicking the blue + next to SP Profile in the upper left corner of the page. This will bring up a page similar to the following:

### 1. Creating a Custom SP Profile



Custom service provider profiles are based on the four default SP profile templates—meaning that custom SP profiles can only have 4, 5, 6, or 8 traffic-classes. The network operator must first select the number of classes in the custom SP profile through the drop-down menu next to Class Model. This will change the Details panel below it to reflect the number of traffic-classes in the model. The network operator can change the admitted DSCP marking to the service provider traffic-class or accept the default value. Likewise, the network operator can change the amount of bandwidth allocation to the particular service provider traffic-class, or accept the default value.

The Voice traffic-class is the only traffic-class that is mapped to a low-latency queue (LLQ), otherwise known as a priority queue. Because the Voice traffic-class is a priority queue, the remaining bandwidth allocations are technically bandwidth remaining allocations—which must total to 100%—regardless of the amount of bandwidth allocation provisioned to the Voice traffic-class.

When the network operator is satisfied with the admitted DSCP markings and bandwidth allocations for the service provider traffic-classes, he/she can click the Create SP Profile button in the upper right corner of the page in order to create the custom SP Profile.

The application of service provider profiles—regardless of whether they are one of the four default SP profiles, or a custom SP profile—to WAN interfaces is done automatically by APIC-EM. It is based on the network operator having previously configured a specific tag within the description of the WAN interface connected to a managed service WAN. This is discussed in detail within the **\*Service Provider Managed-Service WAN QoS Design\*** chapter.

## Policies

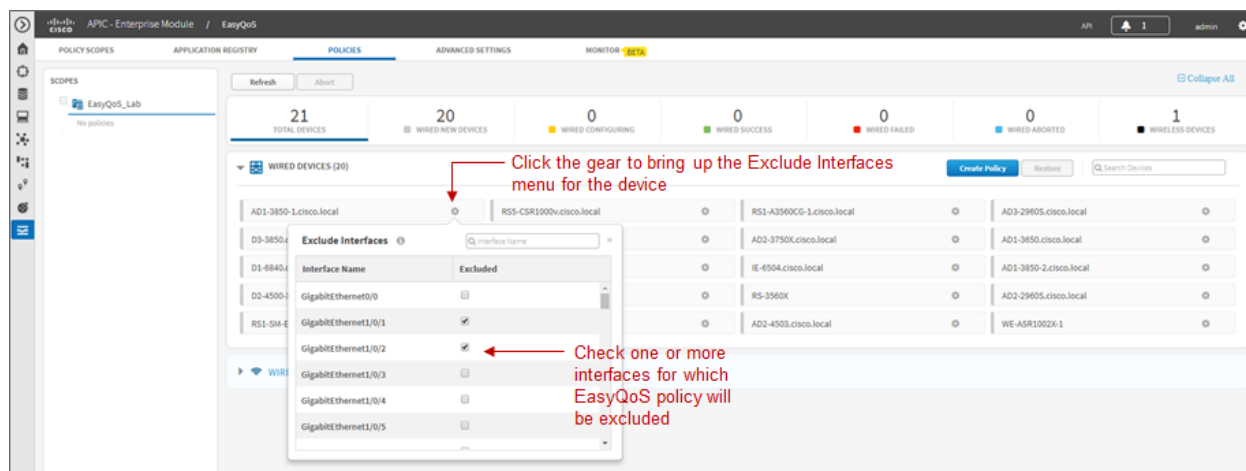
The next step to deploying QoS policy through EasyQoS is to access the Policies tab in order to create a policy under a scope.

### Excluding Interfaces

Before creating a policy, the network operator may wish to exclude certain interfaces on switch and router platforms from the policy. This may be done in situations where different QoS policies or configurations are required on the same router or switch platform. Because a router or switch platform can only be part of a single EasyQoS scope at any given time—and therefore have only one EasyQoS policy applied to it at a time—excluding interfaces provides additional functionality for the network operator to manually configure the desired QoS policy on those interfaces. Alternatively, interfaces may be excluded when the QoS policy provisioned by EasyQoS doesn't specifically meet the requirements of certain interfaces.

APIC-EM release 1.5 and higher provides the ability to exclude interfaces from the QoS policy provisioned by EasyQoS. Interfaces can be excluded by clicking the gear symbol to the right of the name of each switch or router platform within a policy scope, as shown in the figure below.

1. Excluding One or More Interfaces from EasyQoS Policy



This will bring up a drop-down menu listing the interfaces on the particular switch or router platform. The network operator can exclude interfaces simply by checking the Excluded box next to the name of each interface listed within the drop-down menu.

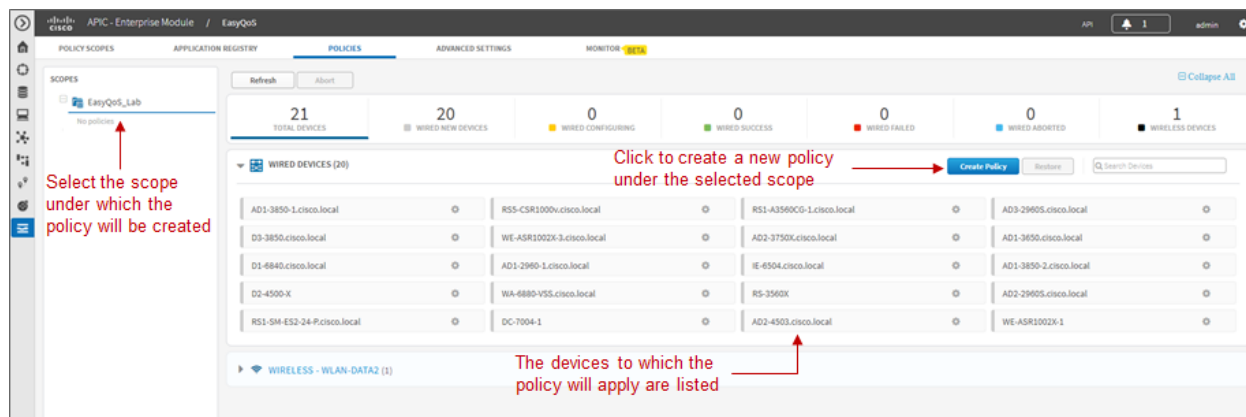
- Note: If a policy has already been applied to one or more devices, the network operator can still go into those devices and exclude interfaces. However, the policy has to be re-applied in order for the changes to take effect.

For port-channel configurations, if one physical interface which is a member of the port-channel is excluded, then all other physical interfaces that are members of the same port-channel should be excluded as well. QoS policy across the physical interfaces that are members of a port-channel configuration should be consistent.

## Creating Policies

When the network operator is done excluding interfaces on router and switch platforms within the policy scope, he/she can then begin creating the policy itself. An example is shown in the figure below.

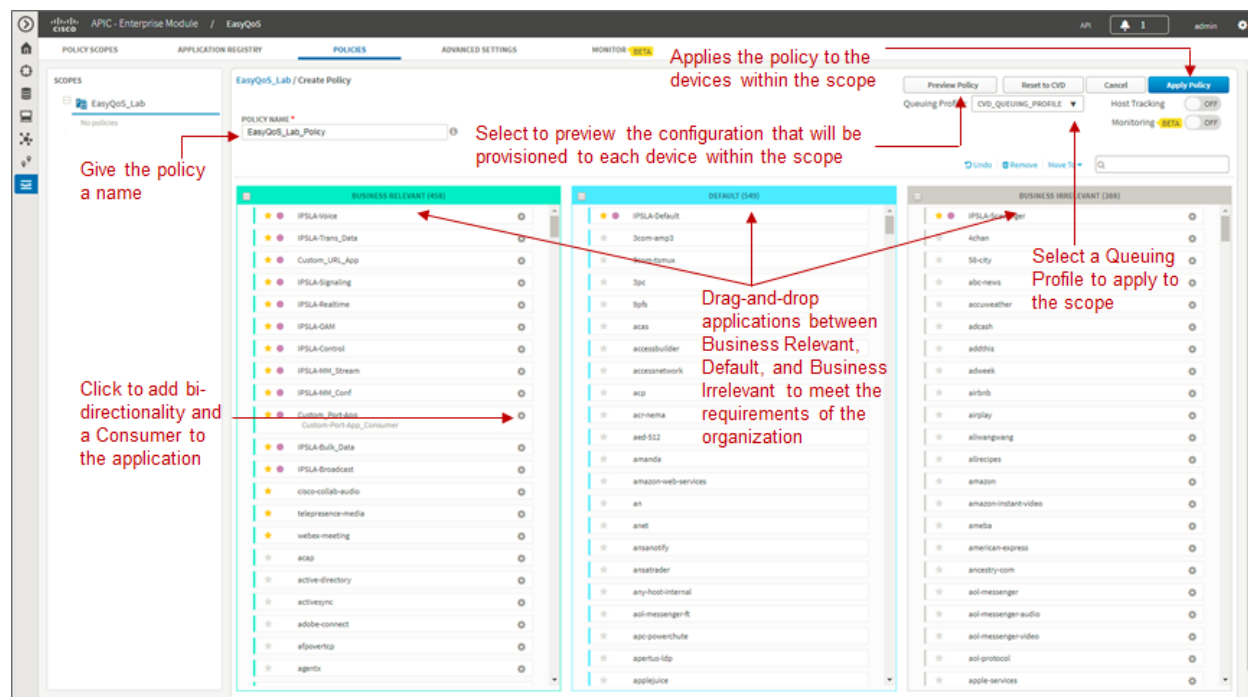
### 1. Creating a Policy Within a Policy Scope



Policies are created and applied per policy scope. Therefore policies only affect those devices that are part of the particular scope to which the policy is applied.

Clicking the Create Policy button brings up the screen used to create, configure, view, and apply the policy. An example is shown in the figure below.

### 1. Configuring EasyQoS Policy



It is mandatory to name each QoS policy. The purpose of the policy is as follows:

- To capture the application-level business intent of the network operator
- To apply a Queuing Profile to the policy
- To transform the business intent and Queuing Profile into network device QoS configuration for each device within the policy scope
- To apply the configuration to the devices within the policy scope
- Finally, to inform the network operator of the status of applying the policy to each device within the policy scope

The application-level business intent of the network operator is captured by dragging-and-dropping individual applications known via the Application Registry between the three business-relevance attribute values of Business Relevant, Default, and Business Irrelevant. All 1300+ applications known within the NBAR taxonomy have default settings for the business-relevance attribute. The network operator can simply choose to accept these default values, or customize as many applications as needed to meet the business requirements of the organization.

The network operator must also select the business-relevance attribute of Custom applications—either Business Relevant, Default, or Business Irrelevant, by dragging-and-dropping Custom applications into the appropriate grouping. By default, custom applications are Unassigned when they are created.

Changing the business-relevance of an application changes its QoS treatment across the network, as discussed in the **\*Mapping Business-Relevance to QoS Treatments\*** section of the **\*Strategic QoS Policy\*** chapter.

- Note: If a policy is applied before changing the business-relevance of the Custom application, the Custom application will not be included within the policy. However, because applications with a business-relevance of Default do not have any actual configuration generated on network devices for those applications, the Custom applications will in effect be treated with a business-relevance of Default across the network infrastructure.

As of APIC-EM 1.5 and higher, the network operator can choose to apply a custom Queuing Profile to a policy. The creation of Queuing Profiles was discussed in the **Queuing Profiles** section above. The network operator can choose to accept the default CVD\_Queueing\_Profile, or choose a custom Queuing Profile from the drop-down menu.

The application-level business intent and Queuing Profile is then transformed by APIC-EM EasyQoS into QoS configuration for each network device within the policy scope covered by the policy. The configurations are based upon

best practice recommendations for QoS configuration, compiled through years of CVD guidance.

### Consumers, Producers, and Bi-Directionality

The Policies page is where the network operator can choose to make the application bi-directional, as well as add a Consumer (a source IP address or IP address range, and/or source port or port range). This is done by clicking the icon next to the name of the application, which brings up a pop-up screen to edit the details of the application. An example using the Custom application discussed earlier is shown below.

#### 1. Adding Bi-Directionality and a Consumer to an Application

The screenshot shows the 'Custom\_Port-App' configuration window. The 'Advanced Policy Settings' section has 'Traffic Direction' set to 'Bidirectional' (selected with a radio button). The 'Consumer' section has a search field and a 'Cancel' button. The 'Add Consumer' section has a 'Consumer Name' field with the value 'Custom-Port-App\_Consumer'. Below this is a table with columns 'IP/Subnet', 'Protocol', and 'Port / Range'. The first row has '10.0.20.20' in the IP/Subnet field, 'UDP' in the Protocol dropdown, and '8100' in the Port / Range field. There is a '+' button to the right of the Port / Range field. Below the table are 'Cancel' and 'Create Consumer' buttons. At the bottom of the window are 'Cancel' and 'Save Settings' buttons. Red arrows point from text annotations to the 'Bidirectional' radio button and the '10.0.20.20' IP address field.

Creates the reverse ACE entries within ACLs for the application

Adds a Consumer (source IP address or range and source port or range) to the application

All Ingress classification & marking policies implemented on Catalyst switches use ACE entries within ACLs. Ingress classification & marking policies for Custom applications implemented on ISR and ASR platforms also use ACE entries within ACLs. These ACE entries are, by default, unidirectional. The bi-directional feature is intended to ensure that return traffic from an application is classified and marked correctly when the destination (the Producer) is not within a data center or on a server where the switch port to which the server is connected can be configured to trust the DSCP markings of traffic from the server.

- Note: On ISR and ASR platforms, ingress classification and marking policies involving any of the 1300+ applications known to the NBAR taxonomy are handled by the AVC/NBAR engine and are bi-directional.

As mentioned in the previous paragraph, ingress classification and marking policies implemented on Catalyst switches, as well as custom applications implemented on ISR and ASR platforms use ACE entries within ACLs. These ACE entries by default only specify a destination IP address or range of IP addresses, as well as a destination port or port range. The source is by default “any” device. In order to specify a source IP address or IP address range as well as a source port or port range, a Consumer is created and added to the application. This can be for a Custom application or for any of the 1300+ applications known to the NBAR taxonomy. The network operator accomplishes this by simply giving the Consumer a name, specifying a source IP address or IP address range, specifying whether the transport layer protocol is UDP or TCP, specifying a port or port range, and clicking the Create Consumer button. This, along with the choice for bi-directionality must be saved before closing the Edit Application Details pop-up screen.

The effects on ASR and ISR router configuration of adding bi-directionality and a Consumer are discussed in the **\*Custom Applications on ASR and ISR Platforms\*** section of the **\*Branch and WAN Static QoS Design\*** chapter. The effects on Catalyst switch platforms is discussed in the **\*Access-Control Lists\*** section of the **\*Campus LAN Static QoS Design\*** chapter.

### Reset to CVD

As applications are dragged-and-dropped between the Business Relevant, Default, and Business Irrelevant groupings within a given policy, the network operator may lose track of their original default settings. Likewise as bi-directionality and consumers are added to individual applications within a policy, the network operator may lose track of which applications have been set for bi-directionality and/or have consumers added. The network operator has the ability to reset the applications back to their original business-relevance attribute setting, and to remove bi-directionality and consumers within a given policy, by clicking the Reset to CVD button. Note that the selection of Favorites is system-wide (that is, across policies and policy scopes) and therefore unaffected by the Reset to CVD button.

### Policy Preview

Before applying the configuration, the network operator can optionally choose to preview the policy. This option is enabled by selecting the Preview Policy button within a policy. When Preview Policy is selected, an additional panel will appear as shown in the following figure.

#### 1. Generating a Policy Preview for a Device

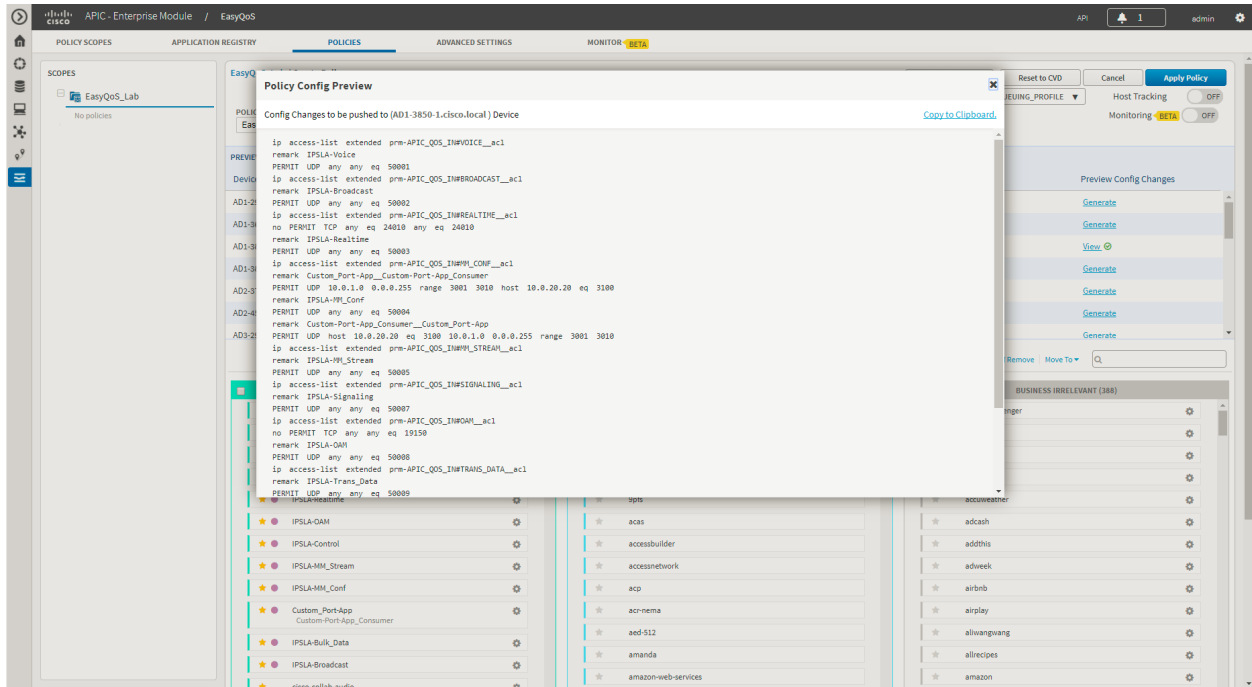
The screenshot shows the EasyQoS interface with the 'POLICIES' tab selected. The 'EasyQoS\_Lab / Create Policy' panel is active. The 'PREVIEW POLICY CONFIG' section displays a table of devices. The table has four columns: Device Name, Device Type, Device Role, and Preview Config Changes. The devices listed are:

Device Name	Device Type	Device Role	Preview Config Changes
AD1-2960-1.cisco.local	Cisco Catalyst 2960 Stack-able Ethernet Switch	ACCESS	Generate
AD1-3650-1.cisco.local	Cisco Catalyst 3650 stack-able ethernet switch	ACCESS	Generate
AD1-3650-2.cisco.local	Cisco Catalyst 3650 stack-able ethernet switch	ACCESS	Generate
AD1-3650-3.cisco.local	Cisco Catalyst 3650 stack-able ethernet switch	ACCESS	Generate
AD1-3750K.cisco.local	Cisco 3750 Stackable Switches	ACCESS	Generate
AD2-4503.cisco.local	Cisco Catalyst 4503-E Switch	DISTRIBUTION	Generate
AD3-2960S.cisco.local	Cisco Catalyst 2960S Stack-able Ethernet Switch	ACCESS	Generate

Red annotations highlight the 'Generate' and 'View' buttons. A red arrow points from the 'Generate' button to the 'View' button, with the text: "Click on 'View' to preview the configuration which will be provisioned to the device by EasyQoS". Another red arrow points from the 'Generate' button to the 'Generate' link in the 'Preview Config Changes' column, with the text: "Click 'Generate' to generate the configuration". A third red arrow points from the 'View' button to the 'View' link in the 'Preview Config Changes' column, with the text: "Link will change from 'Generate' to 'View' when the configuration has been generated".

The Preview Policy Config panel allows the network operator to generate the actual commands that will be provisioned to each device by EasyQoS. This is done by clicking the Generate link adjacent to the specific device. The Generate link will change to View when the configuration has been generated. Clicking the View link will bring up a pop-up window in which the configuration commands will appear. The configuration commands can then be viewed by scrolling up and down within the panel. An example is shown in the figure below.

#### 1. Displaying the Preview Configuration

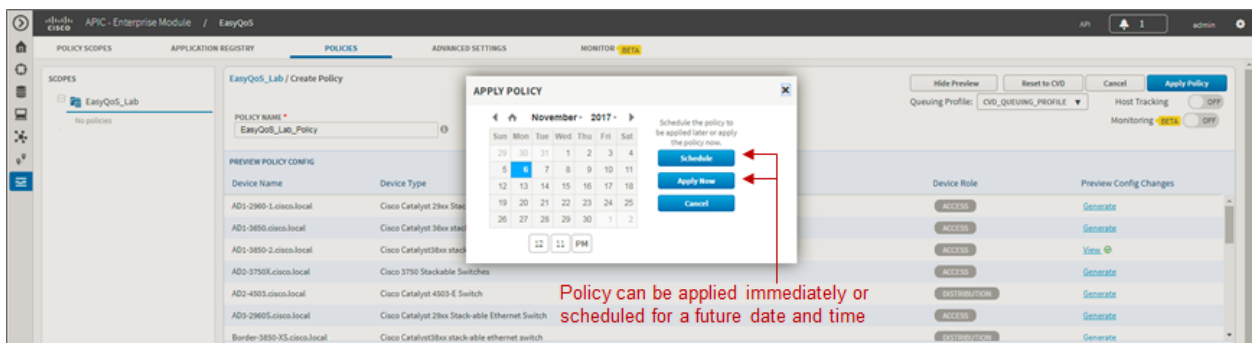


The preview policy option can be useful in uncovering potential errors in applying policy—such as an unsupported line card within a Catalyst 6500 Series switch for instance—before the policy is applied. The network operator can then take remedial actions, such as removing the device from the policy scope, or removing the line card from the switch—before applying the policy. Because the actual configurations that are provisioned by EasyQoS to each device are generated, this may also improve the time taken to deploy the policy to all of the devices within the scope, as well.

### Scheduling a Policy

When the network operator is satisfied with the policy, he/she can click the Apply Policy button in the upper right corner of the policy screen. This will bring up a pop-up window in which the network operator can immediately apply the policy, or schedule the policy to be applied at a future date and time. An example is shown in the following figure.

#### 1. Scheduling a Policy

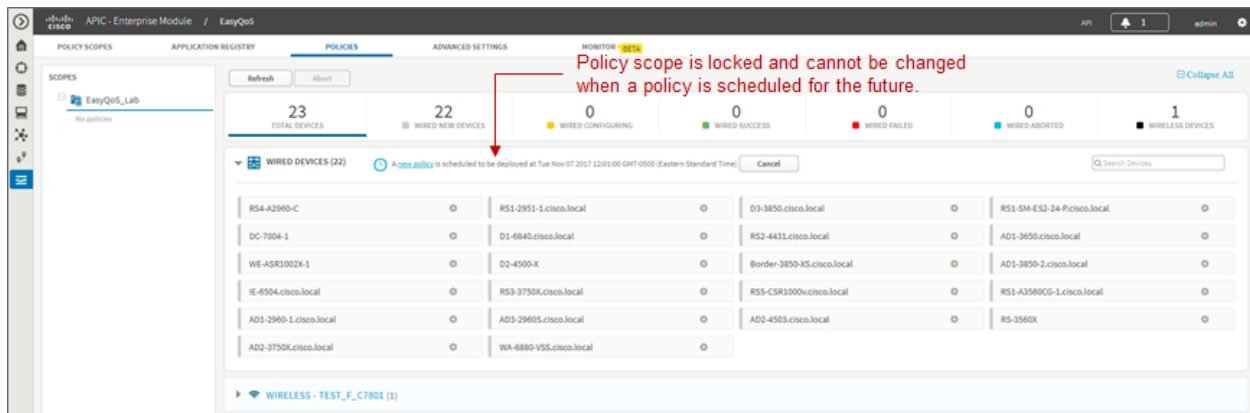


APIC-EM release 1.4 and higher supports the ability to schedule a policy at a future time and date. Scheduled policies are applied only once—meaning that a policy cannot be scheduled to reoccur every day, hour, etc.

When a policy is scheduled to be run at a future date and/or time, the policy screen will appear similar to the example in the figure below.

#### 1. Policy Scheduled for a Future Date and/or Time



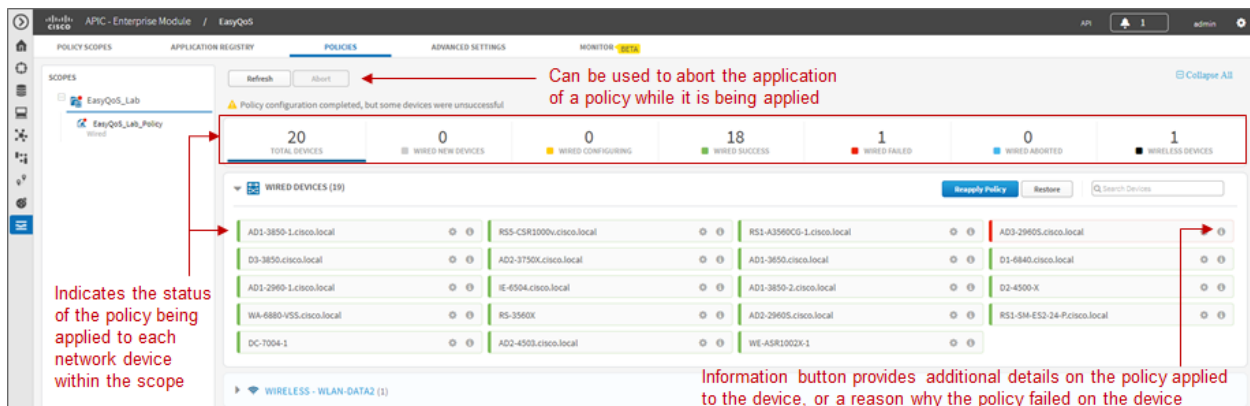


The policy scope to which the policy will be applied is locked when a policy is scheduled to be applied at a future date and/or time. This means the policy scope cannot be modified. The scheduled date and/or time cannot be modified once the policy has been scheduled. The network operator can only cancel the policy by clicking the Cancel button at the top of the policy screen, as shown in the figure above. Cancelling a scheduled policy will result in the policy being deleted if this is a new policy. If the policy is an update to an existing policy, then the updates will be lost if the scheduled policy is cancelled. EasyQoS provides a pop-up screen warning of the potential loss of the policy data and prompting for a confirmation before cancelling a scheduled policy.

### Policy Status

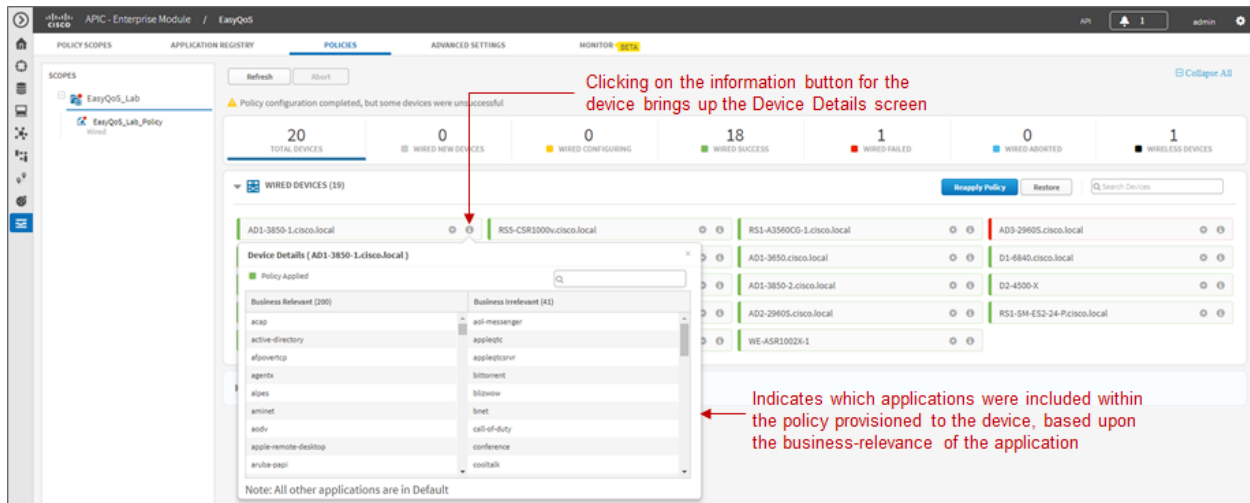
When a policy is applied, EasyQoS provides the status of the policy on each device—as the policy is being applied. Initially each device will appear with a gray bar next to it—indicating that no policy is applied (if this is a new device to EasyQoS with no policy). A yellow bar next to a device indicates that policy is currently being configured onto the device. Finally, a green bar next to the device indicates that the policy has successfully been provisioned onto the device. An example of the policy being applied to devices within the scope is shown in the following figure.

#### 1. Policy Status



Clicking the information button next to each network device brings up a popup window with Device Details. The Device Details window serves two purposes—depending upon whether the policy was successfully applied to the device or not. If the policy was successfully applied to the device, clicking the information button next to the device will display the applications which were deployed in the policy provisioned to the device—based upon the business relevance of each application. An example is shown in the figure below.

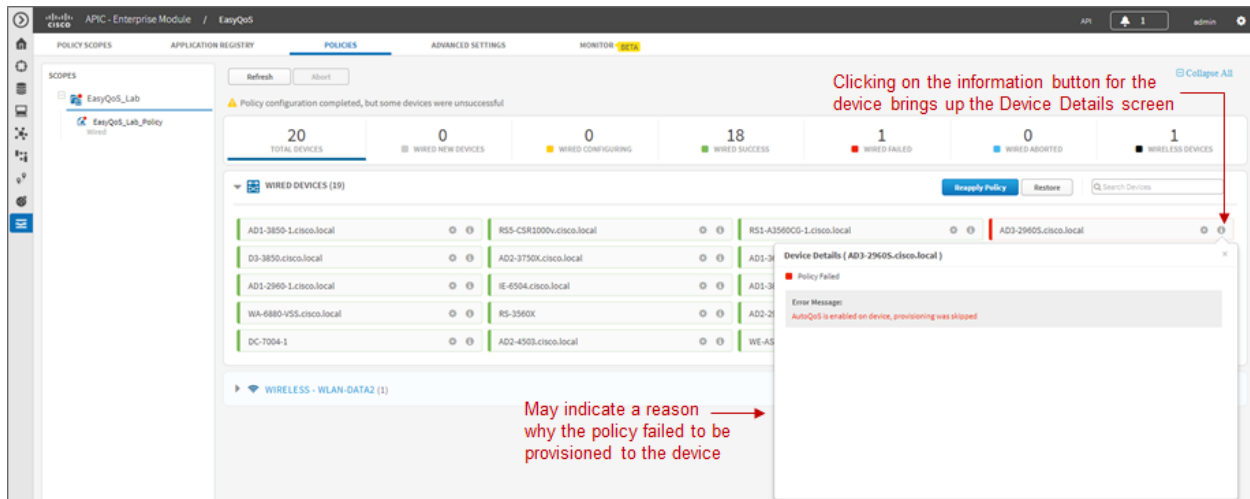
#### 1. Device Details when Policy is Successfully Applied to a Device



Only applications which are business-relevant or business-irrelevant are configured into policies on switch, router, and AireOS WLC platforms. Applications with default business relevance receive best effort treatment, and therefore do not show up within the policy provisioned to network devices.

If the policy failed to be applied to the device, clicking the information button next to the device may display a reason why the policy failed. An example is shown in the figure below.

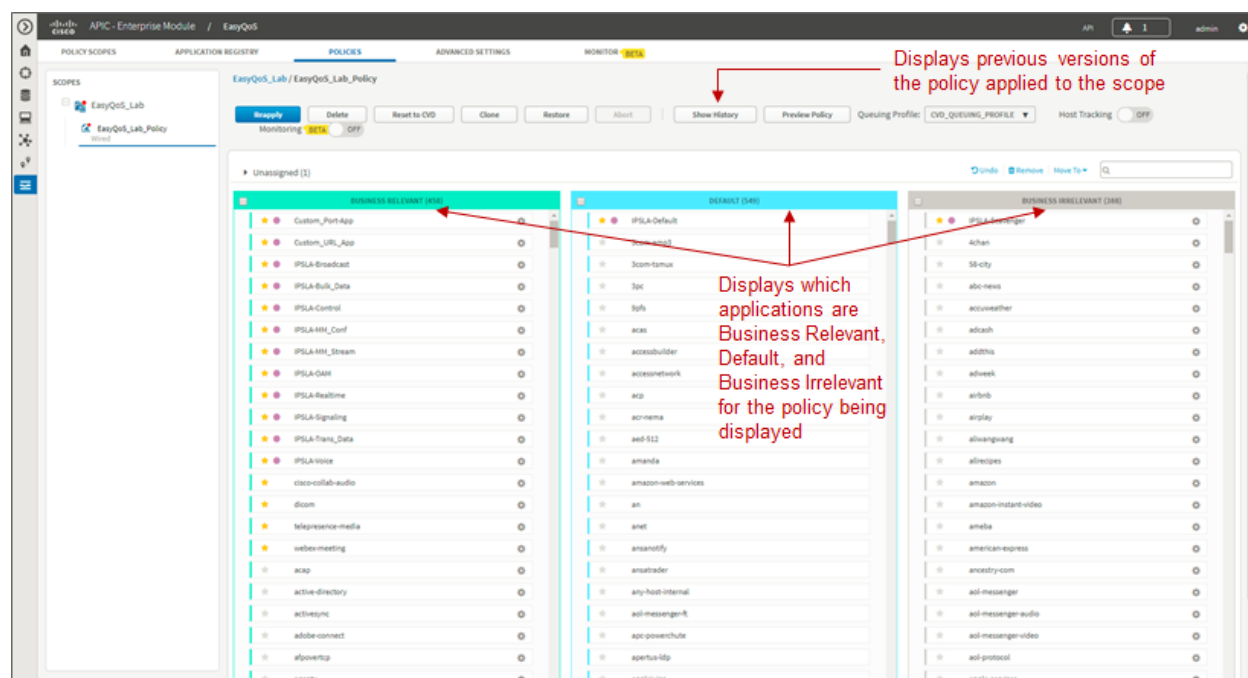
#### 1. Device Details when Policy Fails to be Applied to a Device



In the example above, the information within the Device Details screen indicates that policy was skipped because AutoQoS is currently enabled on the switch platform. EasyQoS currently does not support provisioning QoS policy to devices with AutoQoS enabled. In this case, the network operator can manually remove AutoQoS configuration and resync the device before attempting to re-apply policy. Alternatively, the network operator can simply remove the device from the policy scope.

After a policy has finished being applied to devices within the policy scope, clicking the name of the policy within the left-hand panel displays the policy, as shown in the following figure.

#### 1. Displaying a Policy



The network operator's business intent—in terms of the business-relevance of applications—is applied per policy. This means that applications can be assigned different business-relevance attributes in different policies. Here the network operator can view which applications are Business Relevant, Default, and Business Irrelevant for the policy being displayed.

### Abort

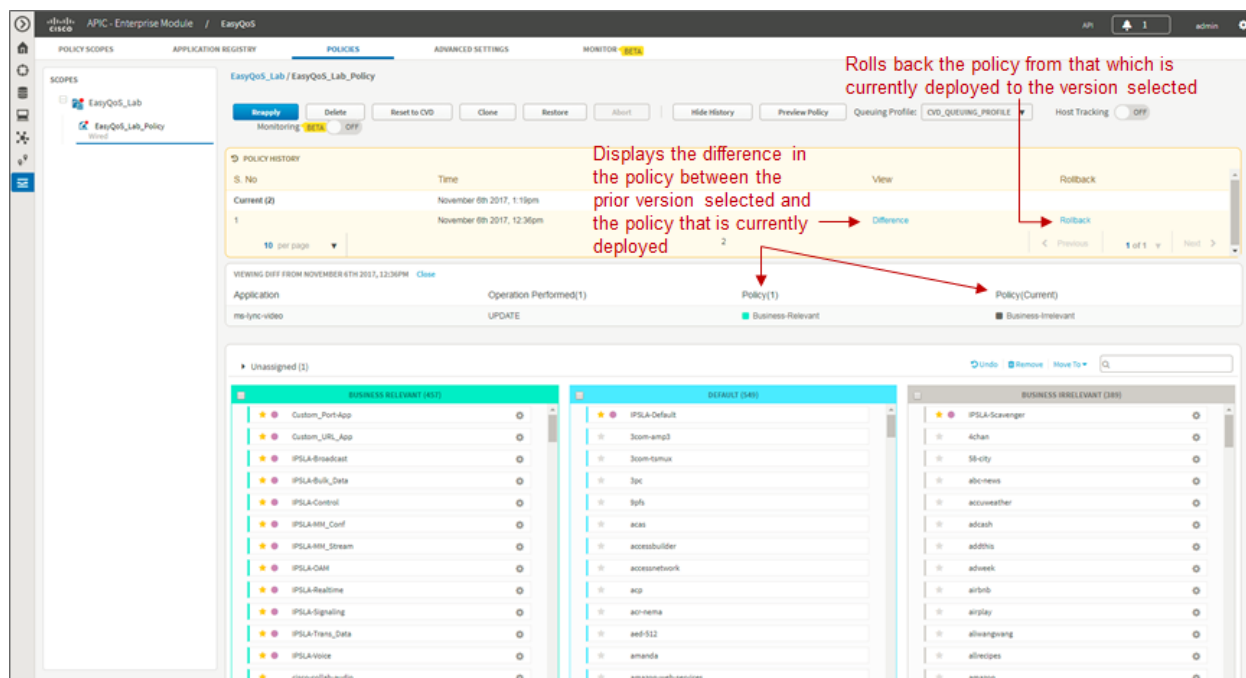
The network operator can abort the provisioning of the policy to network devices after the policy provisioning has begun, but before the policy provisioning process has completed, by clicking the Abort button. EasyQoS provisions multiple (up to 40) devices at a time. Hence, the abort option is only useful when there are a large number of devices (more than 40) within a policy. Rather than waiting for the entire policy to be provisioned to each device, and then either rolling back the policy or restoring the configuration, the network operator can instead terminate the provisioning of the policy with the Abort button. For policies with a small number of devices, it may be more effective to allow the policy to complete and then either Rollback the policy or Restore the devices to their configuration before EasyQoS policy was applied.

When the Abort button is pressed, EasyQoS cancels the provisioning process only on network devices that have not yet been started to be configured. A light blue bar next to these devices will indicate a status of Policy Aborted for these devices. For devices that have started to be configured, EasyQoS will complete the provisioning of the policy. For devices for which the provisioning of the policy has been completed before the Abort button was pressed, EasyQoS will leave the policy on the device and will update the status of each of these devices—a green bar for Success or a red bar for Failed—based on the outcome of the provisioning of the policy to the device. The network operator can then either Rollback the policy or Restore these devices to their original configuration before EasyQoS policy was applied.

### History, Rollback, and Clone

Clicking the Show History button within a policy opens a new Policy History panel in the center of the page, as shown in the following figure.

#### 1. Show History



The Policy History panel displays previous versions of the policy selected. The network operator can view the changes in the policy that have been made in the various versions by selecting the Difference feature under a particular prior version. This will display the difference in the policy between the prior version selected and the policy that is currently deployed (it does not display the difference in policy between the prior version selected and the next lower prior version).

The difference in policy is represented in terms of applications—meaning certain applications may have been moved between business relevance, certain applications may have been added or deleted from the Favorites, or custom applications may have been added or deleted. The Difference feature does not display the difference in the actual configuration applied to each network device.

The Rollback feature under a particular prior version can be used to roll back the policy from that which is currently deployed, to the particular prior version selected. This feature is useful in change management scenarios, where a particular change is found to be undesirable and the network infrastructure needs to be rolled-back to the state it was in prior to the change being implemented.

Finally, the Clone button can be used to copy the entire policy. Upon clicking the Clone button, the network operator will be asked to enter a new policy name for the cloned policy and to select a policy scope to which the new cloned policy will be applied. With complex policies, the network operator can save administrative time by not having to duplicate the same policy across multiple policy scopes. After the policy is cloned, the network operator is free to modify it as needed for the particular policy scope.

#### Restore and Delete

The Restore button deletes an EasyQoS policy and attempts to restore the QoS configuration on all devices covered by the EasyQoS policy back to the original configurations before any EasyQoS policy was applied. Because the EasyQoS policy is deleted when the network operator selects the Restore button, there is no ability to retry the Restore function if it does not succeed in restoring the configuration of all devices to their original (pre-EasyQoS) configuration. This behavior is similar to when the network operator selects the Delete button, in that the EasyQoS policy is deleted. There is no ability to retry the delete function, either.

- Note: If the first attempt to provision an EasyQoS policy to a device (meaning the device initially has no EasyQoS policy) fails, EasyQoS will also automatically attempt to restore the QoS configuration on that device to its original (pre-EasyQoS) configuration.

The network operator should be aware that if a device is removed from an EasyQoS policy after the policy has been

applied to the device, the EasyQoS policy will remain on that device. In other words, EasyQoS will not automatically attempt to delete the QoS policy provisioned to the device, nor will EasyQoS attempt to restore the QoS configuration on that device to the original (pre-EasyQoS) configurations.

The Restore button will also not restore the QoS configuration on that device to the original configuration if the original configuration was already an EasyQoS configuration. This situation may occur when upgrading from APIC-EM 1.2 to APIC-EM 1.3 or higher. APIC-EM did not collect the information required to restore the original configuration before provisioning policy in APIC-EM version 1.2.

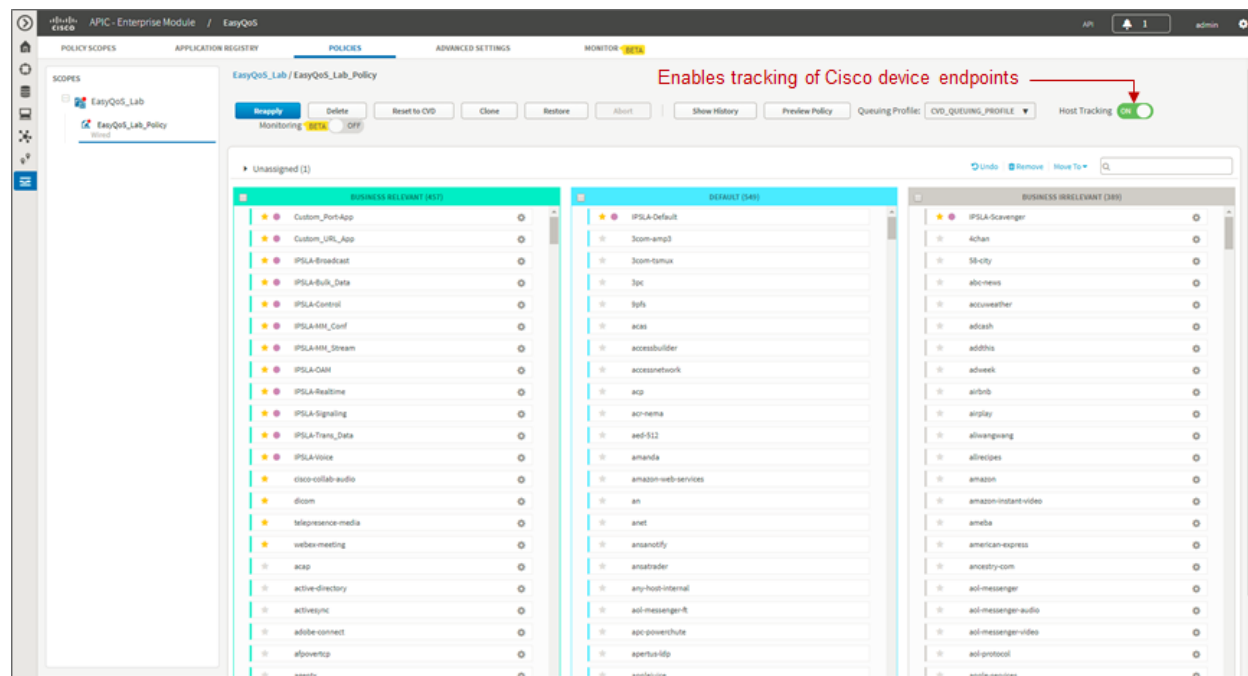
Finally, there are some parts of the EasyQoS policy that may not be restored, depending upon particular network device platform. The **\*Pre-Existing QoS Configuration on ISR and ASR Router Platforms\*** section of the **\*Branch and WAN Static QoS Design\*** chapter details what is restored and not restored on router platforms when clicking the Restore button. Likewise, the **\*Pre-Existing QoS Configuration on Switch Platforms\*** section of the **\*Campus LAN Static QoS Design\*** chapter details what is restored and not restored on switch platforms when clicking the Restore button.

- Note: When an EasyQoS policy is deleted for MLS QoS based switches, the network operator should resynchronize any devices which were part of the policy before applying any new QoS policies. This can be accomplished either by waiting until the polling interval has been exceeded before applying the new policy, or by performing a manual resync of the devices. This will ensure that APIC-EM has the current configuration state of the devices within its database before provisioning EasyQoS policy.

## Host Tracking

The Host Tracking feature allows EasyQoS to track Cisco device endpoints discussed within the **\*Host Inventory\*** section above, and dynamically apply access-control list entries (ACEs) to the switches to which the devices are connected, as the devices are moved. The ACEs match the voice and video traffic generated by the devices. The Host Tracking feature is enabled per EasyQoS policy through the toggle button shown in the following figure.

### 1. Enabling Host Tracking



The Host Tracking feature can be enabled as the EasyQoS policy is being created, or after the EasyQoS policy has been created. However, the policy will need to be reapplied to the policy scope if the Host Tracking feature is enabled after the policy has been created. The specific policy configuration created and provisioned to Cisco Catalyst switches, for each device endpoint, is discussed in the **\*Cisco Device Endpoints\*** section of the **\*Campus LAN Static QoS Design\*** chapter.

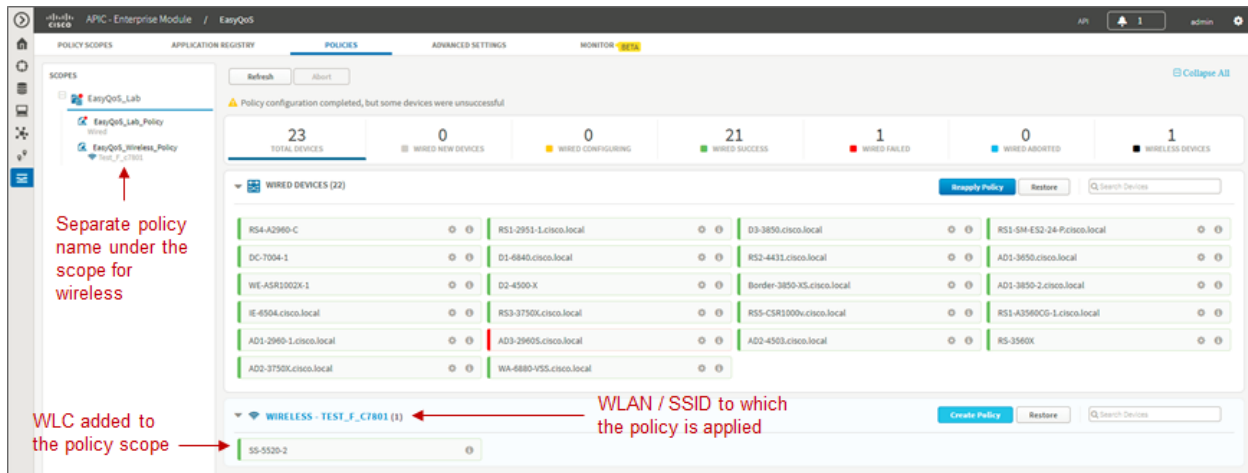
## Wireless Policies

Cisco AireOS WLCs can also be added to policy scopes by dragging-and-dropping the device into a particular policy scope. Optionally, a separate policy scope can be created for wireless devices. Wireless policies are deployed per WLAN/SSID. If there are multiple WLANs/SSIDs to which EasyQoS policies need to be applied, then the network operator must create a policy for each WLAN/SSID.

A wireless policy (separate from the policy applied for wired devices) must be created under the policy scope. This is done by clicking the blue Create Policy button adjacent to the name of the WLAN/SSID within the Wireless section of the page. As with wired policies, the wireless policy must be given a name; individual applications can be moved between Business-Relevant, Default, and Business-Irrelevant groupings; bi-directionality can be selected for individual applications; and the policy can be previewed before being deployed.

An example of a wireless policy created within an existing policy scope is shown in the figure below.

### 1. Adding a Wireless Policy to a Policy Scope



Clicking the wireless policy displays the policy, as shown in the figure below.

### 1. Displaying a Wireless Policy

#### image56l

APIC-EM release 1.6 provides the ability for the network operator to specify whether or not he/she wants to enable the FastLane feature on the WLAN / SSID. The default setting is for the FastLane feature to be disabled. The WLC to which the WLAN / SSID belongs must be running AireOS release 8.3.112 or higher code on order to support the Fastlane feature. Previously with APIC-EM release 1.5, if the WLAN / SSID belonged to a WLC which could support the FastLane feature, the FastLane feature was automatically enabled when EasyQoS policy was provisioned. The FastLane feature is discussed further in **\*Chapter 10: WLAN QoS Design.\***

Applications known via the AVC/NBAR engine within the AireOS WLC are displayed in groupings of Business Relevant, Default, and Business Irrelevant. The network operator can drag-and-drop the applications between the three groupings in order to match the business intent of the organization.

The AVC/NBAR based classification & marking policy deployed to AireOS WLCs specifies an action of mark, rather than drop. For Business Relevant applications, the DSCP marking is by default based on the value of the traffic-class attribute assigned within the NBAR taxonomy. For Business Irrelevant applications, the DSCP marking is by default set to CS1 (DSCP 8). However, DSCP markings for individual applications can be changed within the application registry. DSCP markings for entire traffic-classes can be changed through a custom Queuing Profile applied to the wireless policy. Applications with a business-relevance attribute of Default are not programmed into the AVC/NBAR policy. The AVC/NBAR policy overrides the QoS Profile applied to the WLAN/SSID. Because EasyQoS sets the Maximum Priority field within the QoS Profile to a setting of Voice, for wireless devices which support QoS,



applications with a business-relevance attribute of Default are not reset to a DSCP value of Best Effort (DSCP 0). Instead, the WLC allows such applications to pass through with their DSCP values unaltered.

AireOS WLCs support up to 32 applications per QoS Policy. This is a current limitation of the AVC/NBAR engine within AireOS WLCs. By default, EasyQoS will select the 32 applications that get programmed into the wireless policy based upon which applications are selected as Favorites and then based upon the popularity attribute pre-configured for all of the 1300+ applications within the NBAR taxonomy.

Because the network operator has no view of the popularity attribute for any given application within the NBAR taxonomy, there are two methods by which the network operator can guarantee which 32 applications are provisioned into the AireOS AVC/NBAR-based classification & marking policy. Note that the AVC/NBAR-based policy can have less than 32 applications as well, if desired by the network operator.

- In the first method, the network operator can select up to 32 applications as Favorites. APIC-EM will provision applications marked as Favorites before provisioning other applications within the NBAR taxonomy. However, because the choice of Favorites is a global setting—meaning the selection of Favorite applications is the same across all policies in all policy scopes—this may not be an ideal solution.
- In the second method, the network operator can highlight all applications within each of the three groupings—Business Relevant, Default, and Business Irrelevant—via the checkbox at the top of each group. The network operator can then remove all of the applications. This will place all applications for the wireless policy in the Unassigned group. The network operator can then use the search field in the upper right corner of the page to search for each application he/she wants to add back into the policy. Upon locating the application, the network operator must drag-and-drop that application from the Unassigned group into either the Business Relevant or Business Irrelevant grouping. In this manner, the network operator can add up to 32 applications into the wireless policy and ensure they will be provisioned to the AireOS WLC.

As of APIC-EM version 1.3 and higher, the default behavior of the AVC/NBAR-based classification & marking policy is to mark in the upstream direction only. In order to implement bi-directional policies, the network operator must configure bi-directionality for the application. This is done the same way as discussed for Custom applications in the **\*Policies\*** section above.

Finally, the network operator should note that Custom applications—regardless of whether they are URL-based or port-based—are not provisioned into the AVC/NBAR-based classification & marking policy of WLC platforms. This is a current limitation of AireOS WLC platforms, in that they do not support the ability to define custom applications within the AVC/NBAR policy.

Upgrading from APIC-EM Release 1.3 to APIC-EM Release 1.4 and Higher

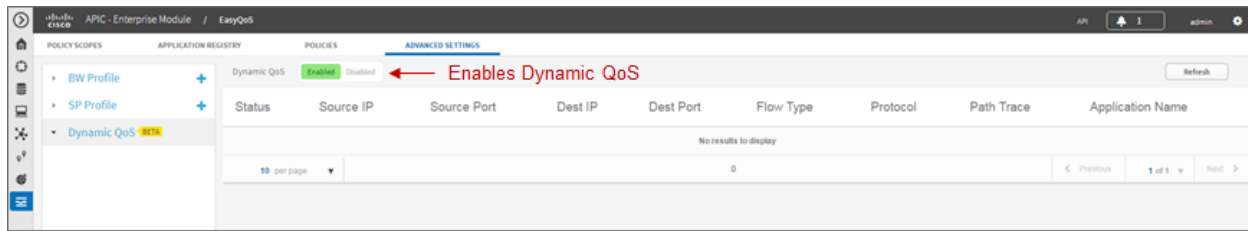
The NBAR protocol pack has been upgraded from version 14.0.0 in APIC-EM release 1.3 to version 27.0.0 in APIC-EM release 1.4 and higher. NBAR protocol pack version 27.0.0 includes additional applications not found in protocol pack 14.0.0. Additionally, some attributes, such as the traffic-class to which an application belongs, may change between protocol pack revisions. This may be the result of better knowledge of how a particular application is used within customer networks over time or the result of changes in how the application itself is used within customer networks over time. Application changes appear as stale applications upon upgrading from APIC-EM release 1.3 to release 1.4 or higher. The network operator should re-apply policies to policy scopes in order to update these stale applications.

## Dynamic QoS

For the APIC-EM 1.6 release, Dynamic QoS is still a Beta application within EasyQoS. In order to enable Dynamic QoS, the network operator must access the Advanced Settings tab and then click Dynamic QoS to bring up the screen shown in the figure below.

1. Enabling Dynamic QoS

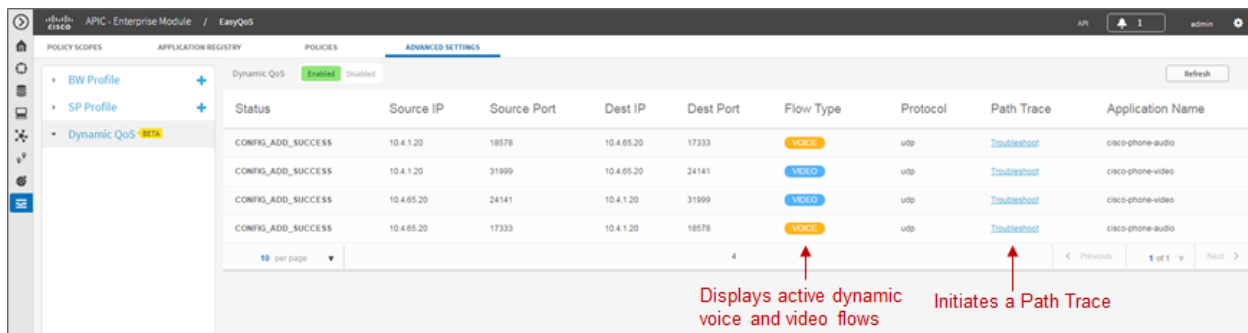




For APIC-EM 1.6 Dynamic QoS is a feature that is enabled globally—meaning across all policy scopes—through the sliding button shown in the figure above. Upon re-applying static QoS policy to a given policy scope, EasyQoS will then provision Dynamic policy-map shells to access-layer switches within that policy scope. The Dynamic policy-map shells are discussed within the **\*Dynamic QoS Design\*** chapter of this document.

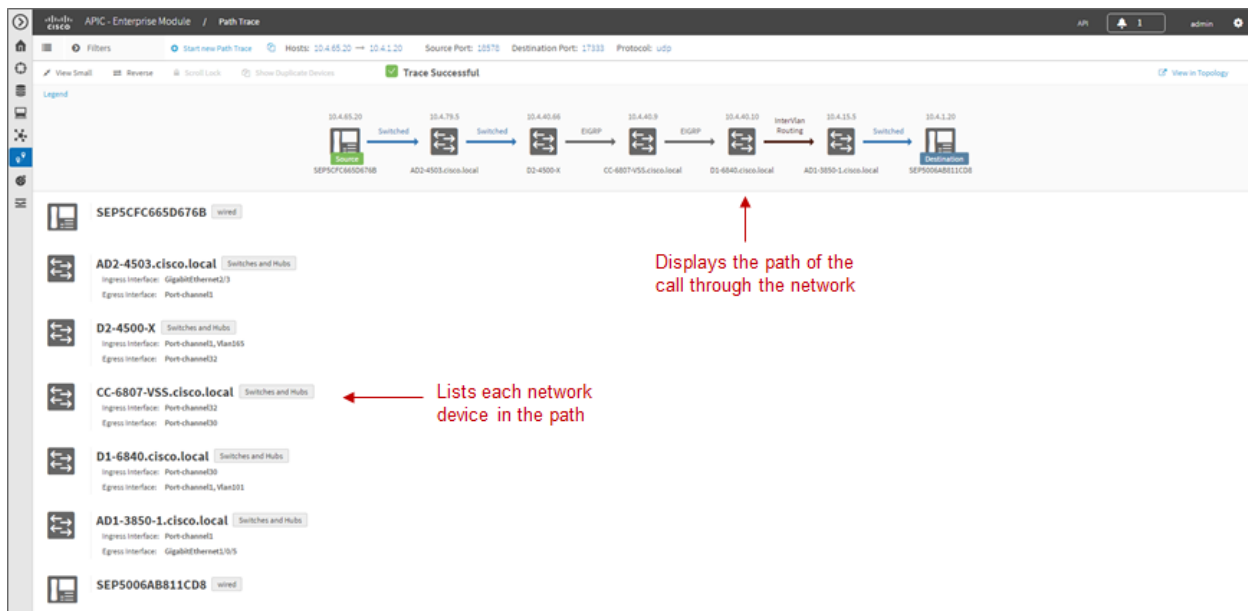
The Dynamic QoS screen displays the status of Dynamic QoS flows when they are active. Dynamic QoS flows are initiated when call signaling systems, such as CUCM, use the northbound REST-based API to signal to APIC-EM that a call has been established. An example of an active Dynamic QoS session—representing a voice call between two endpoints—is shown in the figure below.

#### 1. Example of an Active Dynamic Voice Call



The Path Trace tool can be used to troubleshoot active Dynamic QoS flows by displaying the path of the traffic through the network infrastructure between the endpoints. An example of the Path Trace tool is shown in the figure below.

#### 1. Example of the Output of the Path Trace Tool for a Dynamic Flow



The Path Trace tool displays the path of the traffic associated with the Dynamic QoS flow through the network in-

frastructure within the top panel of the display. The lower panel provides more detail regarding each of the network devices through which the Dynamic QoS flow passes.

APIC-EM release 1.4 and higher enhanced the REST-based API for Dynamic QoS flows. The API call can now include an Application Name. The Application Name can be used to match one of the existing applications within the NBAR taxonomy or a Custom application. The traffic-class attribute for the Custom application or the application within the NBAR taxonomy must be VoIP Telephony, Multimedia Conferencing, or Real-Time Interactive. EasyQoS will generate an error when an API call attempts to set up a Dynamic QoS flow that includes the Application Name, if the application does not have a traffic-class attribute which matches one of these three traffic-classes.

When call signaling systems, such as CUCM, use the northbound REST-based API to signal to APIC-EM that a call has been terminated, APIC-EM will remove the entry for the Dynamic QoS flow. The **\*Dynamic QoS Design\*** chapter of this document has further details regarding the operation of Dynamic QoS.

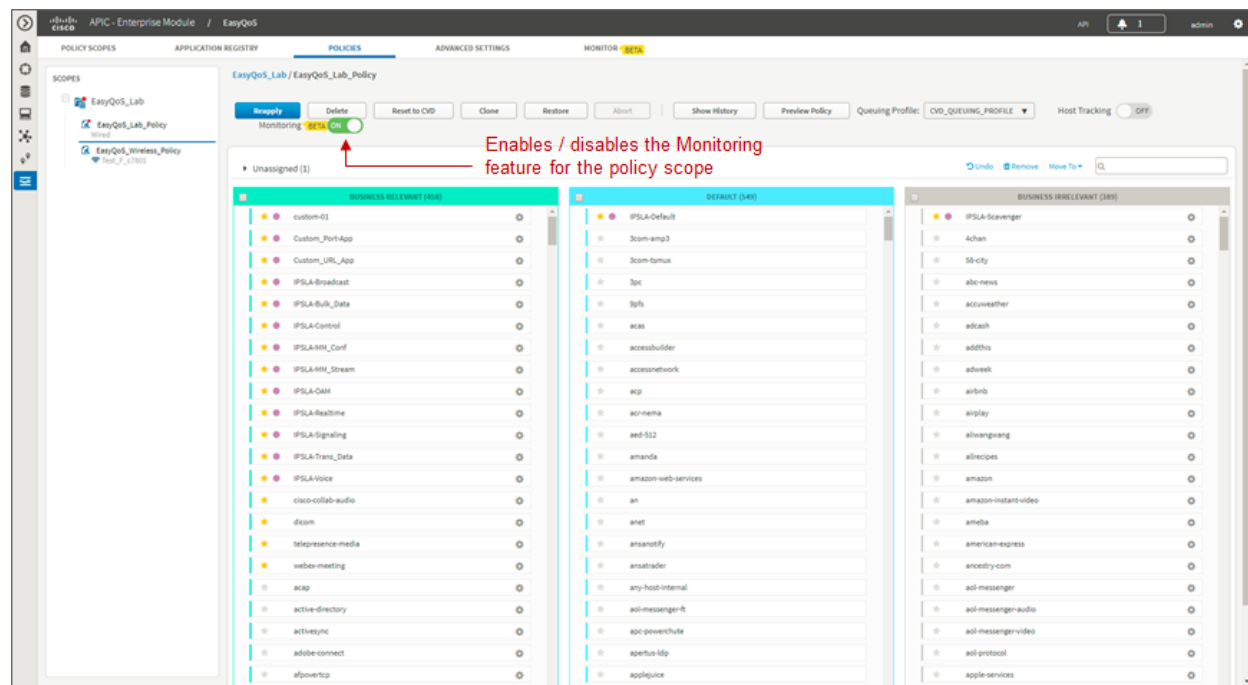
## 1.5 Chapter 5: EasyQoS Monitoring (Beta)

For APIC-EM release 1.6, EasyQoS Monitoring is a Beta feature. The Monitoring feature provides the ability for the network operator to monitoring the health of WAN-connected interfaces on routers to which EasyQoS policy has been applied. Health scores are based solely on packet loss for this release. Future versions of EasyQoS Monitoring may extend the functionality to include additional parameters such as end-to-end latency, jitter, application latency, etc. into the overall health score.

Enabling the Monitoring Feature

The Monitor feature is enabled per policy scope via the sliding button adjacent to Monitoring within the EasyQoS policy screen, as shown in the following figure.

### 1. Enabling EasyQoS Monitoring



The EasyQoS policy should be re-applied to the policy scope after enabling the Monitoring feature. The Monitoring feature will add the following interface-level configuration command to all WAN-facing interfaces on ASR 1K, ISR 4K, ISR G2, and ISR 800 Series routers which support an Active NBAR2 license.

```
ip nbar protocol discovery
```

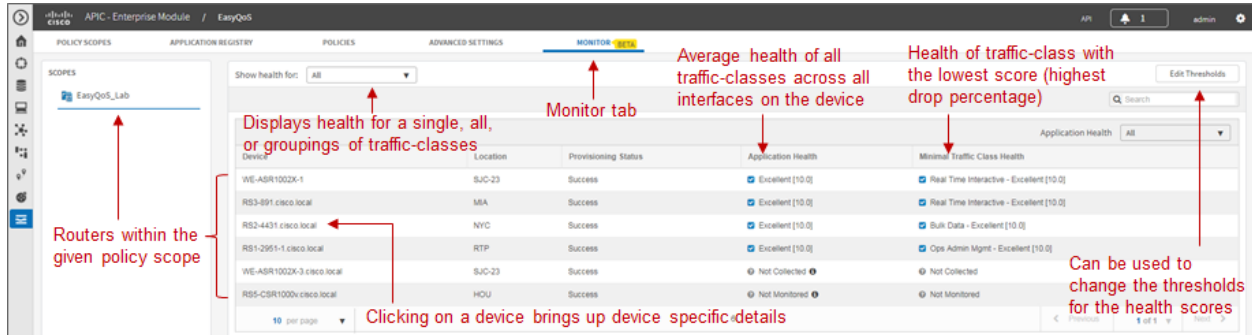
This command is necessary in order to display per-application statistics on ISR and ASR router platforms when drilling down into an interface. This feature will be available in future releases.

### Device-Level Statistics

Device-level statistics may take approximately 20 minutes to appear after enabling the Monitoring feature. This is because EasyQoS polls statistics collected on the WAN interfaces periodically (by default every 10 minutes). Information is not displayed within the GUI until at least two polling cycles have passed.

After the Monitoring feature has been enabled, the network operator can click the Monitor tab in order to bring up a device-level view, as shown in the figure below.

#### 1. Device Level Statistics with All Traffic-Classes Selected



The device-level view displays the router platforms within the selected policy scope, and the status of the Monitoring feature on those devices. Application health can be displayed for all traffic-classes, a single traffic class, or groups of traffic-classes (Data, Video, or Control). The network operator can select this through the drop-down menu next to the **Show health for:** field, shown in the figure above.

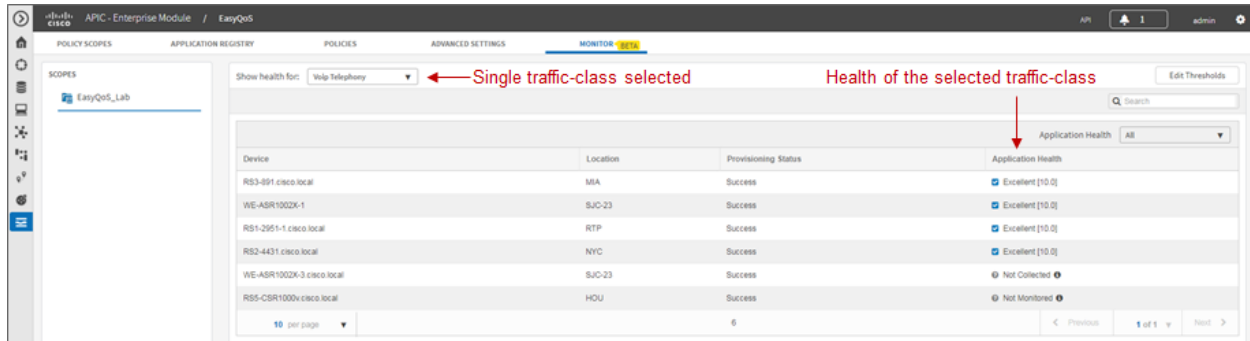
If all traffic-classes have been selected, the Application Health column in the figure above represents the arithmetic mean (average) of the health scores across all traffic-classes and WAN interfaces for the given router. The Minimal Traffic Class Health column displays the traffic-class with the minimal application health score on the given router. Status for these columns can be one of the following:

- An application health score is being generated for the router platform. This indicates that monitoring statistics are being collected on one or more interfaces on the router.
- Not Monitored. This status indicates the router is not being monitored. This status can occur if the router does not support NBAR—meaning it does not have an Active NBAR license—or does not have any WAN-connected interfaces.
- Collection Failure. This status indicates there was an error in collecting statistics from the device for the previous cycle. Therefore the health score could not be calculated.
- Not Collected. This status indicates that no monitoring statistics are being collected for the router. In this situation, the router is capable of being monitored. However, monitoring statistics are not available because either the first health data sample was not collected or the number of monitored interfaces exceeds the supported number of 1,000 interfaces.
- Note: Application health scores are calculated based upon the percentage of drops within each traffic-class over the previous collection interval. By default, the collection interval is 10 minutes. Therefore, the application health score shows the health over the past collection interval only. There is currently no history, regarding application health scores, maintained within APIC-EM. Future versions of the Monitoring feature may extend this functionality to provide the network operator the ability to view historical health scores over selected time periods.

The application health score consists of both a 'grade'—Excellent, Good, Fair, Poor, Bad, or Critical—which is based upon configurable drop thresholds, and a value from 0.0—10.0. The application health score is based upon the percentage of packet drops seen within each of the traffic-classes configured on the WAN interfaces of the router.

If a single traffic-class is selected, then only a single health score column appears in the device-level view, as shown in the figure below.

### 1. Device-Level Statistics with Single Traffic-Class Selected

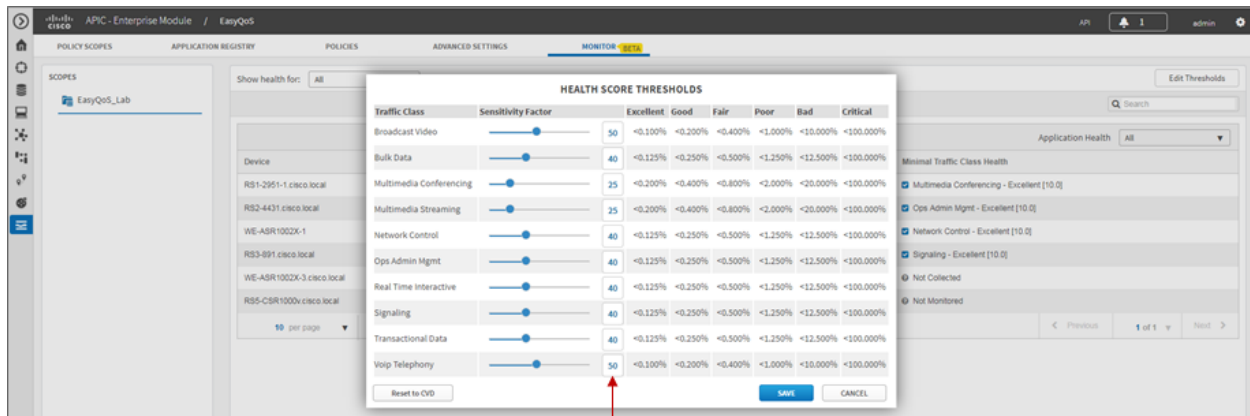


The drop-down menu adjacent to Application Health allows the network operator to filter the output based on the status for the router. For larger deployments this may assist in identifying areas of trouble more quickly. For example, it may be desirable to display only those routers that have a status of collection failure. This would indicate some problem with the collection of health scores on the devices displayed. Alternatively, the network operator may wish to display routers with a health score of critical, in order to allocate resources toward troubleshooting the routers with the most immediate issues first.

### Sensitivity Factor and Health Score Thresholds

The network operator can view and modify the thresholds for each traffic-class used to calculate the application health score by clicking the Edit Thresholds button shown in the figure above. This brings up the Health Score Thresholds popup window shown in the figure below.

### 1. Modifying Health Score Thresholds



Changing the Sensitivity Factor modifies the drop thresholds for that traffic-class

For each traffic-class, the network operator can modify the Sensitivity Factor—either via the slider, or by typing in a value in the box adjacent to each traffic-class. The Sensitivity Factor is used to set the maximum drop percentages acceptable for each of the thresholds (Excellent, Good, Fair, Poor, Bad, and Critical). It has a range from 0 to 100.

The default values for the Sensitivity Factor for each traffic-class are derived from industry standards. In particular, IETF RFC 4594 specifies the expected tolerances to packet loss for each of the 12 traffic-classes—as shown in the following table.

### 1. Service Class Characteristics from IETF RFC 4594

Service Class Name	Tolerance to Loss
Network Control	Low
Telephony	Very Low
Signaling	Low
Multimedia Conferencing	Low-Medium
Real-Time Interactive	Low
Multimedia Streaming	Low—Medium
Broadcast Video	Very Low
Low-Latency Data (Transactional Data)	Low
OAM	Low
High-Throughput Data (Bulk Data)	Low
Standard (Best Effort/Default)	Not Specified
Low Priority Data (Scavenger)	High

- Note: Based upon IETF RFC 4594, the tolerance to packet loss for the Default (Best Effort) traffic-class is not specified. Additionally, the tolerance to packet loss for the Scavenger traffic-classes is high. Application health scores for these two traffic-classes are therefore not collected, and there is no Sensitivity Factor setting for these two traffic-classes.

The baseline for traffic-classes with Very Low tolerance to packet loss (Telephony and Broadcast Video) is aligned with the ITU-T Y.1451 specification at less than 1 in 1,000 packets (<0.100%) for Excellent quality.

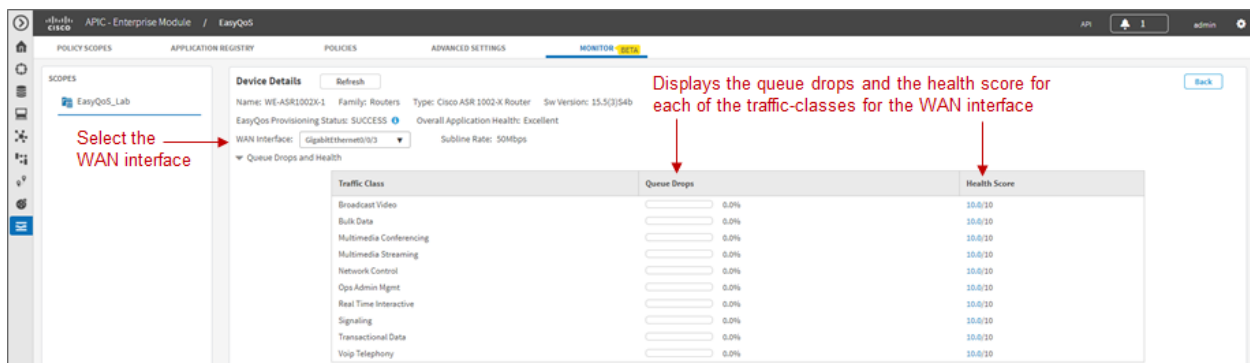
The Sensitivity Factor for the VoIP Telephony and Broadcast Video traffic-classes is set to a value of 50 by default. This is the middle of the range of values from 0 to 100. All of the default values for the Sensitivity Factor for the other eight traffic-classes listed in the Health Score Thresholds popup window are derived from this—based upon the tolerance to packet loss (Low, Low-Medium, or High) of the specific traffic-class. The application health thresholds shown in the Health Score Thresholds window in the figure above are then derived based upon this.

Tuning of the Sensitivity Factor of individual traffic-classes within the Health Score Thresholds popup window allows the network operator to tune the output of the Monitoring feature in situations where the industry standard values do not specifically fit his/her environment. The higher the value of the Sensitivity Factor, the less tolerance to queue drops for the given traffic-class. If at any point, the network operator wants to revert to the default settings of the Sensitivity Factor for each traffic-class, he/she can simply click the Reset to CVD button in the lower left corner of the popup window. When the network operator is satisfied with the tuning, he/she can click the Save button to save the changes and close the popup window.

## Device Details

Clicking a specific router shown in the Monitoring tab screen will bring up details for that particular device. An example is shown in the figure below.

### 1. Monitoring Device Details



The Device Details screen displays the queue drops per traffic-class for the selected WAN interface on the router. It

also displays the health score per traffic-class, based upon the percentage packet loss and Sensitivity Factor for a given traffic-class.

Per traffic-class queue drops for WAN interfaces are collected via the “show policy-map interface <interface> out” command, which is issued by EasyQoS to each WAN interface of monitored routers. An example partial output from the command is shown below.

```
WE-ASR1002X-1#show policy-map interface GigabitEthernet0/0/3 out
GigabitEthernet0/0/3
Service-policy output: prm-dscp#EQ\_SPP1-4Class#shape#50.0
Class-map: class-default (match-any)
48605130 packets, 5809744482 bytes
30 second offered rate 7000 bps, drop rate 0000 bps
Match: any
Queueing
queue limit 208 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 48523512/5803867986
shape (average) cir 50000000, bc 200000, be 200000
target shape rate 50000000
Service-policy : prm-dscp#EQ\_SPP1-4Class
queue stats for all priority classes:
Queueing
queue limit 512 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 730622/54226668
Class-map: prm-EZQOS\_12C#VOICE (match-any)
730622 packets, 54226668 bytes
30 second offered rate 0000 bps, drop rate 0000 bps
Match: dscp ef (46)
**police:**
rate 10 %
rate 5000000 bps, burst 156250 bytes
```

```

**conformed 730622 packets**, 54226668 bytes; actions:
transmit

**exceeded 0 packets**, 0 bytes; actions:
drop

conformed 0000 bps, exceeded 0000 bps

Priority: Strict, b/w exceed drops: 0

QoS Set

dscp ef

Marker statistics: Disabled

Class-map: prm-EZQOS\_12C#BROADCAST (match-any)

730592 packets, 54224448 bytes

30 second offered rate 0000 bps, drop rate 0000 bps

Match: dscp cs5 (40)

Queueing

queue limit 208 packets

(queue depth/\ **total drops**/no-buffer drops) 0/\ **0**/0

(**pkts output**/bytes output) **730592**/54224448

bandwidth remaining 8%

QoS Set

dscp af31

Marker statistics: Disabled

```

...

For traffic-classes which implement priority queuing, the policer configuration is used to determine conformed packets and exceeded packets for each collection interval. Packets which exceed the policer are configured to be dropped by EasyQoS. The queue drops per collection interval are calculated as follows:

Total Packets = Conformed Packets + Exceeded Packets

$\Delta$  Total Packets = Total Packets This Collection Interval – Total Packets Last Collection Interval

$\Delta$  Exceeded Packets = Exceeded Packets This Collection Interval – Exceeded Packets Last Collection Interval

Percentage Queue Drops =  $\Delta$  Exceeded Packets /  $\Delta$  Total Packets

The Exceeded Packets and Conformed Packets counters are highlighted in bold for the VOICE traffic-class in the sample output from the “show policy-map interface <interface> out” command above.

For traffic-classes which do not implement priority queuing, the queue drops per collection interval are calculated



based upon Packets Output (Pkts Output) and Total Drops as follows:

$\Delta$  Pkts Output = Pkts Output This Collection Interval – Pkts Output Last Collection Interval

$\Delta$  Total Drops = Total Drops This Collection Interval – Total Drops Last Collection Interval

Percentage Queue Drops =  $\Delta$  Total Drops /  $\Delta$  Pkts Output

The Pkts Output and Total Drops counters are highlighted in bold for the BROADCAST traffic-class in the sample output from the “show policy-map interface <interface> out” command above.

## 1.6 Chapter 6: WAN and Branch Static QoS Design

Within the EasyQoS solution, different network devices implement the ingress classification & marking QoS policies to the best of their abilities. Cisco ISR G2 Series, ISR 4400 Series, and ASR 1000 Series router platforms implement the following QoS policies:

- Ingress classification & marking policies based on AVC/NBAR2 policy-maps that contain either “match protocol attribute” or “match protocol” statements.
- Egress queuing policies
- Note: As of APIC-EM release 1.3 and higher, port-based Custom applications included within ingress classification & marking policies on ISR and ASR router platforms are implemented through class-maps which match based upon ACL entries.

EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing

The following table summarizes the ingress classification & marking policy provisioned by EasyQoS to Cisco IOS and IOS XE platforms based upon software release, NBAR protocol pack version, and protocol pack license (Standard versus Advanced). Platforms that run IOS software releases include Cisco ISR G2 (3900 Series, 2900 Series, and 800 Series) platforms. Platforms that run IOS XE software releases include Cisco ISR 4400 Series and Cisco ASR 1000 Series platforms.

1. Ingress Classification & Marking Policy for ISR and ASR Platforms

Platform Type	IOS Release	Protocol Pack Version	Ingress Classification & Marking Policy
IOS XE or IOS	Any IOS XE or IOS release	Standard Protocol Pack	No ingress classification & marking policy Ingress classification & marking policies are not supported on devices running Standard Protocol Pack on both IOS and IOS-XE platforms
IOS XE or IOS	IOS XE 3.12 or below Or IOS XE versions 3.13.6 to IOS XE 3.14 (excluding) Or IOS versions below 15.5(1)T	Any Advanced Protocol Pack	Ingress classification & marking policy using “match protocol” statements Custom applications that include a hyphen will not be programmed
IOS XE	IOS XE versions 3.13.1 to 3.13.5 and 3.14 to 3.16 Or IOS 15.5(1)T and 15.5(2)T	Any Protocol Pack	No ingress classification & marking policy (Cisco software defects—see note below)
IOS XE	IOS XE versions 3.16.1 to 3.16.3 Or IOS versions 15.5(3)M to 15.5(3)M3	Advanced Protocol Pack versions below 22.0.0	No ingress classification & marking policy (Cisco software defects—see note below)
IOS XE	IOS XE versions 3.16.1 to 3.16.3 Or IOS versions 15.5(3)M to 15.5(3)M3	Advanced Protocol Pack versions 22.0.0 or higher	Ingress classification & marking policy using “match protocol attribute” statements
IOS XE	IOS XE versions 3.16.4 or later OR IOS 15.5(3)M4 or later	Advanced Protocol Pack versions 14.0.0 or higher	Ingress classification & marking policy using “match protocol attribute” statements

- Note: EasyQoS does not support ISR or ASR routers in port-channel configurations. EasyQoS provisions AVC / NBAR-based ingress classification & marking policies that require individual application flows to be seen bi-directionally on a given interface. With port-channel configurations, this requires the ingress classification & marking policy to be applied on the logical port-channel interface or logical port-channel sub-interface, rather than the physical port-channel member interfaces. As of APIC-EM release 1.6 EasyQoS only applies ingress classification & marking policies to physical interfaces or sub-interfaces.

ISR G2 Series platforms require a Data license for NBAR2 Advanced Protocol Pack. ISR 4000 Series platforms require an Application Experience license for NBAR2 Advanced Protocol Pack. ASR 1000 Series platforms require an Advanced Enterprise Services or Advanced IP Services license for NBAR2 Advanced Protocol Pack. EasyQoS will always push an egress queuing policy to a supported ISR or ASR router platform, regardless of the IOS XE or IOS software version, NBAR protocol pack version, and protocol pack license (Standard or Advanced).

- Note: Although the business-relevance and traffic-class attributes are supported with IOS XE software versions that support Advanced Protocol Pack 14.0.0 and higher, due to Cisco software defect CSCva30089, ingress classification & marking policies are not provisioned to Cisco ISR 4400 and ASR 1000 Series routers by EasyQoS unless the IOS XE software version is upgraded as shown in the table above.

#### NBAR2 QoS Attributes

Cisco NBAR Protocol Pack 14.0.0 introduced two new attributes—“traffic-class” and “business-relevance.” All 1300+ applications known to NBAR have been given a default value for each of these attributes.

#### Traffic-Class Attribute

Every application within the NBAR taxonomy for Protocol Pack 14.0.0 and higher has also been assigned to one of the following 10 traffic-classes:

- VoIP Telephony
- Broadcast Video
- Real Time Interactive
- Multimedia Conferencing
- Multimedia Streaming
- Network Control
- Ops Admin Mgmt
- Signaling
- Transactional Data
- Bulk Data

These 10 traffic-classes are part of the 12-class QoS model recommended in IETF RFC 4594 with minor modifications (Signaling traffic marked CS3 and Broadcast Video traffic marked CS5 with the Cisco model). An example of the Cisco RFC 4594-Based 12-Class QoS model was shown in Figure 5 earlier in this document. The remaining two traffic-classes—Scavenger, and Default—are based on the business-relevance attribute, discussed in the next section.

### Business-Relevance Attribute

Every application within the NBAR taxonomy for NBAR Protocol Pack 14.0.0 and higher has one of the following three settings for the business-relevance attribute:

- Business relevant—these applications directly support business objectives.
- Business irrelevant—these applications do not support business objectives and are typically consumer-oriented.
- Default—these applications may/may not support business objectives (e.g. HTTP/HTTPS/SSL).

Business-relevant applications are intended to be serviced within their respective RFC 4594 traffic-class. Business-irrelevant applications are intended for a RFC 3662 lower than best effort or Scavenger traffic-class treatment. Applications with business-relevancy settings of default are intended for a RFC 2474 Default Forwarding treatment.

### Ingress Classification & Marking Policies

As discussed in the **\*EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing\*** section above, the ingress classification & marking policy pushed by EasyQoS to ISR and ASR router platforms is dependent upon the IOS or IOS XE software version, the NBAR protocol pack version, and the NBAR protocol pack licensing of the platform. The following sections provide details regarding the policy.

#### Class-Map Definitions with “Match Protocol Attribute” Statements

The following is an example of the class-map definitions for the ingress classification & marking policy deployed by EasyQoS to ISR and ASR Series routers—based upon the use of “match protocol attribute” statements.

```
!  
class-map match-all prm-MARKING_IN#TUNNELED-NBAR  
match protocol capwap-data  
!  
class-map match-any prm-MARKING_IN#VOICE_CUSTOM  
match access-group name prm-MARKING_IN#VOICE__acl  
!  
class-map match-any prm-MARKING_IN#BROADCAST_CUSTOM
```

```
match access-group name prm-MARKING_IN#BROADCAST__acl
!
class-map match-any prm-MARKING_IN#REALTIME_CUSTOM
match access-group name prm-MARKING_IN#REALTIME__acl
!
class-map match-any prm-MARKING_IN#MM_CONF_CUSTOM
match access-group name prm-MARKING_IN#MM_CONF__acl
!
class-map match-any prm-MARKING_IN#MM_STREAM_CUSTOM
match access-group name prm-MARKING_IN#MM_STREAM__acl
!
class-map match-any prm-MARKING_IN#CONTROL_CUSTOM
match access-group name prm-MARKING_IN#CONTROL__acl
!
class-map match-any prm-MARKING_IN#SIGNALING_CUSTOM
match access-group name prm-MARKING_IN#SIGNALING__acl
!
class-map match-any prm-MARKING_IN#OAM_CUSTOM
match access-group name prm-MARKING_IN#OAM__acl
!
class-map match-any prm-MARKING_IN#TRANS_DATA_CUSTOM
match access-group name prm-MARKING_IN#TRANS_DATA__acl
!
class-map match-any prm-MARKING_IN#BULK_DATA_CUSTOM
match access-group name prm-MARKING_IN#BULK_DATA__acl
!
class-map match-any prm-MARKING_IN#SCAVENGER_CUSTOM
match access-group name prm-MARKING_IN#SCAVENGER__acl
!
class-map match-all prm-MARKING_IN#VOICE
match protocol attribute traffic-class voip-telephony
match protocol attribute business-relevance business-relevant
!
class-map match-all prm-MARKING_IN#BROADCAST
match protocol attribute traffic-class broadcast-video
match protocol attribute business-relevance business-relevant
```

```
!  
class-map match-all prm-MARKING_IN#REALTIME  
match protocol attribute traffic-class real-time-interactive  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#MM_CONF  
match protocol attribute traffic-class multimedia-conferencing  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#MM_STREAM  
match protocol attribute traffic-class multimedia-streaming  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#CONTROL  
match protocol attribute traffic-class network-control  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#SIGNALING  
match protocol attribute traffic-class signaling  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#OAM  
match protocol attribute traffic-class ops-admin-mgmt  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#TRANS_DATA  
match protocol attribute traffic-class transactional-data  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#BULK_DATA  
match protocol attribute traffic-class bulk-data  
match protocol attribute business-relevance business-relevant  
!  
class-map match-all prm-MARKING_IN#SCAVENGER  
match protocol attribute business-relevance business-irrelevant  
!
```

APIC-EM/EasyQoS release 1.4 and higher added 11 new class-map entries into the ingress classification & marking policy. These new class-map entries are indicated by the word “CUSTOM” for port-based Custom applications. These class-map entries are for port-based Custom applications. Within APIC-EM/EasyQoS release 1.3, port-based Custom applications were provisioned under the `prm-MARKING_IN#TUNNELED-NBAR` class-map entry. Prior to APIC-EM/EasyQoS release 1.3, port-based custom applications were provisioned as NBAR applications. This is discussed further in the **\*Custom Applications on the ASR and ISR Platforms\*** section below. “CUSTOM” class-map entries will only have a “match access-group” statement and an associated ACL if the network operator has configured a port-based Custom application within EasyQoS that belongs to the traffic-class for the “CUSTOM” class-map entry.

The meaning of the “match-all” expression within class-map definitions that contain two “match” statements is that both lines must be true in order for traffic to be classified into the traffic class. For example, for the `prm-MARKING_IN#SIGNALING` class-map definition, matching traffic has to have both an NBAR traffic-class attribute of “signaling” and an NBAR business-relevance attribute of “business-relevant.”

The `prm-MARKING_IN#SCAVENGER` class-map definition, is the only class-map definition that matches on an NBAR business-relevance attribute of “business-irrelevant.” In other words, all applications marked as “business-irrelevant” within the APIC-EM EasyQoS GUI will match the `prm-MARKING_IN#SCAVENGER` class-map definition.

For APIC-EM/EasyQoS release 1.4 and higher, the addition of the `prm-MARKING_IN#TUNNELED-NBAR` class-map definition serves only one purpose for router platforms. It preserves the DSCP marking of Control and Provisioning of Wireless Access Points (CAPWAP) encapsulated data traffic. The DSCP marking of CAPWAP data traffic is based upon DSCP marking of the IP packet sent by the wireless client, in the upstream direction, hence should be preserved.

#### Class-map Definitions with “Match Protocol” Statements

The following is an example of the class-map definitions for the ingress classification & marking policy deployed by EasyQoS to ISR and ASR Series routers—based upon the use of “match protocol” statements.

```
!
class-map match-any prm-MARKING_IN#TUNNELED-NBAR
match protocol capwap-data
!
class-map match-any prm-MARKING_IN#VOICE_CUSTOM
match access-group name prm-MARKING_IN#VOICE__acl
!
class-map match-any prm-MARKING_IN#BROADCAST_CUSTOM
match access-group name prm-MARKING_IN#BROADCAST__acl
!
class-map match-any prm-MARKING_IN#REALTIME_CUSTOM
match access-group name prm-MARKING_IN#REALTIME__acl
!
class-map match-any prm-MARKING_IN#MM_CONF_CUSTOM
match access-group name prm-MARKING_IN#MM_CONF__acl
!
class-map match-any prm-MARKING_IN#MM_STREAM_CUSTOM
match access-group name prm-MARKING_IN#MM_STREAM__acl
```

```
!  
class-map match-any prm-MARKING_IN#CONTROL_CUSTOM  
match access-group name prm-MARKING_IN#CONTROL__acl  
!  
class-map match-any prm-MARKING_IN#SIGNALING_CUSTOM  
match access-group name prm-MARKING_IN#SIGNALING__acl  
!  
class-map match-any prm-MARKING_IN#OAM_CUSTOM  
match access-group name prm-MARKING_IN#OAM__acl  
!  
class-map match-any prm-MARKING_IN#TRANS_DATA_CUSTOM  
match access-group name prm-MARKING_IN#TRANS_DATA__acl  
!  
class-map match-any prm-MARKING_IN#BULK_DATA_CUSTOM  
match access-group name prm-MARKING_IN#BULK_DATA__acl  
!  
class-map match-any prm-MARKING_IN#SCAVENGER_CUSTOM  
match access-group name prm-MARKING_IN#SCAVENGER__acl  
!  
class-map match-any prm-MARKING_IN#VOICE  
match protocol cisco-jabber-audio  
match protocol cisco-phone  
match protocol cisco-phone-audio  
match protocol citrix-audio  
...  
!  
class-map match-any prm-MARKING_IN#BROADCAST  
match protocol cisco-ip-camera  
match protocol dmp  
...  
!  
class-map match-any prm-MARKING_IN#REALTIME  
match protocol telepresence-media  
...  
!  
class-map match-any prm-MARKING_IN#MM_CONF
```



```
match protocol webex-meeting
match protocol rtp
match protocol adobe-connect
match protocol cisco-phone
match protocol adobe-connect
...
!
class-map match-any prm-MARKING_IN#MM_STREAM
match protocol vnc
match protocol radmin-port
match protocol citrix-static
match protocol citrix
match protocol xwindows
...
!
class-map match-any prm-MARKING_IN#CONTROL
match protocol aodv
match protocol aurp
match protocol bgmp
match protocol bgp
match protocol capwap-control
...
!
class-map match-any prm-MARKING_IN#SIGNALING
match protocol cisco-jabber-control
match protocol rtsp
match protocol sip
match protocol sip-tls
match protocol skinny
...
!
class-map match-any prm-MARKING_IN#TRANS_DATA
match protocol activesync
match protocol banyan-rpc
match protocol clearcase
match protocol coauthor
```

```
match protocol corba-iiop
...
!
class-map match-any prm-MARKING_IN#BULK_DATA
match protocol afpovertcp
match protocol bmpp
match protocol cifs
match protocol corba-iiop-ssl
match protocol dicom
...
!
class-map match-any prm-MARKING_IN#SCAVENGER
match protocol 4chan
match protocol 58-city
match protocol abc-news
match protocol accuweather
match protocol adcash
match protocol addthis
...
!
```

As with the previous class-map definitions, APIC-EM/EasyQoS release 1.4 and higher added 11 new class-map entries into the ingress classification & marking policy. These new class-map entries are indicated by the word “CUSTOM” for port-based Custom applications. Within APIC-EM/EasyQoS release 1.3, port-based Custom applications were provisioned under the prm-MARKING\_IN#TUNNELED-NBAR class-map entry. Prior to APIC-EM/EasyQoS release 1.3, port-based custom applications were provisioned as NBAR applications. This is discussed further in the **\*Custom Applications on the ASR and ISR Platforms\*** section below. “CUSTOM” class-map entries will only have a “match access-group” statement and an associated ACL if the network operator has configured a port-based Custom application within EasyQoS that belongs to the traffic-class for the “CUSTOM” class-map entry.

The specific protocols that appear within the “match protocol” statements within the class-map definitions will vary, depending upon the deployment. This is based upon whether the network operator has selected the particular protocol as having a business relevance of “business-relevant,” “business-irrelevant,” or “default” within the EasyQoS application for the particular scope to which the router belongs.

For ISR 4400 Series, ISR G2 Series, and ASR 1000 Series routers, a maximum of 32 “match protocol” statements are supported per non-custom class-map entry. Only NBAR2 taxonomy applications and/or URL-based Custom applications are mapped to the non-custom class. Therefore, only the top 32 applications from the NBAR2 taxonomy or URL-based Custom applications per traffic-class are mapped to each non-custom class-map entry.

#### Modifying the Business Relevance of an Application

Network operators have the ability to modify the business-relevance of applications within the EasyQoS graphical user interface and include these changes within policies pushed by APIC-EM to router and switch platforms. The **\*APIC-EM and the EasyQoS Application\*** chapter shows how to modify the business relevance of applications within EasyQoS.

### Modifying Business Relevance—Policy-maps with “Match Protocol Attribute” Statements

When the business-relevance of an application is modified and pushed to an ASR or ISR router platform that implements a policy-map containing class-map definitions that include “match protocol attribute business-relevance” or “match protocol attribute traffic-class” statements, EasyQoS will generate additional configuration within ISR and ASR router platforms.

First, EasyQoS creates one or all of the following attribute-map definitions shown below. The names of attribute-map definitions match the three values of the business-relevance attribute—APIC-A\_M\_RELEVANT, APIC-A\_M-DEFAULT, and APIC-A\_M-SCAVANGER.

```
!
ip nbar attribute-map APIC-A_M-RELEVANT
attribute business-relevance business-relevant
ip nbar attribute-map APIC-A_M-DEFAULT
attribute business-relevance default
ip nbar attribute-map APIC-A_M-SCAVANGER
attribute business-relevance business-irrelevant
!
```

Under each of these attribute-map definitions, EasyQoS sets the business-relevance attribute.

- For the APIC-A\_M-Relevant attribute-map definition, the business-relevance attribute is set to business-relevant.
- For the APIC-A\_M-Default attribute-map definition, the business-relevance attribute is set to default.
- For the APIC-A\_M-SCAVANGER attribute-map definition, the business-relevance attribute is set to business-irrelevant.

EasyQoS then maps each application that has been modified from whatever its default setting is within the NBAR2 taxonomy to one of the three attribute-map definitions above. This is accomplished via the “ip nbar attribute-set” command. In the example below, the application “ms-lync-video” has been mapped to a business-relevance of “business-irrelevant.”

```
!
ip nbar attribute-set ms-lync-video APIC-A_M-SCAVANGER
!
```

### Modifying Business Relevance—Policy-maps with “Match Protocol” Statements

When the business-relevance of an application is modified and pushed to an ISR or ASR router platform that implements a policy-map containing class-map definitions that include “match protocol” statements, the “match protocol” statement for the application will be modified as follows:

- If an application is moved from “business-relevant” or “default” to “business-irrelevant,” the “match-protocol” statement for the application will appear under the prm-MARKING\_IN#SCAVANGER traffic-class.
- By default, no applications within the NBAR taxonomy are classified with the traffic-class attribute of “scavenger”. Therefore, if an application is moved from either “business-irrelevant” or “default” to “business-relevant”, the “match-protocol” statement for the application will appear under one of the following ten class-map definitions—depending upon the traffic-class attribute of the particular application.
- prm-MARKING\_IN#VOICE
- prm-MARKING\_IN#BROADCAST
- prm-MARKING\_IN#REALTIME

- prm-MARKING\_IN#CONTROL
- prm-MARKING\_IN#SIGNALING
- prm-MARKING\_IN#OAM
- prm-MARKING\_IN#MM\_CONF
- prm-MARKING\_IN#MM\_STREAM
- prm-MARKING\_IN#TRANS\_DATA
- prm-MARKING\_IN#BULK\_DATA
- If the application is moved from either “business-relevant” or “business-irrelevant” to “default,” no “match-protocol” statement for the application will appear under any of the class-map definitions. This is because “match protocol” statements are not programmed for applications with a business-relevance of “default.”

#### Custom Applications on ASR and ISR Platforms

Network operators have the ability to add Custom applications within the EasyQoS graphical user interface and to include these Custom applications within policies pushed by APIC-EM to router and switch platforms. The **\*APIC-EM and the EasyQoS Application\*** chapter shows how Custom applications are created and added to policy scopes within EasyQoS. Custom applications can either be specified by a URL string or by one or more server IP addresses and UDP/TCP ports.

#### URL-Based Applications—Policy-maps with “Match Protocol Attribute” Statements

For Custom applications that are specified based on a URL string, EasyQoS will generate additional configuration within ISR and ASR router platforms similar to the following example:

```
!  
ip nbar attribute-map Custom_URL_App  
attribute traffic-class transactional-data  
attribute business-relevance business-relevant  
attribute category other  
attribute sub-category other  
!  
~  
!  
ip nbar custom Custom_URL_App http url “http://example.custom.com” id 16299  
!  
~  
!  
ip nbar attribute-set Custom_URL_App Custom_URL_App  
!
```

This first block of configuration creates an attribute profile (named Custom\_URL\_App in the example above). The name of the attribute profile corresponds to the name of the Custom application specified by the network operator when creating the Custom application definition within the EasyQoS web-based GUI. The configuration then assigns the attribute profile several attributes, including a traffic-class attribute and a business-relevance attribute. In the example Custom application, a traffic-class attribute of “transactional-data” and a business-relevance attribute of “business-relevant” have been assigned to the attribute profile.

The second block (single line) of configuration above defines a web-based custom protocol match, specifying the URL string that is used to match on the name of the custom protocol (also named Custom\_URL\_App in the example above).

Finally, the third block (single line) of configuration maps the attribute profile to the web-based custom protocol match—both defined in the previous two blocks of configuration. In other words, the custom protocol is assigned the attributes specified within the attribute profile.

The effect of this configuration example is that the custom protocol defined by the URL string “<http://example.custom.com>” will match the prm-MARKING\_IN#TRANS\_DATA class-map definition and be treated as Transactional Data traffic. Additional URL-based Custom applications will generate additional configuration blocks similar to those shown in the example above.

#### URL-Based Applications—Policy-maps with “Match Protocol” Statements

URL-based applications are not programmed into ISR and ASR router platforms that implement a policy-map containing class-map definitions that include “match protocol” statements.

#### Server IP/Port Based Applications

In APIC-EM/EasyQoS release 1.3, port-based Custom applications were moved outside of the AVC/NBAR engine, in order to support new functionality that is not supported by NBAR-based applications on ISR and ASR router platforms. This includes included bi-directionality and consumers (source IP addresses and ports) as well as producers (destination IP addresses and ports). APIC-EM/EasyQoS release 1.4 further changed the way port-based Custom applications are handled on ASR and ISR router platforms.

In APIC-EM/EasyQoS release 1.3, Custom applications were handled through the creation of a single ACL with ACEs. Specifically, an ACL for the prm-MARKING\_IN#TUNNELED-NBAR traffic-class, called prm-MARKING\_IN#TUNNELED-NBAR\_\_acl, was generated and populated with ACE entries for all port-based Custom applications. As of APIC-EM/EasyQoS release 1.4 and higher, ACE entries are created under one of the 11 new class-map entries that include the word “CUSTOM”—based on the traffic-class to which the port-based Custom application belongs.

An example is shown below for a port-based Custom application created within the Multimedia Conferencing traffic-class.

!

```
ip access-list extended prm-MARKING_IN# MM_CONF_CUSTOM__acl
```

```
remark Custom_Port-App
```

```
permit udp any 10.0.10.0 0.0.0.255 range 3001 3010
```

```
permit udp 10.0.10.0 0.0.0.255 range 3001 3010 any
```

!

In the example above, the Custom application—based on a destination server IP address range and port range (also referred to as the producer)—has been specified to be bi-directional by the network operator through the EasyQoS web-based GUI. Hence, the reverse of the ACE entry is also generated to allow traffic from the server IP address and port range to also be treated the same.

In the example above, a server IP address range (10.0.10.0-10.0.10.255) and port range (UDP 3001-3010) is configured. Custom applications also support single IP addresses and ports, or the use of “any” specified as the destination IP address. Although a single UDP port range is specified in the example above, multiple UDP and/or TCP ports can be configured as well—each of which would appear as a separate “permit” statement.

Additional IP Address/Port-based Custom applications will generate additional ACE entries within the prm-MARKING\_IN#MM\_CONF\_CUSTOM\_\_acl, similar to those shown in the example above.

A more sophisticated example shown below, adds a source IP address or range (referred to as the consumer) as well as the destination IP address or range (referred to as the producer) to the Custom application. Again, this is

configured bi-directionally via the APIC-EM EasyQoS web-based GUI by the network operator. An example of the same application—but with a consumer—is shown below.

!

```
ip access-list extended prm-MARKING_IN#MM_CONF_CUSTOM__acl
remark Custom_Port-App__Custom-Port-App_Consumer
permit udp 10.0.1.0 0.0.0.255 range 3001 3010 host 10.0.20.20 eq 3100
remark Custom-Port-App_Consumer__Custom_Port-App
permit udp host 10.0.20.20 eq 3100 10.0.1.0 0.0.0.255 range 3001 3010
```

!

The combination of the producer and consumer, along with the ability to apply the policy bi-directionally, essentially gives the network operator the ability to use nearly the full CLI functionality in terms of being able to configure QoS ACE entries.

After the ACL and ACE entries have been generated, EasyQoS adds the ACL entry to the class-map definition corresponding to the traffic-class to which the Custom application belongs, via a “match access-group” statement. This is regardless of whether the class-map definitions within the ingress classification & marking policy-map uses “match protocol attribute” or “match protocol” statements. For the example discussed above, the ACL entry is added to the prm-MARKING\_IN#MM\_CONF\_CUSTOM class-map, as shown below.

!

```
class-map match-all prm-MARKING_IN#MM_CONF_CUSTOM
match access-group name prm-MARKING_IN#MM_CONF_CUSTOM__acl
```

!

The 11 new class map entries that include the word “CUSTOM” are used for Custom applications because they allow the traffic from port-based Custom applications to be identified and marked correctly within the ingress classification and marking policy-map of ISR and ASR router platforms. This is particularly important for inbound traffic from a Service Provider WAN. This will be discussed more in the **\*Server IP/Port-Based Custom Applications and Managed Service WANS\*** section of this document.

#### Changing the Traffic-Class of Applications on ASR and ISR Platforms

APIC-EM release 1.5 introduces the ability to change the traffic-class of an application within the NBAR2 taxonomy. An example of this was shown in Figure 33 within the **\*APIC-EM and the EasyQoS Application\*** chapter.

For policy-maps with “match protocol attribute” statements, changing the traffic-class of an application will result in configuration similar to the following being provisioned on the ASR or ISR router platform.

```
ip nbar attribute-map cisco-collab-audio
attribute business-relevance business-relevant
attribute traffic-class multimedia-conferencing
```

In the configuration example above, the traffic-class attribute of the cisco-collab-audio application has been changed from the default value of voip-telephony to a new value of multimedia-conferencing. As mentioned previously, for this particular example, network operator may find it desirable to mark both the voice and video components of a collaboration session the same. Hence, providing the ability to set the traffic-class attribute of individual applications is a useful feature.

For policy-maps with “match protocol” statements, changing the traffic-class of an application will result in the “match protocol” statement for the particular application to be defined under the desired class-map entry for the traffic-class. Note, however, that the NBAR protocol pack version must be high enough, such that the particular application is

supported. Further, the application may have to be selected as a Favorite, because a maximum of 32 “match protocol” statements are supported per non-custom class-map entry.

#### NBAR2 Application Changes between Protocol Pack Revisions

As of APIC-EM release 1.4 and higher, EasyQoS utilizes NBAR2 protocol pack 27.0.0 when implementing policy to network devices. The protocol pack revision running on the actual router to which policy is deployed may not necessarily match with the version used by EasyQoS. Occasionally, there are changes to the traffic-class and/or business relevance of an application within the NBAR taxonomy, between protocol pack revisions. This is due to better knowledge of how the application is utilized on customer networks or due to changes in how applications are actually used on customer networks. For example, applications which begin as being consumer oriented—and hence may initially be viewed as business-irrelevant—sometimes become adopted in business organizations over time. In such cases, the application may be viewed as business-relevant within newer versions of the NBAR protocol pack.

In order to accommodate these changes, for policy-maps with “match protocol attribute” statements EasyQoS will automatically configure modifications to the application, such that the traffic-class and business-relevance of the given application matches the protocol pack version used by EasyQoS. This guarantees that the business intent displayed within the EasyQoS GUI is enforced on the given ASR or ISR router device. An example of such changes is shown below for two applications.

```
ip nbar attribute-map netflow
attribute business-relevance business-relevant
attribute traffic-class ops-admin-mgmt
ip nbar attribute-map ipfix
attribute traffic-class ops-admin-mgmt
attribute business-relevance business-relevant
```

For policy-maps with “match protocol” statements, EasyQoS will simply provision the “match protocol” statement for the particular application under the class-map entry for the traffic-class which matches the protocol pack definition running on APIC-EM (protocol pack 27.0.0). Note however, that the NBAR protocol pack version running on the ASR or ISR router platform must be high enough, such that the particular application is supported. Further, the application may have to be selected as a Favorite, because a maximum of 32 “match protocol” statements are supported per non-custom class-map entry.

#### Policy-map Definition

The following is an example of the default policy-map definition for the ingress classification & marking policy deployed by EasyQoS to ISR and ASR routers—regardless of whether the class-map definitions within the ingress classification & marking policy-map uses “match protocol attribute” or “match protocol” statements.

```
!
policy-map prm-MARKING_IN
class prm-MARKING_IN#TUNNELED-NBAR
class prm-MARKING_IN#VOICE_CUSTOM
set dscp ef
class prm-MARKING_IN#BROADCAST_CUSTOM
set dscp cs5
class prm-MARKING_IN#REALTIME_CUSTOM
set dscp cs4
class prm-MARKING_IN#MM_CONF_CUSTOM
```

```
set dscp af41
class prm-MARKING_IN#MM_STREAM_CUSTOM
set dscp af31
class prm-MARKING_IN#CONTROL_CUSTOM
set dscp cs6
class prm-MARKING_IN#SIGNALING_CUSTOM
set dscp cs3
class prm-MARKING_IN#OAM_CUSTOM
set dscp cs2
class prm-MARKING_IN#TRANS_DATA_CUSTOM
set dscp af21
class prm-MARKING_IN#BULK_DATA_CUSTOM
set dscp af11
class prm-MARKING_IN#SCAVENGER_CUSTOM
set dscp cs1
class prm-MARKING_IN#VOICE
set dscp ef
class prm-MARKING_IN#BROADCAST
set dscp cs5
class prm-MARKING_IN#REALTIME
set dscp cs4
class prm-MARKING_IN#MM_CONF
set dscp af41
class prm-MARKING_IN#MM_STREAM
set dscp af31
class prm-MARKING_IN#CONTROL
set dscp cs6
class prm-MARKING_IN#SIGNALING
set dscp cs3
class prm-MARKING_IN#OAM
set dscp cs2
class prm-MARKING_IN#TRANS_DATA
set dscp af21
class prm-MARKING_IN#BULK_DATA
set dscp af11
class prm-MARKING_IN#SCAVENGER
```



```

set dscp cs1
class class-default
set dscp default
!
```

The default policy-map sets the DSCP marking, hence the per-hop behavior, for traffic matching the particular traffic class to meet Cisco's RFC-4594 based recommendations for a 12-class QoS model, shown in Figure 5 earlier in this document.

The 11 traffic-classes to which port-based Custom applications are provisioned appear first within the ingress classification & marking policy-map. This is to ensure that any UDP/TCP ports specified within the Custom application are not accidentally mapped to an existing application within the NBAR taxonomy.

The prm-MARKING\_IN#TUNNELED-NBAR traffic-class is the only class-map definition within the policy-map that specifies no action. Therefore, any DSCP markings for the CAPWAP data specified at the Access Point connected to the ingress access-edge switch are maintained, as the traffic passes through an ISR or ASR router platform.

#### Application of the Ingress Classification & Marking Policy to Interfaces

The ingress classification & marking policy is applied to all Ethernet interfaces on the ISR or ASR router platform, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- WAN interfaces which are not configured to be part of an SPP. Such interfaces are configured with a #WAN# tag in the interface description but do not have the additional #SPP...# tag. For these interfaces, no re-marking is done as the traffic enters the WAN. Therefore, the AVC/NBAR-based ingress classification & marking policy does not need to be applied inbound on the WAN-facing interfaces. SP Profiles and associated tagging of interfaces is discussed in the **\*Service Provider Managed-Service WAN QoS Design\*** chapter of this document.

An example of the application of the ingress classification & marking policy is as follows:

```

!
interface GigabitEthernet0/1
service-policy input prm-MARKING_IN
!
```

For brownfield deployments, EasyQoS will remove any existing ingress classification & marking service-policy statements that appear on the interface, before applying the prm-MARKING\_IN service-policy. However, policy-map and class-map definitions for the existing policy will remain within the configuration of the ASR or ISR router platform.

#### WAN-Edge Egress Queuing Policy

The WAN-edge egress queuing policy is deployed to the following interfaces:

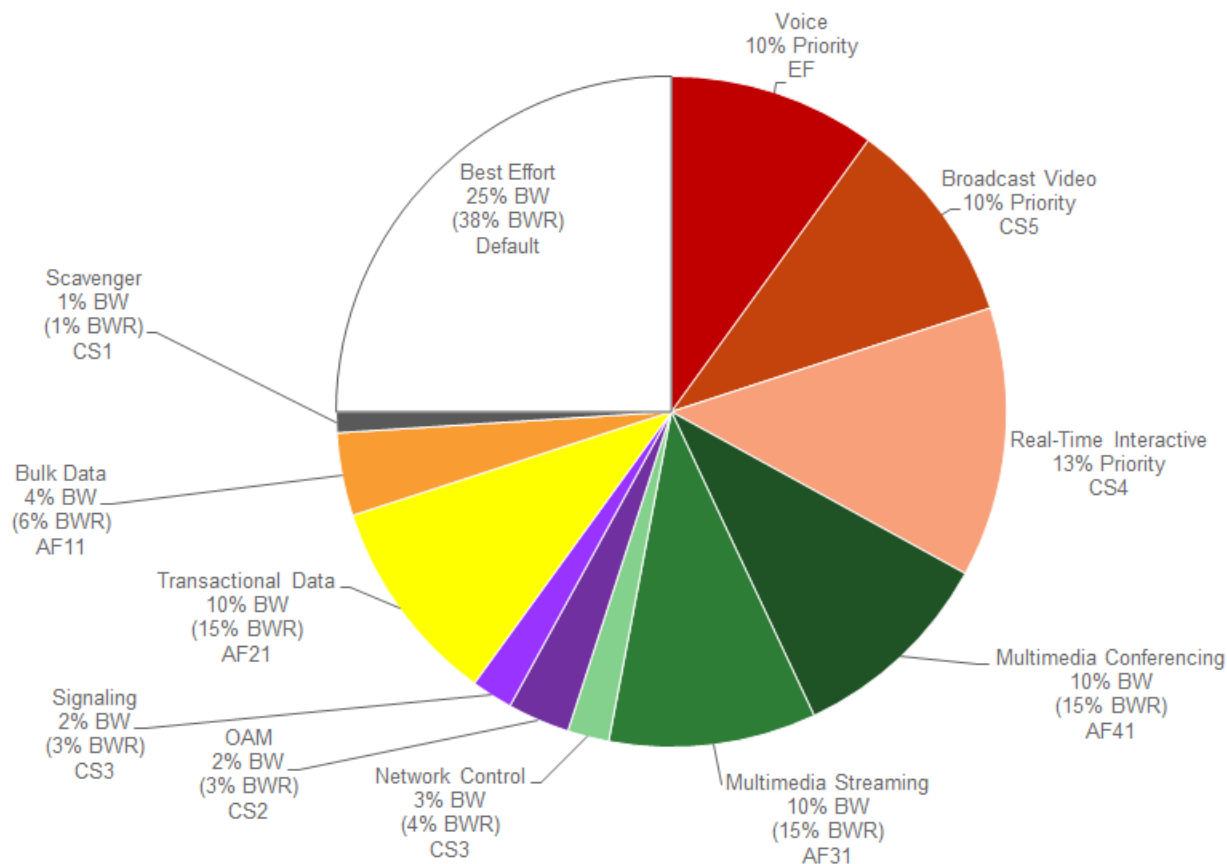
- WAN links that are not connected to service provider managed-service offerings requiring the support of sub-line rate speeds and the re-marking of traffic to meet the traffic-classes provided by the service provider.
- LAN links between the ISR or ASR router and the Catalyst switch

APIC-EM/EasyQoS release 1.5 and higher provides the ability for the network operator to specify the bandwidth allocation and DSCP marking for each of the traffic-classes within the QoS policy applied to a given policy scope. This is accomplished through the application of a Queuing Profile to a policy. As was discussed in the **\*Queuing Profiles\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter of this document, a network operator can either apply the default Queuing Profile—CVD\_Queueing\_Profile (Default)—to the devices within the policy scope or can create a custom Queuing Profile to apply to the devices within the policy scope.

## Default Queuing Profile (CVD\_Queueing\_Profile)

The following figure shows the WAN bandwidth allocation model for the WAN-edge egress queuing policy with the default Queuing profile applied.

## 1. Bandwidth Allocation Model for the WAN-Edge Egress Queuing Policy with Default Queuing Profile



- Note: The bandwidth allocations per traffic-class for the default CVD\_Queueing\_Profile within APIC-EM 1.5 and higher are the same as in the default CVD\_BW\_Profile within APIC-EM 1.4. However, the bandwidth allocations are slightly different for some traffic-classes from the bandwidth allocations for the WAN-edge Queuing Policy within APIC-EM 1.3 and below.

When using the default Queuing Profile (CVD\_Queueing\_Profile), bandwidth allocations for the WAN edge queuing policy are fixed and cannot be modified. Because queuing is done in software on ISR and ASR router platforms, the WAN-edge egress queuing policy implements a 12 queue model—meaning a queue for each of the traffic-classes within the RFC 4594-based 12-class QoS model shown in Figure 5 earlier in this document.

The following table shows the mapping of the traffic-classes and bandwidth allocations from the default EasyQoS CVD\_Queueing\_Profile to the WAN-Edge egress queuing policy structure.

## 1. Default Queuing Profile Mapping to WAN-Edge Egress Queuing Policy

Traffic Class	DSCP Marking	BW % in the Default Queuing Profile	BWR % Calculated from the Default Queuing Profile	WAN-Edge Egress Queue Mapping	BW Allocation in the WAN-Edge Egress Queue
Voice	EF	10%	N/A	VOICE	VOICE bandwidth is priority and policed to 10%
Broadcast Video	CS5	10%	N/A	BROADCAST	BROADCAST bandwidth is priority and policed to 10%
Real-Time Interactive	CS4	13%	N/A	REALTIME	REALTIME bandwidth is priority and policed to 13%
Multi-media Conferencing	AF41	10%	15%	MM_CONF	BWR for MM_CONF = 15%
Multi-media Streaming	AF31	10%	15%	MM_STREAM	BWR MM_STREAM = 15%
Network Control	CS6	3%	4%	CONTROL	BWR for CONTROL = 4%
Signaling	CS3	2%	3%	SIGNALING	BWR for SIGNALING = 3%
OAM	CS2	2%	3%	OAM	BWR for OAM = 3%
Transactional Data	AF21	10%	15%	TRANS_DATA	BWR for TRANS_DATA = 15%
Bulk Data	AF11	4%	6%	BULK_DATA	BWR for BULK_DATA = 6%
Scavenger	CS1	1%	1%	SCAVENGER	BWR for SCAVENGER = 1%
Best Effort	Default	25%	38%	Default Queue	BWR for Default Queue = 38%

Column 3 of the table above shows the percentage bandwidth allocation for each of the traffic-classes as it appears within the EasyQoS GUI for the default CVD\_Queueing\_Profile.

The WAN-Edge Queuing policy implements three low-latency queues via the “police rate percent” commands for the VOICE, BROADCAST, and REALTIME traffic-classes within the policy-map definition. The bandwidth allocated within the EasyQoS GUI for the default Queuing Profile directly maps to the bandwidth within “police rate percent” statements for these three traffic-classes.

The sum of the bandwidth allocated to these three traffic-classes can be considered as the total priority queue bandwidth (Total\_PQ\_BW), as shown in the following formula.

$$\text{Total\_PQ\_BW} = \text{Voice BW} + \text{Broadcast Video BW} + \text{Real-Time Interactive BW}$$

Based on the bandwidth allocations in column 3 in the table above Total\_PQ\_BW can be calculated as follows:

$$\text{Total\_PQ\_BW} = 10\% (\text{Voice}) + 10\% (\text{Broadcast Video}) + 13\% (\text{Real-Time Interactive}) = 33\%$$

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic-class through the EasyQoS GUI, and the amount of Total\_PQ\_BW calculated above. This can be done through the following formula.

$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$

For example, BWR percentage for the Multimedia Streaming traffic class can be calculated as follows.

$\text{Multimedia\_Conferencing\_BWR} = (10\% / (100\% - 33\%)) * 100 = 15\%$  when rounded

Because each traffic-class is mapped to a separate queue, determining the bandwidth ratio allocated to each of the non-priority queues within the WAN-Edge egress queuing model is simply a matter of copying the Traffic\_Class\_BWR numbers to the each of the queues shown in column 6 in the table above.

#### Class-map Definitions

The following are the class-map definitions for each of the 12 queues provisioned by EasyQoS.

!

```
class-map match-any prm-EZQOS_12C#VOICE
```

```
match dscp ef
```

```
class-map match-any prm-EZQOS_12C#BROADCAST
```

```
match dscp cs5
```

```
class-map match-any prm-EZQOS_12C#REALTIME
```

```
match dscp cs4
```

```
class-map match-any prm-EZQOS_12C#CONTROL
```

```
match dscp cs6
```

```
class-map match-any prm-EZQOS_12C#SIGNALING
```

```
match dscp cs3
```

```
class-map match-any prm-EZQOS_12C#OAM
```

```
match dscp cs2
```

```
class-map match-any prm-EZQOS_12C#MM_CONF
```

```
match dscp af41
```

```
match dscp af42
```

```
match dscp af43
```

```
class-map match-any prm-EZQOS_12C#MM_STREAM
```

```
match dscp af31
```

```
match dscp af32
```

```
match dscp af33
```

```
class-map match-any prm-EZQOS_12C#TRANS_DATA
```

```
match dscp af21
```

```
match dscp af22
```

```
match dscp af23
```

```
class-map match-any prm-EZQOS_12C#BULK_DATA
```

```
match dscp af11
```

```
match dscp af12
```

```
match dscp af13
```

```
class-map match-any prm-EZQOS_12C#SCAVENGER
```

```
match dscp cs1
```

```
!
```

#### Policy-map Definition

The following is an example of the policy-map definition for the WAN-edge egress queuing policy for an ISR or ASR router when using the default Queuing Profile (CVD\_Queueing\_Profile), provisioned by EasyQoS.

```
!
```

```
policy-map prm-dscp#QUEUEING_OUT
```

```
class prm-EZQOS_12C#VOICE
```

```
police rate percent 10
```

```
priority
```

```
class prm-EZQOS_12C#BROADCAST
```

```
police rate percent 10
```

```
priority
```

```
class prm-EZQOS_12C#REALTIME
```

```
police rate percent 13
```

```
priority
```

```
class prm-EZQOS_12C#MM_CONF
```

```
bandwidth remaining percent 15
```

```
fair-queue
```

```
random-detect dscp-based
```

```
class prm-EZQOS_12C#MM_STREAM
```

```
bandwidth remaining percent 15
```

```
fair-queue
```

```
random-detect dscp-based
```

```
class prm-EZQOS_12C#CONTROL
```

```
bandwidth remaining percent 4
```

```
class prm-EZQOS_12C#SIGNALING
```

```
bandwidth remaining percent 3
```

```
class prm-EZQOS_12C#OAM
```

```
bandwidth remaining percent 3
```

```
class prm-EZQOS_12C#TRANS_DATA
```

```
bandwidth remaining percent 15
```

```
fair-queue
```

```
random-detect dscp-based
```

```
class prm-EZQOS_12C#BULK_DATA
```

bandwidth remaining percent 6

fair-queue

random-detect dscp-based

class prm-EZQOS\_12C#SCAVENGER

bandwidth remaining percent 1

class class-default

bandwidth remaining percent 38

fair-queue

random-detect dscp-based

random-detect dscp 0 50 64 ! ISR G2 and 800 Series platforms only.

!

The Voice queue supports traffic with an EF per hop behavior. The Broadcast-Video queue supports traffic with a Class Selector 5 (CS5) per hop behavior. The Realtime-Interactive traffic class supports traffic with a CS4 per hop behavior. Broadcast-Video and Realtime-Interactive traffic-classes are meant to support traffic flows that are inelastic—meaning the endpoints generating the flows do not down-speed their transmission rate when packet loss occurs. Because of the inelastic nature of these flows, they are eligible for LLQ treatment on the ISR or ASR router platforms, along with Voice traffic. Explicit policers (10%, 10%, and 13% respectively) ensure that each of the LLQs can use no more than the percentage of the bandwidth of the WAN link allocated to the traffic class, regardless of whether there is available bandwidth.

The remaining nine queues share the remaining bandwidth based on a percentage allocation of bandwidth. This is accomplished via the “bandwidth remaining percent” command. Each of these queues can use more than its percentage allocation, if more bandwidth is available—meaning if the one or more of the other queues is not using its full allocation of remaining bandwidth percentage.

The Multimedia-Conferencing, Multimedia-Streaming, Transactional Data, and Bulk Data queues support traffic with Assured Forwarding (AF) per-hop behaviors (AF4x, AF3x, AF2x, and AF1x respectively). Fair-queuing, along with DSCP-based WRED is implemented for these traffic-classes. The minimum and maximum WRED thresholds for these queues is left at their default values.

For ISR G2 and 800 Series platforms, the default queue limit size is 64 packets per queue. The minimum and maximum WRED thresholds are expressed in terms of the number of packets. The default WRED thresholds for the AF per-hop behaviors, and the drop probability is shown in the following table.

#### 1. ISR G2 WRED Minimum & Maximum Threshold and Drop Probability Default Values

Per-Hop Behavior and DSCP Value	Minimum Threshold (Packets)	Maximum Threshold (Packets)	Drop Probability
AF11 (DSCP 10)	32	40	1/10
AF12 (DSCP 12)	28	40	1/10
AF13 (DSCP 14)	24	40	1/10
AF21 (DSCP 18)	32	40	1/10
AF22 (DSCP 20)	28	40	1/10
AF23 (DSCP 22)	24	40	1/10
AF31 (DSCP 26)	32	40	1/10
AF32 (DSCP 28)	28	40	1/10
AF33 (DSCP 30)	24	40	1/10
AF41 (DSCP 34)	32	40	1/10
AF42 (DSCP 36)	28	40	1/10
AF43 (DSCP 38)	24	40	1/10
Default (DSCP 0)	20	40	1/10

The Default queue also implements fair-queueing, along with DSCP-based WRED. WRED is effective here at preventing TCP synchronization of flows, which can result in overall lower throughput and bandwidth utilization. For the ISR G2 and 800 Series platforms, the default WRED thresholds for the Default queue are considered to be too aggressive—meaning the minimum drop threshold is set lower than desired. Hence, the minimum drop threshold has been adjusted to 50 packets, and the maximum drop threshold adjusted to the depth of the queue—64 packets. For the ISR 4400 and ASR 1000 Series platforms, the default WRED thresholds for the Default queue are left at their default values.

The Control, Signaling, OAM, and Scavenger queues each support a single Class Selector (CS) per hop behavior (CS6, CS3, CS2, and CS2, respectively). For the Control, Signaling, and OAM traffic-classes, WRED is not implemented. Randomly discarding network control, signaling, or operational traffic when a minimum queue depth threshold is exceeded, may simply result in degraded network performance. Hence these queues implement tail-drop at the back of the queue, because the objective is to not drop traffic in these queues by provisioning sufficient remaining bandwidth percentage allocation to these queues.

The Scavenger queue is considered to be a bandwidth-constrained queue for less-than-best-effort treatment. WRED is not implemented for this queue, because the consideration is not to optimize the use of this queue but simply to provision some minimal amount of bandwidth for support of traffic within this queue.

#### Application of the Egress Queuing Policy to Interfaces

The egress queuing policy is applied to all Ethernet interfaces on the ISR or ASR router platform, with the following exception:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.

When using custom Queuing Profiles (discussed in the next section) with different bandwidth allocations for different interface speeds, the service-policy name will match the name of the policy-map generated for the particular interface speed.

An example of the application of the egress queuing policy is as follows:

```
!
interface GigabitEthernet0/1
service-policy output prm-DSCP#QUEUEING_OUT
!
```

For brownfield deployments, EasyQoS will remove any existing egress queuing service-policy statements that appear on the interface, before applying the `prm-DSCP#QUEUEING_OUT` service-policy. However, policy-map and class-map definitions for the existing policy will remain within the configuration of the ASR or ISR router platform. This provides the network operator the option to restore the configuration of the ISR or ASR router platform to its original non-EasyQoS policy, should that be necessary.

### Custom Queuing Profiles

APIC-EM/EasyQoS release 1.5 and higher provides the network operator the ability to change the both the DSCP marking and the bandwidth allocation of traffic-classes through custom Queuing Profiles, within the web-based GUI. This feature was discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Specifically, Figures 36 and 37 showed an example custom Queuing Profile named `EasyQoS_Lab_Queueing_Profile`. The bandwidth allocations for the 12 traffic-classes for this example Queuing Profile (for 1 Gbps interfaces) are shown in column 3 of the following table. Likewise, the DSCP markings for the 12 traffic-classes are shown in column 2.

#### 1. EasyQoS\_Lab\_Queueing Profile Mapping to WAN-Edge Egress Queuing Policy

Traffic Class	DSCP Mark-ing	BW % in the EasyQoS Lab Queueing Profile	BWR % Calculated from the EasyQoS Lab Queueing Profile	WAN-Edge Egress Queue Map-ping	BW Allocation in the WAN-Edge Egress Queue
Voice	EF	5%	N/A	VOICE	VOICE bandwidth is priority and policed to 10%
Broadcast Video	CS3	5%	N/A	BROADCAST	BROADCAST bandwidth is priority and policed to 10%
Real-Time Interac-tive	CS4	5%	N/A	REALTIME	REALTIME bandwidth is priority and policed to 13%
Multi-media Confer-encing	AF41	10%	15%	MM_CONF	BWR for MM_CONF = 15%
Multi-media Stream-ing	AF31	10%	15%	MM_STREAM	BWR MM_STREAM = 15%
Network Control	CS6	3%	4%	CONTROL	BWR for CON-TROL = 4%
Signaling	CS5	3%	3%	SIGNALING	BWR for SIGNAL-ING = 3%
OAM	CS2	8%	3%	OAM	BWR for OAM = 3%
Trans-actional Data	AF21	10%	15%	TRANS_DATA	BWR for TRANS_DATA = 15%
Bulk Data	AF11	10%	6%	BULK_DATA	BWR for BULK_DATA = 6%
Scav-enger	CS1	1%	1%	SCAVENGER	BWR for SCAV-ENGER = 1%
Best Effort	De-fault	30%	38%	Default Queue	BWR for Default Queue = 38%



The effects of the changes in DSCP marking and bandwidth allocation on the ingress classification & marking policy and the egress queuing policy provisioned to ASR and ISR router platforms are discussed in the sections below.

#### Changing the DSCP Markings of Traffic-Classes through Custom Queuing Profiles

Changing the DSCP marking of a traffic-class will modify the policy-action of the ingress classification & marking policy class-map definitions that reference the traffic-class.

- Note: Caution should be used when changing the default DSCP marking of traffic-classes from the Cisco recommended 12-class QoS model. Such changes could result in a less than optimal QoS implementation unless the network operator is highly knowledgeable in QoS design and implementation. This feature is only for customers with advanced knowledge of QoS.

The following output provides an example of the ingress classification & marking policy where Broadcast Video traffic has been marked to CS3 and Signaling traffic has been marked to CS5 (as specified in IETF RFC 4594). The affected class-map definitions in the policy-map are highlighted in bold.

!

```
policy-map prm-MARKING_IN
class prm-MARKING_IN#TUNNELED-NBAR
class prm-MARKING_IN#VOICE_CUSTOM
set dscp ef
class prm-MARKING_IN#BROADCAST_CUSTOM
set dscp cs3
class prm-MARKING_IN#REALTIME_CUSTOM
set dscp cs4
class prm-MARKING_IN#MM_CONF_CUSTOM
set dscp af41
class prm-MARKING_IN#MM_STREAM_CUSTOM
set dscp af31
class prm-MARKING_IN#CONTROL_CUSTOM
set dscp cs6
class prm-MARKING_IN#SIGNALING_CUSTOM
set dscp cs5
class prm-MARKING_IN#OAM_CUSTOM
set dscp cs2
class prm-MARKING_IN#TRANS_DATA_CUSTOM
set dscp af21
class prm-MARKING_IN#BULK_DATA_CUSTOM
set dscp af11
class prm-MARKING_IN#SCAVENGER_CUSTOM
set dscp cs1
class prm-MARKING_IN#VOICE
```

```
set dscp ef
class prm-MARKING_IN#BROADCAST
set dscp cs3
class prm-MARKING_IN#REALTIME
set dscp cs4
class prm-MARKING_IN#MM_CONF
set dscp af41
class prm-MARKING_IN#MM_STREAM
set dscp af31
class prm-MARKING_IN#CONTROL
set dscp cs6
class prm-MARKING_IN#SIGNALING
set dscp cs5
class prm-MARKING_IN#OAM
set dscp cs2
class prm-MARKING_IN#TRANS_DATA
set dscp af21
class prm-MARKING_IN#BULK_DATA
set dscp af11
class prm-MARKING_IN#SCAVENGER
set dscp cs1
class class-default
set dscp default
!
```

As can be seen in the example output above, the “set dscp” policy-action commands are modified to the desired DSCP markings for the traffic-classes.

- Note: Cisco recommends a modified version of RFC 4594 where Signaling traffic is marked to CS3 and Broadcast Video is marked to CS5. The default setting for call signaling within Cisco Unified Communications Manager is set to CS3.

Changing the DSCP markings of traffic-classes within the EasyQoS web-based GUI also affects the “match dscp” statements of class-map definitions within the egress queuing policy of ISR and ASR router platforms. This applies only to the WAN-Edge Egress Queuing Policy discussed previously and not to the egress queuing policies provisioned when WAN SPPs, which are discussed in the next chapter, are used.

The following output is an example of the modification of the class-map definitions provisioned by EasyQoS, based upon the DSCP markings from the EasyQoS\_Lab\_Queueing Profile, shown in the table above. The affected class-map definitions in the policy-map are highlighted in bold.

```
!
class-map match-any prm-EZQOS_12C#VOICE
match dscp ef
```

**class-map match-any prm-EZQOS\_12C#BROADCAST****\*\*match dscp cs3 \*\***

class-map match-any prm-EZQOS\_12C#REALTIME

match dscp cs4

class-map match-any prm-EZQOS\_12C#CONTROL

match dscp cs6

**class-map match-any prm-EZQOS\_12C#SIGNALING****\*\*match dscp cs5 \*\***

class-map match-any prm-EZQOS\_12C#OAM

match dscp cs2

class-map match-any prm-EZQOS\_12C#MM\_CONF

match dscp af41

match dscp af42

match dscp af43

class-map match-any prm-EZQOS\_12C#MM\_STREAM

match dscp af31

match dscp af32

match dscp af33

class-map match-any prm-EZQOS\_12C#TRANS\_DATA

match dscp af21

match dscp af22

match dscp af23

class-map match-any prm-EZQOS\_12C#BULK\_DATA

match dscp af11

match dscp af12

match dscp af13

class-map match-any prm-EZQOS\_12C#SCAVENGER

match dscp cs1

!

As can be seen by comparing the class-map definitions between the default Queuing Profile (CVD\_Queueing\_Profile) and the EasyQoS\_Lab\_Queueing Profile, the Broadcast traffic-class matches on CS3 instead of CS5, and the Signaling traffic-class matches on CS5.

**Changing the Bandwidth Allocation of Traffic-Classes through Custom Queuing Profiles**

Bandwidth allocations done through custom Queuing Profiles modify the amount bandwidth allocated through the “police rate percent” and “bandwidth remaining percent” commands within the egress queuing policy-map definition. Again, this applies only to the WAN-Edge Egress Queuing Policy discussed previously, and not to the egress queuing policies provisioned when WAN SPPs, which are discussed in the next chapter, are used.

Table 6 above shows how changing the amount of bandwidth allocated to each traffic class modifies the bandwidth allocated to the three low-latency and nine non-priority queues within the WAN-Edge Egress Queuing Policy model.

Based on the formula discussed previously, the new total priority queue bandwidth (Total\_PQ\_BW) is calculated as follows:

$$\text{Total\_PQ\_BW} = 5\% \text{ (Voice BW)} + 5\% \text{ (Broadcast Video BW)} + 5\% \text{ (Real-Time Interactive BW)} = 15\%$$

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI, and the amount of Total\_PQ\_BW, through the following formula.

$$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$$

For example, the new BWR percentage for the Multimedia Streaming traffic class can be calculated as follows:

$$\text{Multimedia\_Conferencing\_BWR} = (10\% / (100\% - 15\%)) * 100 = 12\% \text{ when rounded}$$

Because each traffic-class is mapped to a separate queue, determining the bandwidth ratio allocated to each of the non-priority queues within the WAN-Edge Egress Queuing Policy model is simply a matter of copying the Traffic\_Class\_BWR numbers to the each of the queues shown in column 6 in the Table 6 above.

Note that some rounding error may be introduced in order to ensure the “bandwidth remaining percentage” statements within the WAN-Edge Queuing policy-map definition total to 100%.

This results in the following egress queuing policy-map definition when deployed on an ASR or ISR router platform.

!

```
policy-map prm-dscp#QUEUEING_OUT#1G
class prm-EZQOS_12C#VOICE
  police rate percent 5
  priority
class prm-EZQOS_12C#BROADCAST
  police rate percent 5
  priority
class prm-EZQOS_12C#REALTIME
  police rate percent 5
  priority
class prm-EZQOS_12C#MM_CONF
  bandwidth remaining percent 12
  fair-queue
  random-detect dscp-based
class prm-EZQOS_12C#MM_STREAM
  bandwidth remaining percent 12
  fair-queue
  random-detect dscp-based
class prm-EZQOS_12C#CONTROL
  bandwidth remaining percent 4
```

```

class prm-EZQOS_12C#SIGNALING
bandwidth remaining percent 4
class prm-EZQOS_12C#OAM
bandwidth remaining percent 9
class prm-EZQOS_12C#TRANS_DATA
bandwidth remaining percent 12
fair-queue
random-detect dscp-based
class prm-EZQOS_12C#BULK_DATA
bandwidth remaining percent 12
fair-queue
random-detect dscp-based
class prm-EZQOS_12C#SCAVENGER
bandwidth remaining percent 1
class class-default
bandwidth remaining percent 34
fair-queue
random-detect dscp-based
random-detect dscp 0 50 64 ! ISR G2 and 800 Series platforms only.
!
```

The network operator should also note that the bandwidth allocations for each of the traffic-classes within custom Queuing Profiles configured within the EasyQoS GUI can be applied to all interface speeds—referred to as All References within the EasyQoS GUI. Alternatively different bandwidth allocations can be configured for each of the traffic-classes based on the interface speed—1 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10 Gbps, and 100 Gbps.

In the configuration example above, the bandwidth allocations have been modified from the CVD\_Queueing\_Profile for 1 Gbps interface speeds. When different bandwidth allocations are assigned to each of the interface speeds within the EasyQoS GUI for custom Queuing Profiles, EasyQoS will append the interface speed to the name of the policy-map generated, in order to differentiate the policy-map for that particular interface speed. For example, the policy-map name in the configuration above has been changed from “policy-map prm-dscp#QUEUEING\_OUT” to “policy-map prm-dscp#QUEUEING\_OUT#1G” indicating this policy-map is to be applied to 1 Gbps interfaces. In this manner, different policy-maps with different bandwidth allocations for the traffic-classes can be generated by EasyQoS for the various interface speeds supported by the platform—all within a single custom Queuing Profile. The network operator can use this flexibility in order to assign different bandwidth allocations for uplink ports vs. access-edge ports within a single custom Queuing Profile, if desired.

If the bandwidth allocations for each of the traffic-classes within a custom Queuing Profile is the same across all interface speeds (referred to as All References within the EasyQoS GUI), EasyQoS will optimize the configuration, and create a single policy-map with the name “policy-map prm-dscp#QUEUEING\_OUT” with the bandwidth allocations specified within the custom Queuing Profile.

#### ASR-1000 Series Specific Interface-Level Commands

For the ASR-1000 Series platforms, additional interface-level configuration commands are provisioned by APIC-EM EasyQoS. Network input/output on the ASR-1000 Series platforms consists of shared port adapters (SPAs) controlled by one or more SPA interface processors (SIPs). Ethernet and ATM SPAs perform Layer 2 and Layer 3 packet

classification, and they also decide on the internal priority of the packet—high priority or low priority. High-priority packets are sent on separate channels to the embedded services processor (ESP) than low-priority packets. QoS is then performed within the ESP. The SPA queues packets on high channels to high-priority buffers, and packets on low channels to low-priority buffers. Internal classification of packets can be based on DSCP, IPv6 traffic class, MPLS EXP or 802.1Q/P class of service (CoS) values.

APIC-EM EasyQoS enables SPA-based internal scheduling and classification by provisioning the following commands on ASR 1000 Series platforms:

```
!  
plim qos input map ip DSCP-based  
plim qos input map ip DSCP 32 40 46 queue strict-priority  
!
```

The first command enables DSCP-based classification within the SPA. By default, EF (voice) traffic is mapped to the strict-priority internal queue, and all other DSCP values are mapped to the low-priority internal queue. The second command modifies this by mapping CS4 (real-time interactive) and CS5 (broadcast video) traffic to the strict-priority internal queue.

- Note: When restoring the configuration on an ASR 1000 Series platform to a pre-EasyQoS policy, APIC-EM will not remove any of the “plim qos” commands configured on the platform. This must be manually removed by the network operator if desired.

#### Pre-Existing QoS Configurations on ISR and ASR Router Platforms

This section discusses how EasyQoS handles prior QoS configurations on ISR and ASR router platforms when deploying a QoS policy. IOS (ISR G2 and 800 Series routers) and IOS XE (ISR 4400 and ASR 1000 Series routers) platforms implement both ingress classification & marking policies and queuing policies by applying a service-policy definition across interfaces. The service-policy definition references an existing policy-map definition. For both ingress classification & marking policies and queuing policies, EasyQoS will remove any existing service-policy definition from the interface and replace it with its service-policy definitions. The previous class-map and policy-map definitions will not be deleted by EasyQoS. This is necessary for restoring the original pre-EasyQoS (before any EasyQoS configuration was applied) configuration back to the switch platform. Clicking the Restore button within an EasyQoS policy will cause the pre-EasyQoS classification & marking and queuing service-policy statements to be re-applied to the interfaces.

- Note: If the network operator has manually deleted the original QoS configuration (that is, the Pre-EasyQoS configuration)—meaning the policy-map and class-map definitions—the Restore feature will not be able to restore the QoS configuration on the device to its original configuration.

The Restore feature will not remove any “plim qos” commands on the ASR 1000 Series platforms discussed in the **\*ASR-1000 Series Specific Interface-Level Commands\*** section above.

## 1.7 Chapter 7: Service Provider Managed-Service WAN QoS Design

### Challenges

WAN connectivity to a service provider managed-service offering may involve sub-line rate bandwidth provisioning—meaning that the provisioned bandwidth is below the physical interface of the ISR or ASR router platform. For example, it is common to provision a managed-service offering in which the physical connectivity between the Customer Edge router and the Provider Edge router is a Gigabit Ethernet connection. However, the contracted rate between the service provider and the organization is only provisioned for perhaps 50 Mbps or 100 Mbps of total bandwidth.

The contracted rate may be further sub-divided into multiple traffic-classes. It is common for service providers to offer between four and eight traffic-classes. Some of these traffic-classes provide Service Level Agreements for support of real-time (priority) traffic such as voice and video support, while others provide data or best effort service. The number

of traffic-classes supported by the service provider, the percentage bandwidth allocation between the traffic-classes, and the supported DSCP markings of those traffic-classes—are collectively referred to as the SPP.

In order to support deployments that have managed-service offerings, APIC-EM must determine the following when deploying QoS policy to ISR/ASR router platforms:

Is a WAN interface connected to a managed-service offering?

If so, what is the sub-line rate of the managed-service offering (if any)?

What is the service provider profile for this managed-service offering—meaning how many traffic-classes are implemented by the service provider, are any eligible for priority treatment, what is the expected mapping of the DSCP values from the traffic-classes within the organization to the traffic-classes within the service-provider, and what are the percentage bandwidth allocations between the service provider traffic-classes?

EasyQoS supports four default SPP models. Each of the default SPP models supports the following:

- A fixed number of traffic-classes (4, 5, 6, and 8 classes)
- A fixed mapping of the DSCP values and priority treatment from the traffic-classes within the organization to the traffic-classes within the service-provider network
- Fixed bandwidth allocations between the service provider traffic-classes

Additionally, as of APIC-EM release 1.3 and higher, EasyQoS supports the ability to create custom SPPs based on the default 4, 5, 6, and 8 class SPP models. Custom service provider profiles allow the network operator to specify the mapping of the DSCP values from the traffic-classes within the organization to the traffic-classes within the service-provider network, as well as to specify the percentage bandwidth allocations between the service provider traffic-classes.

EasyQoS requires the network operator to tag WAN interfaces with a specific string in the interface-description in order to identify the items listed in the three questions above. This must be configured before deploying a QoS policy to the platform via EasyQoS.

There are up to three important fields within the tag. Each of the fields within the tag is delineated via a “#”. The meaning of the fields within the tag is discussed in the following sections.

#### Identifying WAN Interfaces

EasyQoS requires the network operator to tag WAN interfaces that connect to a service-provider managed service with a specific string in the interface-description: #WAN#. This is the first field in the overall tag discussed in the previous section, and is a required field.

An example of the configuration is shown below with the first part of the tag highlighted.

!

```
interface GigabitEthernet0/0
```

```
description CIRCUIT TO WE-ASR2 GIG-0-0-1 #WAN#50M#SPP:New-6-Class#
```

!

- Note: If the network operator has configured no tag on a WAN interface, EasyQoS applies the WAN-Edge Egress Queuing Policy discussed in the **\*WAN and Branch Static QoS Design\*** chapter. This is because the WAN-Edge Egress Queuing Policy is also applied to LAN connections between the ISR or ASR platform and the Catalyst switch, and LAN connections are not required to have any tag within their interface descriptions.

Currently the #WAN# part of the overall tag provides no additional functionality in the context of a service-provider managed-service other than to identify the interface as a WAN connection.

#### Identifying Sub-Line Rate WAN Interfaces

Optionally, when connecting to a service provider managed-service using sub-line rate connectivity EasyQoS requires the network operator to tag WAN interfaces with the sub-line rate—meaning the overall provisioned bandwidth of

the service contracted from the service provider. The sub-line rate is tagged with a specific string in the interface-description: #rate#. This is the second field in the overall tag discussed previously. If a sub-line rate service is not provisioned, this field can be omitted within the overall tag.

An example of the configuration is shown below with the second part of the tag highlighted.

```
!  
interface GigabitEthernet0/0  
description CIRCUIT TO WE-ASR2 GIG-0-0-1 #WAN#50M#SPP:New-6-Class#  
!
```

The rate is specified using abbreviations—“M” for Mbps. In the example above “50M” stands for a sub-line rate of 50 Mbps contracted from the service provider. This rate is read by APIC-EM during inventory process and is then used by EasyQoS to provision the shaper at the top-level of the hierarchical egress queuing policy. This shaper is necessary to provide the back-pressure in order for QoS to be engaged on the WAN link, when implementing a sub-line rate service.

### Identifying WAN Interfaces Mapped to SP Class-of-Service Models

EasyQoS requires the network operator to tag WAN interfaces with either the name of one of the four default SPPs or the name of a custom profile, when connected to a service provider managed-service. The format of the tag is dependent upon whether one of the four default service provider profiles is to be attached to the interface or whether a custom service provider profile is to be attached to the interface.

#### Default Service Provider Profiles

When implementing one of the four default service provider profiles, the format of the tag can take one of the two forms.

The first form provides backward compatibility with prior versions of APIC-EM EasyQoS.

#WAN#rate#SPPx#

The “x” in “SPPx” refers to one of the four default service provider profiles, which are discussed in detail in the following sections.

The second form is uses the same format as custom service provider profiles.

#WAN#rate#SPP:SPPx-yClass

The “x” in SPP:SPPx-yClass” refers to one of the four default service provider profiles, which are discussed in detail in the following sections. The “y” in “SPP:SPPx-yClass” refers to the number of traffic-classes supported by the service provider.

The two forms can be used to express the same service provider profile as shown below:

- SPP1 = SPP:SPP1-4Class
- SPP2 = SPP:SPP2-5Class
- SPP3 = SPP:SPP3-6Class
- SPP4 = SPP:SPP4-8Class

An example of the configuration of an interface description using the default service provider profile SPP1 within the tag is shown below, with the third part of the tag highlighted.

```
!  
interface GigabitEthernet0/0  
description CIRCUIT TO WE-ASR2 GIG-0-0-1 #WAN#50M#SPP1#  
!
```



## Custom Service Provider Profiles

When implementing one of the custom service provider profiles, the format of the tag is as follows:

```
#WAN#rate#SPP:custom_profile_name#
```

The “custom\_profile\_name” refers to the name of the custom service provider profile created within the EasyQoS GUI. This is discussed in the **\*APIC-EM and the EasyQoS Application\*** chapter of this document. An example of the configuration of an interface description using a custom service provider profile named “New-6-Class” within the tag is shown below, with the third part of the tag highlighted.

```
!
interface GigabitEthernet0/0
description CIRCUIT TO WE-ASR2 GIG-0-0-1 #WAN#50M#SPP1:New-6-Class#
!
```

Each of the four default service provider profiles, as well as custom service provider profiles is discussed in the **\*Service Provider Default Class of Service Models\*** section below.

- Note: If the tag within the interface description is added, removed, or modified, the network operator must wait until APIC-EM re-synchronizes the configuration of the ISR or ASR router by running its inventory process again before re-applying any QoS policy to the device. APIC-EM will synchronize the configuration of network devices approximately every 25 minutes by default, although the polling interval can be modified as of APIC-EM release 1.4 and higher. Alternatively, the network operator can manually sync the device, which is another new feature added to APIC-EM release 1.4 and higher. If a QoS policy is re-applied to the device by EasyQoS before APIC-EM has re-synchronized the configuration with its internal database, the EasyQoS policy may not reflect the desired changes to the policy, based on the changes to the interface description.

## Service Provider Default Class of Service Models

EasyQoS supports connectivity to service provider managed-service offerings, using one of the following four default SPP class-of-service models for ISR and ASR router platforms:

- SPP1/SPP:SPP1-4Class
- SPP2/SPP:SPP2-5Class
- SPP3/SPP:SPP3-6Class
- SPP4/SPP:SPP4-8Class

Because queuing is done in software on ISR and ASR router platforms, all SPP models implement an egress queuing policy consisting of 12 egress queues—one for each of the traffic-classes as shown in Figure 5 earlier in this document.

APIC-EM determines which of the four SPP models to deploy based on the #SPPx#” field (where x is from 1 to 4) or “#SPP:SPPx-yClass#” (where x is from 1 to 4 and y is 4, 5, 6, or 8) within the description configured on the ISR or ASR WAN interface connected to the service provider managed-service.

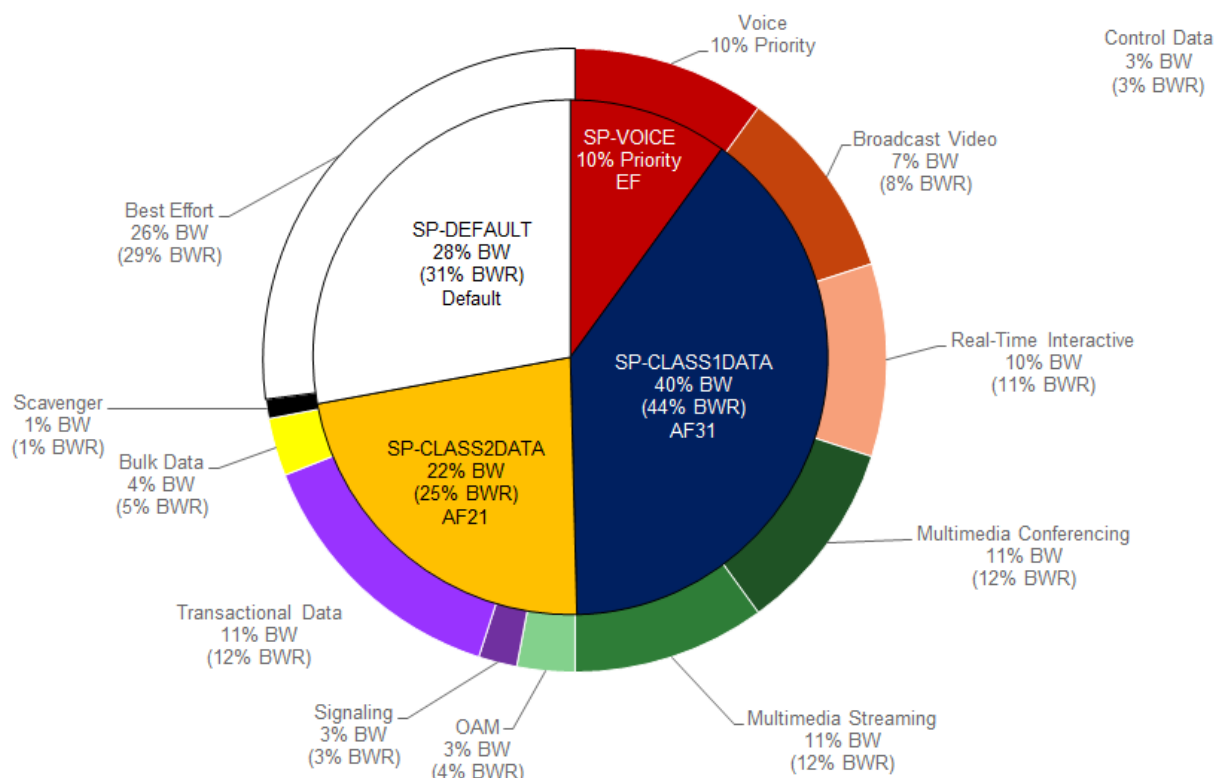
SPP1 or SPP:SPP1-4Class

The SPP1/SPP:SPP1-4Class service provider profile is based on managed-service offerings with four traffic-classes. These traffic-classes are specified as follows within this document:

- SP-Voice
- SP-Class1Data
- SP-Class2Data
- SP-Default

The following figure shows the WAN bandwidth allocation for the SPP1/SPP:SPP1-4Class service provider profile.

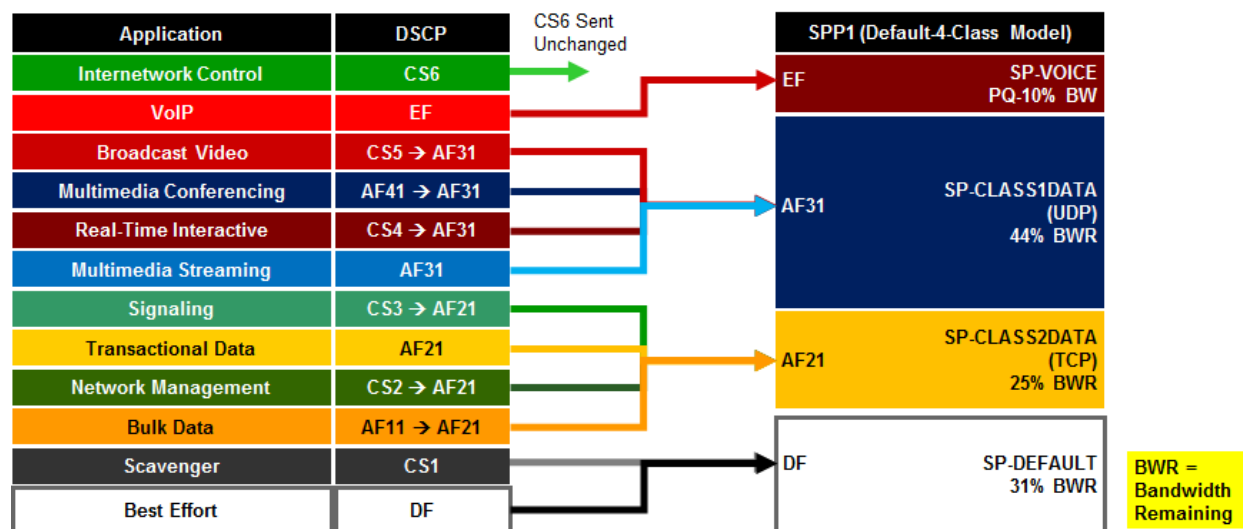
## 1. WAN Bandwidth Allocation for the SPP1/SPP:SPP1-4Class



The egress queuing policy class-map definitions provisioned by EasyQoS for all of the SPPs discussed here are the same as was as discussed in the **\*WAN-Edge Egress Queuing Policy\*** section of the **\*WAN and Branch Static QoS Design\*** chapter, and will not be duplicated here.

For the SPP1/SPP:SPP1-4Class model, EasyQoS must map the RFC 4594-based 12-class QoS model implemented within the organization into the four traffic-classes provide by the service provider. The following figure shows this mapping with the bandwidth allocations and traffic re-marking for the service provider traffic-classes.

## 1. EasyQoS Marking Mappings Into SPP1/SPP:SPP1-4Class



The following is an example of the hierarchical policy-map definition provisioned by EasyQoS that implements the SPP1/SPP:SPP1-4Class egress queuing policy with the bandwidths and traffic re-marking for each of the service provider traffic-classes. It assumes a sub-line rate of 50 Mbps to the service provider network.

```
!  
policy-map prm-dscp#EQ_SPP1-4Class#shape#50.0
```

```
class class-default
```

```
shape average 50000000
```

```
service-policy prm-dscp#EQ_SPP1-4Class
```

```
!
```

```
policy-map prm-dscp#EQ_SPP1-4Class
```

```
class prm-EZQOS_12C#VOICE
```

```
police rate percent 10
```

```
priority
```

```
set dscp ef
```

```
class prm-EZQOS_12C#BROADCAST
```

```
bandwidth remaining percent 8
```

```
set dscp af31
```

```
class prm-EZQOS_12C#REALTIME
```

```
bandwidth remaining percent 11
```

```
set dscp af31
```

```
class prm-EZQOS_12C#MM_CONF
```

```
bandwidth remaining percent 12
```

```
fair-queue
```

```
set dscp af31
```

```
random-detect dscp-based
```

```
class prm-EZQOS_12C#MM_STREAM
```

```
bandwidth remaining percent 12
```

```
fair-queue
```

```
set dscp af31
```

```
random-detect dscp-based
```

```
class prm-EZQOS_12C#CONTROL
```

```
bandwidth remaining percent 3
```

```
class prm-EZQOS_12C#SIGNALING
```

```
bandwidth remaining percent 3
```

```
set dscp af21
```

```
class prm-EZQOS_12C#OAM
```

```
bandwidth remaining percent 4
```

```
set dscp af21
class prm-EZQOS_12C#TRANS_DATA
bandwidth remaining percent 12
fair-queue
set dscp af21
random-detect dscp-based
class prm-EZQOS_12C#BULK_DATA
bandwidth remaining percent 5
fair-queue
set dscp af21
random-detect dscp-based
class prm-EZQOS_12C#SCAVENGER
bandwidth remaining percent 1
set dscp default
class class-default
bandwidth remaining percent 29
fair-queue
set dscp default
random-detect dscp-based
random-detect dscp 0 50 64 ! ISR G2 Series platforms only.
!
```

The names of the parent and child policy-maps reflect the SPP configured for the WAN interface. When using the newer method where the service provider profile is indicated via the #SPP:SPP1-4Class# tag, the format of the parent and child policy-maps will be as follows:

```
!
policy-map prm-dscp#EQ_SPP1-4Class#shape#50.0
policy-map prm-dscp#EQ_SPP1-4Class
!
```

This is the format shown in the configuration example above.

When using the older method where the service provider profile is indicated via the #SPP1#" tag, the format of the parent and child policy-maps will be as follows:

```
!
policy-map prm-dscp#EQ_1#shape#50.0
policy-map prm-dscp#EQ_1
!
```

If a sub-line rate service has been provisioned, the top-level of the SPP1/SPP:SPP1-4Class hierarchical egress queuing policy-map simply implements shaping to an average rate that matches the sub-line bandwidth rate of the managed-service offering provisioned by the service provider. This rate is learned via the `#rate#` field within the tag, which must be pre-configured within the description of the interface connected to the managed service WAN link.

- Note: If a sub-line rate service has not been provisioned, EasyQoS will not configure a hierarchical policy-map with a shaper at the parent-level. Instead, the policy-map will only have a single level with the configuration similar to the child-policy discussed below.

The child-policy of the SPP1/SPP:SPP1-4Class egress queuing policy-map implements a single LLQ policy, meaning a separate LLQ for the Voice traffic class. An explicit policer (10% of bandwidth) for the Voice queue ensures that the LLQ can use no more than the percentage of the bandwidth of the WAN link allocated to the Voice traffic class, regardless of whether there is available bandwidth.

The remaining eleven queues share the remaining bandwidth based on a percentage allocation of bandwidth. This is accomplished via the “bandwidth remaining percent” command. Each of these queues can use more than its percentage allocation, if more bandwidth is available—meaning if one or more of the other queues is not using its full allocation of remaining bandwidth percentage.

The following traffic is admitted (mapped) to the service provider SP-Voice traffic class. Traffic mapped to this service provider traffic class is remarked to EF.

- Traffic exiting the Voice queue

The bandwidth allocated to the Voice queue (10% priority and policed) is meant to match the 10% bandwidth allocation of the service provider SP-Voice traffic class as shown in Figure 66.

The following traffic is admitted (mapped) to the service provider SP-Class1Data traffic class. Traffic mapped to this service provider traffic class is remarked to AF31.

- Traffic exiting the Broadcast-Video queue re-marked from CS5
- Traffic exiting the Realtime-Interactive queue re-marked from CS4
- Traffic exiting the Multimedia-Conferencing queue re-marked from AF4x
- Traffic exiting the Multimedia-Streaming queue re-marked from AF3x

The sum of the bandwidths allocated to four queues—Broadcast-Video (8% bandwidth remaining), Realtime-Interactive (11% bandwidth remaining), Multimedia-Conferencing (12% bandwidth remaining), and Multimedia-Streaming (12% bandwidth remaining)—is meant to roughly match the 44% bandwidth remaining allocation of the service provider SP-Class1Data traffic class as shown in Figure 66.

The following traffic is admitted (mapped) to the service provider SP-Class2Data traffic class. Traffic mapped to this service provider traffic class is remarked to AF21.

- Traffic exiting the Signaling queue re-marked from AF3x
- Traffic exiting the OAM queue remarked from CS2
- Traffic exiting the Transactional-Data queue marked from AF2x
- Traffic exiting the Bulk-Data queue re-marked from AF1x

The sum of the bandwidths allocated to the four queues—Signaling (3% bandwidth), OAM (4% bandwidth), Transactional-Data (12% bandwidth remaining), and Bulk-Data (5% bandwidth remaining)—is meant to roughly match the 25% bandwidth remaining allocation of the service provider SP-Class2Data traffic class, as shown in Figure 66.

The following traffic is admitted (mapped) to the service provider SP-Default traffic class. Traffic mapped to this service provider traffic class is remarked to Default (Best Effort).

- Traffic exiting the Scavenger queue is re-marked from CS1

- Traffic exiting the Default queue

The sum of the bandwidth allocated to two queues—Scavenger (1% bandwidth remaining) and Default (29% bandwidth remaining)—is meant to roughly match the default 31% bandwidth remaining allocation of the service provider SP-Default traffic class, as shown in Figure 66.

Fair-queuing, along with DSCP-based WRED is implemented for the following queues:

- Multimedia-Conferencing
- Multimedia-Streaming
- Transactional-Data
- Bulk-Data
- Default

For ISR 3900, 2900, and 800 Series (ISR G2) platforms only, with the exception of the Default queue, minimum and maximum WRED thresholds for the queues are left at their default values. Table 5 summarized these minimum and maximum thresholds. The default WRED thresholds for the Default queue are considered to be too aggressive—meaning the minimum drop threshold is set lower than desired. Hence, the minimum drop threshold has been adjusted to 50 packets, and the maximum drop threshold adjusted to the depth of the queue—64 packets. For ISR 4400 and ASR 1000 Series platforms the minimum and maximum WRED thresholds for the queues are left at their default values.

Traffic within the Control queue is sent unchanged to the service provider network and is not considered to be mapped into one of the four service provider traffic-classes.

The SPP1/SPP:SPP1-4Class egress queuing policy is applied to WAN interfaces that include the #WAN#rate#SPP1# or #WAN#rate#SPP:SPP1-4Class# tag within the interface description.

An example of the application of the egress queuing policy is as follows:

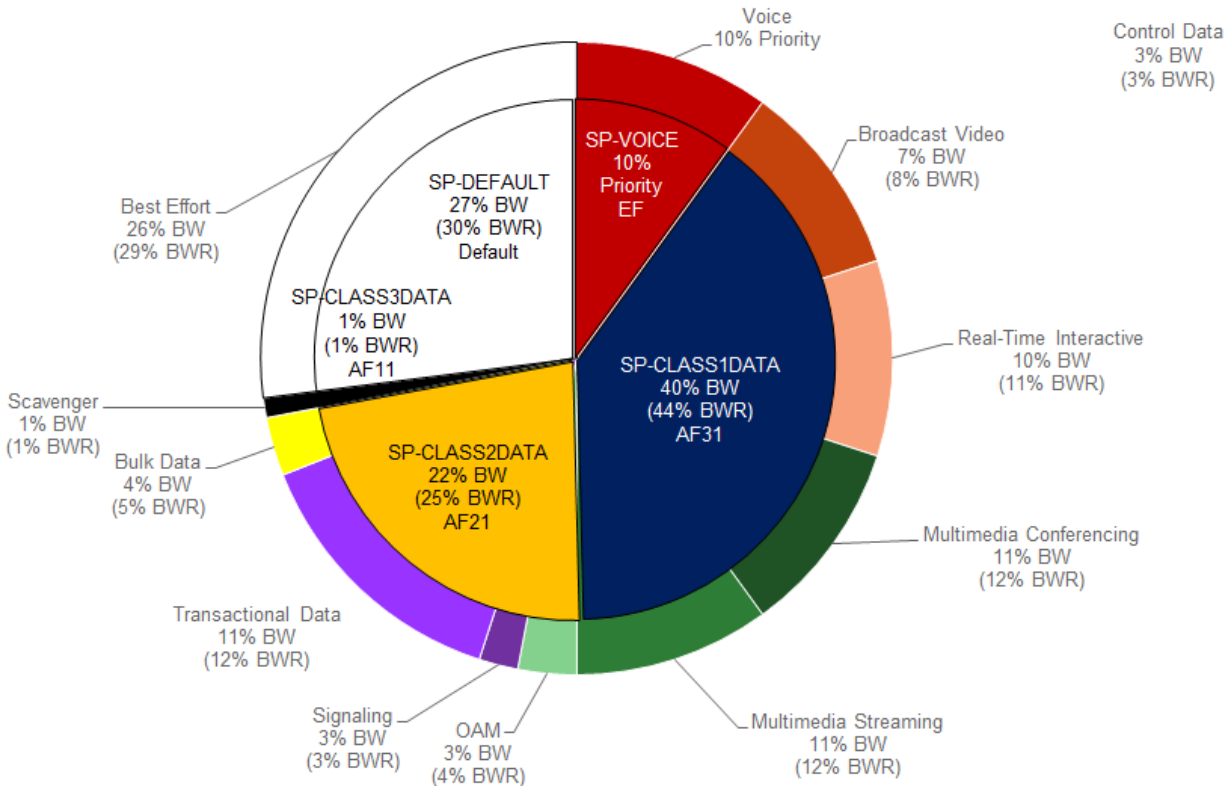
```
!  
interface GigabitEthernet0/0/3  
description TO PE2-3600X #WAN#50M#SPP:SPP1-4Class#  
service-policy output prm-dscp#EQ_SPP1-4Class#shape#50.0  
!  
SPP2/SPP:SPP2-5Class
```

The SPP2/SPP:SPP2-5Class service provider profile is based on managed-service offerings with five traffic-classes. These traffic-classes are specified as follows within this document:

- SP-Voice
- SP-Class1Data
- SP-Class2Data
- SP-Class3Data
- SP-Default

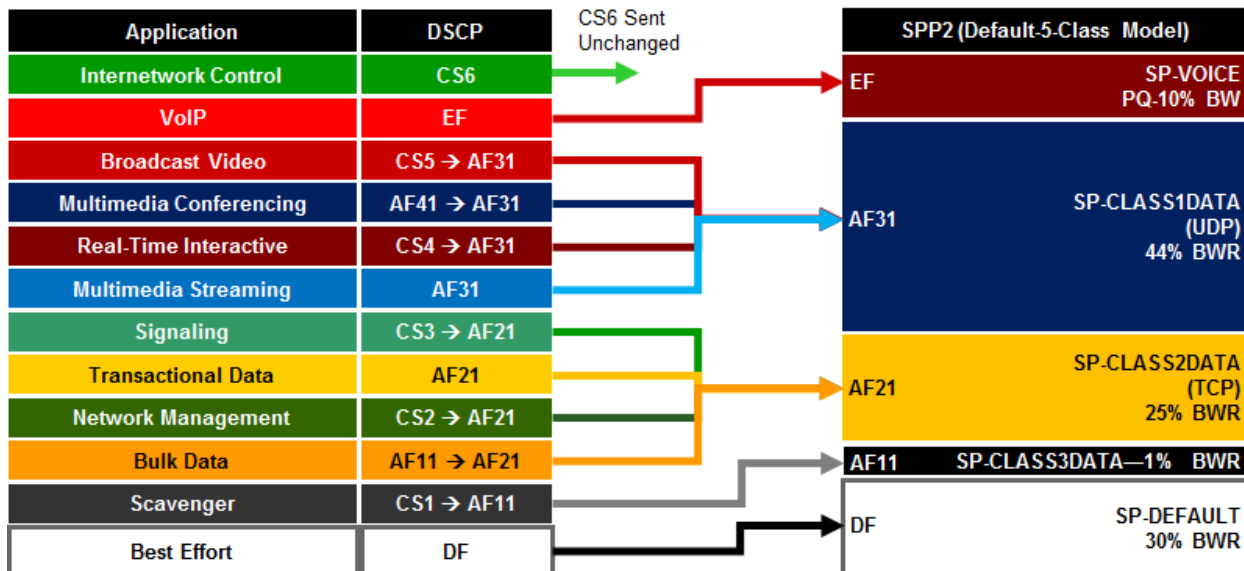
The following figure shows the WAN bandwidth allocation model for the SPP2/SPP:SPP2-5Class service provider profile.

1. WAN Bandwidth Allocation for the SPP2/SPP:SPP2-5Class



For the SPP2/SPP:SPP2-5Class, EasyQoS must map the RFC 4594-based 12-class QoS model implemented within the organization into the five traffic-classes provide by the service provider. The following figure shows this mapping with the bandwidth allocations and traffic re-marking for the service provider traffic-classes.

#### 1. EasyQoS Marking Mappings into SPP2/SPP:SPP2-5Class



The following is an example of the hierarchical policy-map definition provisioned by EasyQoS that implements the SPP2/SPP:SPP2-5Class queuing policy with the bandwidths and traffic re-marking for each of the service provider traffic-classes. It assumes a sub-line rate of 50 Mbps to the service provider network.

```
!  
policy-map prm-dscp#EQ_SPP2-5Class#shape#50.0  
class class-default  
shape average 50000000  
service-policy prm-dscp#EQ_SPP2-5Class  
!  
policy-map prm-dscp#EQ_SPP2-5Class  
class prm-EZQOS_12C#VOICE  
police rate percent 10  
priority  
set dscp ef  
class prm-EZQOS_12C#BROADCAST  
bandwidth remaining percent 8  
set dscp af31  
class prm-EZQOS_12C#REALTIME  
bandwidth remaining percent 11  
set dscp af31  
class prm-EZQOS_12C#MM_CONF  
bandwidth remaining percent 12  
fair-queue  
set dscp af31  
random-detect dscp-based  
class prm-EZQOS_12C#MM_STREAM  
bandwidth remaining percent 12  
fair-queue  
set dscp af31  
random-detect dscp-based  
class prm-EZQOS_12C#CONTROL  
bandwidth remaining percent 3  
class prm-EZQOS_12C#SIGNALING  
bandwidth remaining percent 3  
set dscp af21  
class prm-EZQOS_12C#OAM  
bandwidth remaining percent 4  
set dscp af21  
class prm-EZQOS_12C#TRANS_DATA
```



```

bandwidth remaining percent 12
fair-queue
set dscp af21
random-detect dscp-based
class prm-EZQOS_12C#BULK_DATA
bandwidth remaining percent 5
fair-queue
set dscp af21
random-detect dscp-based
class prm-EZQOS_12C#SCAVENGER
bandwidth remaining percent 1
set dscp af11
class class-default
bandwidth remaining percent 29
fair-queue
set dscp default
random-detect dscp-based
random-detect dscp 0 50 64 ! ISR G2 Series platforms only.
!
```

Again, the names of the parent and child policy-maps reflect the SPP configured for the WAN interface. When using the newer method where the service provider profile is indicated via the #SPP:SPP2-5Class# tag, the format of the parent and child policy-maps will be as follows:

```

!
policy-map prm-dscp#EQ_SPP2-5Class#shape#50.0
policy-map prm-dscp#EQ_SPP2-5Class
!
```

This is the format shown in the configuration example above.

When using the older method where the service provider profile is indicated via the #SPP2#” tag, the format of the parent and child policy-maps will be as follows:

```

!
policy-map prm-dscp#EQ_2#shape#50.0
policy-map prm-dscp#EQ_2
!
```

The difference between the SPP1 and SPP2 models is that a 5th service provider traffic class—SP-Class3Data—is provisioned specifically for handling traffic with a lower than best-effort treatment (Scavenger traffic).

The policy-map admits and re-marks traffic exiting the Scavenger queue from CS1 to AF11, corresponding to the service provider SP-Class3Data traffic class. The bandwidth allocated to the Scavenger queue (1% bandwidth remaining)

is meant to match the 1% bandwidth remaining allocated to the service provider SP-Class3Data traffic class, as shown in Figure 68.

The SPP2/SPP:SPP2-5Class egress queuing policy is applied to WAN interfaces that include the #WAN#rate#SPP2# or #WAN#rate#SPP:SPP2-5Class# tag within the interface description.

An example of the application of the egress queuing policy is as follows:

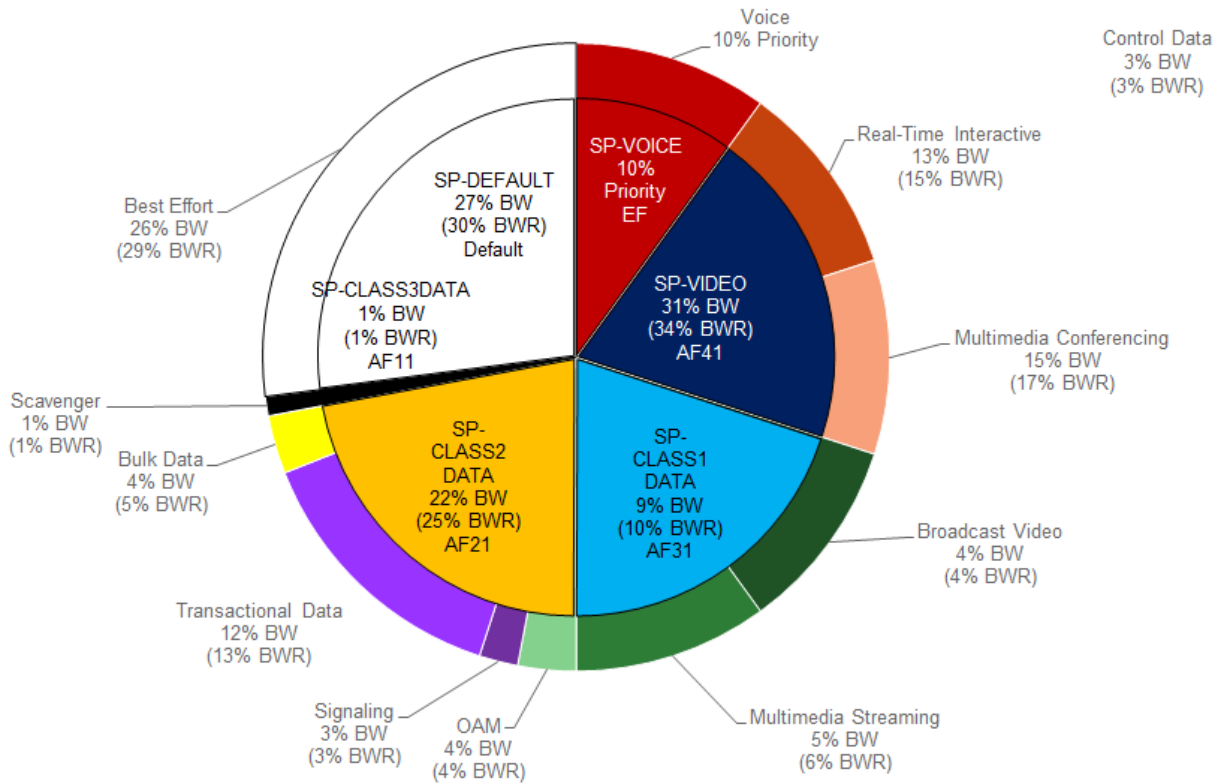
```
!  
interface GigabitEthernet0/0/5  
description APIC-EM-1.4-TEST #WAN#50M#SPP:SPP2-5Class#  
service-policy output prm-dscp#EQ_SPP2-5Class#shape#50.0  
!  
SPP3/SPP:SPP3-6Class
```

The SPP3/SPP:SPP3-6Class service provider profile is based on managed-service offerings with six traffic-classes. These traffic-classes are specified as follows within this document:

- SP-Voice
- SP-Video
- SP-Class1Data
- SP-Class2Data
- SP-Class3Data
- SP-Default

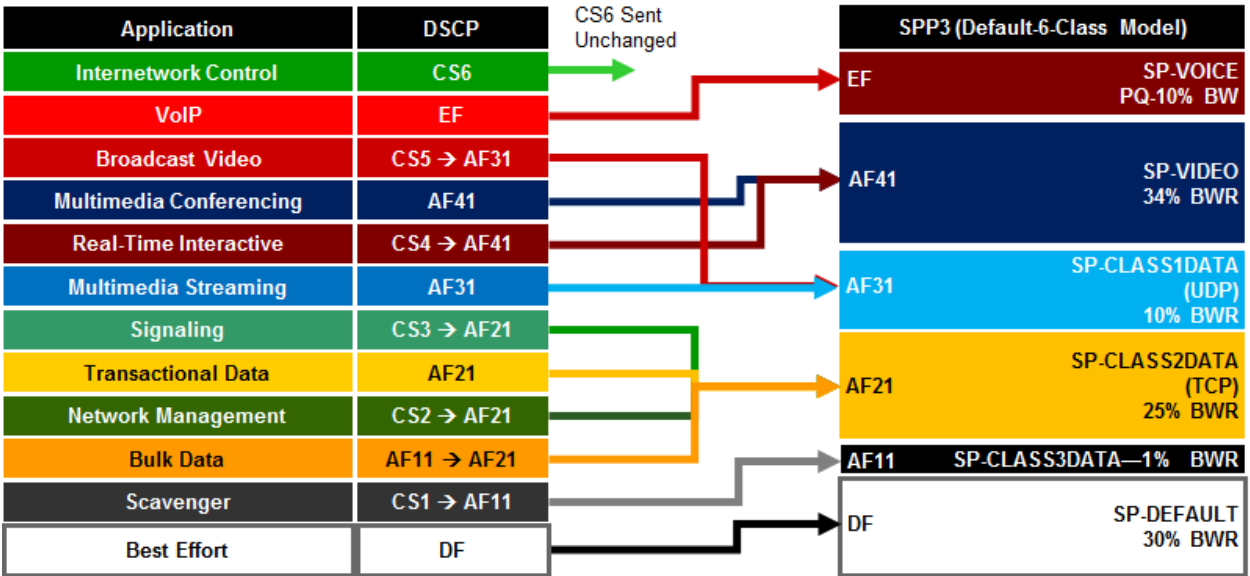
The following figure shows the WAN bandwidth allocation model for the SPP3/SPP:SPP3-6Class service provider profile.

1. WAN Bandwidth Allocation for the SPP3/SPP:SPP3-6Class



For the SPP3/SPP:SPP3-6Class, EasyQoS must map the RFC 4594-based 12-class QoS model implemented within the organization into the six traffic-classes provide by the service provider. The following figure shows this mapping with the bandwidth allocations and traffic re-marking for the service provider traffic-classes.

1. EasyQoS marking Mappings Into SPP3/SPP:SPP3-6Class



The following is an example of the hierarchical policy-map definition provisioned by EasyQoS that implements the SPP3/SPP:SPP3-6Class queuing policy, with the bandwidths and traffic re-marking for each of the service provider traffic-classes. It assumes a sub-line rate of 50 Mbps to the service provider network.

```
!  
policy-map prm-dscp#EQ_SPP3-6Class#shape#50.0  
class class-default  
shape average 50000000  
service-policy prm-dscp#EQ_SPP3-6Class  
!  
policy-map prm-dscp#EQ_SPP3-6Class  
class prm-EZQOS_12C#VOICE  
police rate percent 10  
priority  
set dscp ef  
class prm-EZQOS_12C#BROADCAST  
bandwidth remaining percent 4  
set dscp af31  
class prm-EZQOS_12C#REALTIME  
bandwidth remaining percent 15  
set dscp af41  
class prm-EZQOS_12C#MM_CONF  
bandwidth remaining percent 17  
fair-queue  
set dscp af41  
random-detect dscp-based  
class prm-EZQOS_12C#MM_STREAM  
bandwidth remaining percent 6  
fair-queue  
set dscp af31  
random-detect dscp-based  
class prm-EZQOS_12C#CONTROL  
bandwidth remaining percent 3  
class prm-EZQOS_12C#SIGNALING  
bandwidth remaining percent 3  
set dscp af21  
class prm-EZQOS_12C#OAM  
bandwidth remaining percent 4  
set dscp af21  
class prm-EZQOS_12C#TRANS_DATA
```

```

bandwidth remaining percent 13
fair-queue
set dscp af21
random-detect dscp-based
class prm-EZQOS_12C#BULK_DATA
bandwidth remaining percent 5
fair-queue
set dscp af21
random-detect dscp-based
class prm-EZQOS_12C#SCAVENGER
bandwidth remaining percent 1
set dscp af11
class class-default
bandwidth remaining percent 29
fair-queue
set dscp default
random-detect dscp-based
random-detect dscp 0 50 64 ! ISR G2 Series platforms only.
!
```

The names of the parent and child policy-maps reflect the SPP configured for the WAN interface. When using the newer method where the service provider profile is indicated via the #SPP:SPP3-6Class# tag, the format of the parent and child policy-maps will be as follows:

```

!
policy-map prm-dscp#EQ_SPP3-6Class#shape#50.0
policy-map prm-dscp#EQ_SPP3-6Class
!
```

This is the format shown in the configuration example above.

When using the older method where the service provider profile is indicated via the #SPP3#” tag, the format of the parent and child policy-maps will be as follows:

```

!
policy-map prm-dscp#EQ_3#shape#50.0
policy-map prm-dscp#EQ_3
!
```

The difference between the SPP2 and SPP3 models is that a 6th service provider traffic class—SP-Video—is provisioned specifically for handling video traffic.

The following traffic is admitted (mapped) to the service provider SP-Video traffic class. Traffic mapped to this service provider traffic class is remarked to AF41.

- Traffic exiting the Realtime-Interactive queue is re-marked from CS4

- Traffic exiting the Multimedia-Conferencing re-marked from AF4x

The sum of the bandwidth allocated to two queues—Realtime-Interactive (15% bandwidth remaining) and Multimedia-Conferencing (17% bandwidth remaining)—is meant to roughly match the 34% bandwidth remaining allocation of the service provider SP-Class1Data traffic class as shown in Figure 70.

The mappings are also adjusted so that the following is admitted (mapped) to the service provider SP-Class1Data traffic class. Traffic mapped to this service provider traffic class is remarked to AF31.

- Traffic exiting the Broadcast-Video queue is re-marked from CS5
- Traffic exiting the Multimedia-Streaming queue is re-marked from AF3x

The sum of the bandwidth allocated to two queues—Broadcast-Video (4% bandwidth remaining) and Multimedia-Streaming (6% bandwidth remaining)—is meant to roughly match the 10% bandwidth remaining allocation of the service provider SP-Streaming-Video traffic class as shown in Figure 70.

The SPP3/SPP:SPP3-6Class egress queuing policy is applied to WAN interfaces that include the #WAN#rate#SPP3# or #WAN#rate#SPP:SPP3-6Class# tag within the interface description.

An example of the application of the egress queuing policy is as follows:

```
!  
interface GigabitEthernet0/0/3.10  
description #WAN#50M#SPP:SPP3-6Class#  
service-policy output prm-dscp#EQ_SPP3-6Class#shape#50.0  
!
```

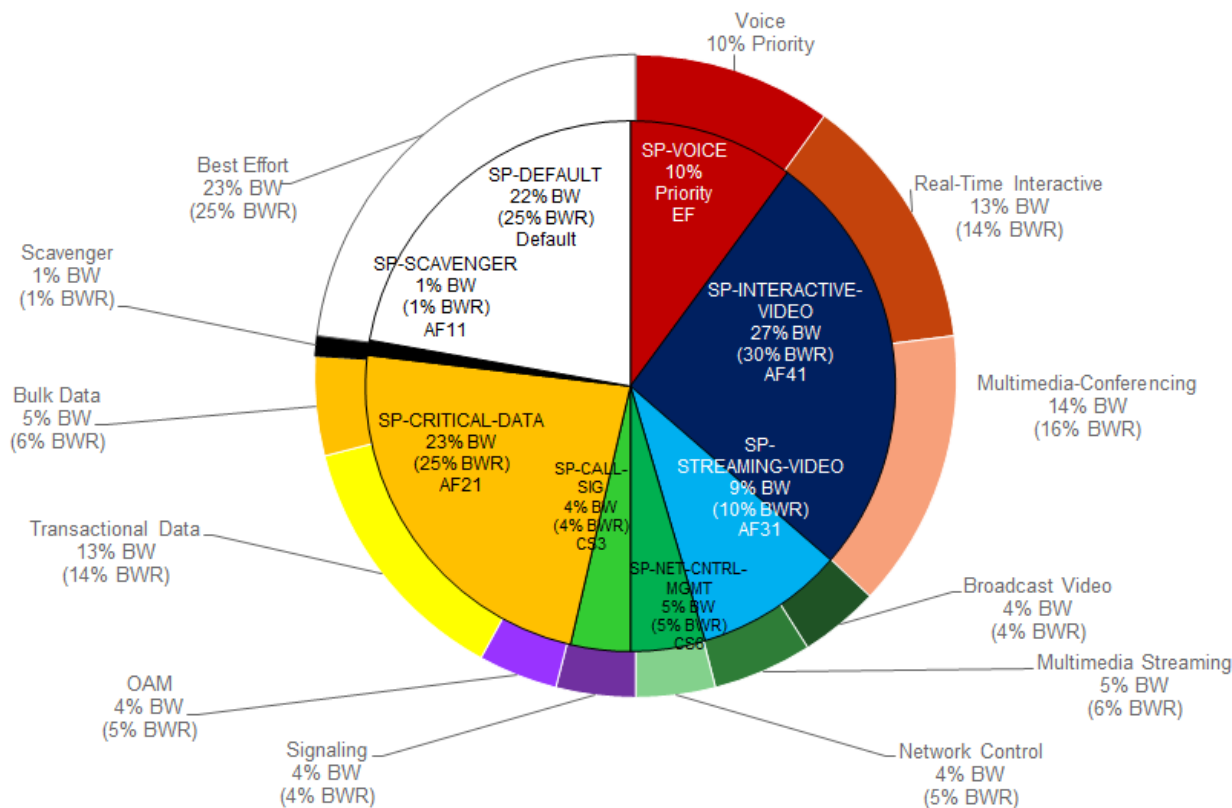
SPP4/SPP:SPP4-8Class

The SPP4/SPP:SPP4-8Class service provider profile is based on managed-service offerings with eight traffic-classes. These traffic-classes are specified as follows within this document:

- SP-Voice
- SP-Interactive-Video
- SP-Streaming-Video
- SP-Net-Ctrl-Mgmt
- SP-Call-Sig
- SP-Critical-Data
- SP-Scavenger
- SP-Default

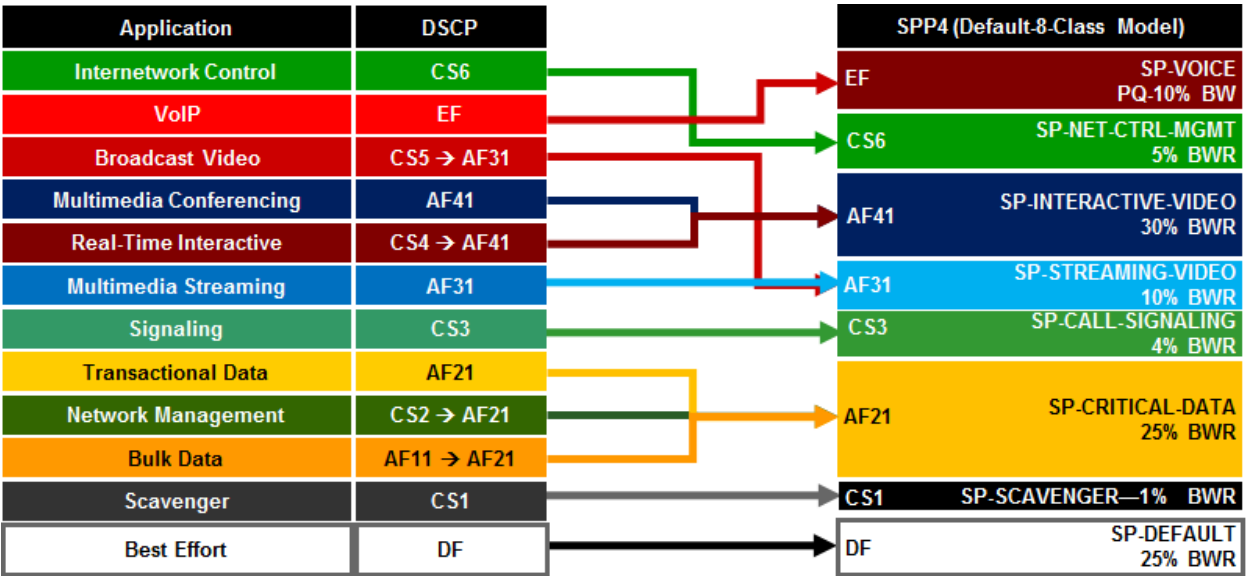
The following figure shows the WAN bandwidth allocation model for the SPP4/SPP:SPP4-8Class service provider profile.

1. WAN Bandwidth Allocation for the SPP4/SPP:SPP4-8Class



For the SPP4/SPP:SPP4-8Class, EasyQoS must map the RFC 4594-based 12-class QoS model implemented within the organization into the eight traffic-classes provide by the service provider. The following figure shows this mapping with the bandwidth allocations and traffic re-marking for the service provider traffic-classes.

1. EasyQoS Marking Mappings into SPP4



The following is an example of the hierarchical policy-map definition provisioned by EasyQoS that implements the SPP4/SPP:SPP4-8Class queuing policy with the bandwidths and traffic re-marking for each of the service provider traffic-classes. It assumes a sub-line rate of 50 Mbps to the service provider network.

```
!  
policy-map prm-dscp#EQ_SPP4-8Class#shape#50.0  
class class-default  
shape average 50000000  
service-policy prm-dscp#EQ_SPP4-8Class  
!  
policy-map prm-dscp#EQ_SPP4-8Class  
class prm-EZQOS_12C#VOICE  
police rate percent 10  
priority  
set dscp ef  
class prm-EZQOS_12C#BROADCAST  
bandwidth remaining percent 4  
set dscp af31  
class prm-EZQOS_12C#REALTIME  
bandwidth remaining percent 14  
set dscp af41  
class prm-EZQOS_12C#MM_CONF  
bandwidth remaining percent 16  
fair-queue  
set dscp af41  
random-detect dscp-based  
class prm-EZQOS_12C#MM_STREAM  
bandwidth remaining percent 6  
fair-queue  
set dscp af31  
random-detect dscp-based  
class prm-EZQOS_12C#CONTROL  
bandwidth remaining percent 5  
set dscp cs6  
class prm-EZQOS_12C#SIGNALING  
bandwidth remaining percent 4  
set dscp cs3  
class prm-EZQOS_12C#OAM  
bandwidth remaining percent 5  
set dscp af21
```



```

class prm-EZQOS_12C#TRANS_DATA
bandwidth remaining percent 14
fair-queue
set dscp af21
random-detect dscp-based
class prm-EZQOS_12C#BULK_DATA
bandwidth remaining percent 6
fair-queue
set DSCP af21
random-detect dscp-based
class prm-EZQOS_12C#SCAVENGER
bandwidth remaining percent 1
set dscp cs1
class class-default
bandwidth remaining percent 25
fair-queue
set dscp default
random-detect dscp-based
random-detect dscp 0 50 64 ! ISR G2 Series platforms only.
!
```

As with the previous service provider profile models, the names of the parent and child policy-maps reflect the SPP configured for the WAN interface. When using the newer method where the service provider profile is indicated via the #SPP:SPP4-8Class# tag, the format of the parent and child policy-maps will be as follows:

```

!
policy-map prm-dscp#EQ_SPP4-8Class#shape#50.0
policy-map prm-dscp#EQ_SPP4-8Class
!
```

This is the format shown in the configuration example above.

When using the older method where the service provider profile is indicated via the #SPP4#” tag, the format of the parent and child policy-maps will be as follows:

```

!
policy-map prm-dscp#EQ_4#shape#50.0
policy-map prm-dscp#EQ_4
!
```

If a sub-line rate service has been provisioned, the top-level of the SPP4/SPP:SPP4-8Class hierarchical egress queuing policy-map simply implements shaping to an average rate that matches the sub-line bandwidth rate of the managed-service offering provisioned by the service provider. This rate is learned via the #rate# field within the tag, which must be pre-configured within the description of the interface connected to the managed service WAN link.

The child-policy of the SPP4/SPP:SPP4-8Class egress queuing policy-map implements a single LLQ policy, meaning a separate LLQ for the Voice traffic class. An explicit policer (10% of the bandwidth) for the Voice queue ensures that the LLQ can use no more than the percentage of the bandwidth of the WAN link allocated to the traffic class, regardless of whether there is available bandwidth.

The remaining eleven queues share the remaining bandwidth based on a percentage allocation of bandwidth. This is accomplished via the “bandwidth remaining percent” command. Each of these queues can use more than its percentage allocation, if more bandwidth is available—meaning if one or more of the other queues is not using its full allocation of remaining bandwidth percentage.

The following traffic is admitted (mapped) to the service provider SP-Voice traffic class. Traffic mapped to this service provider traffic class is remarked to EF.

- Traffic exiting the Voice queue

The bandwidth allocated to the Voice queue (10% priority and policed) is meant to match the 10% bandwidth remaining allocation of the service provider SP-Voice traffic class as shown in Figure 72.

The following traffic is admitted (mapped) to the service provider SP-Net-Ctrl-Mgmt traffic class. Traffic mapped to this service provider traffic class is remarked to CS6.

- Traffic exiting the Control queue

The bandwidth allocated to the Control queue (5% bandwidth remaining) is meant to roughly match the 5% bandwidth remaining allocation of the service provider SP-Net-Ctrl-Mgmt traffic class as shown in Figure 72.

The following traffic is admitted (mapped) to the service provider SP-Interactive-Video traffic class. Traffic mapped to this service provider traffic class is remarked to AF41

- Traffic exiting the Realtime-Interactive queue re-marked from CS4
- Traffic exiting the Multimedia-Conferencing queue re-marked from AF4x

The sum of the bandwidth allocated to two queues—Realtime-Interactive (14% bandwidth remaining) and Multimedia-Conferencing (16% bandwidth remaining)—is meant to roughly match the 30% bandwidth remaining allocation of the service provider SP-Class1Data traffic class as shown in Figure 72.

The following traffic is admitted (mapped) to the service provider SP-Streaming-Video traffic class. Traffic mapped to this service provider traffic class is remarked to AF31

- Traffic exiting the Broadcast-Video queue re-marked from CS5
- Traffic exiting the Multimedia-Streaming queue re-marked from AF3x

The sum of the bandwidth allocated to two queues—Broadcast-Video (4% bandwidth remaining) and Multimedia-Streaming (6% bandwidth remaining)—is meant to roughly match the default 10% bandwidth remaining allocation of the service provider SP-Streaming-Video traffic class as shown in Figure 72.

The following traffic is admitted (mapped) to the service provider SP-Call-Signaling traffic class. By default traffic mapped to this service provider traffic class is remarked to CS3

- Traffic exiting the Signaling queue

The bandwidth allocated to the Signaling queue (4% bandwidth remaining) is meant to roughly match the 4% bandwidth remaining allocation of the service provider SP-Call-Signaling traffic class as shown in Figure 72.

The following traffic is admitted (mapped) to the service provider SP-Critical-Data traffic class. Traffic mapped to this service provider traffic class is remarked to AF21

- Traffic exiting the OAM queue re-marked from CS2
- Traffic exiting the Transactional-Data queue re-marked from AF2x
- Traffic exiting the Bulk-Data queue re-marked from AF1x

The sum of the bandwidth allocated to the three queues—OAM (5% bandwidth remaining), Transactional-Data (14% bandwidth remaining), and Bulk-Data (6% bandwidth remaining)—is meant to roughly match the 25% bandwidth remaining allocation of the service provider SP-Critical-Data traffic class, as shown in Figure 72.

The following traffic is admitted (mapped) to the service provider SP-Scavenger traffic class. Traffic mapped to this service provider traffic class is remarked to CS1.

- Traffic exiting the Scavenger queue

The bandwidth allocated to the Scavenger queue (1% bandwidth remaining) is meant to roughly match the 1% bandwidth remaining allocation of the service provider SP-Scavenger traffic class as shown in Figure 72.

The following traffic is admitted (mapped) to the service provider Default traffic class:

- Traffic exiting the Default queue

The bandwidth allocated to the Default queue (25% bandwidth remaining) is meant to roughly match the 25% bandwidth remaining allocation of the service provider SP-Default traffic class as shown in Figure 72.

Fair-queuing, along with DSCP-based WRED is implemented for the following queues:

- Multimedia-Conferencing
- Multimedia-Streaming
- Transactional-Data
- Bulk-Data
- Default

For ISR 3900, 2900, and 800 Series (ISR G2) platforms only, with the exception of the Default queue, minimum and maximum WRED thresholds for the queues are left at their default values. Table 5 summarized these minimum and maximum thresholds. The default WRED thresholds for the Default queue are considered to be too aggressive—meaning the minimum drop threshold is set lower than desired. Hence, the minimum drop threshold has been adjusted to 50 packets, and the maximum drop threshold adjusted to the depth of the queue—64 packets. For ISR 4400 Series platforms the minimum and maximum WRED thresholds for the queues are left at their default values.

The SPP4/SPP:SPP4-8Class egress queuing policy is applied to WAN interfaces that include the #WAN#rate#SPP4# or #WAN#rate#SPP:SPP4-8Class# tag within the interface description.

An example of the application of the egress queuing policy is as follows:

```
!
interface GigabitEthernet0/0/4.100
description APIC-EM-1.4-TEST #WAN#50M#SPP:SPP4-8Class#
service-policy output prm-dscp#EQ_SPP4-8Class#shape#50.0
!
```

### Custom Service Provider Profiles

Configuration of custom service provider profiles is discussed in the **\*APIC-EM and the EasyQoS Application\*** chapter. Custom service provider profiles use one of the four default service provider profiles discussed in the sections above as a template for the custom profile. Hence the basic structure of the egress queuing policy is the same as discussed in the sections above.

The mapping of the internal queues to the service provider traffic-classes is fixed, depending upon which of the four default service provider profiles has been selected as the template upon which to base the custom service provider profile. In other words, the internal traffic-classes that are admitted to each service provider traffic class is fixed based upon the 4, 5, 6, or 8-class template chosen for the custom service provider profile. However, the DSCP value to which

the internal traffic-classes are re-marked as they enter the service provider network can be specified by the network operator when configuring the custom service provider profile.

The percentage of bandwidth allocated to the service provider traffic-classes can also be specified by the network operator when configuring the custom service provider profile. If a sub-line rate service has been provisioned and the interface includes a `#rate#` tag within the description, then a hierarchical policy-map will be configured by EasyQoS, with a shaper matching the sub-line rate configured at the parent level.

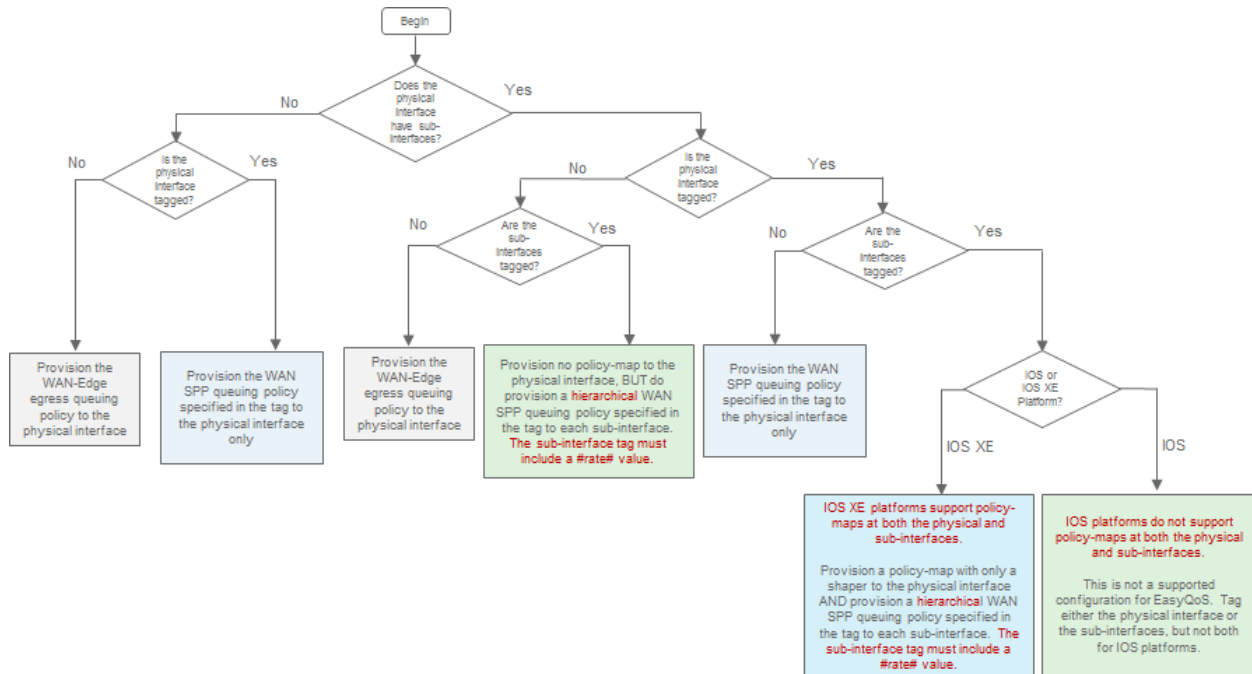
The child-policy of the egress queuing policy-map will still implement a single LLQ policy, meaning a separate LLQ for only the Voice traffic class. An explicit policer for the Voice queue ensures that the LLQ can use no more than the percentage of the bandwidth of the WAN link allocated to the Voice traffic class, regardless of whether there is available bandwidth. For a custom service provider profile, the percentage of bandwidth allocated to the policer is directly dependent upon the amount of bandwidth allocated to the service provider Voice traffic class.

The remaining queues still share the remaining bandwidth based on a percentage allocation of remaining bandwidth. This is accomplished via the “bandwidth remaining percent” command. For the custom service provider profile, the percentage of remaining bandwidth allocated to each queue is dependent upon the amount of remaining bandwidth allocated to the service provider traffic class to which the queue is mapped. EasyQoS will automatically divide the bandwidth specified for the service provider traffic class among the various traffic-classes of the organization that map to the particular service provider traffic class. The bandwidth allocated for each traffic class of the organization is adjusted up or down, such that the proportion of bandwidth allocated for it remains the same as was within the default 4, 5, 6, or 8-class template chosen for the custom service provider profile. Again, the amount of remaining bandwidth allocated to the service provider traffic class is specified by the network operator when configuring the custom service provider profile. Each of these queues can use more than its percentage allocation, if more bandwidth is available—meaning if one or more of the other queues is not using its full allocation of remaining bandwidth percentage.

#### Service Policies Applied to Sub-Interfaces

APIC-EM release 1.4 and higher provide the ability for the network operator to apply an SP Profile tag to Ethernet WAN logical sub-interfaces. This functionality applies only to ISR and ASR router WAN interfaces, because SP Profile tagging only applies to these interfaces. The ability to support hierarchical ingress classification & marking policy-maps at both the physical interface and the logical sub-interface varies between IOS routers (Cisco ISR 3900, 2900, and 800 Series) and IOS XE routers (Cisco ASR 1000 Series and 4000 Series). The following flowchart shows the egress queuing policy provisioned by EasyQoS in the various configurations where SP Profile tagging is applied to physical interfaces and/or logical sub-interfaces.

1. Flowchart for Egress Queuing Policy Based on SPP Tagging of Interface and Sub-Interface



There are seven outcomes for provisioning the egress queuing policy in the figure above. Each is discussed below.

- **Note:** Bandwidth allocations within custom Queuing Profiles do not apply to physical interfaces or logical sub-interfaces considered to be connected to a service provider managed service. However, DSCP markings within custom Queuing Profiles are provisioned within the ingress classification & marking policy applied to physical interfaces or logical sub-interfaces considered to be connected to a service provider managed service.

#### No Sub-Interfaces, Physical Interface Not Tagged

If the physical interface does not have any logical sub-interfaces defined under it, and the physical interface is not configured with a SP Profile tag—EasyQoS will provision the WAN-Edge egress queuing policy to the physical interface. In this configuration, the physical interface is not considered to be connected to a service provider–managed service. Therefore, the WAN-Edge egress queuing policy discussed in the **WAN-Edge Queuing Policy** section of the **\*WAN and Branch Static QoS Design\*** chapter is applied to the physical interface. This is the same behavior as in APIC-EM release 1.3. Because EasyQoS does not consider the physical interface to be connected to a service provider managed WAN service, any custom Queuing Profiles, discussed in the **Custom Queuing Profiles** section of the **\*WAN and Branch Static QoS Design\*** chapter could also apply to the interface.

The ingress classification & marking policy—if applied—is also applied to the physical interface. Table 3 in the **EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing** section of the **\*WAN and Branch Static QoS Design\*** chapter discusses when an ingress classification & marking policy is applied to ISR and ASR router platforms.

#### No Sub-Interfaces, Physical Interface Tagged

If the physical interface does not have any logical sub-interfaces defined under it, and the physical interface is configured with a SP Profile tag, EasyQoS will provision an egress queuing policy (based on the SP Profile name in the tag) to the physical interface. In this configuration, the physical interface is considered to be connected to a service provider managed service. Therefore, the egress queuing policy specified by the SP Profile name within the tag (either a Custom SP Profile or one of the four default SP Profiles) is applied to the physical interface. This is the same behavior as in APIC-EM release 1.3.

The ingress classification & marking policy—if applied—is also applied to the physical interface. Table 3 in the **EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing** section of the **\*WAN and Branch Static QoS Design\*** chapter discusses when an ingress classification & marking policy is applied to ISR and ASR router platforms.

### Sub-Interfaces, Physical Interface Not Tagged, Sub-Interfaces Not Tagged

If the physical interface has one or more logical sub-interfaces defined under it, but neither the physical interface nor the logical sub-interfaces are configured with a SP Profile tag, EasyQoS will provision the WAN-Edge egress queuing policy to the physical interface only. In this configuration, the physical interface and logical sub-interfaces are not considered to be connected to a service provider managed service. Therefore, the WAN-Edge egress queuing policy discussed in the **WAN-Edge Queuing Policy** section of the **\*WAN and Branch Static QoS Design\*** chapter is applied only to the physical interface. Because EasyQoS does not consider the physical interface and logical sub-interfaces to be connected to a service provider managed WAN service, any custom Queuing Profiles, discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter could also apply to the physical interface. No egress queuing policies will be provisioned to the logical sub-interfaces. This is the same behavior as in APIC-EM release 1.3.

The ingress classification & marking policy—if applied—is also applied to the physical interface only. An ingress classification & marking policy applied to a physical interface also applies to traffic on its sub-interfaces. Table 3 in the **EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing** section the **\*WAN and Branch Static QoS Design\*** chapter discusses when an ingress classification & marking policy is applied to ISR and ASR router platforms.

The following provides an example of this configuration.

```
!  
interface GigabitEthernet0/0/4  
description APIC-EM-1.4-TEST  
service-policy input prm-MARKING_IN  
service-policy output prm-dscp#QUEUEING_OUT  
!  
interface GigabitEthernet0/0/4.100  
description APIC-EM-1.4-TEST  
!  
interface GigabitEthernet0/0/4.200  
description APIC-EM-1.4-TEST  
!
```

### Sub-Interfaces, Physical Interface Not Tagged, Sub-Interfaces Tagged

If the physical interface has one or more logical sub-interfaces defined under it, and the physical interface is not configured with a SP Profile tag, but the logical sub-interfaces are configured with a SP Profile tag, EasyQoS will provision an egress queuing policy (based on the SP Profile name within the tag) to the logical sub-interfaces. In this configuration, the physical interface and logical sub-interfaces are considered to be connected to a service provider–managed service. Therefore, the egress queuing policy specified by the SP Profile name within the tag (either a Custom SP Profile or one of the four default SP Profiles) is applied to the logical sub-interfaces.

The SP Profile tag must include a #rate# field. The logical sub-interface egress queuing policy must be a hierarchical policy, in order for the ASR or ISR router to accept the service-policy statement. Otherwise, the router will generate an error such as “CBWFV: Not supported on sub-interface”. Therefore the #rate# field of the SP Profile tag must be included within the logical sub-interface description.

- Note: The SP Profile tags defined within logical sub-interface descriptions under the same physical sub-interface must all specify the same SP Profile name (either a Custom SP Profile name or one of the four default SP Profile names). For example, specifying an SPP-4Class model and an SPP-8Class module on two logical sub-interfaces under the same physical interface is not a supported configuration. However, the values of the #rate# field can

be different for each sub-interface. Because of this restriction, if one logical sub-interface under a physical interface has a SP Profile tag configured, then all logical sub-interfaces under the same physical interface must have SP Profile tags configured.

The ingress classification & marking policy—if applied—is applied to each logical sub-interface. Although an ingress classification & marking policy applied to a physical interface also applies to traffic on its sub-interfaces, applying the ingress classification & marking policy to individual sub-interfaces may provide more granular visibility into traffic on each sub-interface. Table 3 in the **EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing** section the **\*WAN and Branch Static QoS Design\*** chapter discusses when an ingress classification & marking policy is applied to ISR and ASR router platforms.

The following provides a simplified example of this configuration.

```
!
interface GigabitEthernet0/0/2
description APIC-EM-1.4-TEST
!
interface GigabitEthernet0/0/2.100
description APIC-EM-1.4-TEST #WAN#60M#SPP1#
service-policy input prm-MARKING_IN
service-policy output prm-dscp#EQ_1#shape#60.0
!
interface GigabitEthernet0/0/2.200
description APIC-EM-1.4-TEST #WAN#15M#SPP1#
service-policy input prm-MARKING_IN
service-policy output prm-dscp#EQ_1#shape#15.0
!
```

#### Sub-Interfaces, Physical Interface Tagged, Sub-Interfaces Not Tagged

If the physical interface has one or more logical sub-interfaces defined under it, and the physical interface is configured with a SP Profile tag, but the logical sub-interfaces are not configured with SP Profile tags—EasyQoS will provision an egress queuing policy (based on the SP Profile name within the tag) to the physical interface only. In this configuration, the physical interface and logical sub-interfaces are considered to be connected to a service provider managed service. Therefore, the egress queuing policy specified by the SP Profile name within the tag (either a Custom SP Profile or one of the four default SP Profiles) is applied to the physical interface.

- **Note:** If one logical sub-interface under a physical interface has a SP Profile tag configured, then all logical sub-interfaces under the same physical interface must have SP Profile tags configured. Defining some logical sub-interfaces with SP Profile tags and other logical sub-interfaces without SP Profile tags under the same physical interface is not a supported configuration.

The ingress classification & marking policy—if applied—is applied to the physical interface only. An ingress classification & marking policy applied to a physical interface also applies to traffic on its sub-interfaces. Table 3 in the **EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing** section the **\*WAN and Branch Static QoS Design\*** chapter discusses when an ingress classification & marking policy is applied to ISR and ASR router platforms.

The following provides a simplified example of this configuration.

```
!
```

```
interface GigabitEthernet0/0/5
description APIC-EM-1.4-TEST #WAN#50M#SPP:SPP2-5Class#
service-policy input prm-MARKING_IN
service-policy output prm-dscp#EQ_SPP2-5Class#shape#50.0
!
interface GigabitEthernet0/0/5.100
!
interface GigabitEthernet0/0/5.200
!
```

#### Sub-Interfaces, Physical Interface Tagged, Sub-Interfaces Tagged, IOS XE Device

If the physical interface has one or more logical sub-interfaces defined under it, and both the physical interface and logical sub-interfaces are configured with SP Profile tags, *and* the device is an IOS XE router, EasyQoS will provision a more complex egress queuing policy. IOS XE routers include the ASR 1000 Series and the ISR 4000 Series. In this configuration, the physical interface and logical sub-interfaces are considered to be connected to a service provider managed service.

At the physical interface, EasyQoS will provision a non-hierarchical policy-map with only a shaper. A simplified example of the provisioning of the physical interface by EasyQoS is shown below.

```
!
policy-map prm-interface-shaper#Gig0/0/4
class class-default
shape average 100000000
!
~
!
interface GigabitEthernet0/0/4
description APIC-EM-1.4-TEST #WAN#100M#SPP:SPP4-8Class#
service-policy output prm-interface-shaper#Gig0/0/4
!
```

The name of the policy-map will include the physical interface name in order for the network operator to more easily identify it within the router configuration.

SP Profile tag configured within the physical interface description must include all three fields - #WAN#, #rate#, and #SP\_Profile\_Name#. The #rate# field is used to determine the shaper average value within the policy-map of the physical interface. Although the SP Profile name is configured within the physical interface—IOS XE devices do not allow a hierarchical policy-map to be applied at both the physical interface and logical sub-interfaces. Only a shaper is allowed at the physical interface in this configuration.

- Note: The SP Profile name in the tag (either a Custom SP Profile or one of the four default SP Profiles) configured within the description of the physical interface must be the same as the SP Profile names configured in the descriptions of each of the logical sub-interfaces. For example, specifying an SPP-8Class model at the physical interface and an SPP-5Class model on one or more of the logical sub-interfaces under the same physical interface is not a supported configuration. However, the values of the #rate# field can be different for the physical interface and for each logical sub-interface.



At each logical sub-interface, EasyQoS will provision an egress queuing policy (based on the SP Profile name within the tag) to the logical sub-interfaces. Therefore, the egress queuing policy specified by the SP Profile name within the tag (either a Custom SP Profile or one of the four default SP Profiles) is applied to the logical sub-interfaces.

The SP Profile tag must include a #rate# field. The logical sub-interface egress queuing policy must be a hierarchical policy, in order for the router to accept the service-policy statement. Otherwise, the router will generate an error such as “CBFWF: Not supported on sub-interface”. Therefore the #rate# field of the SP Profile tag must be included within the logical sub-interface description.

- **Note:** If one logical sub-interface under a physical interface has a SP Profile tag configured, then all logical sub-interfaces under the same physical interface must have SP Profile tags configured. Defining some logical sub-interfaces with SP Profile tags and other logical sub-interfaces without SP Profile tags under the same physical interface is not a supported configuration.

A simplified example of the provisioning of the sub-interfaces by EasyQoS is shown below.

```
!
interface GigabitEthernet0/0/4.100
description APIC-EM-1.4-TEST #WAN#20M#SPP:SPP4-8Class#
service-policy input prm-MARKING_IN
service-policy output prm-dscp#EQ_SPP4-8Class#shape#20.0
!
interface GigabitEthernet0/0/4.200
description APIC-EM-1.4-TEST #WAN#10M#SPP:SPP4-8Class#
service-policy input prm-MARKING_IN
service-policy output prm-dscp#EQ_SPP4-8Class#shape#10.0
!
```

The ingress classification & marking policy—if applied—is applied to each logical sub-interface. Although an ingress classification & marking policy applied to a physical interface also applies to traffic on its sub-interfaces, applying the ingress classification & marking policy to individual sub-interfaces may provide more granular visibility into traffic on each sub-interface. Table 3 in the **EasyQoS Policy Based on Platform, NBAR2 Protocol Pack, and Licensing** section the **\*WAN and Branch Static QoS Design\*** chapter discusses when an ingress classification & marking policy is applied to ISR and ASR router platforms.

Sub-Interfaces, Physical Interface Tagged, Sub-Interfaces Tagged, IOS Device

IOS routers—which include the ISR G2 3900 and 2900 Series and the ISR 800 Series—do not support policy-maps configured at both the physical interface and logical sub-interfaces. Therefore, configuring a WAN SPP tag at both a physical interface and its sub-interfaces is not a valid configuration supported by EasyQoS for IOS routers. An error will be generated, and the QoS policy will fail for the IOS router if the network operator has tagged both a physical interface and its sub-interfaces. The network operator should modify the configuration on the IOS router so that only the physical interface is tagged or only its sub-interfaces are tagged. The resulting QoS policy provisioned to the WAN interface, based upon whether the physical interface is tagged, or the sub-interfaces are tagged, was discussed in previous sections.

Server IP/Port-Based Custom Applications and Managed Service WANs

Custom applications based on server IP addresses and/or ports do not pass through the NBAR engine within an ASR or ISR router platform. As discussed in the **\*Custom Applications on ASR and ISR Platforms\*** section in the **\*Branch and WAN Static QoS Design\*** chapter, port-based Custom applications are provisioned under one of the 11 new class-map entries that include the word “CUSTOM”—based on the traffic-class to which the port-based Custom application belongs. This is a new behavior, as of APIC-EM release 1.4 and higher.

In APIC-EM release 1.3 port-based Custom applications were added to the `prm-MARKING_IN#TUNNELED-NBAR` traffic-class in ASR and ISR router platforms by EasyQoS. Prior to APIC-EM release 1.3 Custom applications were configured as NBAR applications. No action is specified for the `prm-MARKING_IN#TUNNELED-NBAR` traffic class within the ingress classification & marking policy on ASR and ISR router platforms. When traffic from such a Custom application exits the organization's network, entering a service provider managed-service network, the Custom application traffic may be remarked to match the allowed DSCP markings for the service provider traffic-class to which the Custom application is mapped.

With APIC-EM release 1.3, when the Custom application traffic re-enters the organization's network at the other end of service provider managed-service network, the traffic would not be remarked back to its original DSCP marking. Instead, port-based Custom applications would retain the DSCP markings to which they were mapped when entering the service provider managed-service network. APIC-EM release 1.4 and higher modifies this behavior. Traffic re-entering the organization's network at the other end of the service provider managed-service network is now classified to one of the 11 new class-map entries that include the word "CUSTOM"—based on the traffic-class to which the port-based Custom application belongs. Therefore traffic from port-based Custom applications is now remarked back to its original DSCP marking.

## 1.8 Chapter 8: Campus LAN Static QoS Design

Within the EasyQoS solution, different network devices implement the QoS policy to the best of their abilities. With APIC-EM/EasyQoS release 1.3 and higher, Catalyst switches implement one or more of the following QoS policies, depending upon their role within the network infrastructure:

- Ingress classification & marking policies on wired ports based on policy-maps that contain ACLs with Layer 2-4 ACEs.
- Ingress and/or egress queuing policies

The role of the Catalyst switch within the network infrastructure is discussed in detail in the **\*Catalyst Switch Roles\*** section below.

- Note: Catalyst 3850 and 3650 Series switches support wired AVC/NBAR-based ingress classification & marking policies with IOS XE 16.3.1 and higher software versions. The APIC-EM 1.6 release of EasyQoS does not use AVC/NBAR-based ingress classification & marking policies. Future versions of EasyQoS may add this support.

### TCAM Utilization Challenges

Cisco Catalyst switch platforms implement ingress classification & marking policies that include ACL entries in hardware for performance reasons. This hardware is commonly referred to as Ternary Content Addressable Memory (TCAM). Most Catalyst switch platforms have sufficient QoS TCAM space, such that the ingress classification & marking QoS policies provisioned by EasyQoS do not exceed the available QoS TCAM space. However, a few older Catalyst switch platforms supported by EasyQoS do have limited QoS TCAM space. Because QoS TCAM space is limited on these older Catalyst switch platforms, the ACEs that are provisioned by the EasyQoS ingress classification & marking policies across various platforms can vary slightly. The EasyQoS application is aware of the QoS TCAM space available in supported switch platforms; and will implement ACEs up to the limits of the TCAM-constrained platforms—leaving sufficient TCAM space for additional functionality such as Dynamic QoS and statically learned Cisco devices.

In order to minimize the impact of limited TCAM space on these older platforms, APIC-EM deploys Custom and Favorite applications first. Custom applications are by default marked as Favorite applications, as well. This ensures that the applications most relevant to the network operator are included within the ACEs deployed by EasyQoS.

The following table summarizes the QoS TCAM space for various Catalyst access-layer switch platforms supported by EasyQoS.

#### 1. QoS TCAM Space per ASIC for Various Catalyst Access-Layer Switches

Switch Platform	QoS TCAM Entries
Catalyst 2960-X Series	504 with the lanbase-default SDM template 384 with the default and lanbase-routing SDM Templates
Catalyst 2960-XR Series	512 with all SDM templates
Catalyst 2960-S Series	384 with all SDM templates
Catalyst 3560-C Series	384 with the default SDM template
Catalyst 3560-X Series	512 with all SDM templates other than the routing template 384 with the routing SDM template
Catalyst 3750-X Series	512 with all SDM templates other than the routing template 384 with the routing template
Catalyst 3850 Series	2816 with the Advanced (high scale) SDM template 3072 with the VLAN SDM template
Catalyst 3650 Series	3072 with both the Advanced (low scale) and the VLAN (high scale) SDM templates
SM-ES2 Series EtherSwitch Module	128 with the default and dual-ipv4-and-ipv6 templates 384 with the qos template

Due to the algorithm for converting ACEs into QoS TCAM masks and entries, there is not necessarily a one-to-one correlation between a single ACE within an ACL and a single TCAM entry. However, a general guideline that can be used is that EasyQoS will require a single TCAM entry for each ACE. Put more simply, if a particular platform has room for 384 QoS TCAM entries (ignoring masks), then in general it can support approximately 384 ACEs within the ACLs of the class-maps within the ingress classification & marking policy, minus any TCAM entries reserved for the platform itself. However, it should be noted that individual applications may be identified via multiple TCP and UDP ports or port ranges. Bi-directionality will also double the ACE entries. Hence each application may result in multiple ACEs within the ingress classification & marking policy. Therefore, those platforms with limited QoS TCAM size have limited ability to support applications specified within the policy created by EasyQoS.

#### Methodology and Workflow

The general method by which the applications selected within the EasyQoS web-based GUI are translated into ACLs with ACE entries is discussed in the following sections.

#### CAPWAP Control and Data Traffic

EasyQoS will check to see if there is QoS TCAM space available for additional ACEs within any of the ACLs that are part of the ingress classification & marking QoS policy-map. If so, EasyQoS will generate and deploy ACEs for the `prm-APIC_QOS_IN#TUNNELED__acl` ACL first. This currently consists of only two ACEs—one for CAPWAP control traffic that uses destination UDP port 5246 and one for CAPWAP data traffic that uses destination UDP port 5247.

#### Custom Applications

Following the deployment of ACEs for the `prm-APIC_QOS_IN#TUNNELED__acl`, EasyQoS will again determine if there is sufficient QoS TCAM space available for additional ACEs within any of the ACLs that are part of the ingress classification & marking QoS policy-map. If sufficient QoS TCAM space is available for additional ACEs, EasyQoS will check to see if all ACEs for all Custom applications have been deployed. EasyQoS assigns a Rank to all Custom and Favorite applications. Custom applications have a Rank of 1. Applications within the NBAR taxonomy do not have a Rank by default. However, they are given a Rank of 10,000 when assigned as a Favorite application. EasyQoS processes applications by Rank first—from lowest number to highest number.

If the ACEs for all of the Custom applications have not been deployed, EasyQoS will select the next Custom application. Only Custom applications consisting IP addresses, IP ports, and TCP/UDP ports can be provisioned onto Catalyst switch platforms. This is discussed in the **\*Access-Control Lists\*** section below. How EasyQoS determines which ACL to deploy ACE entries for applications, based on the business-relevance and traffic-class attribute values of the application, is also discussed in the **\*Access-Control Lists\*** section below.

EasyQoS will continue to check for available QoS TCAM space and continue to deploy ACEs for Custom applications until either all Custom applications have been deployed, or the available QoS TCAM space is exhausted.

### Favorite Applications

After ACEs for all Custom applications have been deployed, EasyQoS will begin parsing the applications within the NBAR taxonomy. If sufficient QoS TCAM space is available for additional ACEs, EasyQoS will check to see if all ACEs for Favorite applications have been deployed. This is because EasyQoS processes applications by Rank first, and Favorite applications are assigned a rank of 10,000. If the ACEs for all of the Favorite applications have not been deployed, EasyQoS will select the next Favorite application.

EasyQoS will check to see if the Favorite application has the traffic-class attribute set to one of the following:

- VoIP Telephony
- Broadcast Video
- Real-Time Interactive
- Multimedia Conferencing.

If the traffic-class attribute for the Favorite application matches one of these, EasyQoS will check to see if any of the indicative ports for the Favorite application are duplicates. Many voice and video apps known to NBAR include indicative ports for signaling protocols such as SIP, Cisco SCCP, STUN, etc. Signaling protocols should not be configured into voice and video ACLs. Instead they should appear within the Signaling ACL. Hence they should not be duplicated within the voice and video ACLs. Additionally many collaboration applications include indicative ports for additional functionality such as IMAP, etc. Email protocols should appear within the Bulk Data ACL. Hence they should not be duplicated within the voice and video ACLs either.

For the purposes of this document voice and video ACLs refer to the following ACLs:

- prn-APIC\_QOS\_IN#VOICE\_\_acl
- prn-APIC\_QOS\_IN#BROADCAST\_\_acl
- prn-APIC\_QOS\_IN#REALTIME\_\_acl
- prn-APIC\_QOS\_IN#MM\_CONF\_\_acl.

EasyQoS will also check to see if the Favorite application is identified by any other indicative TCP or UDP ports. If the ports by which the application is identified correspond to TCP destination ports 80, 443, or 8080, EasyQoS will again not implement ACEs for these ports. This is because many applications use the ports corresponding to HTTP (port 80 or 8080) and HTTPS (port 443). Hence, Layer 2-4 ACEs are not effective at identifying applications that use these ports.

If the Favorite application is identified by any other indicative UDP or TCP ports, EasyQoS will generate ACEs for that Favorite application. The ACE entry(s) will be generated under the class-map definition based on the traffic-class attribute to which the Favorite application belongs to within the NBAR taxonomy—only if the business-relevance attribute is set for Business Relevant. If the business-relevance attribute is set for Business Irrelevant, the ACE entry(s) will be generated under the class-map definition for Scavenger traffic. If the business-relevance attribute is set for Default, no ACE entry(s) will be generated under any class-map definition. EasyQoS will continue to do this until either all Favorite applications have been deployed or the available QoS TCAM space is exhausted.

### Other Applications within the NBAR Taxonomy

After all Favorite applications are deployed, EasyQoS will determine if there is any available QoS TCAM space left for additional ACE entries. If available space exists, EasyQoS will distribute the available space across the various traffic-classes. By distributing the available TCAM space across the various traffic-classes, EasyQoS ensures that at least some applications from the NBAR taxonomy for each traffic class are represented in the ACLs that are generated for each traffic class. EasyQoS selects applications from each of the traffic-classes based upon popularity—otherwise known as the *NBAR commonly-used attribute*. Every application within the NBAR taxonomy is assigned a value for the commonly-used attribute. Values range from 10 (most popular) to 1 (least popular).

EasyQoS will select an application from one of the traffic-classes based upon popularity. If multiple applications have the same popularity, EasyQoS will select the next application alphabetically from those that have the same popularity. EasyQoS will check to see if the application has the traffic-class attribute set to one of the following:

- VoIP Telephony
- Broadcast Video
- Real-Time Interactive
- Multimedia Conferencing

If the traffic-class attribute for the application matches one of these, EasyQoS will check to see if any of the indicative ports for the application are duplicates. Many voice and video apps known to NBAR include indicative ports for signaling protocols such as SIP, Cisco SCCP, STUN, etc. Signaling protocols should not be configured into voice and video ACLs. Instead they should appear within the Signaling ACL. Hence they should not be duplicated within the voice and video ACLs. Additionally many collaboration apps include indicative ports for additional functionality such as IMAP, etc. Email protocols should appear within the Bulk Data ACL. Hence they should not be duplicated within the voice and video ACLs either. For the purposes of this document voice and video ACLs refer to the following ACLs:

- `prm-APIC_QOS_IN#VOICE__acl`
- `prm-APIC_QOS_IN#BROADCAST__acl`
- `prm-APIC_QOS_IN#REALTIME__acl`
- `prm-APIC_QOS_IN#MM_CONF__acl`.

EasyQoS will also check to see if the application is identified by any other indicative TCP or UDP ports. If the ports by which the application is identified correspond to TCP destination ports 80, 443, or 8080, EasyQoS will again not implement ACEs for these ports. This is because many applications use the ports corresponding to HTTP (port 80 or 8080) and HTTPS (port 443). Hence, Layer 2-4 ACEs are not effective at identifying applications that use these ports.

If the application is identified by any other indicative UDP or TCP ports, EasyQoS will generate ACEs for that application. The ACE entry(s) will be generated under the class-map definition based on the traffic-class attribute to which the application belongs to within the NBAR taxonomy—only if the business-relevance attribute is set for Business Relevant. If the business-relevance attribute is set for Business Irrelevant, the ACE entry(s) will be generated under the class-map definition for Scavenger traffic. If the business-relevance attribute is set for Default, no ACE entry(s) will be generated under any class-map definition. EasyQoS will continue to do this until either all applications within the traffic-class have been deployed or the available QoS TCAM space for the traffic-class is exhausted.

EasyQoS will continue to do this for all traffic-classes until either all applications within all traffic-classes have been deployed or the available QoS TCAM space for all traffic-classes is exhausted.

#### Catalyst Switch Roles

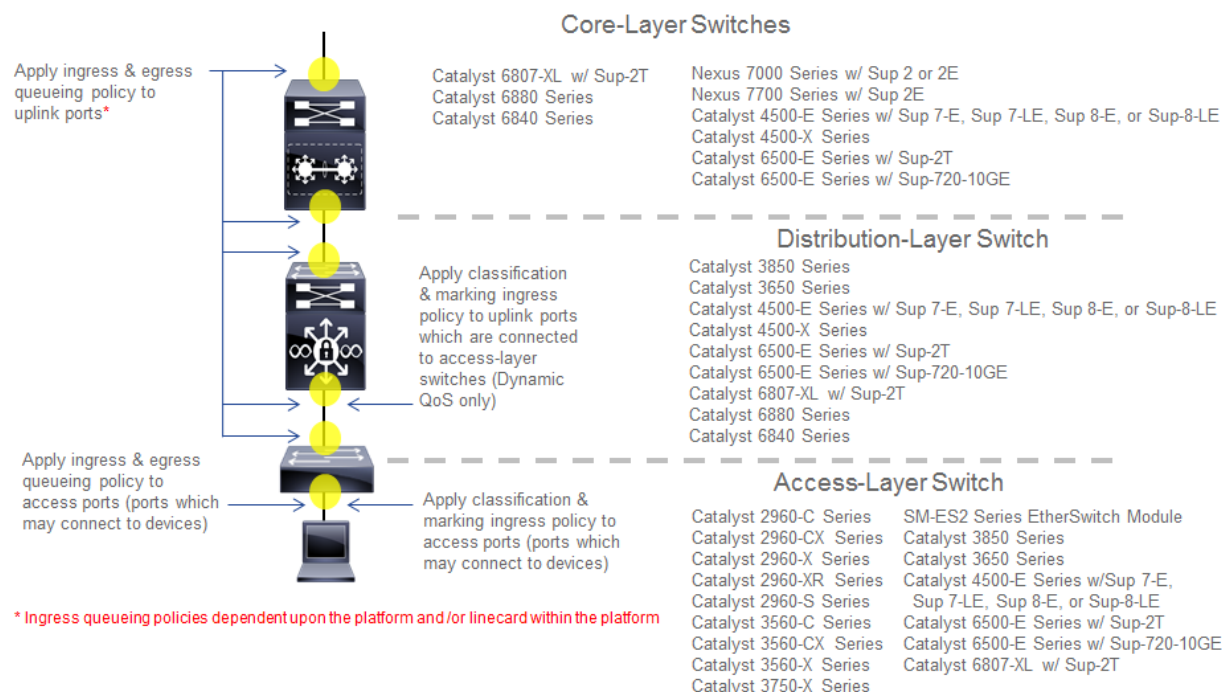
Catalyst and Nexus switch platforms can function in one of the following three possible roles within APIC-EM—reflecting a traditional 3-tiered campus architecture:

- Core-layer switch
- Distribution-layer switch
- Access-layer switch

When APIC-EM discovers and places network devices into the device inventory database, it will classify each network device in one of five roles, discussed in the **\*APIC-EM and the EasyQoS Application\*** chapter of this document. For Catalyst and Nexus switches, EasyQoS uses the device role in order to determine what, if any, ingress classification & marking QoS policy to apply to each switch port, based on the role of the switch within the network infrastructure. Hence, it is highly important that the network operator review (and if necessary modify) the role of each network device within APIC-EM before implementing EasyQoS policies.

The following figure shows the roles the various supported Catalyst and Nexus switches can participate within the EasyQoS Solution; as well as the QoS policies applied to each switch based upon its role.

### 1. Catalyst and Nexus Switch Roles within the EasyQoS Solution



The following are the restrictions regarding the roles that the various supported Catalyst and Nexus switch platforms can have within the EasyQoS solution.

- Catalyst 6500-E Series switches with Sup-2T supervisors, Catalyst 6500-E Series switches with Sup-720-10GE supervisors, Catalyst 6807-XL switches with Sup-2T, and Catalyst 4500-E Series switches with Sup7-E, Sup7-LE, and Sup-8E supervisors are supported in the roles of a core-layer, distribution-layer, or access-layer switch.
- Nexus 7000 Series with Sup2 or 2E supervisors, and Nexus 7700 with Sup2E supervisors are supported only in the role of a core-layer switch.
- Catalyst 6880 Series switches, Catalyst 6840 Series switches, and Catalyst 4500-X Series switches are supported only in the roles of a core-layer or distribution-layer switch.
- Catalyst 3850 Series switches and Catalyst 3650 Series switches are supported in the roles of a distribution-layer or an access-layer switch.
- Catalyst 2960-X, 2960-XR, 2960-S, 3560-X, 3560-C, and 3560-CX Series switches, as well as the SM-ES2 Series EtherSwitch module, are only supported in the role of an access-layer switch.

A single switch functioning as both a distribution-layer switch and an access-layer switch simultaneously is not supported. Multiple switch platforms of the same model can individually function in the role of a distribution-layer switch or access-layer switch within a single deployment.

#### Core-Layer Switch QoS Design

For devices operating as core-layer switches, EasyQoS will only apply ingress and/or egress queueing policies to the uplinks ports. *Uplink ports* refer to ports that connect to other core-layer switches or to distribution-layer switches. The specifics as to whether both ingress and egress queueing policies, or only egress queueing policies are applied, are dependent upon whether the particular Catalyst or Nexus switch platform and/or line card within the platform supports both ingress and egress queueing, or only egress queueing. This is discussed in detail for each platform and/or line card in the queueing design sections of this document.

Because only queuing policies are pushed to core-layer switches by EasyQoS, the QoS policy is the same for core-layer switches, regardless of whether the customer chooses to implement Static or Dynamic QoS. Dynamic QoS is discussed within the **\*Dynamic QoS Design\*** chapter.

### Access-Layer Switch QoS Design

Access-layer switch QoS design consists of the following policies:

- Ingress/egress queuing policies applied to access-edge switch ports and uplink switch ports
- Ingress classification & marking policies applied to access-edge switch ports

### Ingress/Egress Queuing Policies

Regardless of whether the network operator has implemented Static or Dynamic QoS, queuing policies will always be pushed to access-layer switches. The EasyQoS application will apply ingress and/or egress queuing policies to both access-edge ports and uplink ports. Access-edge ports refer to ports that directly connect to end devices, such as laptops, PCs, IP Phones, wireless Access Points, etc. Uplink ports refer to ports that connect to distribution-layer switches. The specifics as to whether both ingress and egress queuing policies, or only egress queuing policies are applied, are dependent upon whether the particular Catalyst switch platform and/or line card within that platform supports both ingress and egress queuing, or only egress queuing. This is discussed in detail for each platform and/or line card in the queuing design sections of this document.

### Ingress Classification & Marking Policies

The ingress classification & marking policy provisioned onto access-layer switches by EasyQoS is dependent upon whether the network operator chooses to implement Static QoS or Dynamic QoS. For Static QoS, EasyQoS will apply an access-layer ingress classification & marking policy to all access-edge ports, with the following exceptions:

- Access-edge switch ports which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter of this document.
- Access-edge switch ports which are connected to Access Points are configured by EasyQoS to trust DSCP markings.

The ingress classification & marking policy consists of policy-maps, which contain class-maps, which in turn contain ACLs with Layer 3 & 4 ACEs. Layer 3 & 4 refers to IP addresses, protocols (that is, TCP, UDP, etc.) and higher-layer ports (HTTP, Telnet, FTP, etc.). The access-layer classification & marking policy establishes the QoS trust boundary and policy enforcement point at the ingress edge of the network.

The following are the class-map definitions for the ingress classification & marking policy pushed by EasyQoS to Catalyst switch platforms, when configured in the role of an access-layer switch within APIC-EM.

!

```
class-map match-any prm-APIC_QOS_IN#VOICE
match access-group name prm-APIC_QOS_IN#VOICE__acl
class-map match-any prm-APIC_QOS_IN#BROADCAST
match access-group name prm-APIC_QOS_IN#BROADCAST__acl
class-map match-any prm-APIC_QOS_IN#REALTIME
match access-group name prm-APIC_QOS_IN#REALTIME__acl
class-map match-any prm-APIC_QOS_IN#MM_CONF
match access-group name prm-APIC_QOS_IN#MM_CONF__acl
class-map match-any prm-APIC_QOS_IN#MM_STREAM
match access-group name prm-APIC_QOS_IN#MM_STREAM__acl
```

```
class-map match-any prm-APIC_QOS_IN#SIGNALING
match access-group name prm-APIC_QOS_IN#SIGNALING__acl
class-map match-any prm-APIC_QOS_IN#OAM
match access-group name prm-APIC_QOS_IN#OAM__acl
class-map match-any prm-APIC_QOS_IN#TRANS_DATA
match access-group name prm-APIC_QOS_IN#TRANS_DATA__acl
class-map match-any prm-APIC_QOS_IN#BULK_DATA
match access-group name prm-APIC_QOS_IN#BULK_DATA__acl
class-map match-any prm-APIC_QOS_IN#SCAVENGER
match access-group name prm-APIC_QOS_IN#SCAVENGER__acl
class-map match-any prm-APIC_QOS_IN#TUNNELED
match access-group name prm-APIC_QOS_IN#TUNNELED__acl
!
```

The following is the policy-map definition for the ingress classification & marking policy pushed by EasyQoS to the switch platforms, when the default Queuing Profile (CVD\_Queueing\_Profile) is selected within the Advanced Settings section of the EasyQoS web-based GUI.

```
!
policy-map prm-APIC_QOS_IN
class prm-APIC_QOS_IN#VOICE
set dscp ef
class prm-APIC_QOS_IN#BROADCAST
set dscp cs5
class prm-APIC_QOS_IN#REALTIME
set dscp cs4
class prm-APIC_QOS_IN#MM_CONF
set dscp af41
class prm-APIC_QOS_IN#MM_STREAM
set dscp af31
class prm-APIC_QOS_IN#SIGNALING
set dscp cs3
class prm-APIC_QOS_IN#OAM
set dscp cs2
class prm-APIC_QOS_IN#TRANS_DATA
set dscp af21
class prm-APIC_QOS_IN#BULK_DATA
set dscp af11
class prm-APIC_QOS_IN#SCAVENGER
```



```

set dscp cs1
class prm-APIC_QOS_IN#TUNNELED
class class-default
set dscp default
!

```

Eleven of the twelve classes defined within the RFC 4594-based Cisco 12-Class QoS model are defined within the class-maps and policy-map above. The 12th traffic class corresponds to Network Control traffic. The access-layer ingress classification & marking policy is intended to be applied to switch ports that connect directly to end-user devices—not network equipment, such as routers and other switches. Network Control traffic should never be seen by access-layer switch ports connected to end-user devices. Hence the ingress classification & marking policy does not define a class-map or traffic-class definition to account for Network Control traffic.

A Cisco wireless Access Point may be connected to an access-layer switch port. EasyQoS identifies Cisco Access Points through CDP and configures the switch port to trust DSCP markings. This means that for centralized (local mode) deployments, the CAPWAP traffic from the Access Point is trusted. CAPWAP tunneled traffic can be either CAPWAP control traffic or CAPWAP data traffic. For CAPWAP data traffic, the DSCP marking of the outer CAPWAP header is set by the Access Point, and is based on the DSCP marking of the IP packet sent by the wireless client. This is discussed further in the **\*WLC QoS Design\*** chapter. For CAPWAP control traffic, the DSCP marking of the outer CAPWAP header is set with a DSCP marking of Class Selector 6 (CS6).

- Note: APIC-EM/EasyQoS release 1.6 does not support Cisco Access Points operating in FlexConnect mode. More specifically, a wireless QoS policy is currently not supported when the Access Points are operating in FlexConnect mode, because EasyQoS does not currently provision FlexConnect AVC policies. However, a Cisco Access Point operating in FlexConnect mode may be connected to a switch port which does have an EasyQoS policy applied to the switch. In such cases, because the Catalyst switch will detect the presence of the Access Point via CDP, EasyQoS will configure the switch port to trust the DSCP markings of the traffic from the Access Point which is locally terminated on the switch. Likewise, the CAPWAP control traffic from the Access Point will also be trusted by the switch port.

The prm-APIC\_QOS\_IN#TUNNELED traffic-class is used to match on tunneled traffic, such as CAPWAP control and data traffic. Within the policy-map definition, no action is taken for prm-APIC\_QOS\_IN#TUNNELED traffic. However, because EasyQoS configures switch ports to trust DSCP when connected to Access Points, the prm-APIC\_QOS\_IN#TUNNELED traffic-class does not currently serve a useful purpose—other than if CDP is disabled on the Cisco Access Point. As additional requirements for tunneled traffic arise, they may be added to this traffic-class in future revisions of APIC-EM/EasyQoS.

The default-class within the policy-map definition is configured to set all traffic that does not match any of the previous traffic-classes to a DSCP marking of default (Best Effort). This ensures that all traffic that does not match one of the traffic-classes is bleached—in other words provided a best effort service.

The ingress classification & marking policy is applied to access-edge switch ports on each switch in a stackable switch platform or line card in a modular switch platform; and all switches within a switch stack or a VSS pair. Access-edge switch ports are switch ports that are used to connect end-user devices.

- Note: Interfaces configured as StackWise Virtual links (SVL) or Dual-Active-Detection links on Catalyst 3850 or Catalyst 3650 Series platforms; or interfaces configured as Virtual Switch Link (VSL) or Dual-Active-Detection links on Catalyst 6500/6800 and/or Catalyst 4500 Series platforms, do not support QoS. As of APIC-EM release 1.6, the network operator must exclude these interfaces from EasyQoS policy in order to prevent EasyQoS from attempting to provision QoS policy to these interfaces.

The following show an example of the application of the service-policy to a Gigabit Ethernet access-edge switch port.

```

interface GigabitEthernetx/x/x
service-policy input prm-APIC_QOS_IN

```

For uplink ports on switches configured with the role of an access-layer switch within APIC-EM, no ingress classification & marking policy is applied to the switch port. Instead, the switch port is configured to trust DSCP markings from devices attached to the switch port. This is the same behavior described earlier for switch ports connected to Cisco Access Points. For MLS QoS-based switches (Catalyst 2960 Series, Catalyst 3560 Series, Catalyst 3750 Series, SM-ES2 EtherSwitch Series, and Catalyst 6500 Series switches with Sup-720 Supervisors), this must be explicitly configured via the following command, because the default port trust-state is untrusted on MLS QoS-based switches.

```
mls qos trust dscp
```

For MQC-based platforms (Catalyst 3850 Series, Catalyst 3650 Series, and Catalyst 4500 Series), C3PL-based platforms (Catalyst 6500 Series with Sup-2T supervisors, 6807-XL, 6880 Series, and 6840 Series), and NX OS platforms (Nexus 7000 and 7700 Series), the default port trust-state is trusted. No explicit configuration command needs to be pushed from APIC-EM to these switch platforms.

### Changing the DSCP Markings of Traffic-Classes through Custom Queuing Profiles

Table 1 in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter of this document summarizes the custom Queuing Profile support (both BW allocation and DSCP markings) for various switch and router platforms. Custom DSCP markings for traffic-classes are supported (meaning DSCP markings are modified through custom Queuing Profiles) for Catalyst 3850, 3650, and 4500 Series platforms. Line cards with DSCP-to-queue mapping on Catalyst 6500 Series with Supervisor 2T are also supported.

Changing the DSCP marking of a traffic-class for supported Catalyst switch platforms will modify the policy-action of the ingress classification & marking policy class-map definitions that reference the traffic-class.

- Note: Caution should be used when changing the default DSCP marking of traffic-classes from the Cisco recommended 12-class QoS model. Such changes could result in a less than optimal QoS implementation unless the network operator is highly knowledgeable in QoS design and implementation. This feature is only for customers with advanced knowledge of QoS.

The following output provides an example of the ingress classification & marking policy where Broadcast Video traffic has been marked to CS3 and Signaling traffic has been marked to CS5 (as specified in IETF RFC 4594). The affected class-map definitions in the policy-map are highlighted in bold.

```
!  
policy-map prm-APIC_QOS_IN  
class prm-APIC_QOS_IN#VOICE  
set dscp ef  
class prm-APIC_QOS_IN#BROADCAST  
set dscp cs3  
class prm-APIC_QOS_IN#REALTIME  
set dscp cs4  
class prm-APIC_QOS_IN#MM_CONF  
set dscp af41  
class prm-APIC_QOS_IN#MM_STREAM  
set dscp af31  
class prm-APIC_QOS_IN#SIGNALING  
set dscp cs5  
class prm-APIC_QOS_IN#OAM  
set dscp cs2
```

```

class prm-APIC_QOS_IN#TRANS_DATA
set dscp af21
class prm-APIC_QOS_IN#BULK_DATA
set dscp af11
class prm-APIC_QOS_IN#SCAVENGER
set dscp cs1
class prm-APIC_QOS_IN#TUNNELED
class class-default
set dscp default
!
```

As can be seen in the example output above, the “set dscp” policy-action commands are modified to the desired DSCP markings for the traffic-classes.

- Note: Cisco recommends a modified version of RFC 4594 where Signaling traffic is marked to CS3 and Broadcast Video is marked to CS5. The default setting for call signaling within Cisco Unified Communications Manager is set to CS3.

Changing the DSCP markings of traffic-classes within the EasyQoS web-based GUI also affects the “match dscp” statements of class-map definitions within the queuing policy of supported Catalyst switch platforms. This is discussed within the queuing configuration sections for the Catalyst 3850/3650 Series, Catalyst 4500 Series, and Catalyst 6500/6800 Series with Supervisor 2T platforms.

#### Access-Control Lists

The following are the ACL definitions for the ingress classification & marking policy pushed by EasyQoS to all of the Catalyst switching platforms supported by EasyQoS, when the platform functions as an access-layer switch. The specific ACE entries within each ACL are not shown.

```

!
ip access-list extended prm-APIC_QOS_IN#VOICE__acl
ip access-list extended prm-APIC_QOS_IN#BROADCAST__acl
ip access-list extended prm-APIC_QOS_IN#REALTIME__acl
ip access-list extended prm-APIC_QOS_IN#MM_CONF__acl
ip access-list extended prm-APIC_QOS_IN#MM_STREAM__acl
ip access-list extended prm-APIC_QOS_IN#SIGNALING__acl
ip access-list extended prm-APIC_QOS_IN#OAM__acl
ip access-list extended prm-APIC_QOS_IN#TRANS_DATA__acl
ip access-list extended prm-APIC_QOS_IN#BULK_DATA__acl
ip access-list extended prm-APIC_QOS_IN#SCAVENGER__acl
ip access-list extended prm-APIC_QOS_IN#TUNNELED__acl
!
```

The following provides an example of what the ACL entries will look like after the ACE entries have been populated—with just a few of the ACE entries shown for compactness.

```

!
```

```
ip access-list extended prm-APIC_QOS_IN#VOICE__acl
ip access-list extended prm-APIC_QOS_IN#BROADCAST__acl
ip access-list extended prm-APIC_QOS_IN#REALTIME__acl
ip access-list extended prm-APIC_QOS_IN#MM_CONF__acl
ip access-list extended prm-APIC_QOS_IN#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
...
ip access-list extended prm-APIC_QOS_IN#SIGNALING__acl
...
remark skinny
permit tcp any any eq 2000
permit tcp any any eq 2001
permit tcp any any eq 2002
remark sip
permit tcp any any eq 3478
permit udp any any eq 3478
...
ip access-list extended prm-APIC_QOS_IN#OAM__acl
...
remark dhcp—Dynamic Host Configuration Protocol
permit udp any any range 67 68
remark dns—Domain Name System
permit tcp any any eq 53
permit udp any any eq 53
permit tcp any any eq 5353
permit udp any any eq 5353
...
ip access-list extended prm-APIC_QOS_IN#TRANS_DATA__acl
...
remark ibm-db2—IBM-DB2
permit tcp any any eq 523
```

```
permit udp any any eq 523
remark sap—SAP
permit tcp any any eq 3200
permit tcp any any eq 3300
permit tcp any any eq 3600
...
ip access-list extended prm-APIC_QOS_IN#BULK_DATA__acl
...
remark ftp—File Transfer Protocol
permit tcp any any eq 21
permit tcp any any eq 21000
remark imap—Internet Message Access Protocol version 4
permit tcp any any eq 143
permit udp any any eq 143
permit tcp any any eq 220
permit udp any any eq 220
...
ip access-list extended prm-APIC_QOS_IN#SCAVENGER__acl
...
remark blizwow—World of Warcraft
permit tcp any any eq 3724
permit udp any any eq 3724
remark call-of-duty—Call of Duty
permit tcp any any eq 20500
permit tcp any any eq 20510
permit tcp any any eq 28960
permit udp any any eq 20500
...
ip access-list extended prm-APIC_QOS_IN#TUNNELED__acl
remark CAPWAP Control Traffic
permit udp any any eq 5246
remark CAPWAP Data Traffic
permit udp any any eq 5247
!
```

Remarks are used in order to make it visually easy for the network operator to determine which applications have been deployed.

The specific applications that appear within each ACL are dependent upon the applications declaratively selected by the network operator as being business-relevant, default, or business-irrelevant, as well as any DSCP, IP address, or TCP/UDP port based Custom applications defined by the network operator within the EasyQoS web-based GUI.

### Effects of Changing Business Relevance on ACLs

For Catalyst switch platforms, ACLs with ACE entries corresponding to the IP addresses and ports used to identify an application, are provisioned by EasyQoS in order to classify and mark the application as it enters the access-edge switch port. Therefore, changing the business relevance of an application within the EasyQoS web-based GUI simply changes the placement of the ACE entry within the ACLs that are referenced from the class-map definitions for each traffic class—based on the following rules:

- If an application is moved from having a business relevance attribute value of business-relevant to business-irrelevant (that is, moved from the business-relevant grouping to the business-irrelevant grouping within the application registry for the policy applied to the device), the ACE entry for the application will be provisioned within the `prm-APIC_QOS_IN#SCAVENGER__acl` ACL. Hence, all applications that have been identified as being business-irrelevant are classified into the Scavenger traffic class and re-marked to a Class Selector 1 (CS1) per-hop behavior. This assumes the application can be uniquely identified by IP addresses, IP ports, or UDP/TCP ports and that there is sufficient TCAM space available to provision the ACE entries.
- If an application is moved from having a business relevance attribute of either business-relevant or business-irrelevant, to default (that is, moved from either the business-relevant or business-irrelevant grouping to the default grouping within the application registry for the policy applied to the device), no ACE entry for this application will be provisioned in any ACL. All applications with a default business relevance are classified in the Default traffic class and re-marked to a best effort per-hop behavior.
- If an application is moved from having a business relevance attribute value of either business-irrelevant or default, to business-relevant (that is, moved from the business-irrelevant or the default grouping to the business-relevant grouping within the application registry for the policy applied to the device), the ACE entry for the application will be provisioned into the ACL corresponding to the traffic-class attribute for that particular application. All 1300+ applications identified within the NBAR taxonomy have a default setting for the traffic-class attribute—meaning the traffic-class to which the application belongs. This attribute can be modified within the EasyQoS web-based GUI as of APIC-EM release 1.5 and higher. All Custom applications created within the EasyQoS web-based GUI must have a traffic-class value assigned to them when they are created. Note that the traffic-class attribute value assigned to Custom applications and all 1300+ applications known by the NBAR taxonomy does not include values for Scavenger or Default traffic-classes. Hence applications identified as being business-relevant have ACE entries generated within the traffic class to which the application belongs. This assumes the application can be uniquely identified by IP addresses, IP ports, or UDP/TCP ports and that there is sufficient TCAM space available to provision the ACE entries.

### Custom Applications Provisioned within ACLs

EasyQoS is not able to deploy Layer 2-4 ACE entries for Custom applications that consist of URL strings. APIC-EM will therefore skip over the deployment of Custom applications consisting of URL strings when configuring Catalyst switch platforms. Hence Catalyst switches are unable to implement a Custom application that is based on the use of a URL to identify the application. Catalyst switches can only implement Custom applications that are based upon DSCP values, IP addresses, IP ports, and TCP/UDP ports. Custom applications based on IP addresses, ports, and/or DSCP values are simply added as additional ACE entries under the ACL corresponding to the particular traffic-class to which the Custom application has been defined by the network operator.

Custom applications are by default marked as a Favorite application by EasyQoS. In order to include a Custom application within a QoS policy, the network operator must drag-and-drop Custom applications into one of the three business relevance groupings within the EasyQoS web-based GUI interfaces. This is discussed in the **\*APIC-EM and the EasyQoS Application\*** chapter.

An example of a Custom application configured for the multimedia-conferencing traffic class is shown below.

!

```
ip access-list extended prm-APIC_QOS_IN#MM_CONF__acl
remark Custom_Port-App
permit udp any 10.0.10.0 0.0.0.255 range 3001 3010
permit udp 10.0.10.0 0.0.0.255 range 3001 3010 any
!
```

In the example above, the Custom application, based on a destination server IP address range and port range—also referred to as the *producer*—has been specified to be bi-directional by the network operator, through the EasyQoS web-based GUI. Hence, the reverse of the ACE entry is also generated to allow traffic from the server IP address and port range to also be treated the same.

In the example above, a server IP address range (10.0.10.0-10.0.10.255) and port range (UDP 3001-3010) is configured. Custom applications also support single IP addresses and ports, and the use of “any” specified as the destination IP address. Although a single UDP port range is specified in the example above, multiple UDP and/or TCP ports can be configured as well—each of which would appear as a separate “permit” statement.

Additional IP Address/Port-based Custom applications will generate additional ACE entries within ACLs, similar to those shown in the example above, based on the rules discussed within the **\*Effects of Changing Business Relevance on ACLs\*** section above.

A more sophisticated example, shown below, adds a source IP address or range—also referred to as the *consumer*—as well as the destination IP address or range—referred to as the *producer* to the Custom application. Again, this is configured bi-directionally via the APIC-EM EasyQoS web-based GUI by the network operator. An example of the same application—but with a consumer this time—is shown below.

```
!
ip access-list extended prm-APIC_QOS_IN#MM_CONF__acl
remark Custom-Port-App_Consumer__Custom_Port-App
permit udp host 10.0.20.20 eq 3100 10.0.1.0 0.0.0.255 range 3001 3010
remark Custom_Port-App__Custom-Port-App_Consumer
permit udp 10.0.1.0 0.0.0.255 range 3001 3010 host 10.0.20.20 eq 3100
!
```

The combination of the producer and consumer, along with the ability to apply the policy bi-directionally, essentially gives the network operator the ability to use nearly the full CLI functionality in terms of being able to configure QoS ACE entries.

### Changing the Traffic-Class of Applications on Switch Platforms

APIC-EM release 1.5 and higher supports the ability to change the traffic-class of an application within the NBAR2 taxonomy. An example of this was shown in Figure 33 within **Application Registry** section the **\*APIC-EM and the EasyQoS Application\*** chapter of this document.

For switch platforms, changing the traffic-class of an application will simply result in the ACE entry for the particular application to be defined under the desired class-map entry for the traffic-class. Note, however, that the application may have to be selected as a Favorite, in order to give preference to including the application within the ACL-based ingress classification & marking policy on Catalyst switch platforms which have TCAM constraints.

### Cisco Device Endpoints

APIC-EM also discovers Cisco endpoints, such as Cisco IP phones, Cisco video surveillance cameras, Cisco TelePresence devices, and Cisco video conferencing endpoints. CDP information provided by the Cisco device endpoint also identifies the device type. This information is necessary because different device types are populated via ACE entries within different ACLs with different DSCP markings.

As part of Static QoS, the IP addresses of these endpoints, along with the appropriate DSCP markings for traffic generated by these devices are also added to the ingress classification & marking policy for each switch to which the endpoints are connected. The DSCP values populated into the ACLs for Static QoS is shown in the table below.

#### 1. Wired Cisco Device Endpoints and DSCP Markings

Wired Endpoint Device Type	Allowed DSCP Values	Static QoS ACL in Which the ACE Entry Will be Added	Description
Cisco IP Phone	EF AF41	prm-APIC_QOS_IN#VOICE__acl prm-APIC_QOS_IN#MM_CONF__acl	Cisco IP Phones typically send VoIP media (and associated RTCP flows) marked as EF when a call is audio only, and VoIP and video media both marked as AF41 when a call is both audio and video.
Cisco Video Conferencing Endpoints	EF AF41	prm-APIC_QOS_IN#VOICE__acl prm-APIC_QOS_IN#MM_CONF__acl	Cisco Video Conferencing Endpoints typically send VoIP media (and associated RTCP flows) marked as EF when a call is audio only, and VoIP and video media both marked as AF41 when a call is both audio and video.
Cisco TelePresence Device	CS4 EF	prm-APIC_QOS_IN#REALTIME__acl prm-APIC_QOS_IN#VOICE__acl	Cisco TelePresence devices typically send VoIP and video media (and associated RTCP flows) both marked as CS4 when a call is audio and video; and VoIP media (and associated RTCP flows) marked as EF when a call is audio only.
Cisco Video Surveillance Cameras	CS5	prm-APIC_QOS_IN#BROADCAST__acl	H.264 or H.265 encoded streaming video surveillance typically uses the RTP protocol for transport. The network operator may need to ensure that streaming video is sent with a CS5 marking.

The DSCP marking of voice and video media for devices under the control of CUCM can be modified via the CUCM GUI. Hence, the CUCM administrator should ensure that the markings of audio and video media are the same for the endpoints as listed in the table above.

APIC-EM populates both the `prm-APIC_QOS_IN#VOICE__acl` and the `prm-APIC_QOS_IN#MM_CONF__acl` within the static ingress classification & marking policy on the switch to which a wired Cisco IP Phone endpoint is discovered with permit statements for the source IP address of a Cisco IP Phone along with the expected media markings (DSCP values). An example is as follows:

```
!
ip access-list extended prm-APIC_QOS_IN#VOICE__acl
permit ip host 10.4.81.21 any dscp ef
!
ip access-list extended prm-APIC_QOS_IN#MM_CONF__acl
permit ip host 10.4.81.21 any dscp af41
!
```

Cisco IP Phones are expected to generate voice traffic with a DSCP marking of EF in an audio-only call, and voice & video traffic with a DSCP marking of AF41 in a video call.

APIC-EM populates both the `prm-APIC_QOS_IN#VOICE__acl` and the `prm-APIC_QOS_IN#MM_CONF__acl` within the static ingress classification & marking policy on the switch to which a wired Cisco video conferencing



endpoint is discovered with permit statements for the source IP address of the Cisco video conferencing endpoint along with the expected media markings (DSCP values). An example is as follows:

```
!
ip access-list extended prm-APIC_QOS_IN#VOICE__acl
permit ip host 10.4.81.22 any dscp ef
!
ip access-list extended prm-APIC_QOS_IN#MM-CONF__acl
permit ip host 10.4.81.22 any dscp af41
!
```

Cisco video conferencing endpoints are also expected to generate voice traffic with a DSCP marking of EF in an audio-only call, and voice & video traffic with a DSCP marking of AF41 in a video call.

APIC-EM populates both the prm-APIC\_QOS\_IN#VOICE\_\_acl and the prm-APIC\_QOS\_IN#REALTIME\_\_acl within the static ingress classification & marking policy on the switch to which a wired Cisco TelePresence endpoint is discovered with permit statements for the source IP address of the Cisco TelePresence endpoint along with the expected media markings (DSCP values).

```
!
ip access-list extended prm-APIC_QOS_IN#VOICE__acl
permit ip host 10.4.81.23 any dscp ef
!
ip access-list extended prm-APIC_QOS_IN#REALTIME__acl
permit ip host 10.4.81.23 any dscp cs4
!
```

Cisco TelePresence endpoints are expected to generate voice traffic with a DSCP marking of EF in an audio-only call and voice & video traffic with a DSCP marking of CS4 in a video call.

- Note: The default marking for Cisco TelePresence devices may change from CS4 to AF41 within future CUCM software versions. This reflects the fact that TelePresence video media has evolved over time from exhibiting a behavior more similar to an inelastic flow to exhibiting a behavior more similar to an elastic flow. There is currently no means for the network operator to change the value of DSCP markings populated in the static ACLs by APIC-EM for discovered endpoint devices. Therefore, the network operator must ensure that Cisco TelePresence devices mark video media as CS4 within the CUCM GUI, in order to correctly operate with APIC-EM EasyQoS.

Voice and video media from Cisco IP Phones, Cisco video conferencing endpoints, and Cisco TelePresence endpoints use RTP/UDP transport, typically in the port range from UDP ports 16384-32767, using even numbered ports. However, these endpoints may also generate other traffic, such as RTP Control Protocol (RTCP) traffic. RTCP traffic typically uses the next higher odd numbered UDP port. For example, if the audio media port is UDP 16384, the associated RTCP control stream is typically UDP 16385. RTCP provides feedback information regarding the quality of the media stream, including information regarding lost packets. Cisco IP Phones, Cisco video conferencing endpoints, and Cisco TelePresence endpoints send RTCP streams with the same DSCP marking as their corresponding media flow. Hence the ACE entries listed in Table 1 above apply to RTCP flows as well.

APIC-EM will populate the prm-APIC\_QOS\_IN-#BROADCAST\_\_acl within the static ingress classification & marking policy on the switch to which a wired Cisco video surveillance camera is discovered with permit statements for the source IP address of the Cisco video surveillance camera along with the expected media marking (DSCP value). An example is as follows:

```
!  
ip access-list extended prm-APIC_QOS_IN#VOICE__acl  
permit ip host 10.4.81.24 any dscp cs5  
!
```

Cisco video surveillance cameras are expected to generate video traffic with a DSCP marking of CS5. This video traffic is typically H.264 or H.265 encoded streaming video sent via the RTP protocol that uses UDP transport. Cisco video surveillance cameras may also sent RTSP control traffic using TCP ports 554 or 8554. This traffic should not be sent with a DSCP marking of CS5, because it is not streaming media (i.e. video). RTSP traffic should automatically be categorized as signaling traffic and an ACE entry for RTSP traffic placed into the prm-APIC\_QOS\_IN#SIGNALING-ACL.

If the Host Tracking feature has been enabled within the EasyQoS policy, APIC-EM will periodically re-discover devices on the network and automatically update the entries in the ACLs for devices that have been added/moved/changed. The Host Tracking feature was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. As a prerequisite for adds/moves/changes, the network operator will need to enable SNMP traps on the access switches to be sent to APIC-EM. After the interface connected to a Cisco IP Phone, Cisco video conferencing endpoint, Cisco Telepresence device, or Cisco video surveillance camera goes up or down APIC-EM will receive an SNMP trap and starts collecting information from the access switch that generated the SNMP trap, about the new Cisco endpoints. This takes approximately 80 seconds plus the time needed for the collection of the device information. After the Cisco endpoint information is collected, APIC-EM automatically pushes ACE entries containing the source IP address of the endpoint device to any destination, with the prm-APIC\_QOS\_IN#VOICE\_\_acl, prm-APIC\_QOS\_IN#BROADCAST\_\_acl, prm-APIC\_QOS\_IN#REALTIME\_\_acl, and prm-APIC\_QOS\_IN#MM\_CONF\_\_acl entries with IP + DSCP in both static and dynamic policies.

### Dynamic QoS

When the network operator has implemented Dynamic QoS, EasyQoS will configure a dynamic policy-map shell for ingress classification and marking of voice and video traffic only, for each switch port. These policy-map shells are dynamically populated with ACEs and dynamically placed/removed across the required switch port, based upon notification of calls beginning/ending from CUCM. This is discussed further in the **\*Dynamic QoS Design\*** chapter.

### Distribution-Layer Switch QoS Design

The QoS policy configuration pushed to distribution-layer switches by APIC-EM EasyQoS is dependent upon whether the network operator chooses to implement Static or Dynamic QoS.

### Ingress/Egress Queuing Policies

Regardless of whether the network operator has chosen to implement Static or Dynamic QoS, the EasyQoS application will always apply ingress and/or egress queuing policies to the uplinks ports. For a switch in the role of a distribution-layer switch, *uplink ports* refer to ports that connect to core-layer switches, to other distribution-layer switches, or to access-layer switches. The specifics as to whether both ingress and egress queuing policies, or only egress queuing policies are applied, are dependent upon whether the particular Catalyst switch platform and/or line card within that platform supports both ingress and egress queuing, or only egress queuing. This is discussed in detail for each platform and/or line card in the **\*Catalyst and Nexus Switch Platform Queuing Design\*** chapter.

### Ingress Classification & Marking Policies

With APIC-EM release 1.4 and higher, only when the network operator has chosen to implement Dynamic QoS will the EasyQoS application additionally create and apply an ingress classification & marking policy to all uplink ports that connect to access-layer switches. The ingress classification & marking policy applied to distribution-layer switch ports that are connected to access-layer switches is discussed in the **\*Dynamic QoS for Wired Devices\*** section of the **\*Dynamic QoS Design\*** chapter.

### Pre-Existing QoS Configurations on Switch Platforms

This section discusses how EasyQoS handles prior QoS configurations on switch platforms, when deploying an EasyQoS policy. For ingress classification & marking policies, EasyQoS will remove any existing service-policy definition from the interface and replace it with its service-policy definitions. The previous class-map and policy-map definitions will not be deleted by EasyQoS. This is necessary for restoring the original pre-EasyQoS (before any EasyQoS configuration was applied) configuration back to the switch platform. The Restore feature is a feature supported in APIC-EM EasyQoS release 1.3 and higher.

- Note: APIC-EM release 1.4.0 did not remove all per-VLAN QoS policies or per-port per-VLAN QoS policies (where supported) configured under all switch platforms. For example, QoS policies applied under global “vlan configuration” statements on Catalyst 4500 Series platforms were not removed as of APIC-EM release 1.4.0. Likewise, “mls qos vlan-based” and “platform qos vlan-based” commands on MLS QoS Platforms (Catalyst 3750, 3560, or 2960 Series, and older Catalyst 6K Series with Sup720) and C3PL platforms (Catalyst 6K Series with Sup2T) were not removed. This may result in the application of EasyQoS policy failing or the QoS policy itself to be non-deterministic in its behavior. However, as of the APIC-EM 1.4.1 maintenance release and higher per-VLAN and per-port per-VLAN QoS policies are removed from these platforms.

For queuing policies, the behavior depends on whether the platform is an MQC platform (Catalyst 3850, 3650, or 4500 Series), a C3PL platform (Catalyst 6K Series with Sup2T), an NX OS platform (Nexus 7000 or 7700 Series), or an older MLS QoS platform (Catalyst 3750, 3560, or 2960 Series, Catalyst 6K Series with Sup720, or SM-ES2 Series EtherSwitch module).

- For MQC and C3PL platforms, queuing policies are applied via service-policy statements similar to ingress classification & marking policies. The behavior is the same as with ingress classification & marking policies. The previous class-map and policy-map definitions will not be deleted by EasyQoS. Clicking the Restore button within an EasyQoS policy will cause the pre-EasyQoS queuing service-policy statements to be re-applied to the interfaces.
- For MLS QoS platforms, the queuing policy is configured directly on the interface. EasyQoS may change the policy, so there is no previous configuration saved on the switch platform. Therefore, clicking the Restore button may not restore the pre-EasyQoS queuing policy for these platforms, although the ingress classification & marking policy will be restored, because it uses service-policy definitions applied to the interfaces.
- For NX OS platforms, the class-map definitions are system-defined, and not user-defined. EasyQoS may modify the mapping of DSCP and/or CoS values to the ingress and/or egress queues. This will not be restored to their pre-EasyQoS configuration. However, policy-map definitions are user-defined (or extended from the default template). Existing policy-map definitions are not deleted by EasyQoS. Therefore, clicking the Restore button within an EasyQoS policy will cause the pre-Existing queuing service-policy statements to be re-applied to the interfaces.

EasyQoS does not currently remove Auto QoS statements. Depending on the platform and what form of Auto QoS is implemented, this can cause EasyQoS policy to not function properly. Therefore, the network operator should either completely remove Auto QoS configurations before applying any EasyQoS policy or not implement EasyQoS policy when Auto QoS is configured on the platform. Future versions of APIC-EM EasyQoS may remove Auto QoS configuration as well.

## 1.9 Chapter 9: Catalyst and Nexus Switch Platform Queuing Design

The following sections discuss the ingress and/or egress queuing structures provisioned by EasyQoS to the various supported Catalyst and Nexus Series switch platforms.

EasyQoS within the APIC-EM release 1.4 added the ability for the network operator to specify the bandwidth allocation for each of the traffic-classes within the QoS policy applied to a given policy scope. APIC-EM release 1.5 and higher extends this, by allowing the network operator to specify the DSCP marking per traffic-class. This is accomplished through the application of a custom Queuing Profile to a policy.

Table 1 in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter summarizes the custom Queuing Profile support (both BW allocation and DSCP markings) for various switch and router platforms. As was discussed within that chapter, the network operator can either apply the default Queuing Profile—CVD\_Queueing\_Profile (Default)—or create a custom Queuing Profile to apply to the devices within the policy scope.

The bandwidth allocations for each of the traffic-classes within a custom Queuing Profile can be applied to all interface speeds—referred to as All References within the EasyQoS GUI. Alternatively, different bandwidth allocations can be configured for each of the traffic-classes based on the interface speed—1 Mbps, 10 Mbps, 100 Mbps, 1 Gbps, 10/40 Gbps, and 100 Gbps.

### Catalyst 2K / 3K Series Switches and SM-ES2 EtherSwitch Module Queuing Design

This section applies to the following switch platforms:

- Catalyst 2960-C Series
- Catalyst 2960-CX Series
- Catalyst 2960-S Series
- Catalyst 2960-X Series
- Catalyst 2960-XR Series
- Catalyst 3560-C Series
- Catalyst 3560-CX Series
- Catalyst 3560-X Series
- Catalyst 3750-X Series
- SM-ES2 Series EtherSwitch Module

#### Platform Specific Requirements

Catalyst 2960-S and 2960-X Series platforms must be running a LAN Base image in order to support the following QoS features:

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

Because these features are used by EasyQoS, only Catalyst 2960-S and 2960-X Series platforms that run a LAN Base image are supported by EasyQoS.

Catalyst 2960-C and 2960-CX Series platforms only run a LAN Base image.

The SM-ES2 Series EtherSwitch module only runs a LAN Base image.

Catalyst 2960-S and 2960-X Series switches, as well as the SM-ES2 Series EtherSwitch module, only support Layer 2 switching.

Catalyst 2960-XR Series platforms run an IP Lite image, which includes Layer 3 switching support.

Catalyst 3750-X and 3560-X Series platforms run one of the following three feature sets, all of which support QoS:

- IP Services Feature Set
- IP Base Feature Set (IP Base or Universal on the Catalyst 3560-X Series)
- LAN Base Feature Set

Catalyst 3750-X and 3560-X Series platforms support Layer 2 and Layer 3 switching, as well as ingress queuing.

#### Globally Enabling QoS

Catalyst 2K and 3K Series platforms, as well as the SM-ES2 Series EtherSwitch module, are MLS QoS-based platforms. MLS QoS based platforms require QoS to be enabled globally first before configuring any other QoS commands. The following global-level commands provisioned by EasyQoS enable QoS and set the internal COS-to-DSCP mapping table within the platform.

!

```
mls qos
```

! Globally Enables QoS

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

! Maps CoS 5 to 46 (rest are default)

!

- Note: The configurations shown for the Catalyst 2K and 3K Series switches include comments, either before or after the actual commands. Comments are not part of the configuration provisioned by EasyQoS. They are included only to provide additional detail to the reader regarding the meaning of the command. Comment lines begin with a “!” within the configuration examples.

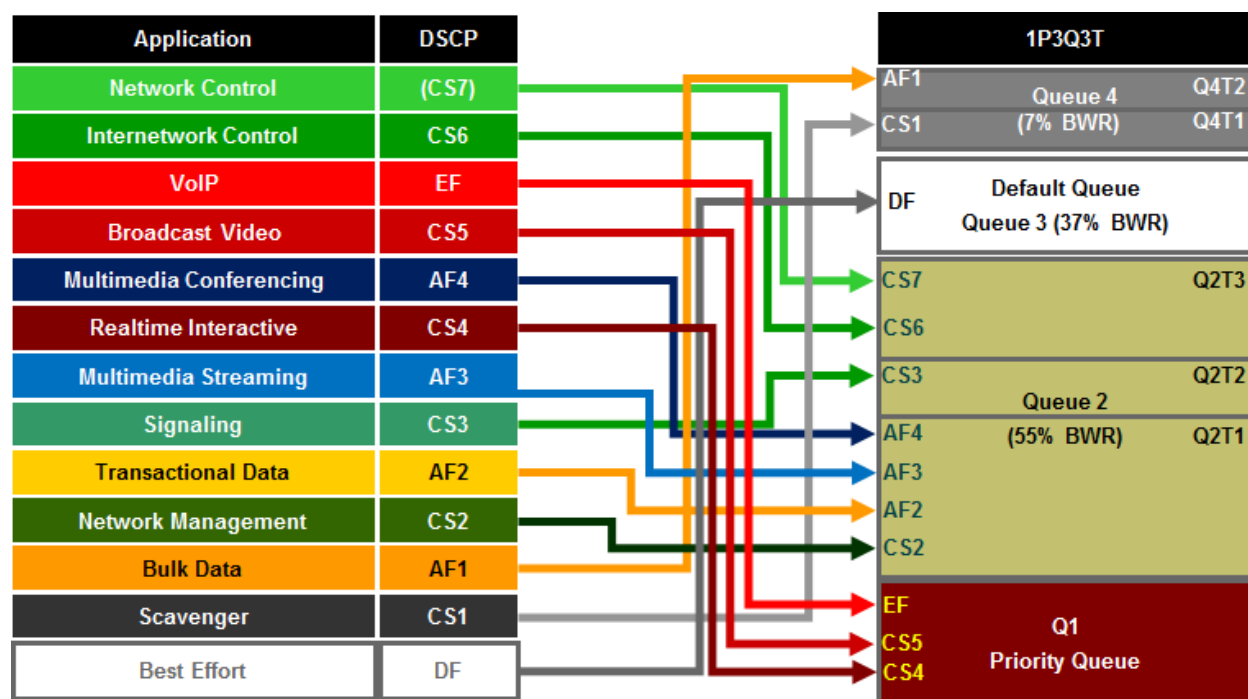
#### Default 1P3Q3T Egress Queuing Design

Catalyst 2K and 3K Series switches, as well as the SM-ES2 Series EtherSwitch module, support a 1P3Q3T egress queuing structure. APIC-EM release 1.4 changed the default bandwidth allocations for the 1P3Q3T egress queuing design. With APIC-EM release 1.4 and higher, the default bandwidth allocations are part of the CVD\_Queueing\_Profile which is applied by default, unless the network operator applies a custom Queueing Profile to the policy scope containing these switches.

The 1P3Q3T egress queuing structure for these platforms implements DSCP-to-queue mapping with WTD for congestion avoidance. Although there are three WTD thresholds, only two are configurable. The third threshold is by default set to the depth of the queue (that is, 100% queue depth).

The following figure shows the 1P3Q3T egress queuing model deployed by EasyQoS within the default CVD\_Queueing\_Profile.

1. Default 1P3Q3T Egress Queuing for Catalyst 2K / 3K and SM-ES2 EtherSwitch Module



The following configuration provisioned by EasyQoS implements the 1P3Q3T egress queuing structure. Comments have been added to the configuration in order to explain each of the commands.

!

! Tunes Egress Queuing Buffers and Thresholds

```
mls qos queue-set output 1 buffers 15 30 35 20
```

! Allocates 15% for Q1-PQ; 30% for Q2; 35% for Q3-Default Queue; 20% for Q4

```
mls qos queue-set output 1 threshold 1 100 100 100 100
```

! No WTD thresholds for PQ; reserve full 100% of buffers; no need to borrow more

```
mls qos queue-set output 1 threshold 2 80 90 100 400
```

! Tunes Q2T1 for Call Signaling (CS); Tunes Q2T2 for Network Control (NC);

! reserve full 100% of buffers; borrow up to 400% as needed

```
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

! No WTD thresholds in BE queue (all packets have same CoS/DSCP weight of 0);

! reserve full 100%; borrow max as needed

```
mls qos queue-set output 1 threshold 4 60 80 100 400
```

! Tunes Q4T1 for Scavenger (SCV); Tunes Q4T2 for Bulk Data (BD)

! Maps CoS to Egress Queues (although we're not trusting CoS with APIC-EM;

! but for the sake of a comprehensive policy, this is included)

```
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
```

! Maps Real-Time Interactive (RTI) and MM\_CONF (MMC) and

! Broadcast Video (BVI) and Voice (VO) to PQ

```

mls qos srr-queue output cos-map queue 2 threshold 1 2
! Maps Operations-Administration-Management (OAM) and Transactional Data (TD) to Q2T1
mls qos srr-queue output cos-map queue 2 threshold 2 3
! Maps Call Signaling (CS) + Multimedia Streaming (MMS) to Q2T2
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
! Maps Network Control (NC) to Q2T3
mls qos srr-queue output cos-map queue 4 threshold 3 1
! Maps BD + SCV to Q4 (tail)
! Maps DSCP to Egress Queues
mls qos srr-queue output DSCP-map queue 1 threshold 3 32 40 46
! Maps RTI + BV + VO (DSCP EF)
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
! Maps MMS + TD + MMC to Q2T1
mls qos srr-queue output DSCP-map queue 2 threshold 2 24
! Maps CS to Q2T2
mls qos srr-queue output DSCP-map queue 2 threshold 3 48 56
! Maps NC to Q2T3 (Per RFC 4594 NC = DSCP CS6/48; but this class also includes
! CS7/56, which Cisco uses for internal DSCP of spanning tree & other protocols)
mls qos srr-queue output DSCP-map queue 3 threshold 3 0 1 2 3 4 5 6 7
! Maps BE + non-standard DSCPs to Q3 (tail)
mls qos srr-queue output DSCP-map queue 3 threshold 3 9 11 13 15
mls qos srr-queue output DSCP-map queue 3 threshold 3 17 19 21 23
mls qos srr-queue output DSCP-map queue 3 threshold 3 25 27 29 31
mls qos srr-queue output DSCP-map queue 3 threshold 3 33 35 37 39
mls qos srr-queue output DSCP-map queue 3 threshold 3 41 42 43 44 45 47
mls qos srr-queue output DSCP-map queue 3 threshold 3 49 50 51 52 53 54 55
mls qos srr-queue output DSCP-map queue 3 threshold 3 57 58 59 60 61 62 63
! Maps non-standard DSCPs to Q3 (tail)
mls qos srr-queue output DSCP-map queue 4 threshold 1 8 14
! Maps SCV + BD (AF13) to Q4T1
mls qos srr-queue output DSCP-map queue 4 threshold 2 12
! Maps Bulk (AF12) to Q4T2
mls qos srr-queue output DSCP-map queue 4 threshold 3 10
! Maps Bulk (AF11) to Q4 (tail)
!

```

- Note: APIC-EM release 1.5 and higher modifies the maximum buffers that the default queue (Q3) can borrow, if buffer space is available. Previously the maximum was set for 400%. With APIC-EM release 1.5 and higher, this has been increased to 3200%.

The above configuration maps CoS 4 and 5, as well as DSCP values 46 (EF), 40 (CS5), and 32 (CS4) to queue 1, threshold 3 (Q1T3). By default, drop threshold 3 is set for 100% of the queue depth. Queue 1 is configured as a strict priority queue within the interface configuration show below. Queue 1 is allocated approximately 15% of the buffers.

CoS 7 and 6, as well as DSCP values 48 (CS6) and 56 (CS7) are mapped to queue 2, threshold 3 (Q2T3), because these are considered to be control traffic. Again, by default, drop threshold 3 is set for 100% of the queue depth. CoS 3, as well as DSCP value 24 (CS3) is mapped to queue 2, threshold 2 (Q2T2) with a drop threshold of 90% of the queue depth. CoS 2, as well as DSCP values 34 (AF41), 36 (AF42), 38 (AF43), 26 (AF31), 28 (AF32), 30 (AF30), 18 (AF21), 20 (AF22), 22 (AF23), and 16 (CS2) are mapped to queue 2 threshold 1 (Q2T1) with a drop threshold of 80% of the queue depth. Queue 2 is allocated approximately 30% of the buffers.

DSCP values 8 (CS1) and 14 (AF13) are mapped to queue 4 threshold 1 (Q4T1) with a drop threshold of 60%. DSCP value 12 (AF12) is mapped to queue 4 threshold 2 (Q4T2) with a drop threshold of 80%. CoS 1, as well as DSCP value 10 (AF11) is mapped to queue 4 threshold 3 (Q4T3) with a default drop threshold of 100%. Queue 4 is allocated approximately 20% of the buffers.

Finally all other CoS and DSCP values are mapped to queue 3, threshold 3 (Q3T3) with a default drop threshold of 100% of the queue depth. Queue 1 is configured for approximately 35% of the buffers.

In the configuration above, WTD is only applied to queues 2 and 4. Queue 1 is a priority queue, for real-time multimedia traffic, hence WTD is not necessary. Queue 4 is the queue with default traffic, hence WTD is not necessary there either.

The 1P3Q3T egress queuing structure is applied by EasyQoS to all FastEthernet, GigabitEthernet, and TenGigabitEthernet interfaces, with the following exception:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.

An example of the provisioning to a single GigabitEthernet and single TenGigabitEthernet interface is shown below.

!

```
interface GigabitEthernetx/x/x
```

```
no mls qos trust
```

```
! Default setting for access port interfaces (not explicitly provisioned by EasyQoS)
```

```
queue-set 1
```

```
! Default queue set for access port interfaces (not explicitly provisioned by EasyQoS)
```

```
srr-queue bandwidth share 1 55 37 7
```

```
! Sets the remaining queues to share the remaining bandwidth in a ratio of
```

```
! 55, 37, and 7
```

```
! Queue 1 bandwidth ratio is ignored when priority queueing is enabled
```

```
priority-queue out
```

```
! Implements egress priority queueing for queue 1
```

```
interface TenGigabitEthernetx/x/x
```

```
mls qos trust DSCP
```

```
! Explicitly sets access interface to trust DSCP markings
```



```
queue-set 1
```

```
! Default queue set for access port interfaces (not explicitly provisioned by EasyQoS)
```

```
srr-queue bandwidth share 1 55 37 7
```

```
! Sets the remaining queues to share the remaining bandwidth in a ratio of
```

```
! 55, 37, and 7
```

```
! Queue 1 bandwidth ratio is ignored when priority queueing is enabled
```

```
priority-queue out
```

```
! Implements egress priority queueing for queue 1
```

```
!
```

Interfaces that connect to end-devices (access-edge ports) are set to not trust DSCP or CoS markings (unless a Cisco Access Point is connected). Interfaces that connect to distribution-layer switches (uplink ports) are explicitly set to trust DSCP.

The bandwidth allocations within the EasyQoS GUI for Queuing Profiles require the sum of the bandwidth percentages to total 100%. These bandwidth allocations are absolute bandwidth percentages. Because the 1P3Q3T egress queuing policy implements a four-queue model in hardware on these switch platforms, multiple traffic-classes are mapped to each queue. The 1P3Q3T egress policy implements a low-latency queue via the interface-level “priority-queue out” command. The Voice, Broadcast Video, and Real-Time Interactive traffic-classes are mapped to the priority queue within “mls qos srr-queue output dscp-map” definitions. The priority queue on these platforms is unconstrained in terms of the amount of bandwidth it can consume. Therefore, the bandwidth allocated in the EasyQoS GUI within Queuing Profiles (default or custom) for these three traffic-classes is not enforced on these platforms.

The remaining nine traffic-classes within the 1P3Q3T egress queuing policy are mapped to the remaining three egress hardware queues. Bandwidth allocation for these three queues is implemented as bandwidth remaining ratios through the “srr-queue bandwidth share” interface-level command. Bandwidth remaining refers to bandwidth remaining after servicing the low-latency queue. Bandwidth ratio refers to the bandwidth being allocated in a ratio of the numbers configured within the “srr-queue bandwidth share” command. For example, the BW allocation within the default CVD\_Queueing\_Profile is specified as follows:

```
srr-queue bandwidth share 1 55 37 7
```

The four numbers (1, 55, 37, and 7) refer to the amount of bandwidth allocated to the PQ, Q2, Q3 (which is also the default queue) and Q4, respectively. The first number is not used in the bandwidth allocation if the “priority-queue out” command is configured on the interface and can therefore be set to anything. Bandwidth is allocated to the remaining three queues in a ratio of 55:37:7 in the example above. The bandwidth allocation is shared—meaning that any given queue can use more than its allocated share if one or more of the other queues is not currently using their share and bandwidth is available.

The following table shows the mapping of the traffic-classes and bandwidth allocations from the default EasyQoS CVD\_Queueing\_Profile to the 1P3Q3T egress queuing structure.

#### 1. Default Queuing Profile Mapping to 1P3Q3T Egress Queuing Policy

Traffic Class	DSCP Marking	BW % in the Default Queuing Profile	BWR % Calculated from the Default Queuing Profile	1P3Q3T Egress Queue Mapping	BWR % Allocation in 1P3Q3T Egress Queue
Voice	EF	10%	N/A	Q1 (PQ)	PQ bandwidth is unconstrained and consists of traffic from the Voice, Broadcast Video, and Real-Time Interactive traffic-classes
Broadcast Video	CS5	10%	N/A	Q1 (PQ)	
Real-Time Interactive	CS4	13%	N/A	Q1 (PQ)	
Multimedia Conferencing	AF41	10%	15%	Q2	Sum of BWR for traffic-classes mapped to Q2 = 15% (Multimedia Conferencing) + 15% (Multimedia Streaming) + 4% (Network Control) + 3% (Signaling) + 3% (OAM) + 15% (Transactional Data) = 55%
Multimedia Streaming	AF31	10%	15%	Q2	
Network Control	CS6	3%	4%	Q2	
Signaling	CS3	2%	3%	Q2	
OAM	CS2	2%	3%	Q2	
Transactional Data	AF21	10%	15%	Q2	
Bulk Data	AF11	4%	6%	Q4	Sum of BWR for traffic-classes mapped to Q4 = 6% (Bulk Data) + 1% (Scavenger) = 7%
Scavenger	CS1	1%	1%	Q4	
Best Effort	Default	25%	37%	Q3	BWR for Best Effort traffic-class mapped to Q3 = 37%

Column 3 of the table above shows the percentage bandwidth allocation for each of the traffic-classes as it appears within the EasyQoS GUI for the default CVD\_Queueing\_Profile. In the 1P3Q3T egress queuing policy, the Voice, Broadcast Video, and Real-Time Interactive traffic-classes are mapped to the PQ, as shown in column 5. The sum of the bandwidth allocated to these three traffic-classes can be considered as the total priority queue bandwidth (Total\_PQ\_BW), as shown in the following formula.

$$\text{Total\_PQ\_BW} = \text{Voice BW} + \text{Broadcast Video BW} + \text{Real-Time Interactive BW}$$

Based on the bandwidth allocations in column 3 in the table above Total\_PQ\_BW can be calculated as follows:

$$\text{Total\_PQ\_BW} = 10\% (\text{Voice BW}) + 10\% (\text{Broadcast Video BW}) + 13\% (\text{Real-Time Interactive BW}) = 33\%$$

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated

based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI, and the amount of Total\_PQ\_BW calculated above. This can be done through the following formula.

$$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$$

For example, BWR percentage for the Multimedia Conferencing traffic class can be calculated as follows:

$$\text{Multimedia\_Conferencing\_BWR} = (10\% / (100\% - 33\%)) * 100 = 15\% \text{ when rounded}$$

Finally, determining the bandwidth ratio allocated to each of the non-priority queues within the 1P3Q3T egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above.

### EtherChannel Configuration

When implementing an EtherChannel configuration on Catalyst 2K and 3K Series switches, queuing policies are applied to the physical interfaces. However, classification & marking policies are applied to the logical port-channel associated with the physical interfaces that make up the EtherChannel group. Because these switches are only supported in the role of an access-layer switch for the EasyQoS solution, no distribution-layer ingress classification & marking policies are ever applied to the logical port-channel associated with the physical interfaces that make up the EtherChannel group.

An example of the configuration pushed by EasyQoS to a Catalyst 2K and 3K Series switch when operating as an access-layer switch with EtherChannel connectivity to the distribution-layer switch is shown below.

```
!
interface Port-channelx
!
interface TenGigabitEthernety/y
srr-queue bandwidth share 1 55 37 7
priority-queue out
mls qos trust DSCP
channel-group x mode auto
!
```

Note that this configuration is no different than the configuration shown earlier, when EtherChannel is not implemented. EtherChannel interfaces could be GigabitEthernet interfaces or FastEthernet interfaces as well, depending upon the type of interface supported by the switch platform. A TenGigabitEthernet interface was shown only as an example in the configuration above.

### Custom Queuing Profiles with 1P3Q3T Egress Queuing

DSCP markings within custom Queuing Profiles are ignored for Catalyst 2K and 3K series switches, as well as the SM-ES2 Series EtherSwitch module. Instead, the DSCP markings per traffic-class from the default CVD\_Queueing\_Profile are always used. The EasyQoS web-based GUI provides a warning indicator of this to the network operator when changing DSCP markings of traffic-classes within a custom Queuing Profile.

Bandwidth allocations within custom Queuing Profiles do modify the amount bandwidth allocated through the “srr-queue bandwidth share” command applied to the physical interface of Catalyst 2K and 3K Series switches, as well as the SM-ES2 Series EtherSwitch module.

Figure 37 in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter showed an example custom Queuing Profile named EasyQoS\_Lab\_Queueing\_Profile. The bandwidth allocations for the 12 traffic-classes within the EasyQoS GUI for this Queuing Profile (for 1 Gbps interfaces) are shown in column 3 of the following table.

1. Example Custom Queuing Profile Mapping to 1P3Q3T Egress Queuing Policy

Traffic Class	DSCP Mark-ing	PBW % in the example EasyQoS Lab Queuing Profile	BWR % Calculated from the EasyQoS Lab Queuing Profile	1P3Q3T Egress Queue Map-ping	BWR Allocation in 1P3Q3T Egress Queue
Voice	EF	5%	N/A	Q1 (PQ)	PQ bandwidth is unconstrained and consists of traffic from the Voice, Broadcast Video, and Real-Time Interactive traffic-classes
Broad-cast Video	CS5	5%	N/A	Q1 (PQ)	
Real-Time In-ter-ac-tive	CS4	5%	N/A	Q1 (PQ)	
Mul-ti-me-dia Con-fer-enc-ing	AF41	10%	12%	Q2	Sum of BWR for traffic-classes mapped to Q2 = 12% (Multimedia Conferencing) + 12% (Multimedia Streaming) + 4% (Network Control) + 4% (Signaling) + 9% (OAM) + 12% (Transactional Data) = 53% (Actual value configured within switch platforms is rounded down to 52% to reach 100% BWR.)
Mul-ti-me-dia Stream-ing	AF31	10%	12%	Q2	
Net-work Con-trol	CS6	3%	4%	Q2	
Sig-nal-ing	CS3	3%	4%	Q2	
OAM	CS2	8%	9%	Q2	
Trans-ac-tional Data	AF21	10%	12%	Q2	
Bulk Data	AF11	10%	12%	Q4	Sum of BWR for traffic-classes mapped to Q4 = 12% (Bulk Data) + 1% (Scavenger) = 13%
Scav-enger	CS1	1%	1%	Q4	
Best Ef-fort	De-fault	30%	35%	Q3	BWR for Best Effort traffic-class mapped to Q3 = 35%

The table above shows how changing the amount of bandwidth allocated to each traffic class modifies the bandwidth ratios for the three non-priority queues within the 1P3Q3T egress queuing model.

Based on the formula discussed previously, the new total priority queue bandwidth (Total\_PQ\_BW) is calculated as follows:

$$\text{Total\_PQ\_BW} = 5\% (\text{Voice BW}) + 5\% (\text{Broadcast Video BW}) + 5\% (\text{Real-Time Interactive BW}) = 15\%$$

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI, and the amount of Total\_PQ\_BW, through the following formula.

$$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$$

For example, the new BWR percentage for the Multimedia Conferencing traffic class can be calculated as follows:

$$\text{Multimedia\_Conferencing\_BWR} = (10\% / (100\% - 15\%)) * 100 = 12\% \text{ when rounded}$$

Finally, determining the new bandwidth ratio allocated to each of the non-priority queues within the 1P3Q3T egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above.

- Note: Some rounding may occur in calculating the bandwidth remaining ratios for the non-priority queues in the egress policies, based on the mapping of the bandwidth allocated to each traffic-class via the EasyQoS GUI within a custom Queuing Profile, and in achieving 100% BWR. These rounding discrepancies may result in the actual ratio configured within the switch being higher or lower by a percent or so from the output from the formulas presented in this section.

This results in the following bandwidth allocation ratio configured on GigabitEthernet switch ports.

srr-queue bandwidth share 1 52 35 13

In the configuration example above, the bandwidth allocations have been modified from the CVD\_Queueing\_Profile for 1 Gbps interface speeds. When different bandwidth allocations are assigned to each of the interface speeds within the EasyQoS GUI for custom Queuing Profiles, EasyQoS will automatically calculate the appropriate bandwidth ratios for the non-priority egress queues and apply them to the interface via an “srr-queue bandwidth share” command, based on the interface speed. In this manner, different bandwidth allocations for the traffic-classes can be generated by EasyQoS for the various interface speeds supported by the platform—all within a single custom Queuing Profile. The network operator can use this flexibility in order to assign different bandwidth allocations for uplink ports vs. access-edge ports within a single custom Queuing Profile, if desired.

EasyQoS determines the interface speed based on the ifSpeed Object Identifier (OID) within the SNMP Interfaces MIB (IF-MIB). This value can also be displayed via a “show interface” exec-level command on the Catalyst switch. An example is shown below.

```
AD1-2960-1#show int gig 2/0/1
```

```
GigabitEthernet2/0/1 is up, line protocol is up (connected)
```

```
Hardware is Gigabit Ethernet, address is f84f.57ee.9d01 (bia f84f.57ee.9d01)
```

```
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
```

```
Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX
```

```
input flow-control is off, output flow-control is unsupported
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

Last input 00:00:05, output 00:00:01, output hang never  
Last clearing of "show interface" counters never  
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0  
Queueing strategy: fifo  
Output queue: 0/40 (size/max)  
30 second input rate 6000 bits/sec, 6 packets/sec  
30 second output rate 17000 bits/sec, 4 packets/sec  
29098826 packets input, 2364414813 bytes, 0 no buffer  
Received 12316466 broadcasts (12316463 multicasts)  
0 runs, 0 giants, 0 throttles  
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored  
0 watchdog, 12316463 multicast, 0 pause input  
0 input packets with dribble condition detected  
52964503 packets output, 20038284115 bytes, 0 underruns  
0 output errors, 0 collisions, 2 interface resets  
0 unknown protocol drops  
0 babbles, 0 late collision, 0 deferred  
0 lost carrier, 0 no carrier, 0 pause output  
0 output buffer failures, 0 output buffers swapped out

For Catalyst 2K and 3K Series platforms and the SM-ES2 Series EtherSwitch module, when a GigabitEthernet or FastEthernet interface is administratively down or in a line-protocol down state, the default bandwidth of the interface (interface speed) is 10 Mbps. This is highlighted in the example output below.

AD1-2960-1#show int gig1/0/1

**GigabitEthernet1/0/1 is down, line protocol is down (notconnect)**

Hardware is Gigabit Ethernet, address is f84f.57ee.ab81 (bia f84f.57ee.ab81)

Description: EtherChannel link to AD1-2960-1

MTU 1500 bytes, **BW 10000 Kbit/sec**, DLY 1000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX

input flow-control is off, output flow-control is unsupported

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:16:24, output 00:17:12, output hang never

Last clearing of "show interface" counters never

Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/40 (size/max)

30 second input rate 0 bits/sec, 0 packets/sec

30 second output rate 0 bits/sec, 0 packets/sec

28129991 packets input, 5130118196 bytes, 0 no buffer

Received 669103 broadcasts (669099 multicasts)

0 runs, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 669099 multicast, 0 pause input

0 input packets with dribble condition detected

If an EasyQoS policy is provisioned to a Catalyst 2K or 3K or SM-ES2 EtherSwitch Module that has FastEthernet or GigabitEthernet interfaces in an administratively down or line-protocol down state, these interfaces will receive the bandwidth allocations for the 10 Mbps interface speed within the custom Queuing Profile.

Because changes to the network are often performed after hours in specified “change windows,” and end-users often power down laptop and/or desktop computers after hours, this could result in some access-edge ports receiving the incorrect bandwidth allocations. A workaround for this is to ensure that the bandwidth allocations for the 10 Mbps speed within the custom Queuing Profile are the same as the 1 Gbps (GigabitEthernet) and/or 100 Mbps (FastEthernet) speed within the custom Queuing Profile. This will ensure that the access-edge switch ports receive the same bandwidth allocations regardless of whether they are up or down.

On some platforms, such as the Catalyst 3560-X Series, TenGigabitEthernet interfaces may show an interface speed of 10 Mbps when in an administratively down or line protocol down state as well. Other platforms, such as the Catalyst 3750-X and 2960-XR, TenGigabitEthernet interfaces may show an interface speed of 10 Gbps when in an administratively down or line protocol down state. Because TenGigabitEthernet ports are typically used for uplink ports, and such ports are always enabled, EasyQoS should provision the correct bandwidth allocations based on the 10 Gbps speed within the custom Queuing Profile for active uplink ports. If a new TenGigabitEthernet uplink port is being provisioned on one of these platforms, perhaps as part of an EtherChannel group, the EasyQoS policy may need to be re-applied after bringing the new uplink port—in order to ensure the correct bandwidth allocations are applied based on the interface speed and the custom Queuing Profile.

If the bandwidth allocations for each of the traffic-classes within a custom Queuing Profile is the same across all interface speeds (referred to as All References within the EasyQoS GUI), EasyQoS will apply the same bandwidth ratios for the non-priority egress queues to all of the interfaces, regardless of whether they are up or down.

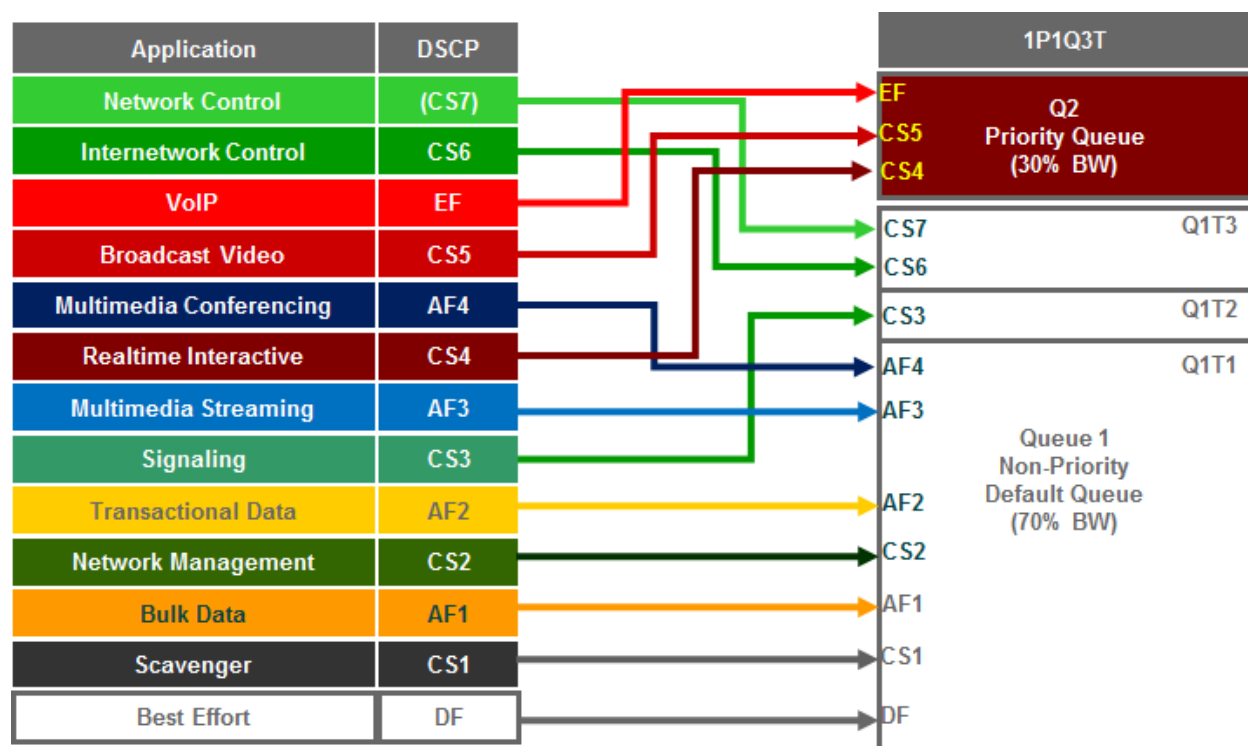
### Ingress Queuing Design

Catalyst 3750-X, 3560-X, and Catalyst 2960-C Series switches also support ingress queuing. Ingress queuing is a 1P1Q3T queuing structure. The ingress queuing structure implements DSCP-to-queue mapping and WTD for congestion avoidance. Although there are three WTD thresholds, only two are configurable. The third threshold is by default set to the depth of the queue (that is, 100% queue depth).

- Note: Ingress queuing was not implemented by EasyQoS for the Catalyst 3560-X Series platform in APIC-EM versions 1.3 and 1.4. However, Ingress queuing is implemented by EasyQoS for the Catalyst 3560-X series platform in APIC-EM version 1.5 and higher.

The following figure shows the 1P1Q3T ingress queuing model deployed by EasyQoS.

1. 1P1Q3T Ingress Queuing for the Catalyst 3K / 2K Series Platforms



The following configuration implements the 1P1Q3T ingress queuing structure deployed by EasyQoS.

!

! This section configures the ingress queues and thresholds

```
mls qos srr-queue input priority-queue 2 bandwidth 30
```

! Q2 is enabled as a strict-priority ingress queue with 30% BW

```
mls qos srr-queue input bandwidth 70 30
```

! Q1 is assigned 70% BW via SRR shared weights—Q2 SRR shared weight

! is ignored (as it has been configured as a PQ)

```
mls qos srr-queue input buffers 90 10
```

! Q1 is assigned 90% of queuing buffers and Q2 (PQ) is assigned 10%

```
mls qos srr-queue input threshold 1 80 90
```

! Q1 thresholds are configured at 80% (Q1T1) and 90% (Q1T2)

! This section configures the ingress CoS-to-Queue mappings

```
mls qos srr-queue input cos-map queue 1 threshold 1 0 1 2
```

! CoS values 0, 1 and 2 are mapped to Q1T1

```
mls qos srr-queue input cos-map queue 1 threshold 2 3
```

! CoS value 3 is mapped to ingress Q1T2

```
mls qos srr-queue input cos-map queue 1 threshold 3 6 7
```

! CoS values 6 and 7 are mapped to ingress Q1T3

```
mls qos srr-queue input cos-map queue 2 threshold 1 4 5
```



```

! CoS values 4 and 5 are mapped to ingress Q2 (the PQ)
! This section configures ingress DSCP-to-Queue Mappings
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
! DSCP CS2 and AF2 are mapped to ingress Q1T1
mls qos srr-queue input DSCP-map queue 1 threshold 2 24
! DSCP CS3 is mapped to ingress Q1T2
mls qos srr-queue input DSCP-map queue 1 threshold 3 48 56
! DSCP CS6 and CS7 are mapped to ingress Q1T3 (the tail of Q1)
mls qos srr-queue input DSCP-map queue 2 threshold 3 32 40 46
! DSCP CS4, CS5 and EF are mapped to ingress Q2T3 (the tail of the PQ)
!

```

Custom Queuing Profiles do not apply to ingress queuing on the Catalyst 2K and 3K Series platforms. Bandwidth allocation for the ingress queues is fixed.

The above configuration maps CoS 4 and 5, as well as DSCP values 46 (EF), 40 (CS5), and 32 (CS4) to queue 2, threshold 3 (Q2T3). By default, drop threshold 3 is set for 100% of the queue depth. Queue 2 is configured as a strict priority queue but is limited to 30% of the bandwidth and 10% of the buffers.

CoS 7 and 6, as well as DSCP values 48 (CS6) and 56 (CS7) are mapped to queue 1, threshold 3 (Q1T3), because these are considered to be control traffic. Again, by default, drop threshold 3 is set for 100% of the queue depth. CoS 3, as well as DSCP value 24 (CS3) is mapped to queue 1, threshold 2 (Q1T2) with a drop threshold of 90% of the queue depth. Finally, all other CoS and DSCP values are mapped to queue 1, threshold 1 (Q1T1) with a drop threshold of 80% of the queue depth. Queue 1 is configured for approximately 70% of the bandwidth (because queue 2 is limited to 30% of the bandwidth) and 90% of the buffers, because Q2 is a strict priority queue and will be serviced first.

### Catalyst 3650/3850 Queuing Design

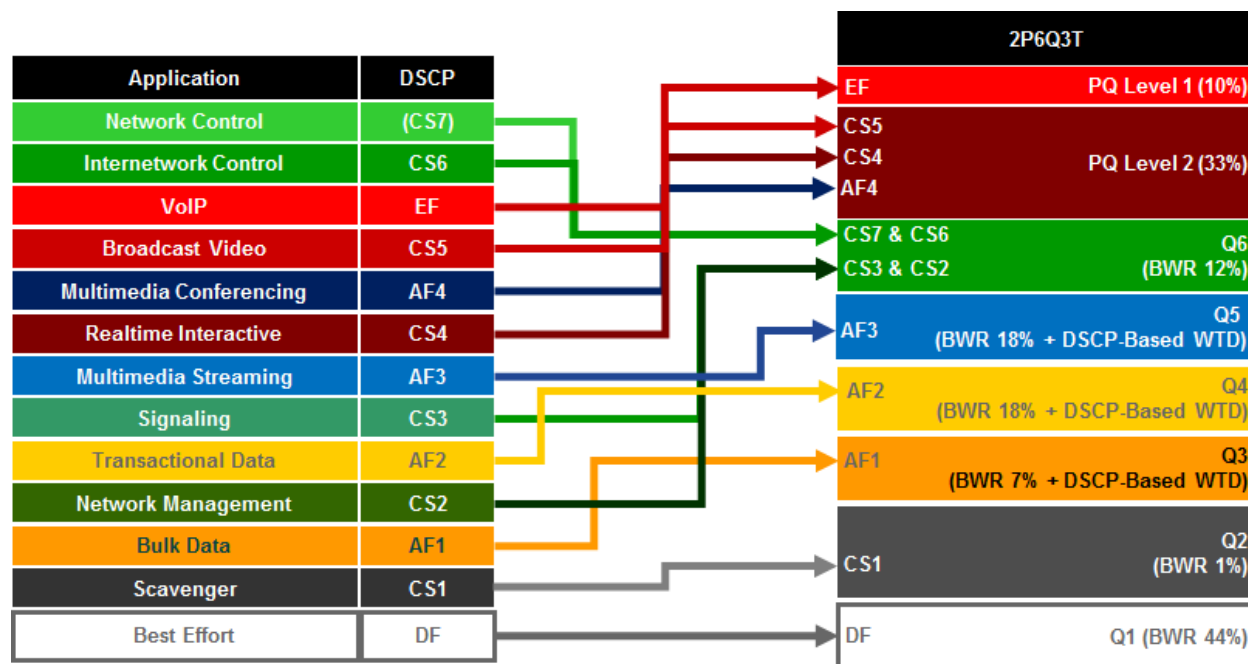
This section discusses the egress queuing structure provisioned by EasyQoS to the switch ports of Catalyst 3850 and 3650 Series switches.

#### Default 2P6Q3T Egress Queuing

Catalyst 3850 and 3650 Series switches support only egress queuing. Within EasyQoS policies, a 2P6Q3T egress queuing structure is implemented, with DSCP-to-queue mapping and WTD for congestion avoidance. APIC-EM release 1.4 changed the default bandwidth allocations for the 2P6Q3T egress queuing design. With APIC-EM release 1.5 and higher, the bandwidth allocations are part of the CVD\_Queueing\_Profile that is applied by default, unless the network operator applies a custom Queueing Profile to the policy scope containing these switches.

The following figure shows the 2P6Q3T egress queuing model.

1. Default 2P6Q3T Egress Queuing for the Catalyst 3650 and 3850 Series Switches



The following configuration, provisioned by EasyQoS, implements the class-maps for the 2P6Q3T egress queuing structure.

!

```

class-map match-any prm-EZQOS_2P6Q3T#VOICE-PQ1
match dscp ef
class-map match-any prm-EZQOS_2P6Q3T#VIDEO-PQ2
match dscp cs4
match dscp af41
match dscp af42
match dscp af43
match dscp cs5
class-map match-any prm-EZQOS_2P6Q3T#CONTROL-PLANE
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
class-map match-any prm-EZQOS_2P6Q3T#MULTIMEDIA-STREAMING
match dscp af31
match dscp af32
match dscp af33
class-map match-any prm-EZQOS_2P6Q3T#TRANSACTIONAL-DATA
match dscp af21

```

```
match dscp af22
match dscp af23
class-map match-any prm-EZQOS_2P6Q3T#BULK-DATA
match dscp af11
match dscp af12
match dscp af13
class-map match-any prm-EZQOS_2P6Q3T#SCAVENGER
match dscp cs1
!
```

The following configuration, provisioned by EasyQoS, implements the default policy-map for the 2P6Q3T egress queuing structure.

```
!
policy-map prm-dscp#APIC_QOS_Q_OUT
class prm-EZQOS_2P6Q3T#VOICE-PQ1
priority level 1 percent 10
queue-buffers ratio 5
class prm-EZQOS_2P6Q3T#VIDEO-PQ2
priority level 2 percent 33
queue-buffers ratio 5
class prm-EZQOS_2P6Q3T#CONTROL-PLANE
bandwidth remaining percent 12
queue-buffers ratio 5
class prm-EZQOS_2P6Q3T#MULTIMEDIA-STREAMING
bandwidth remaining percent 18
queue-buffers ratio 10
queue-limit dscp af31 percent 100
queue-limit dscp af32 percent 90
queue-limit dscp af33 percent 80
class prm-EZQOS_2P6Q3T#TRANSACTIONAL-DATA
bandwidth remaining percent 18
queue-buffers ratio 10
queue-limit dscp af21 percent 100
queue-limit dscp af22 percent 90
queue-limit dscp af23 percent 80
class prm-EZQOS_2P6Q3T#BULK-DATA
bandwidth remaining percent 7
```

```
queue-buffers ratio 20
queue-limit dscp af11 percent 100
queue-limit dscp af12 percent 90
queue-limit dscp af13 percent 80
class prm-EZQOS_2P6Q3T#SCAVENGER
bandwidth remaining percent 1
queue-buffers ratio 5
class class-default
bandwidth remaining percent 44
queue-buffers ratio 40
!
```

APIC-EM release 1.6 makes a change to the buffer allocation for the egress queuing policy. The following global configuration command is also provisioned by EasyQoS as part of the QoS policy on Catalyst 3850 and 3650 Series switches.

```
qos queue-softmax-multiplier 1200
```

The “*qos queue-softmax-multiplier*” command has a range from 100 to 1200, with the default setting being 100.

Catalyst 3850 and 3650 Series switches have a flexible, automatic buffer allocation scheme consisting of hard buffers and soft buffers, referred to as Dynamic Thresholding & Scaling (DTS). Hard buffers are dedicated to priority queues. Soft buffers are not dedicated. They are allocated as needed from a shared pool of buffers per ASIC across switch ports and queues – with a minimum (softmin) and a maximum (softmax) value per queue. With the default setting of the “*qos queue-softmax-multiplier*”, each queue can use up to 400% of the default allocated buffers from a shared common pool, if buffers are available. With the softmax-multiplier set for 1200, each queue (with the exception of the priority-level 1 queue) can use up to 400% x 1200% of the default allocated buffers from the shared common pool, if buffers are available. The overall effect of the change is to allow DTS to more efficiently control the allocation of buffer space on the Catalyst 3850 or 3650 Series switch, by allowing the queues to use more buffer space if needed and if the buffer space within the shared pool is available.

Note however that within APIC-EM release 1.6 the third drop-threshold for the multimedia-streaming, transactional-data, and bulk-data traffic-classes is specified at 100% of the queue-depth by the following command:

```
queue-limit dscp afx1 percent 100
```

where “x” refer-streaming traffic-class, “2” (af21) for the transactional-data traffic-class, or “1” (af11) for the bulk-data s to the values “3” (af31) for the multimedia traffic class.

When the third drop-threshold is not specified on Catalyst 3850 or 3650 series switches, it defaults to 400%. This value corresponds to the maximum soft queues (softmax) which can be allocated per queue. When the third drop-threshold is explicitly set for 100%, it limits the maximum amount of buffer space which DTS can allocate to the multimedia-streaming, transactional-data, and bulk-data queues to 100% x 1200% of the default allocated buffers from the shared common pool, if buffers are available. The softmax-multiplier command also does not apply to the priority-level 1 queue.

The 2P6Q3T egress queuing structure is applied by EasyQoS to all GigabitEthernet and TenGigabitEthernet interfaces, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.

- Note: Interfaces configured as StackWise Virtual links (SVL) or Dual-Active-Detection links on Catalyst 3850 or Catalyst 3650 Series platforms do not support QoS. As of APIC-EM release 1.6, the network operator must exclude these interfaces from EasyQoS policy in order to prevent EasyQoS from attempting to provision QoS policy to these interfaces.

An example of the provisioning to a single GigabitEthernet and single TenGigabitEthernet interface is shown below.

```
!
interface GigabitEthernetx/x/x
service-policy output prm-DSCP#APIC_QOS_Q_OUT
!
interface TenGigabitEthernetx/x/x
service-policy output prm-DSCP#APIC_QOS_Q_OUT
!
```

The Catalyst 3850 and 3650 Series platforms support two strict priority queues. DSCP value EF (voice traffic) is assigned to the first priority queue (prm-EZQOS\_2P6Q3T#VOICE-PQ1) which is allocated 10% of the bandwidth. DSCP values CS5, CS4, AF41, AF42, and AF43 (broadcast video, real-time interactive video, and multimedia conferencing traffic) are assigned to the second priority queue (prm-EZQOS\_2P6Q3T#VIDEO-PQ2), which is allocated 33% of the bandwidth. Both of these queues are allocated only approximately 5% of the buffers because they are priority queues. PQ1 is serviced first. If there are no packets in PQ1, then PQ2 is serviced. All other queues are serviced after the priority queues are serviced.

- Note: Due to Dynamic Thresholding & Scaling (DTS), buffer allocation is dynamic on the Catalyst 3850 / 3650 Series platforms – meaning that buffer allocation per queue can grow and shrink to meet demand, as long as the buffer space is available. Hence, buffer allocation more specifically sets the minimum soft (softmin) and hard (hardmin) buffers per queue.

DSCP values CS6, CS7, CS3, and CS2 are mapped to the prm-EZQOS\_2P6Q3T#CONTROL-PLANE queue, which is allocated 12% of the remaining bandwidth, after the priority queues are serviced. Because this queue holds control traffic (CS6 and CS7), signaling traffic (CS3), and OAM traffic (CS2), which is not expected to be a lot of traffic, approximately 5% of the buffers are allocated to the queue. WTD thresholds are not implemented for this queue because the objective is not to drop any of this traffic.

DSCP values AF31, AF32, and AF33 are mapped to the prm-EZQOS\_2P6Q3T#MULTIMEDIA-STREAMING queue, which is allocated approximately 18% of the remaining bandwidth, after the priority queues are serviced. Because AF classes are specifically intended for marking down traffic, WTD is implemented within this traffic class. AF33 traffic is set with a drop threshold of 80% of the buffer depth, AF32 traffic is set with a drop threshold of 90% of the buffer depth, and AF31 traffic implicitly has a drop threshold of 400% of the buffer depth. Approximately 10% of the buffers are allocated to the queue.

DSCP values AF21, AF22, and AF23 are mapped to the prm-EZQOS\_2P6Q3T#TRANSACTIONAL-DATA queue, which is allocated approximately 18% of the remaining bandwidth, after the priority queues are serviced. Because AF classes are specifically intended for marking down traffic, WTD is implemented within this traffic class. AF23 traffic is set with a drop threshold of 80% of the buffer depth, AF22 traffic is set with a drop threshold of 90% of the buffer depth, and AF21 traffic implicitly has a drop threshold of 400% of the buffer depth. Approximately 10% of the buffers are allocated to the queue.

DSCP values AF11, AF12, and AF13 are mapped to the prm-EZQOS\_2P6Q3T#BULK-DATA queue, which is allocated approximately 7% of the remaining bandwidth, after the priority queues are serviced. Because AF classes are specifically intended for marking down traffic, WTD is implemented within this traffic class. AF13 traffic is set with a drop threshold of 80% of the buffer depth, AF12 traffic is set with a drop threshold of 90% of the buffer depth, and AF11 traffic implicitly has a drop threshold of 400% of the buffer depth. Approximately 20% of the buffers are allocated to the queue.

DSCP value CS1 is mapped to the `prm-EZQOS_2P6Q3T#SCAVENGER` queue, which is allocated approximately 1% of the remaining bandwidth, after the priority queues are serviced. This is a scavenger class, specifically intended for traffic that has a business relevancy of business-irrelevant. WTD is not implemented within this traffic class and approximately 5% of the buffers are allocated to the queue.

All other DSCP values are by default mapped to the class-default queue, which is allocated approximately 44% of the remaining bandwidth, after the priority queues are serviced. The default class is specifically intended for traffic that has a business relevancy of default. WTD is not implemented within this traffic class, and approximately 40% of the buffers are allocated to the queue.

There are no mappings of CoS values to queues with the Catalyst 3850 and 3650 Series platforms. These platforms only fall back to the use of CoS values for non-IP packets.

The bandwidth allocations within the EasyQoS GUI for Queuing Profiles require the sum of the bandwidth percentages to total 100%. These bandwidth allocations are absolute bandwidth percentages. Because the 2P6Q3T egress queuing policy implements an eight queue model in hardware on these switch platforms, multiple traffic-classes may be mapped to a single queue.

The following table shows the mapping of the traffic-classes and bandwidth allocations from the default EasyQoS CVD\_Queueing\_Profile to the 2P6Q3T egress queuing structure.

1. Default Queuing Profile Mapping to 2P6Q3T Egress Queuing Policy

Traffic Class	DSCP Marking	BW % in the Default Queuing Profile	BWR % Calculated from the Default Queuing Profile	2P6Q3T Egress Queue Mapping	BWR % Allocation in 2P6Q3T Egress Queue
Voice	EF	10%	N/A	Voice-PQ1	Voice-PQ1 bandwidth is constrained to 10%, and consists of traffic from the Voice traffic-class.
Broadcast Video	CS5	10%	N/A	Video-PQ2	Video-PQ2 bandwidth is constrained to 33% and consists of traffic from the Broadcast Video, Real-Time Interactive, and Multimedia Conferencing traffic-classes.
Real-Time Interactive	CS4	13%	N/A	Video-PQ2	
Multimedia Conferencing	AF41	10%	N/A	Video-PQ2	
Multimedia Streaming	AF31	10%	18%	Multimedia-Streaming Queue	BWR for traffic-class mapped to Multimedia-Streaming Queue = 18%
Network Control	CS6	3%	5%	Control-Plane Queue	BWR for traffic-classes mapped to Control-Plane Queue = 5% (Network Control) + 4% (Signaling) + 4% (OAM) = 13%. (Actual value configured within switch platforms is rounded down to 12% to reach 100% BWR.)
Signaling	CS3	2%	4%	Control-Plane Queue	
OAM	CS2	2%	4%	Control-Plane Queue	
Transactional Data	AF21	10%	18%	Transactional-Data Queue	BWR for traffic-class mapped to Transactional-Data Queue = 18%
Bulk Data	AF11	4%	7%	Bulk-Data Queue	BWR for traffic-class mapped to Bulk-Data Queue = 7%
Scavenger	CS1	1%	2%	Scavenger Queue	BWR for traffic-class mapped to Scavenger Queue = 2% due to rounding to whole numbers in the formulas presented here. (Actual value configured within switch platforms is rounded down to 1% to reach 100% BWR.)
Best Effort	Default	25%	44%	Default Queue	BWR for Best Effort traffic-class mapped to Default Queue = 44%

Column 3 of the table above shows the percentage bandwidth allocation for each of the traffic-classes as it appears within the EasyQoS GUI for the default CVD\_Queueing\_Profile. In the 2P6Q3T egress queuing policy, the Voice traffic-class is mapped to PQ1-Voice, and the Broadcast Video, Real-Time Interactive, and Multimedia-Conferencing

traffic-classes are mapped to the PQ2-Video, as shown in column 5. The sum of the bandwidth allocated to these three traffic-classes can be considered as the total priority queue bandwidth (Total\_PQ\_BW), as shown in the following formula.

$$\text{Total\_PQ\_BW} = \text{Voice BW} + \text{Broadcast Video BW} + \text{Real-Time Interactive BW} + \text{Multimedia Conferencing BW}$$

Based on the bandwidth allocations in column 3 in the table above Total\_PQ\_BW can be calculated as follows:

$$\text{Total\_PQ\_BW} = 10\% (\text{Voice}) + 10\% (\text{Broadcast Video}) + 13\% (\text{Real-Time Interactive}) + 10\% (\text{Multimedia Conferencing}) = 43\%$$

For the remaining eight traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI and the amount of Total\_PQ\_BW calculated above. This can be done through the following formula.

$$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$$

For example, BWR percentage for the Multimedia Streaming traffic class can be calculated as follows:

$$\text{Multimedia\_Streaming\_BWR} = (10\% / (100\% - 43\%)) * 100 = 18\% \text{ when rounded}$$

Finally, determining the bandwidth ratio allocated to each of the non-priority queues within the 2P6Q3T egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above.

#### EtherChannel Configuration

When implementing an EtherChannel connection on Catalyst 3850 and 3650 Series platforms, both queuing policies and classification & marking policies are applied to the physical interfaces that make up the EtherChannel group. An example of the configuration pushed by EasyQoS to a Catalyst 3850 or 3650 Series switch when operating as a distribution-layer switch with EtherChannel connectivity to the access-layer switch is shown below.

```
!  
interface Port-channelx  
!  
interface TenGigabitEthernety/y/y  
channel-group x mode auto  
service-policy input APIC_EM-MARKING-DIST-IN  
service-policy output prm-DSCP#APIC_QOS_Q_OUT  
!
```

#### Custom Queuing Profiles

EasyQoS within APIC-EM release 1.5 and higher provides the network operator the ability to change the both the DSCP marking and the bandwidth allocation of traffic-classes through custom Queuing Profiles in the web-based GUI. This feature was discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Figures 36 and 37 showed an example custom Queuing Profile named EasyQoS\_Lab\_Queueing\_Profile. The bandwidth allocations for the 12 traffic-classes for this example Queuing Profile (for 1 Gbps interfaces) are shown in column 3 of the following table. Likewise, the DSCP markings for the 12 traffic-classes are shown in column 2.

##### 1. Example Custom Queuing Profile Mapping to 2P6Q3T Egress Queuing Policy



Traffic Class	DSCP Marking	BW % in the example EasyQoS Lab Queuing Profile	BWR % Calculated from the EasyQoS Lab Queuing Profile	2P6Q3T Egress Queue Mapping	BWR % Allocation in 2P6Q3T Egress Queue
Voice	EF	5%	N/A	Voice-PQ1	Voice-PQ1 bandwidth is constrained to 5% and consists of traffic from the Voice traffic-class.
Broadcast Video	CS3	5%	N/A	Video-PQ2	Video-PQ2 bandwidth is constrained to 20% and consists of traffic from the Broadcast Video, Real-Time Interactive, and Multimedia Conferencing traffic-classes.
Real-Time Interactive	CS4	5%	N/A	Video-PQ2	
Multimedia Conferencing	AF41	10%	N/A	Video-PQ2	
Multimedia Streaming	AF31	10%	13%	Multimedia-Streaming Queue	BWR for traffic-class mapped to Multimedia-Streaming Queue = 13%
Network Control	CS6	3%	4%	Control-Plane Queue	BWR for traffic-classes mapped to Control-Plane Queue = 4% (Network Control) + 4% (Signaling) + 11% (OAM) = 19%
Signaling	CS5	3%	4%	Control-Plane Queue	
OAM	CS2	8%	11%	Control-Plane Queue	
Transactional Data	AF21	10%	13%	Transactional-Data Queue	BWR for traffic-class mapped to Transactional-Data Queue = 13%
Bulk Data	AF11	10%	13%	Bulk-Data Queue	BWR for traffic-class mapped to Bulk-Data Queue = 13%
Scavenger	CS1	1%	1%	Scavenger Queue	BWR for traffic-class mapped to Scavenger Queue = 1%
Best Effort	Default	30%	40%	Default Queue	BWR for Best Effort traffic-class mapped to Default Queue = 40% (Actual value configured within switch platforms is rounded up to 41% to reach 100% BWR.)

Changing the DSCP markings of traffic-classes within the EasyQoS web-based GUI affects the “match dscp” statements of class-map definitions within the egress queuing policy of Catalyst 3850 and 3650 Series switches. The following output is an example of the modification of the class-map definitions provisioned by EasyQoS, based upon

the DSCP markings from the EasyQoS\_Lab\_Queueing Profile, shown in the table above. The affected class-map definitions are highlighted in bold.

!

```
class-map match-any prm-EZQOS_2P6Q3T#VOICE-PQ1
```

```
match dscp ef
```

```
class-map match-any prm-EZQOS_2P6Q3T#VIDEO-PQ2
```

```
match dscp cs4
```

```
match dscp af41
```

```
match dscp af42
```

```
match dscp af43
```

```
match dscp cs3
```

```
class-map match-any prm-EZQOS_2P6Q3T#CONTROL-PLANE
```

```
match dscp cs2
```

```
match dscp cs5
```

```
match dscp cs6
```

```
match dscp cs7
```

```
class-map match-any prm-EZQOS_2P6Q3T#MULTIMEDIA-STREAMING
```

```
match dscp af31
```

```
match dscp af32
```

```
match dscp af33
```

```
class-map match-any prm-EZQOS_2P6Q3T#TRANSACTIONAL-DATA
```

```
match dscp af21
```

```
match dscp af22
```

```
match dscp af23
```

```
class-map match-any prm-EZQOS_2P6Q3T#BULK-DATA
```

```
match dscp af11
```

```
match dscp af12
```

```
match dscp af13
```

```
class-map match-any prm-EZQOS_2P6Q3T#SCAVENGER
```

```
match dscp cs1
```

!

As can be seen by comparing the class-map definitions between the default Queueing Profile (CVD\_Queueing\_Profile) and the EasyQoS\_Lab\_Queueing Profile, the Video-PQ2 queue which services the Broadcast Video traffic-class matches on CS3 instead of CS5, and the Control-Plane queue which services the Signaling traffic-class matches on CS5 instead of CS3.

Bandwidth allocations within custom Queueing Profiles modify the amount bandwidth allocated through the “priority level x percent” or “bandwidth remaining percent” commands within the egress queueing policy-map applied to physical interfaces of Catalyst 3850 and 3650 Series switches.

The table above shows how changing the amount of bandwidth allocated to each traffic class modifies the bandwidth allocated to the two priority queues and six non-priority queues within the 2P6Q3T egress queuing model.

Based on the formula discussed previously, the new total priority queue bandwidth (Total\_PQ\_BW) is calculated as follows:

$\text{Total\_PQ\_BW} = 5\% \text{ (Voice BW)} + 5\% \text{ (Broadcast Video BW)} + 5\% \text{ (Real-Time Interactive BW)} + 10\% \text{ (Multimedia Conferencing BW)} = 25\%$

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI, and the amount of Total\_PQ\_BW, through the following formula.

$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$

For example, the new BWR percentage for the Multimedia Streaming traffic class can be calculated as follows:

$\text{Multimedia\_Streaming\_BWR} = (10\% / (100\% - 25\%)) * 100 = 13\%$  when rounded

Finally, determining the new bandwidth ratio allocated to each of the non-priority queues within the 2P6Q3T egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above.

This results in the following policy-map definition when deployed on a Catalyst 3850 or 3650 Series platform.

!

```
policy-map prm-dscp#APIC_QOS_Q_OUT#1G
class prm-EZQOS_2P6Q3T#VOICE-PQ1
priority level 1 percent 5
queue-buffers ratio 5
class prm-EZQOS_2P6Q3T#VIDEO-PQ2
priority level 2 percent 20
queue-buffers ratio 5
class prm-EZQOS_2P6Q3T#CONTROL-PLANE
bandwidth remaining percent 19
queue-buffers ratio 5
class prm-EZQOS_2P6Q3T#MULTIMEDIA-STREAMING
bandwidth remaining percent 13
queue-buffers ratio 10
queue-limit dscp af31 percent 100
queue-limit dscp af32 percent 90
queue-limit dscp af33 percent 80
class prm-EZQOS_2P6Q3T#TRANSACTIONAL-DATA
bandwidth remaining percent 13
queue-buffers ratio 10
queue-limit dscp af21 percent 100
queue-limit dscp af22 percent 90
```

```
queue-limit dscp af23 percent 80
class prm-EZQOS_2P6Q3T#BULK-DATA
bandwidth remaining percent 13
queue-buffers ratio 20
queue-limit dscp af11 percent 100
queue-limit dscp af12 percent 90
queue-limit dscp af13 percent 80
class prm-EZQOS_2P6Q3T#SCAVENGER
bandwidth remaining percent 1
queue-buffers ratio 5
class class-default
bandwidth remaining percent 41
queue-buffers ratio 40
!
```

In the configuration example above, the bandwidth allocations have been modified from the CVD\_Queueing\_Profile for 1 Gbps interface speeds. When different bandwidth allocations are assigned to each of the interface speeds within the EasyQoS GUI for custom Queueing Profiles, EasyQoS will append the interface speed to the name of the policy-map generated. This differentiates the policy-map for that particular interface speed. For example, the policy-map name in the configuration above has been changed from “policy-map prm-DSCP#APIC\_QOS\_Q\_OUT” to “policy-map prm-dscp#APIC\_QOS\_Q\_OUT#1G” indicating this policy-map is to be applied to 1 Gbps interfaces. In this manner, different policy-maps with different bandwidth allocations for the traffic-classes can be generated by EasyQoS for the various interface speeds supported by the platform—all within a single custom Queueing Profile. The network operator can use this flexibility in order to assign different bandwidth allocations for uplink ports vs. access-edge ports within a single custom Queueing Profile, if desired.

If the bandwidth allocations for each of the traffic-classes within a custom Queueing Profile is the same across all interface speeds (referred to as All References within the EasyQoS GUI), EasyQoS will optimize the configuration, and create a single policy-map with the name “policy-map prm-DSCP#APIC\_QOS\_Q\_OUT” with the bandwidth allocations specified within the custom Queueing Profile.

EasyQoS determines the interface speed based on the OID within the SNMP IF-MIB. This value can also be displayed via a “show interface” exec-level command on the Catalyst switch. An example is shown below.

```
AD1-3850-1#show interfaces GigabitEthernet 1/0/10
GigabitEthernet1/0/10 is down, line protocol is down (notconnect)
Hardware is Gigabit Ethernet, address is 1ce8.5d17.e78a (bia 1ce8.5d17.e78a)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed, media type is 10/100/1000BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
```

Last input never, output never, output hang never

Last clearing of “show interface” counters never

Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: Class-based queueing

Output queue: 0/40 (size/max)

30 second input rate 0 bits/sec, 0 packets/sec

30 second output rate 0 bits/sec, 0 packets/sec

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts (0 multicasts)

0 runs, 0 giants, 0 throttles

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

0 watchdog, 0 multicast, 0 pause input

0 input packets with dribble condition detected

0 packets output, 0 bytes, 0 underruns

0 output errors, 0 collisions, 1 interface resets

0 unknown protocol drops

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier, 0 pause output

0 output buffer failures, 0 output buffers swapped out

For Catalyst 3850 and 3650 Series platforms when a GigabitEthernet interface is administratively down or in a line-protocol down state, the default bandwidth of the interface (interface speed) is 1 Gbps. Likewise, when a TenGigabitEthernet interface is administratively down or in a line-down protocol state, the default bandwidth of the interface (interface speed) is 10 Gbps. Therefore, if an EasyQoS policy is provisioned to a Catalyst 3850 or 3650 Series switch which has GigabitEthernet or TenGigabitEthernet interfaces in an administratively down or line-protocol down state, all interfaces should still receive the bandwidth allocations for their respective speeds within the custom Queuing Profile, regardless of whether they are up or down.

### Catalyst 4500 Queuing Design

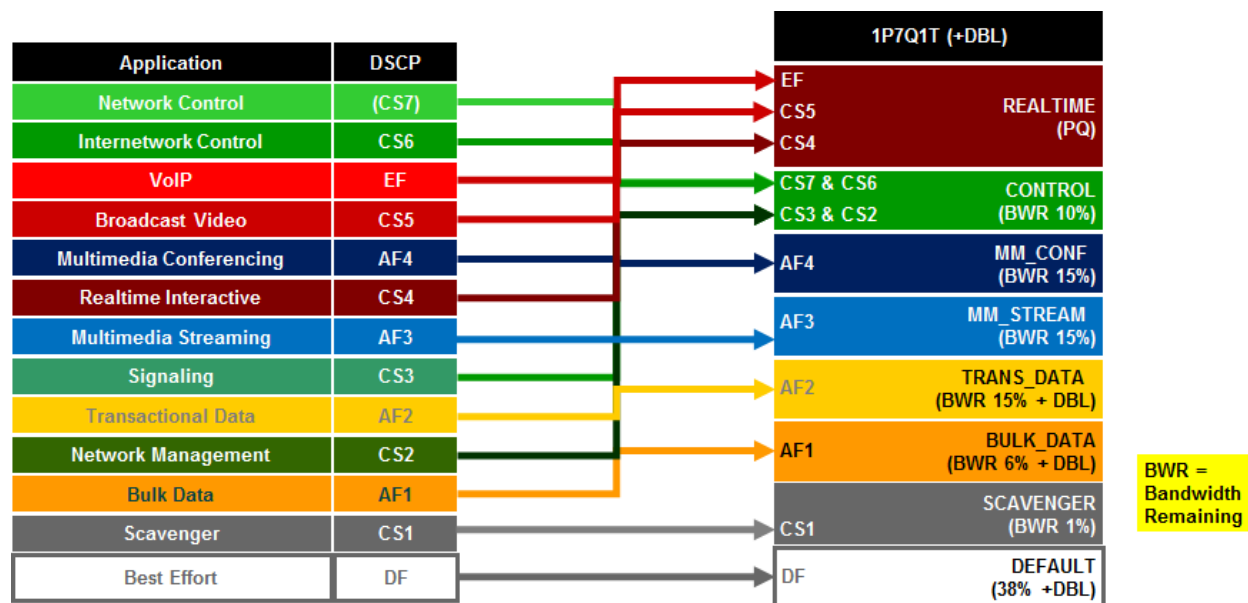
This section discusses the egress queuing structure provisioned by APIC-EM to the ports of each of the line cards and supervisors supported by EasyQoS for the Catalyst 4500-E Series and Catalyst 4500-X Series switches.

#### Default 1P7Q1T Egress Queuing

Catalyst 4500-E Series switches with Supervisor 7-E, 7-LE, 8-E, and 8-LE; and Catalyst 4500-X Series switches support only egress queuing. The 1P7Q1T egress queuing structure for the Catalyst 4500-E and Catalyst 4500-X Series implements DSCP-to-queue mapping and Dynamic Buffer Limiting (DBL) for congestion avoidance instead of DSCP-based WRED or WTD. APIC-EM release 1.4 changed the default bandwidth allocations for the 1P7Q1T egress queuing design. With APIC-EM release 1.5 and higher, the default bandwidth allocations are part of the CVD\_QUEUEING\_PROFILE that is applied by default, unless the network operator applies a custom Queuing Profile to the policy scope containing these switches.

The following figure shows the default 1P7Q1T egress queueing model.

1. Default 1P7Q1T+DBL Egress Queuing for the Catalyst 4500 Series



The following configuration, provisioned by EasyQoS, implements the default class-maps for the 1P7Q1T egress queuing structure.

!

```
class-map match-any prm-EZQOS_1P7Q1T#REALTIME
match dscp cs4
match dscp cs5
match dscp ef
class-map match-any prm-EZQOS_1P7Q1T#CONTROL
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
class-map match-any prm-EZQOS_1P7Q1T#MM_CONF
match dscp af41
match dscp af42
match dscp af43
class-map match-any prm-EZQOS_1P7Q1T#MM_STREAM
match dscp af31
match dscp af32
match dscp af33
class-map match-any prm-EZQOS_1P7Q1T#TRANS_DATA
match dscp af21
match dscp af22
```

```

match dscp af23
class-map match-any prm-EZQOS_1P7Q1T#BULK_DATA
match dscp af11
match dscp af12
match dscp af13
class-map match-any prm-EZQOS_1P7Q1T#SCAVENGER
match dscp cs1
!
```

The following configuration, provisioned by EasyQoS, implements the default policy-map for the 1P7Q1T egress queuing structure.

```

!
policy-map prm-DSCP#APIC_QOS_Q_OUT
class prm-EZQOS_1P7Q1T#REALTIME
priority
class prm-EZQOS_1P7Q1T#CONTROL
bandwidth remaining percent 10
class prm-EZQOS_1P7Q1T#MM_CONF
bandwidth remaining percent 15
class prm-EZQOS_1P7Q1T#MM_STREAM
bandwidth remaining percent 15
class prm-EZQOS_1P7Q1T#TRANS_DATA
bandwidth remaining percent 15
dbl
class prm-EZQOS_1P7Q1T#BULK_DATA
bandwidth remaining percent 6
dbl
class prm-EZQOS_1P7Q1T#SCAVENGER
bandwidth remaining percent 1
class class-default
bandwidth remaining percent 38
dbl
!
```

The 1P7Q1T egress queuing structure is applied by EasyQoS to all GigabitEthernet and TenGigabitEthernet interfaces, with the following exception:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.

An example of the provisioning to a single GigabitEthernet and single TenGigabitEthernet interface is shown below.

!

```
interface GigabitEthernetx/x/x
```

```
service-policy output prm-DSCP#APIC_QOS_Q_OUT
```

!

```
interface TenGigabitEthernetx/x/x
```

```
service-policy output prm-DSCP#APIC_QOS_Q_OUT
```

!

In the configuration above, DBL is only applied to the transactional data, bulk data, and default queues. DBL has a congestion-avoidance function, similar to WRED in that it can help prevent synchronization of TCP flows that result in under-utilization of the available bandwidth. DBL is not recommended to be deployed on real-time multimedia and control queues. DBL is not deployed on the scavenger queue, simply because the traffic is already considered to be scavenger traffic using whatever bandwidth is available.

The bandwidth allocations within the EasyQoS GUI for Queuing Profiles require the sum of the bandwidth percentages to total 100%. These bandwidth allocations are absolute bandwidth percentages. The EasyQoS egress queuing policy on the Catalyst 4500 Series platforms implements a single priority queue. The priority queue is unconstrained in terms of the amount of bandwidth it can consume. Because the 1P7Q1T egress queuing policy implements an eight-queue model in hardware on these switch platforms, multiple traffic-classes may be mapped to a single queue.

The following table shows the mapping of the traffic-classes and bandwidth allocations from the default EasyQoS CVD\_Queueing\_Profile to the 1P7Q1T egress queuing structure.

1. Default Queuing Profile Mapping to 1P7Q1T Egress Queuing Policy



Traffic Class	DSCP Marking	BW in the Default Queuing Profile	BWR % Calculated from the Default Queuing Profile	1P7Q1T Egress Queue Mapping	BWR % Allocation in 1P7Q1T Egress Queue
Voice	EF	10%	N/A	REAL-TIME	REALTIME priority queue bandwidth is unconstrained and consists of traffic from the Voice, Broadcast Video, and Real-Time Interactive traffic-classes.
Broadcast Video	CS5	10%	N/A	REAL-TIME	
Real-Time Interactive	CS4	13%	N/A	REAL-TIME	
Multimedia Conferencing	AF41	10%	15%	MM_CONF	BWR for traffic-class mapped to Multimedia-Conferencing Queue = 15%
Multimedia Streaming	AF31	10%	15%	MM_STREAM	BWR for traffic-class mapped to Multimedia-Streaming Queue = 15%
Network Control	CS6	3%	4%	CONTROL	BWR for traffic-classes mapped to Control-Plane Queue = 4% (Network Control) + 3% (Signaling) + 3% (OAM) = 10%.
Signaling	CS3	2%	3%	CONTROL	
OAM	CS2	2%	3%	CONTROL	
Transactional Data	AF21	10%	15%	TRANS_DATA	BWR for traffic-class mapped to Transactional-Data Queue = 15%
Bulk Data	AF11	4%	6%	BULK_DATA	BWR for traffic-class mapped to Bulk-Data Queue = 6%.
Scavenger	CS1	1%	1%	SCAV-ENGINEER	BWR for traffic-class mapped to Scavenger Queue = 1%
Best Effort	Default	25%	37%	Default Queue	BWR for Best Effort traffic-class mapped to Default Queue = 37%. (Actual value configured within switch platforms is rounded up to 38% to reach 100% BWR.)

Column 3 of the table above shows the percentage bandwidth allocation for each of the traffic-classes as it appears within the EasyQoS GUI for the default CVD\_Queueing\_Profile. In the 1P7Q1T egress queuing policy, the Voice, Broadcast Video, and Real-Time Interactive traffic-classes are mapped to the single REALTIME priority queue, as shown in column 5. The sum of the bandwidth allocated to these three traffic-classes can be considered as the total priority queue bandwidth (Total\_PQ\_BW), as shown in the following formula.

$\text{Total\_PQ\_BW} = \text{Voice BW} + \text{Broadcast Video BW} + \text{Real-Time Interactive BW}$

Based on the bandwidth allocations in column 3 in the table above Total\_PQ\_BW can be calculated as follows:

Total\_PQ\_BW = 10% (Voice) + 10% (Broadcast Video) + 13% (Real-Time Interactive) = 33%

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI and the amount of Total\_PQ\_BW calculated above. This can be done through the following formula.

Traffic\_Class\_BWR = (Traffic\_Class\_BW / (100% – Total\_PQ\_BW)) \* 100

For example, BWR percentage for the Multimedia Streaming traffic class can be calculated as follows:

Multimedia\_Conferencing\_BWR = (10% / (100% – 33%)) \* 100 = 15% when rounded

Finally, determining the bandwidth ratio allocated to each of the non-priority queues within the 1P7Q1T egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above.

### EtherChannel Configuration

When implementing an EtherChannel connection on Catalyst 4500-E and Catalyst 4500-X Series platforms, queuing policies are applied to the physical interfaces. However, classification & marking policies are applied to the logical port-channel associated with the physical interfaces that make up the EtherChannel group. An example of the configuration pushed by EasyQoS to a Catalyst 4500-E or Catalyst 4500-X series switch when operating as a distribution-layer switch with EtherChannel connectivity to the access-layer switch is shown below.

```
!  
interface Port-channelx  
service-policy input prm-APIC_QOS_IN  
!  
interface range TenGigabitEthernetx/x/x—xx  
channel-group x mode auto  
service-policy output prm-DSCP#APIC_QOS_Q_OUT  
!
```

### Custom Queuing Profiles

EasyQoS within APIC-EM release 1.5 and higher provides the network operator the ability to change the both the DSCP marking and the bandwidth allocation of traffic-classes through custom Queuing Profiles in the web-based GUI. This feature was discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Figures 36 and 37 showed an example custom Queuing Profile named EasyQoS\_Lab\_Queueing\_Profile. The bandwidth allocations for the 12 traffic-classes for this example Queuing Profile (for 1 Gbps interfaces) are shown in column 3 of the following table. Likewise, the DSCP markings for the 12 traffic-classes are shown in column 2.

#### 1. Example Custom Queuing Profile Mapping to 1P7Q1T Egress Queuing Policy

Traffic Class	DSCP Marking	BW % in the example EasyQoS Lab Queuing Profile	BWR % Calculated from the EasyQoS Lab Queuing Profile	1P7Q1T Egress Queue Mapping	BWR % Allocation in 1P7Q1T Egress Queue
Voice	EF	5%	N/A	REAL-TIME	REALTIME priority queue bandwidth is unconstrained and consists of traffic from the Voice, Broadcast Video, and Real-Time Interactive traffic-classes.
Broadcast Video	CS3	5%	N/A	REAL-TIME	
Real-Time Interactive	CS4	5%	N/A	REAL-TIME	
Multimedia Conferencing	AF41	10%	12%	MM_CONF	BWR for traffic-class mapped to Multimedia-Conferencing Queue = 12%
Multimedia Streaming	AF31	10%	12%	MM_STREAM	BWR for traffic-class mapped to Multimedia-Streaming Queue = 12%
Network Control	CS6	3%	4%	CONTROL	BWR for traffic-classes mapped to Control-Plane Queue = 4% (Network Control) + 4% (Signaling) + 9% (OAM) = 17% (Actual value configured within switch platforms is rounded down to 16% to reach 100% BWR.)
Signaling	CS5	3%	4%	CONTROL	
OAM	CS2	8%	9%	CONTROL	
Transactional Data	AF21	10%	12%	TRANS_DATA	BWR for traffic-class mapped to Transactional-Data Queue = 12%
Bulk Data	AF11	10%	12%	BULK_DATA	BWR for traffic-class mapped to Bulk-Data Queue = 12%
Scavenger	CS1	1%	1%	SCAV-ENGER	BWR for traffic-class mapped to Scavenger Queue = 1%
Best Effort	Default	30%	35%	Default Queue	BWR for Best Effort traffic-class mapped to Default Queue = 35%

Changing the DSCP markings of traffic-classes within the EasyQoS web-based GUI affects the “match dscp” statements of class-map definitions within the egress queuing policy of Catalyst 4500-E and Catalyst 4500-X Series platforms. The following output is an example of the modification of the class-map definitions provisioned by EasyQoS, based upon the DSCP markings from the EasyQoS\_Lab\_Queueing Profile, shown in the table above. The affected

class-map definitions are highlighted in bold.

!

**class-map match-any prm-EZQOS\_1P7Q1T#REALTIME**

match dscp cs4

**\*\*match dscp cs3 \*\***

match dscp ef

**class-map match-any prm-EZQOS\_1P7Q1T#CONTROL**

match dscp cs2

**\*\*match dscp cs5 \*\***

match dscp cs6

match dscp cs7

class-map match-any prm-EZQOS\_1P7Q1T#MM\_CONF

match dscp af41

match dscp af42

match dscp af43

class-map match-any prm-EZQOS\_1P7Q1T#MM\_STREAM

match dscp af31

match dscp af32

match dscp af33

class-map match-any prm-EZQOS\_1P7Q1T#TRANS\_DATA

match dscp af21

match dscp af22

match dscp af23

class-map match-any prm-EZQOS\_1P7Q1T#BULK\_DATA

match dscp af11

match dscp af12

match dscp af13

class-map match-any prm-EZQOS\_1P7Q1T#SCAVENGER

match dscp cs1

!

As can be seen by comparing the class-map definitions between the default Queuing Profile (CVD\_Queueing\_Profile) and the EasyQoS\_Lab\_Queueing Profile, the Realtime queue which services the Broadcast Video traffic-class matches on CS3 instead of CS5, and the Control queue which services the Signaling traffic-class matches on CS5 instead of CS3.

Custom Queuing Profiles modify the amount bandwidth allocated through the “bandwidth remaining percent” commands within the egress queuing policy-map applied to physical interfaces of Catalyst 4500-E and Catalyst 4500-X Series switches. The table above shows how changing the amount of bandwidth allocated to each traffic class modifies the bandwidth allocated to the seven non-priority queues within the 1P7Q1T egress queuing model.

Based on the formula discussed previously, the new total priority queue bandwidth (Total\_PQ\_BW) is calculated as follows:

$$\text{Total\_PQ\_BW} = 5\% \text{ (Voice BW)} + 5\% \text{ (Broadcast Video BW)} + 5\% \text{ (Real-Time Interactive BW)} = 15\%$$

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI, and the amount of Total\_PQ\_BW, through the following formula.

$$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$$

For example, the new BWR percentage for the Multimedia Conferencing traffic class can be calculated as follows:

$$\text{Multimedia\_Conferencing\_BWR} = (10\% / (100\% - 15\%)) * 100 = 12\% \text{ when rounded}$$

Finally, determining the new bandwidth ratio allocated to each of the non-priority queues within the 1P7Q1T egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above.

This results in the following policy-map definition when deployed on a Catalyst 4500-E and Catalyst 4500-X Series platform.

```
!
policy-map prm-dscp#APIC_QOS_Q_OUT#1G
class prm-EZQOS_1P7Q1T#REALTIME
priority
class prm-EZQOS_1P7Q1T#CONTROL
bandwidth remaining percent 16
class prm-EZQOS_1P7Q1T#MM_CONF
bandwidth remaining percent 12
class prm-EZQOS_1P7Q1T#MM_STREAM
bandwidth remaining percent 12
class prm-EZQOS_1P7Q1T#TRANS_DATA
bandwidth remaining percent 12
dbl
class prm-EZQOS_1P7Q1T#BULK_DATA
bandwidth remaining percent 12
dbl
class prm-EZQOS_1P7Q1T#SCAVENGER
bandwidth remaining percent 1
class class-default
bandwidth remaining percent 35
dbl
!
```

In the configuration example above, the bandwidth allocations have been modified from the CVD\_Queueing\_Profile for 1 Gbps interface speeds. When different bandwidth allocations are assigned to each of the interface speeds within

the EasyQoS GUI for custom Queuing Profiles, EasyQoS will append the interface speed to the name of the policy-map generated. This is in order to differentiate the policy-map for that particular interface speed. For example, the policy-map name in the configuration above has been changed from “policy-map prm-DSCP#APIC\_QOS\_Q\_OUT” to “policy-map prm-dscp#APIC\_QOS\_Q\_OUT#1G,” indicating this policy-map is to be applied to 1 Gbps interfaces. In this manner, different policy-maps with different bandwidth allocations for the traffic-classes can be generated by EasyQoS for the various interface speeds supported by the platform—all within a single custom Queuing Profile. The network operator can use this flexibility in order to assign different bandwidth allocations for uplink ports vs. access-edge ports within a single custom Queuing Profile, if desired.

If the bandwidth allocations for each of the traffic-classes within a custom Queuing Profile is the same across all interface speeds (referred to as All References within the EasyQoS GUI), EasyQoS will optimize the configuration and create a single policy-map with the name “policy-map prm-DSCP#APIC\_QOS\_Q\_OUT” with the bandwidth allocations specified within the custom Queuing Profile.

EasyQoS determines the interface speed based on the ifSpeed OID within the SNMP IF-MIB. This value can also be displayed via a “show interface” exec-level command on the Catalyst switch. An example is shown below.

```
AD2-4503#show interfaces GigabitEthernet 2/1
GigabitEthernet2/1 is down, line protocol is down (notconnect)
Hardware is Gigabit Ethernet Port, address is c89c.1de3.f950 (bia c89c.1de3.f950)
MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto-speed, link type is auto, media type is 10/100/1000-TX
input flow-control is off, output flow-control is off
Auto-MDIX on (operational: on)
ARP type: ARPA, ARP Timeout 04:00:00
Last input 12w3d, output never, output hang never
Last clearing of “show interface” counters never
Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: Class-based queueing
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
1262032 packets input, 110647886 bytes, 0 no buffer
Received 12041 broadcasts (9823 multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 input packets with dribble condition detected
5195136 packets output, 6514113799 bytes, 0 underruns
0 output errors, 0 collisions, 3 interface resets
0 unknown protocol drops
```

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier

0 output buffer failures, 0 output buffers swapped out

For Catalyst 4500-E and Catalyst 4500-X Series platforms when a GigabitEthernet interface is administratively down or in a line-protocol down state, the default bandwidth of the interface (interface speed) is 1 Gbps. Likewise, when a TenGigabitEthernet interface is administratively down or in a line-down protocol state, the default bandwidth of the interface (interface speed) is 10 Gbps. Therefore, if an EasyQoS policy is provisioned to a Catalyst 4500-E and Catalyst 4500-X Series switch that has GigabitEthernet or TenGigabitEthernet interfaces in an administratively down or line-protocol down state, all interfaces should still receive the bandwidth allocations for their respective speeds within the custom Queuing Profile, regardless of whether they are up or down.

### Catalyst 6500 Sup2T Queuing Design

The following sections discussing the ingress and egress queuing structures provisioned by APIC-EM EasyQoS to the ports of each of the line cards and supervisors supported by EasyQoS for the Catalyst 6500 Series platform with a Sup2T supervisor.

Ingress & egress queuing structures are dependent upon the following:

- The model of the line card
- Whether the line card supports a Centralized Forwarding Card (CFC) or Distributed Forwarding Card (DFC). This applies to WS-X6704, WS-X6724, and WS-X6748 series line cards.
- Whether the Sup2T supervisor (VS-2T-10G or VS-2T-10G-XL) Gigabit Ethernet ports are enabled or disabled

For the Catalyst 6500 Series and Catalyst 6807-XL switch with Supervisor 2T (Sup2T), if an unsupported line card is detected within the chassis, the behavior of APIC-EM EasyQoS is to skip over the line card—meaning not provision a QoS configuration for the unsupported line card—and attempt to continue provisioning the rest of the platform. The network operator will also be notified via the EasyQoS web-based GUI that an unsupported line card was detected within the chassis.

### VSS and Dual-Active Fast-Hello Configurations

Catalyst 6K and 4K switches are supported in VSS and non-VSS configurations. When operating in a VSS configuration, switch ports that belong to a port-group, which in turn are part of the VSL between the individual switches in the VSS configuration, cannot be configured with any QoS policy. APIC-EM EasyQoS has the ability to identify ports that are part of a VSL and not apply QoS policy.

- Note: On line cards which share ASICs between switch ports, configuring one switch port to be part of a VSL may also prevent other switch ports which share the same ASIC from supporting any QoS policy.

Dual-active fast-hello is a special configuration. When Catalyst 6K switches are in a VSS configuration, the Virtual Switch Link (VSL) is used send control and data between the two chassis. The VSL can have 10 GigabitEthernet or 40 GigabitEthernet ports, and is typically configured redundantly with up to eight links. Typically the two 10 GigabitEthernet ports on the Sup2T are used. However, ports on other 10 GigabitEthernet or 40 GigabitEthernet line cards can also be used for VSL links. Because the VSL is an EtherChannel configuration (physical ports assigned to a port-channel and the port-channel configured as a VSL) it has high-availability built in. If one link fails, traffic is moved to the remaining links. There is, however, a corner case of what happens if the entire VSL fails. In that scenario, both switches in the VSS could consider themselves the active supervisor. This is an undesirable situation, because both supervisors share IP addresses, MAC addresses, etc.

In order to get around this possible scenario, there are two mechanisms available on the Catalyst 6K for dual-active detection. The first mechanism involves using existing Multi-Chassis EtherChannel (MEC) configurations with enhanced Port Aggregation Protocol (PAgP). Special PAgP messages are sent across the MEC which allows the two supervisors in the two switches to realize they are both alive when the VSL goes down. However, this requires that the VSS pair is connected to an access, distribution, or core-layer switch via MEC.

The second method involves special dedicated Ethernet connections (at least two ports per switch) between the two switches in the VSS pair. These dedicated Ethernet connections are configured with the interface-level command “dual-active fast-hello”.

One of the restrictions for dual-active detection is that ASIC-specific QoS commands are not configurable on dual-active detection fast hello ports directly but are allowed to remain on the fast hello port if the commands were configured on another non-fast hello port in that same ASIC group. Because of this restriction, EasyQoS cannot configure QoS policy on the interfaces configured with “dual-active fast-hello”. The network operator must manually exclude these interfaces from QoS policy.

### 1Q8T Ingress Queuing

1Q8T ingress queuing is supported by the following line cards:

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

The WS-X6724-SFP, WS-X6748-SFP, WS-X6748-GE-TX, and WS-X6704-10GE line cards are supported in the Catalyst 6500 Series or 6807-XL with Sup-2T with either a CFC or DFC version 4 or 4-XL upgrade. The DFC is daughter card that sits on the line card itself.

Individual line card models can be identified within Catalyst 6500 Series or Catalyst 6807-XL switches via the “show module” exec-level command. An example of the output of the “show module” command is shown below, with a WS-X6748-GE-TX line card with a CFC in slot 1 highlighted.

```
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
```

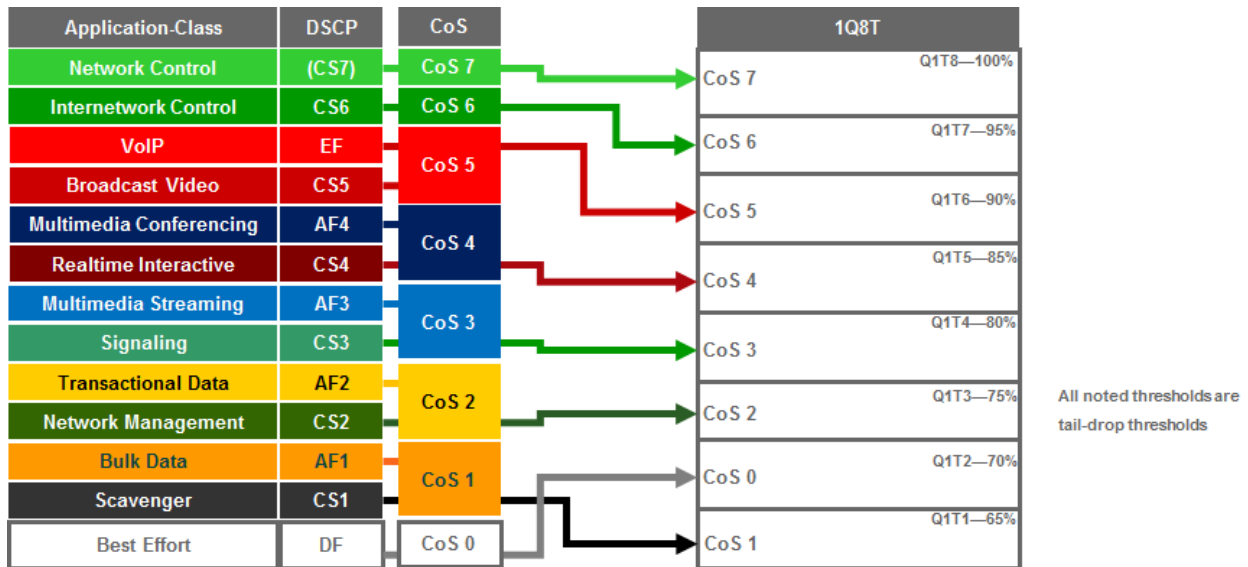
```
6 Centralized Forwarding Card WS-F6700-CFC SAL1518CRZ3 4.1 PwrDown
```

- Note: For Catalyst 6500 or 6800 Series switches in a VSS configuration, the exec-level command “show module switch all” can be used to display modules in both switches.

1Q8T ingress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. The following figure shows the 1Q8T ingress queuing model.

#### 1. 1Q8T Ingress Queuing Models—CoS-to-Queue Mapping with CoS-Based Tail-Drop





Because the 1Q8T ingress queuing structure only supports one queue, there are no class-map definitions. All traffic is mapped to class-default, corresponding to the default queue. The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the 1Q8T ingress queuing structure.

!

```
policy-map type lan-queuing prm-dscp#EZQOS_1Q8T-IN
```

```
class class-default
```

```
queue-limit cos 0 percent 70
```

```
queue-limit cos 1 percent 65
```

```
queue-limit cos 2 percent 75
```

```
queue-limit cos 3 percent 80
```

```
queue-limit cos 4 percent 85
```

```
queue-limit cos 5 percent 90
```

```
queue-limit cos 6 percent 95
```

```
queue-limit cos 7 percent 100
```

!

The 1Q8T ingress queuing structure is applied by EasyQoS to all GigabitEthernet and TenGigabitEthernet interfaces on the line card that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a single Gigabit Ethernet interface is shown below.

!

```
interface GigabitEthernetx/x
```

```
service-policy type lan-queuing input prm-dscp#EZQOS_1Q8T-IN
```

!

For the WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX line cards with CFCs, the ports are meant to be connected to end-user devices. Because line cards that support the 1Q8T queuing structure support only CoS-to-queue mapping, if the end-device does not send traffic with an 802.1p header, all traffic is treated with the default CoS mapping for the port (CoS 0) and mapped to Q1T2 with a tail-drop threshold of 70%.

Note, however, that interfaces may be configured with separate VLANs for voice, video, etc. by the network operator. If the end-device does send traffic with an 802.1p header—such as a Cisco IP phone that sends traffic marked as CoS 5—then ingress traffic from the IP phone will be mapped to Q1T6 with a tail-drop threshold of 90%, while a device chained-off the IP phone may have its traffic remarked to CoS 0 by the IP phone and mapped to Q1T2 with a tail-drop threshold of 70%.

Ports on the WS-X6704-10GE with CFC, are assumed to be uplink ports. If the Catalyst 6500 Series or Catalyst 6807-XL with Sup-2T is deployed as a distribution or core switch, and the link connecting the WS-X6704-10GE switch port is not a trunk port, then all ingress traffic will not have an 802.1p header. Hence all ingress traffic will be treated with the default CoS mapping for the port (CoS 0) and mapped to Q1T2 with a tail-drop threshold of 70%.

Due to the internal ASIC structure of the ports on the WS-X6748-SFP and WS-X6748-GE-TX line cards, the ingress and egress queuing structures of the ports cannot be configured independently. Instead, the queuing policy is applied to groups of ports on the line card by APIC-EM EasyQoS.

#### 2Q4T Ingress Queuing

2Q4T ingress queuing is supported by the following line cards:

- All ports on the VS-S2T-10G and VS-S2T-10G-XL (Supervisor 2T) when the Gigabit Ethernet ports are enabled.

The Gigabit Ethernet ports on the Sup-2T are enabled with the following global configuration command.

!

```
no platform qos 10g-only
```

!

APIC-EM EasyQoS does not set this command but will look to see if this command has been set by the network operator, in order to determine the correct queuing structure to apply to ports on the Sup2T supervisor. The default setting is for the Gigabit Ethernet ports on the Sup-2T to be enabled, so this command will not appear in the configuration.

The status of whether the Gigabit Ethernet ports are enabled or disabled can be displayed by the network operator via the exec-level “show platform qos module x” command, where “x” refers to the slot with the Sup-2T. An example of the output from the command is shown below:

```
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 V11

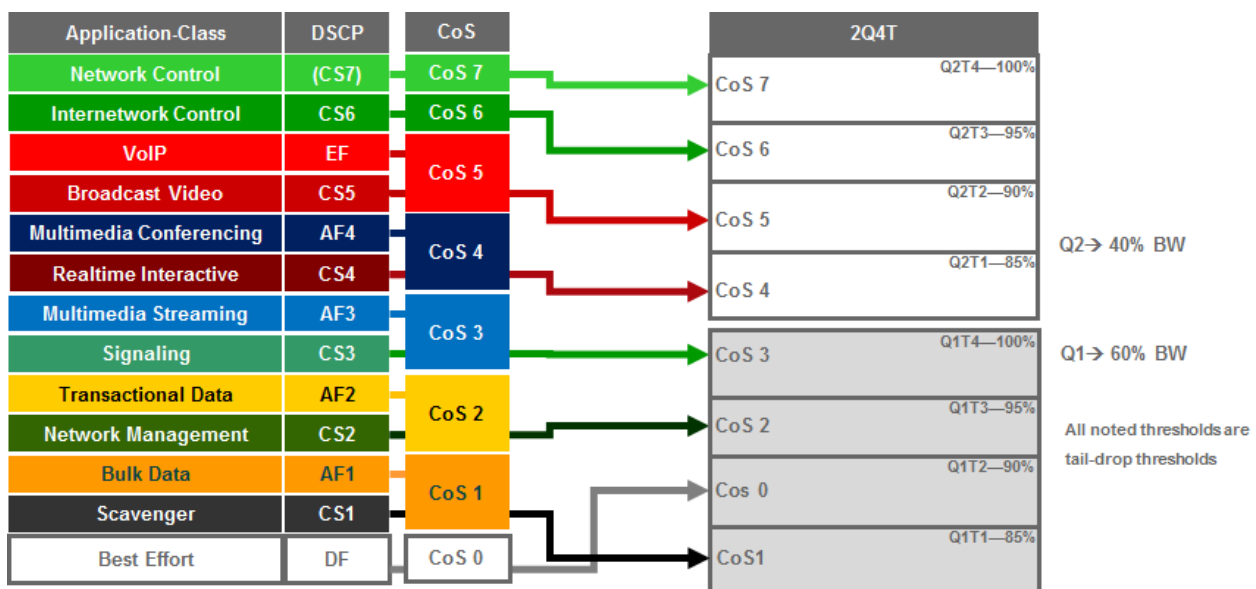
QoS 10g-only mode supported: Yes [Current mode: Off]

Global Policy-map: ingress[]

A setting of “Current mode: off” means that the Gigabit Ethernet ports are enabled.

2Q4T ingress queuing for the Sup-2T implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. The following figure shows the 2Q4T ingress queuing model.

#### 1. 2Q4T Ingress Queuing Models—CoS-to-Queue Mapping with CoS-Based Tail-Drop



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-map for the 2Q4T ingress queuing structure.

!

```
class-map type lan-queuing match-any prm-EZQOS_2Q4T#Q2
```

```
match cos 7
```

```
match cos 6
```

```
match cos 5
```

```
match cos 4
```

!

The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the 2Q4T ingress queuing structure.

!

```
policy-map type lan-queuing prm-dscp#EZQOS_2Q4T-IN
```

```
class type lan-queuing prm-EZQOS_2Q4T#Q2
bandwidth percent 40
queue-limit cos 4 percent 85
queue-limit cos 5 percent 90
queue-limit cos 6 percent 95
queue-limit cos 7 percent 100
class class-default
queue-limit cos 0 percent 90
queue-limit cos 1 percent 85
queue-limit cos 2 percent 95
queue-limit cos 3 percent 100
!
```

The 2Q4T ingress queuing policy-map is provisioned by EasyQoS to all Gigabit Ethernet and TenGigabitEthernet interfaces on the Sup2T, when the Sup2T is configured for this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are part of a VSL configuration or share an ASIC with other interfaces which are part of a VSL configuration, or interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a single Gigabit Ethernet interface is shown below.

```
!
interface GigabitEthernetx/x/x
service-policy type lan-queuing input prm-dscp#EZQOS_2Q4T-IN
!
interface TenGigabitEthernetx/x/x
service-policy type lan-queuing input prm-dscp#EZQOS_2Q4T-IN
!
```

Cisco does not recommend connecting end-user devices to any ports on the Sup-2T. Hence, all ports on the Sup-2T are assumed to be uplink ports by EasyQoS. The Sup-2T ports with 2Q4T queuing structure only support CoS-to-queue mapping. If the Catalyst 6500 Series or Catalyst 6807-XL with Sup-2T is deployed as a distribution or core switch, and the link connecting the Sup-2T port is not a trunk port, then all ingress traffic will not have an 802.1p header. Hence all ingress traffic will be treated with the default CoS mapping for the port (CoS 0) and mapped to Q1T2 with a tail-drop threshold of 90%.

It should be noted that QoS policies cannot be applied to TenGigabitEthernet ports on the Sup-2T when either one or both of the TenGigabitEthernet ports are part of a port-channel group that is part of a VSL. Therefore EasyQoS will not apply the 2Q4T ingress queuing policy when the switch port is part of a VSL. Switch ports can be identified as part of a VSL based upon the switch configuration. An example of this is shown below.

```
!
interface Port-channel63
```

```

no switchport
no ip address
no platform qos channel-consistency
switch virtual link 1
~
interface TenGigabitEthernet1/3/4
no switchport
no ip address
no cdp enable
channel-group 63 mode on
!
interface TenGigabitEthernet1/3/5
no switchport
no ip address
no cdp enable
channel-group 63 mode on
!
```

Physical interfaces are assigned to a port-group via the “channel-group” interface-level command. Port-channel interfaces are assigned to a VSL via the “switch virtual link” interface-level command, as shown in the configuration output example above.

Note also that QoS policies cannot be applied to a Gigabit Ethernet port on the Sup2T when the TenGigabitEthernet ports on the Sup-2T are part of a port-channel group that is part of a VSL. This is because the GigabitEthernet ports share the same ASIC as the TenGigabitEthernet ports. Hence, EasyQoS will not apply the 2Q4T ingress queuing policy to Gigabit Ethernet ports on the Sup2T when the TenGigabitEthernet ports are part of a VSL.

Finally, due to the internal ASIC structure of the ports on the Sup2T, the ingress and egress queuing structure of the ports cannot be configured independently. Instead, when configuring an ingress or egress queuing policy to one of the interfaces, the same policy will be propagated to the rest of the interfaces on the Sup-2T. Because of the hardware design, EasyQoS applies the same ingress or egress queuing policy on all interfaces of the Sup2T.

### 2Q8T Ingress Queuing

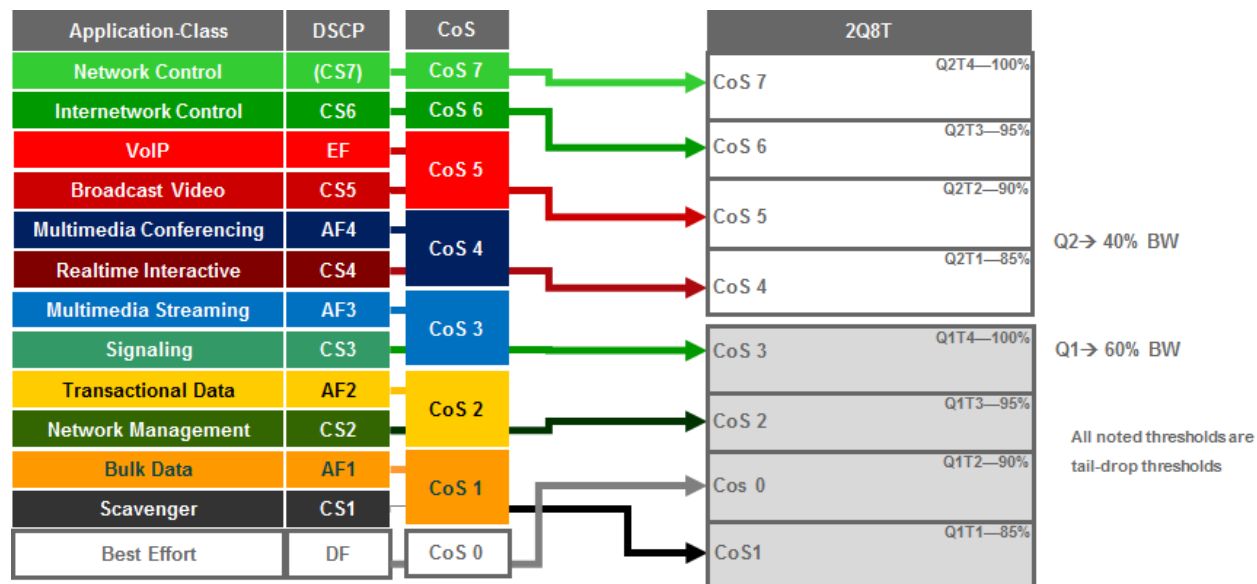
2Q8T ingress queuing is supported by the following line cards:

- 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

2Q8T ingress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance.

The following figure shows the 2Q8T ingress queuing model.

1. 2Q8T Ingress Queuing Models—CoS-to-Queue Mapping with CoS-based Tail-Drop



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-maps for the 2Q8T ingress queuing structure.

!

```
class-map type lan-queuing match-any prm-EZQOS_2Q8T#Q2
```

```
match cos 7
```

```
match cos 6
```

```
match cos 5
```

```
match cos 4
```

!

The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the 2Q8T ingress queuing structure.

!

```
policy-map type lan-queuing prm-dscp#EZQOS_2Q8T-IN
```

```
class type lan-queuing prm-EZQOS_2Q8T#Q2
```

```
bandwidth percent 40
```

```
queue-limit cos 4 percent 85
```

```
queue-limit cos 4 percent 90
```

```
queue-limit cos 6 percent 95
```

```
queue-limit cos 7 percent 100
```

```
class class-default
```

```
queue-limit cos 0 percent 90
```

```
queue-limit cos 1 percent 85
```

```
queue-limit cos 2 percent 95
```

```
queue-limit cos 3 percent 100
```

!

The 2Q8T ingress queuing policy-map is provisioned by EasyQoS to all Gigabit Ethernet interfaces on the line cards that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a single Gigabit Ethernet interface is shown below.

!

```
interface GigabitEthernetx/x/x
service-policy type lan-queuing input prm-dscp#EZQOS_2Q8T-IN
```

!

For all of the line cards that support the 2Q8T ingress queuing structure listed above, the ports are meant to be connected to end-user devices. Because line cards that support the 2Q8T queuing structure support only CoS-to-queue mapping, if the end-device does not send traffic with an 802.1p header, all traffic is treated with the default CoS mapping for the port (CoS 0) and mapped to Q1T2 with a tail-drop threshold of 90%.

Note, however, that interfaces may be configured with separate VLANs for voice, video, etc. by the network operator. If the end-device does send traffic with an 802.1p header—such as a Cisco IP phone that sends traffic marked as CoS 5—then ingress traffic from the IP phone will be mapped to Q2T2 with a tail-drop threshold of 90%, while a device chained-off the IP phone may have its traffic remarked to CoS 0 by the IP phone and mapped to Q1T2 with a tail-drop threshold of 90%.

### 8Q4T Ingress Queuing

8Q4T ingress queuing is supported by the following line cards:

- VS-S2T-10G, VS-S2T-10G-XL with Gigabit Ethernet ports disabled
- WS-X6908-10G-2T, WS-X6908-10G-2TXL

The Gigabit Ethernet ports on the Sup-2T are disabled with the following global configuration command.

!

```
platform qos 10g-only
```

!

APIC-EM EasyQoS does not set this command but will look to see if this command has been set by the network operator, in order to determine the correct queuing structure to apply to ports on the Sup2T supervisor. The default setting is for the Gigabit Ethernet ports on the Sup-2T to be enabled, so this command will appear in the configuration when the Gigabit Ethernet ports are disabled.

The status of whether the Gigabit Ethernet ports are enabled or disabled can be displayed by the network operator via the exec-level “show platform qos module x” command, where “x” refers to the slot with the Sup-2T. An example of the output from the command is shown below:

```
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 V11

QoS 10g-only mode supported: Yes [Current mode: On]

Global Policy-map: ingress[]

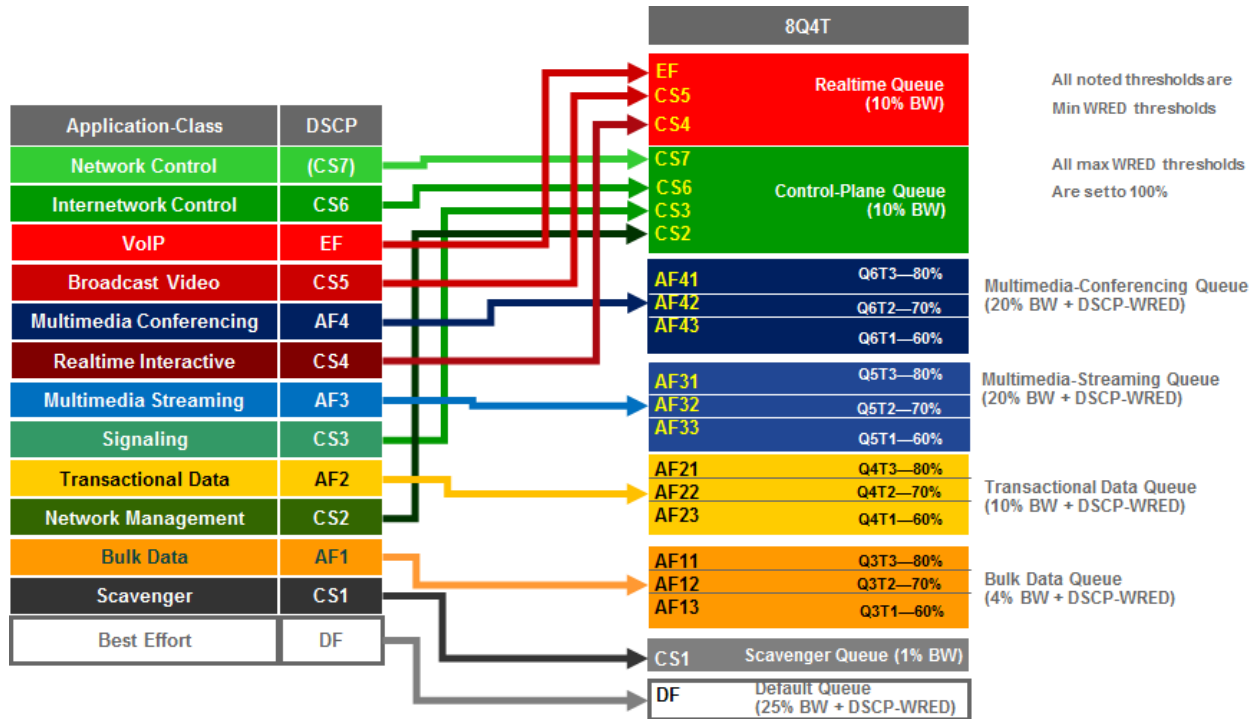
A setting of “Current mode: On” means that the Gigabit Ethernet ports are disabled.

8Q4T ingress queuing for these line cards implements DSCP-to-queue mapping, with DSCP-based WRED for congestion avoidance. APIC-EM release 1.5 and higher does not allow per traffic-class bandwidth allocations to be modified in the ingress direction for line cards which support the 8Q4T ingress queuing structure. However, per traffic-class DSCP markings are supported in the ingress direction for line cards which support the 8Q4T ingress queuing structure, because these line cards support DSCP-to-queue mapping. The default DSCP markings are part of the CVD\_QUEUEING\_PROFILE that is applied by default, unless the network operator applies a custom Queuing Profile to the policy scope containing these line cards.

The following figure shows the default 8Q4T ingress queuing model.

1. Default 8Q4T Ingress Queuing Model—DSCP-to-Queue Mapping with DSCP-based WRED





The following configuration, provisioned by APIC-EM EasyQoS, implements the default class-maps for the 8Q4T ingress queuing structure.

!

```

class-map type lan-queuing match-any prm-EZQOS_8Q4T#REALTIME
match dscp cs4
match dscp cs5
match dscp ef
class-map type lan-queuing match-any prm-EZQOS_8Q4T#CONTROL
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
class-map type lan-queuing match-any prm-EZQOS_8Q4T#MM_CONF
match dscp af41
match dscp af42
match dscp af43
class-map type lan-queuing match-any prm-EZQOS_8Q4T#MM_STREAM
match dscp af31
match dscp af32
match dscp af33
class-map type lan-queuing match-any prm-EZQOS_8Q4T#TRANS_DATA

```

```
match dscp af21
match dscp af22
match dscp af23
class-map type lan-queuing match-any prm-EZQOS_8Q4T#BULK_DATA
match dscp af11
match dscp af12
match dscp af13
class-map type lan-queuing match-any prm-EZQOS_8Q4T#SCAVENGER
match dscp cs1
!
```

The following configuration, provisioned by APIC-EM EasyQoS, implements the default policy-map for the 8Q4T ingress queuing structure.

```
!
policy-map type lan-queuing prm-dscp#EZQOS_8Q4T-IN
class type lan-queuing prm-EZQOS_8Q4T#REALTIME
bandwidth percent 10
class type lan-queuing prm-EZQOS_8Q4T#CONTROL
bandwidth percent 10
class type lan-queuing prm-EZQOS_8Q4T#MM_CONF
bandwidth percent 20
random-detect dscp-based
random-detect dscp 34 percent 80 100
random-detect dscp 36 percent 70 100
random-detect dscp 38 percent 60 100
class type lan-queuing prm-EZQOS_8Q4T#MM_STREAM
bandwidth percent 20
random-detect dscp-based
random-detect dscp 26 percent 80 100
random-detect dscp 28 percent 70 100
random-detect dscp 30 percent 60 100
class type lan-queuing prm-EZQOS_8Q4T#TRANS_DATA
bandwidth percent 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 type lan-queuing prm-EZQOS_8Q4T#BULK_DATA
bandwidth percent 4
random-detect dscp-based
random-detect dscp 10 percent 80 100
random-detect dscp 12 percent 70 100
random-detect dscp 14 percent 60 100
class type lan-queuing prm-EZQOS_8Q4T#SCAVENGER
bandwidth percent 1
class class-default
random-detect dscp-based
random-detect dscp 0 percent 80 100
!
```

The 8Q4T ingress queuing policy-map is provisioned by EasyQoS to all TenGigabitEthernet interfaces on the line cards that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are part of a VSL configuration or share an ASIC with other interfaces which are part of a VSL configuration, or interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a single TenGigabitEthernet interface is shown below.

```

!
interface TenGigabitEthernetx/x
service-policy type lan-queuing input prm-dscp#EZQOS_8Q4T-IN
!
```

For all of the line cards that support the 8Q4T ingress queuing structure listed above, the ports are assumed to be uplink ports, because they are all TenGigabitEthernet ports. If the Catalyst 6500 Series or Catalyst 6807-XL with Sup-2T is deployed as a distribution or core switch, and the link connecting the Sup-2T port is not a trunk port, then all ingress traffic will not have an 802.1p header. However, because these line cards support DSCP-to-queue mapping, ingress traffic will still be mapped into the correct queue based on the DSCP value of the IP packets.

### Custom Queuing Profiles

EasyQoS within APIC-EM release 1.5 and higher provides the network operator the ability to change the both the DSCP marking and the bandwidth allocation of traffic-classes through custom Queuing Profiles in the web-based GUI. Bandwidth allocations configured within custom Queuing Profiles are not implemented on line cards which support the 8Q4T ingress queuing structure. Instead, the default 8Q4T ingress queuing structure discussed in the previous section is always implemented by EasyQoS. However, for line cards which support the 8Q4T ingress queuing structure, custom DSCP markings are implemented.

Custom Queuing Profiles were discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Figures 37 showed an example of setting the DSCP markings within custom Queuing Profile named EasyQoS\_Lab\_Queueing\_Profile. Within that example, Broadcast Video traffic was configured with a DSCP marking of CS3, and Signaling traffic was configured with a DSCP marking of CS5.

Changing the DSCP markings of traffic-classes within the EasyQoS web-based GUI affects the “match dscp” statements of class-map definitions within the ingress queuing policy of line cards which support the 8Q4T ingress queuing structure. The following output is an example of the modification of the class-map definitions provisioned by EasyQoS, based upon the DSCP markings from the EasyQoS\_Lab\_Queueing Profile, shown in the table above. The affected class-map definitions are highlighted in bold.

!

**class-map type lan-queuing match-any prm-EZQOS\_8Q4T#REALTIME**

match dscp cs4

**match dscp cs3**

match dscp ef

**class-map type lan-queuing match-any prm-EZQOS\_8Q4T#CONTROL**

match dscp cs2

**\*\*match dscp cs3 \*\***

match dscp cs6

match dscp cs7

class-map type lan-queuing match-any prm-EZQOS\_8Q4T#MM\_CONF

match dscp af41

match dscp af42

match dscp af43

class-map type lan-queuing match-any prm-EZQOS\_8Q4T#MM\_STREAM

match dscp af31

match dscp af32

match dscp af33

class-map type lan-queuing match-any prm-EZQOS\_8Q4T#TRANS\_DATA

match dscp af21

match dscp af22

match dscp af23

class-map type lan-queuing match-any prm-EZQOS\_8Q4T#BULK\_DATA

match dscp af11

match dscp af12

match dscp af13

class-map type lan-queuing match-any prm-EZQOS\_8Q4T#SCAVENGER

match dscp cs1

!

As can be seen by comparing the the class-map definitions between the default 8Q4T ingress queuing structure and the EasyQoS\_Lab\_Queueing Profile; the Realtime queue which services the Broadcast Video traffic-class matches on CS3 instead of CS5, and the Control queue which services the Signaling traffic-class matches on CS5 instead of CS3.

8Q8T Ingress Queuing

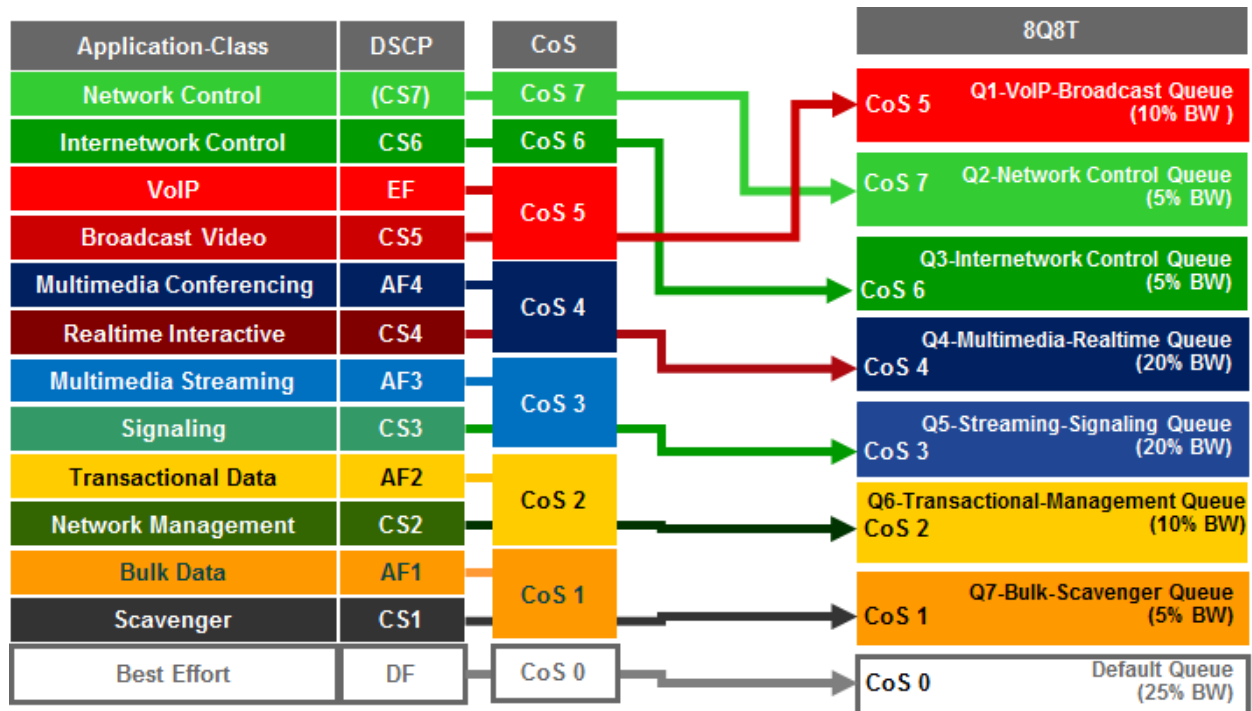
8Q8T ingress queuing is supported by the following line cards:

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

The WS-X6704-10GE line card can support either a CFC or a DFC version 4 or 4XL upgrade, in order to operate with the Sup-2T. With a CFC, the WS-X6704-10GE line card supports 1Q8T ingress queuing. With a DFC4/4XL upgrade, the WS-X6704-10GE line card supports 8Q8T ingress queuing. Whether or not the WS-X6704-10GE line card has a CFC or DFC can be displayed via the exec-level “show module” command, as discussed in the **\*1Q8T Ingress Queuing\*** section above.

8Q8T ingress queuing for the WS-X6704-10GE implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. The following figure shows the 8Q8T ingress queuing model.

#### 1. 8Q8T Ingress Queuing Models—CoS-to-Queue Mapping with CoS-based Tail-Drop



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-maps for the 8Q8T ingress queuing structure.

!

```
class-map type lan-queuing match-any prm-EZQOS_8Q8T#Q1
match cos 5

class-map type lan-queuing match-any prm-EZQOS_8Q8T#Q2
match cos 7

class-map type lan-queuing match-any prm-EZQOS_8Q8T#Q3
match cos 6

class-map type lan-queuing match-any prm-EZQOS_8Q8T#Q4
match cos 4

class-map type lan-queuing match-any prm-EZQOS_8Q8T#Q5
match cos 3
```

```
class-map type lan-queuing match-any prm-EZQOS_8Q8T#Q6
match cos 2
class-map type lan-queuing match-any prm-EZQOS_8Q8T#Q7
match cos 1
!
```

The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the 8Q8T ingress queuing structure.

```
!
policy-map type lan-queuing prm-dscp#EZQOS_8Q8T-IN
class prm-EZQOS_8Q8T#Q1
bandwidth percent 10
class prm-EZQOS_8Q8T#Q2
bandwidth percent 5
class prm-EZQOS_8Q8T#Q3
bandwidth percent 5
class prm-EZQOS_8Q8T#Q4
bandwidth percent 20
class prm-EZQOS_8Q8T#Q5
bandwidth percent 20
class prm-EZQOS_8Q8T#Q6
bandwidth percent 10
class prm-EZQOS_8Q8T#Q7
bandwidth percent 5
class class-default
!
```

The 8Q8T ingress queuing policy-map is provisioned by EasyQoS to all TenGigabitEthernet interfaces on the line cards that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a single TenGigabitEthernet interface is shown below.

```
!
interface TenGigabitEthernetx/x/x
service-policy type lan-queuing input prm-dscp#EZQOS_8Q8T-IN
!
```

Ports on the WS-X6704-10GE with DFC4/4XL are assumed to be uplink ports. If the Catalyst 6500 Series or Catalyst 6807-XL with Sup-2T is deployed as a distribution or core switch, and the link connecting the WS-X6704-10GE switch port is not a trunk port, then all ingress traffic will not have an 802.1p header. Hence all ingress traffic will be treated with the default CoS mapping for the port (CoS 0) and mapped to the default queue. Because no other traffic will be in other queues, the default queue will essentially have 100% of the bandwidth available.

### 2P6Q4T Ingress and Egress Queuing

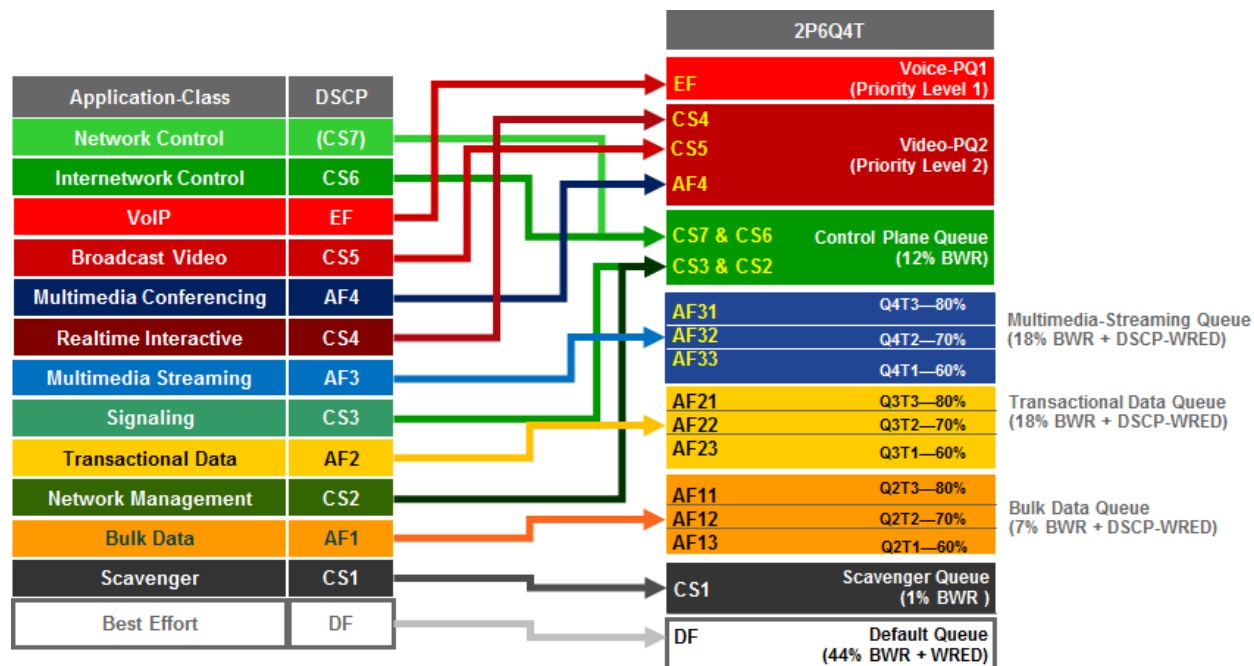
2P6Q4T ingress and egress queuing is supported by the following line cards:

- C6800-8P10G, C6800-8P10G-XL
- C6800-16P10G, C6800-16P10G-XL
- C6800-32P10G, C6800-32P10G-XL

APIC-EM release 1.4 changed the default bandwidth allocations for the 2P6Q4T egress queuing design. With APIC-EM release 1.5 and higher, the default bandwidth allocations are part of the CVD\_Queueing\_PROFILE that is applied by default, unless the network operator applies a custom Queueing Profile to the policy scope containing these switches. However, APIC-EM release 1.5 only allowed per traffic-class bandwidth allocations to be modified in the egress direction for line cards which support the 2P6Q4T queuing structure. APIC-EM release 1.6 allows per traffic-class bandwidth allocations to be modified in both the ingress and egress directions for line cards which support the 2P6Q4T queuing structure. Per traffic-class DSCP markings are also supported in both the ingress and egress direction for these line cards.

2P6Q4T ingress and egress queuing for these line cards implements DSCP-to-queue mapping, with DSCP-based WRED for congestion avoidance. The following figure shows the default 2P6Q4T ingress and egress queuing model.

#### 1. Default 2P6Q4T Ingress and Egress Queuing Model—DSCP-to-Queue Mapping with DSCP-based WRED



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-maps for the default 2P6Q4T queuing structure.

!

```
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#VOICE-PQ1
```

```
match dscp ef
```

```
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#VIDEO-PQ2
match dscp cs4
match dscp cs5
match dscp af41
match dscp af42
match dscp af43
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#CONTROL
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#MM_STREAM
match dscp af31
match dscp af32
match dscp af33
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#TRANS_DATA
match dscp af21
match dscp af22
match dscp af23
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#BULK_DATA
match dscp af11
match dscp af12
match dscp af13
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#SCAVENGER
match dscp cs1
```

!

The following configuration, provisioned by APIC-EM EasyQoS, implements the default ingress policy-map for the 2P6Q4T ingress queuing structure.

!

```
policy-map type lan-queuing prm-dscp#EZQOS_2P6Q4T-IN
class type lan-queuing prm-EZQOS_2P6Q4T#VOICE-PQ1
priority level 1
class type lan-queuing prm-EZQOS_2P6Q4T#VIDEO-PQ2
priority level 2
class type lan-queuing prm-EZQOS_2P6Q4T#CONTROL
bandwidth remaining percent 12
```



```

class type lan-queuing prm-EZQOS_2P6Q4T#MM_STREAM
bandwidth remaining percent 18
random-detect dscp-based
random-detect dscp 26 percent 80 100
random-detect dscp 28 percent 70 100
random-detect dscp 30 percent 60 100
class type lan-queuing prm-EZQOS_2P6Q4T#TRANS_DATA
bandwidth remaining percent 18
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 type lan-queuing prm-EZQOS_2P6Q4T#BULK_DATA
bandwidth remaining percent 7
random-detect dscp-based
random-detect dscp 10 percent 80 100
random-detect dscp 12 percent 70 100
random-detect dscp 14 percent 60 100
class type lan-queuing prm-EZQOS_2P6Q4T#SCAVENGER
bandwidth remaining percent 1
class class-default
random-detect dscp-based
random-detect dscp 0 percent 80 100
!
```

The following configuration, provisioned by APIC-EM EasyQoS, implements the default egress policy-map for the 2P6Q4T egress queuing structure.

```

!
policy-map type lan-queuing prm-dscp#EZQOS_2P6Q4T-OUT
class type lan-queuing prm-EZQOS_2P6Q4T#VOICE-PQ1
priority level 1
class type lan-queuing prm-EZQOS_2P6Q4T#VIDEO-PQ2
priority level 2
class type lan-queuing prm-EZQOS_2P6Q4T#CONTROL
bandwidth remaining percent 12
class type lan-queuing prm-EZQOS_2P6Q4T#MM_STREAM
bandwidth remaining percent 18
```

```
random-detect dscp-based
random-detect dscp 26 percent 80 100
random-detect dscp 28 percent 70 100
random-detect dscp 30 percent 60 100
class type lan-queuing prm-EZQOS_2P6Q4T#TRANS_DATA
bandwidth remaining percent 18
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 type lan-queuing prm-EZQOS_2P6Q4T#BULK_DATA
bandwidth remaining percent 7
random-detect dscp-based
random-detect dscp 10 percent 80 100
random-detect dscp 12 percent 70 100
random-detect dscp 14 percent 60 100
class type lan-queuing prm-EZQOS_2P6Q4T#SCAVENGER
bandwidth remaining percent 1
class class-default
random-detect dscp-based
random-detect dscp 0 percent 80 100
!
```

The bandwidth allocations within the EasyQoS GUI for Queuing Profiles require the sum of the bandwidth percentages to total 100%. These bandwidth allocations are absolute bandwidth percentages. Because the 2P6Q4T ingress and egress queuing policy implements an eight-queue model in hardware on these switch platforms, multiple traffic-classes may be mapped to a single queue. The following table shows the mapping of the traffic-classes and bandwidth allocations from the default EasyQoS CVD\_Queueing\_Profile to the 2P6Q4T ingress and egress queuing structure.

1. Default Queuing Profile Mapping to 2P6Q4T Ingress and Egress Queuing Policy

Traffic Class	DSCP Marking	BW % in the Default Queuing Profile	BWR % Calculated from the Default Queuing Profile	2P6Q4T Ingress and Egress Queue Mapping	BWR % Allocation in 2P6Q4T Ingress and Egress Queue
Voice	EF	10%	N/A	Voice-PQ1	Voice-PQ1 bandwidth is unconstrained and consists of traffic from the Voice traffic-class.
Broadcast Video	CS5	10%	N/A	Video-PQ2	Video-PQ2 bandwidth is unconstrained and consists of traffic from the Broadcast Video, Real-Time Interactive, and Multimedia Conferencing traffic-classes.
Real-Time Interactive	CS4	13%	N/A	Video-PQ2	
Multimedia Conferencing	AF41	10%	N/A	Video-PQ2	
Multimedia Streaming	AF31	10%	18%	Multimedia-Streaming Queue	BWR for traffic-class mapped to Multimedia-Streaming Queue = 18%
Network Control	CS6	3%	5%	Control-Queue	BWR for traffic-classes mapped to Control-Plane Queue = 5% (Network Control) + 4% (Signaling) + 4% (OAM) = 13%. (Actual value configured within switch platforms is rounded down to 12% to reach 100% BWR.)
Signaling	CS3	2%	4%	Control-Queue	
OAM	CS2	2%	4%	Control-Queue	
Transactional Data	AF21	10%	18%	Transactional-Data Queue	BWR for traffic-class mapped to Transactional-Data Queue = 18%
Bulk Data	AF11	4%	7%	Bulk-Data Queue	BWR for traffic-class mapped to Bulk-Data Queue = 7%
Scavenger	CS1	1%	2%	Scavenger Queue	BWR for traffic-class mapped to Scavenger Queue = 2% due to rounding to whole numbers in the formulas presented here. (Actual value configured within switch platforms is rounded down to 1% to reach 100% BWR.)
Best Effort	Default	25%	44% Implicit	Default Queue	Best Effort traffic-class mapped to Default Queue receives the remaining bandwidth, which is implicitly 44%.

Column 3 of the table above shows the percentage bandwidth allocation for each of the traffic-classes as it appears within the EasyQoS GUI for the default CVD\_Queueing\_Profile. In the 2P6Q4T ingress and egress queuing policy,

the Voice traffic-class is mapped to Voice-PQ1, while the Broadcast Video, Real-Time Interactive, and Multimedia-Conferencing traffic-classes are mapped to the Video-PQ2, as shown in column 5. The sum of the bandwidth allocated to these three traffic-classes can be considered as the total priority queue bandwidth (Total\_PQ\_BW), as shown in the following formula.

$$\text{Total\_PQ\_BW} = \text{Voice BW} + \text{Broadcast Video BW} + \text{Real-Time Interactive BW} + \text{Multimedia Conferencing BW}$$

Based on the bandwidth allocations in column 3 in the table above Total\_PQ\_BW can be calculated as follows:

$$\text{Total\_PQ\_BW} = 10\% (\text{Voice}) + 10\% (\text{Broadcast Video}) + 13\% (\text{Real-Time Interactive}) + 10\% (\text{Multimedia Conferencing}) = 43\%$$

For the remaining eight traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI, and the amount of Total\_PQ\_BW calculated above. This can be done through the following formula.

$$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$$

For example, BWR percentage for the Multimedia Streaming traffic class can be calculated as follows:

$$\text{Multimedia\_Streaming\_BWR} = (10\% / (100\% - 43\%)) * 100 = 18\% \text{ when rounded}$$

Finally, determining the bandwidth ratio allocated to each of the non-priority queues within the 2P6Q4T ingress and egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above. The default queue implicitly gets the remaining bandwidth not configured with “bandwidth remaining” statements for the other queues. Note that the priority queues are unconstrained in the 2P6Q4T ingress and egress queuing structure provisioned by EasyQoS. Although there are bandwidth allocations for the traffic-classes that map to the priority queues within default Queuing Profile within the EasyQoS GUI, these bandwidth allocations are unenforced with the 2P6Q4T ingress and egress queuing structure.

The 2P6Q4T queuing policy-map is provisioned by EasyQoS to all TenGigabitEthernet and FortyGigabitEthernet interfaces, in the ingress and egress direction, on the line cards that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are part of a VSL configuration or share an ASIC with other interfaces which are part of a VSL configuration, or interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a TenGigabitEthernet and FortyGigabitEthernet interface in the ingress and egress directions is shown below.

```
!  
interface TenGigabitEthernetx/x  
service-policy type lan-queuing input prm-dscp#EZQOS_2P6Q4T-IN  
service-policy type lan-queuing output prm-dscp#EZQOS_2P6Q4T-OUT  
!  
interface FortyGigabitEthernetx/x  
service-policy type lan-queuing input prm-dscp#EZQOS_2P6Q4T-IN  
service-policy type lan-queuing output prm-dscp#EZQOS_2P6Q4T-OUT  
!
```

For the line cards listed above that support the 2P6Q4T ingress queuing structure, the ports are assumed to be uplink ports, because they are either TenGigabitEthernet or FortyGigabitEthernet ports. If the Catalyst 6500 Series or Catalyst 6807-XL with Sup-2T is deployed as a distribution or core switch, and the link connecting the Sup-2T port is not a trunk port, then all ingress traffic will not have an 802.1p header. However, because these line cards support DSCP-to-queue mapping, ingress traffic will still be mapped into the correct queue based on the DSCP value of the IP packets.

Custom Queuing Profiles with 2P6Q4T Ingress and Egress Queuing

EasyQoS within APIC-EM release 1.5 and higher provides the network operator the ability to change the both the DSCP marking and the bandwidth allocation of traffic-classes through custom Queuing Profiles in the web-based GUI. As of APIC-EM release 1.6, for line cards which support the 2P6Q4T queuing structure, custom bandwidth allocations apply to both ingress and egress queuing policy-maps. Custom Queuing Profiles were discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Figures 36 and 37 showed an example custom Queuing Profile named EasyQoS\_Lab\_Queueing\_Profile. The bandwidth allocations for the 12 traffic-classes for this example Queuing Profile (for 1 Gbps interfaces) are shown in column 3 of the following table. Likewise, the DSCP markings for the 12 traffic-classes are shown in column 2.

1. Example Custom Queuing Profile Mapping to 2P6Q4T Ingress and Egress Queuing Policy

Traffic Class	DSCP Marking	BW % in the example EasyQoS Lab Queuing Profile	BWR % Calculated from the EasyQoS Lab Queuing Profile	2P6Q4T Ingress and Egress Queue Mapping	BWR % Allocation in 2P6Q4T Ingress and Egress Queue
Voice	EF	5%	N/A	Voice-PQ1	Voice-PQ1 bandwidth is constrained to 5% and consists of traffic from the Voice traffic-class.
Broadcast Video	CS3	5%	N/A	Video-PQ2	Video-PQ2 bandwidth is constrained to 20% and consists of traffic from the Broadcast Video, Real-Time Interactive, and Multimedia Conferencing traffic-classes.
Real-Time Interactive	CS4	5%	N/A	Video-PQ2	
Multimedia Conferencing	AF41	10%	N/A	Video-PQ2	
Multimedia Streaming	AF31	10%	13%	Multimedia-Streaming Queue	BWR for traffic-class mapped to Multimedia-Streaming Queue = 13%
Network Control	CS6	3%	4%	Control-Plane Queue	BWR for traffic-classes mapped to Control-Plane Queue = 4% (Network Control) + 4% (Signaling) + 11% (OAM) = 19%
Signaling	CS5	3%	4%	Control-Plane Queue	
OAM	CS2	8%	11%	Control-Plane Queue	
Transactional Data	AF21	10%	13%	Transactional-Data Queue	BWR for traffic-class mapped to Transactional-Data Queue = 13%
Bulk Data	AF11	10%	13%	Bulk-Data Queue	BWR for traffic-class mapped to Bulk-Data Queue = 13%
Scavenger	CS1	1%	1%	Scavenger Queue	BWR for traffic-class mapped to Scavenger Queue = 1%
Best Effort	Default	30%	41% Implicit	Default Queue	Best Effort traffic-class mapped to Default Queue receives the remaining bandwidth, which is implicitly 41%.

Changing the DSCP markings of traffic-classes within the EasyQoS web-based GUI affects the “match dscp” statements of class-map definitions within the ingress and egress queuing policy of line cards which support the 2P6Q4T queuing structure. The following output is an example of the modification of the class-map definitions provisioned by EasyQoS, based upon the DSCP markings from the EasyQoS\_Lab\_Queueing Profile, shown in the table above. The affected class-map definitions are highlighted in bold.

!

```
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#VOICE-PQ1
```

```

match dscp ef
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#VIDEO-PQ2
match dscp cs4
**match dscp cs3 **
match dscp af41
match dscp af42
match dscp af43
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#CONTROL
match dscp cs2
**match dscp cs5 **
match dscp cs6
match dscp cs7
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#MM_STREAM
match dscp af31
match dscp af32
match dscp af33
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#TRANS_DATA
match dscp af21
match dscp af22
match dscp af23
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#BULK_DATA
match dscp af11
match dscp af12
match dscp af13
class-map type lan-queuing match-any prm-EZQOS_2P6Q4T#SCAVENGER
match dscp cs1
!
```

As can be seen by comparing the class-map definitions between the default Queuing Profile (CVD\_Queueing\_Profile) and the EasyQoS\_Lab\_Queueing Profile, the Video-PQ2 queue which services the Broadcast Video traffic-class matches on CS3 instead of CS5, and the Control queue which services the Signaling traffic-class matches on CS5 instead of CS3.

Custom Queuing Profiles modify the amount bandwidth allocated through the “bandwidth remaining percent” commands within the ingress and egress queuing policy-map applied to physical interfaces of line cards that support the 2P6Q4T egress queuing structure. The table above shows how changing the amount of bandwidth allocated to each traffic class modifies the bandwidth allocated to the queues within the 2P6Q4T ingress and egress queuing model.

Based on the formula discussed previously, the new total priority queue bandwidth (Total\_PQ\_BW) is calculated as follows:

$$\text{Total\_PQ\_BW} = 5\% \text{ (Voice BW)} + 5\% \text{ (Broadcast Video BW)} + 5\% \text{ (Real-Time Interactive BW)} + 10\% \text{ (Multimedia Conferencing BW)} = 25\%$$

For the remaining nine traffic-classes the BWR percentages shown in column 4 of the table above can be calculated based on the amount of bandwidth allocated to each traffic class through the EasyQoS GUI, and the amount of Total\_PQ\_BW, through the following formula.

$$\text{Traffic\_Class\_BWR} = (\text{Traffic\_Class\_BW} / (100\% - \text{Total\_PQ\_BW})) * 100$$

For example, the new BWR percentage for the Multimedia Streaming traffic class can be calculated as follows:

$$\text{Multimedia\_Streaming\_BWR} = (10\% / (100\% - 25\%)) * 100 = 13\% \text{ when rounded}$$

Finally, determining the new bandwidth ratio allocated to each of the non-priority queues within the 2P6Q3T egress queuing model is simply a matter of summing the Traffic\_Class\_BWR numbers for the traffic-classes that are mapped into a given queue. This is shown in column 6 in the table above. The default queue implicitly gets the remaining bandwidth not configured with “bandwidth remaining” statements for the other queues.

This results in the following policy-map definition when deployed on a line card which supports 2P6Q4T egress queuing policy.

!

```
policy-map type lan-queuing prm-dscp#EZQOS_2P6Q4T-OUT
```

```
class type lan-queuing prm-EZQOS_2P6Q4T#VOICE-PQ1
```

```
priority level 1
```

```
class type lan-queuing prm-EZQOS_2P6Q4T#VIDEO-PQ2
```

```
priority level 2
```

```
class type lan-queuing prm-EZQOS_2P6Q4T#CONTROL
```

```
bandwidth remaining percent 19
```

```
class type lan-queuing prm-EZQOS_2P6Q4T#MM_STREAM
```

```
bandwidth remaining percent 13
```

```
random-detect dscp-based
```

```
random-detect dscp 26 percent 80 100
```

```
random-detect dscp 28 percent 70 100
```

```
random-detect dscp 30 percent 60 100
```

```
class type lan-queuing prm-EZQOS_2P6Q4T#TRANS_DATA
```

```
bandwidth remaining percent 13
```

```
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 type lan-queuing prm-EZQOS_2P6Q4T#BULK_DATA
```

```
bandwidth remaining percent 13
```

```
random-detect dscp-based
```

```
random-detect dscp 10 percent 80 100
```

```
random-detect dscp 12 percent 70 100
```

```
random-detect dscp 14 percent 60 100
```



```

class type lan-queuing prm-EZQOS_2P6Q4T#SCAVENGER
bandwidth remaining percent 1
class class-default
random-detect dscp-based
random-detect dscp 0 percent 80 100
!
```

Likewise, this results in the following the policy-map definition for the 2P6Q4T ingress queuing policy.

```

!
policy-map type lan-queuing prm-dscp#EZQOS_2P6Q4T-IN
class type lan-queuing prm-EZQOS_2P6Q4T#VOICE-PQ1
priority level 1
class type lan-queuing prm-EZQOS_2P6Q4T#VIDEO-PQ2
priority level 2
class type lan-queuing prm-EZQOS_2P6Q4T#CONTROL
bandwidth remaining percent 19
class type lan-queuing prm-EZQOS_2P6Q4T#MM_STREAM
bandwidth remaining percent 13
random-detect dscp-based
random-detect dscp 26 percent 80 100
random-detect dscp 28 percent 70 100
random-detect dscp 30 percent 60 100
class type lan-queuing prm-EZQOS_2P6Q4T#TRANS_DATA
bandwidth remaining percent 13
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 type lan-queuing prm-EZQOS_2P6Q4T#BULK_DATA
bandwidth remaining percent 13
random-detect dscp-based
random-detect dscp 10 percent 80 100
random-detect dscp 12 percent 70 100
random-detect dscp 14 percent 60 100
class type lan-queuing prm-EZQOS_2P6Q4T#SCAVENGER
bandwidth remaining percent 1
class class-default
```

random-detect dscp-based

random-detect dscp 0 percent 80 100

!

In the configuration example above, the bandwidth allocations have been modified from the CVD\_Queueing\_Profile for 10/40 Gbps interface speeds.

EasyQoS determines the interface speed based on the ifSpeed OID within the SNMP Interfaces MIB (IF-MIB). This value can also be displayed via a “show interface” exec-level command on the Catalyst switch. An example is shown below.

```
D1-6840#show interface TenGigabitEthernet 1/1
```

```
TenGigabitEthernet1/1 is up, line protocol is up (connected)
```

```
Hardware is C6k 10000Mb 802.3, address is bcf1.f260.8f2f (bia bcf1.f260.8f2f)
```

```
Description: link to C1-6807-VSS ten 2/3/1
```

```
MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
```

```
reliability 255/255, txload 1/255, rxload 1/255
```

```
Encapsulation ARPA, loopback not set
```

```
Keepalive set (10 sec)
```

```
Carrier delay is 0 msec
```

```
Full-duplex, 10Gb/s, media type is 10Gbase-CU2M
```

```
input flow-control is on, output flow-control is off
```

```
Clock mode is auto
```

```
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Last input never, output never, output hang never
```

```
Last clearing of “show interface” counters never
```

```
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
```

```
Queueing strategy: fifo
```

```
Output queue: 0/40 (size/max)
```

```
30 second input rate 31000 bits/sec, 30 packets/sec
```

```
30 second output rate 25000 bits/sec, 8 packets/sec
```

```
L2 Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
```

```
L3 in Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
```

```
L3 out Switched: ucast: 0 pkt, 0 bytes - mcast: 0 pkt, 0 bytes
```

```
234872286 packets input, 40486657342 bytes, 0 no buffer
```

```
Received 626410 broadcasts (626410 multicasts)
```

```
0 runs, 0 giants, 0 throttles
```

```
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
```

```
0 watchdog, 0 multicast, 0 pause input
```

```
0 input packets with dribble condition detected
```

164172075 packets output, 78129771843 bytes, 0 underruns

0 output errors, 0 collisions, 3 interface resets

0 unknown protocol drops

0 babbles, 0 late collision, 0 deferred

0 lost carrier, 0 no carrier, 0 pause output

0 output buffer failures, 0 output buffers swapped out

### 1P3Q8T Egress Queuing

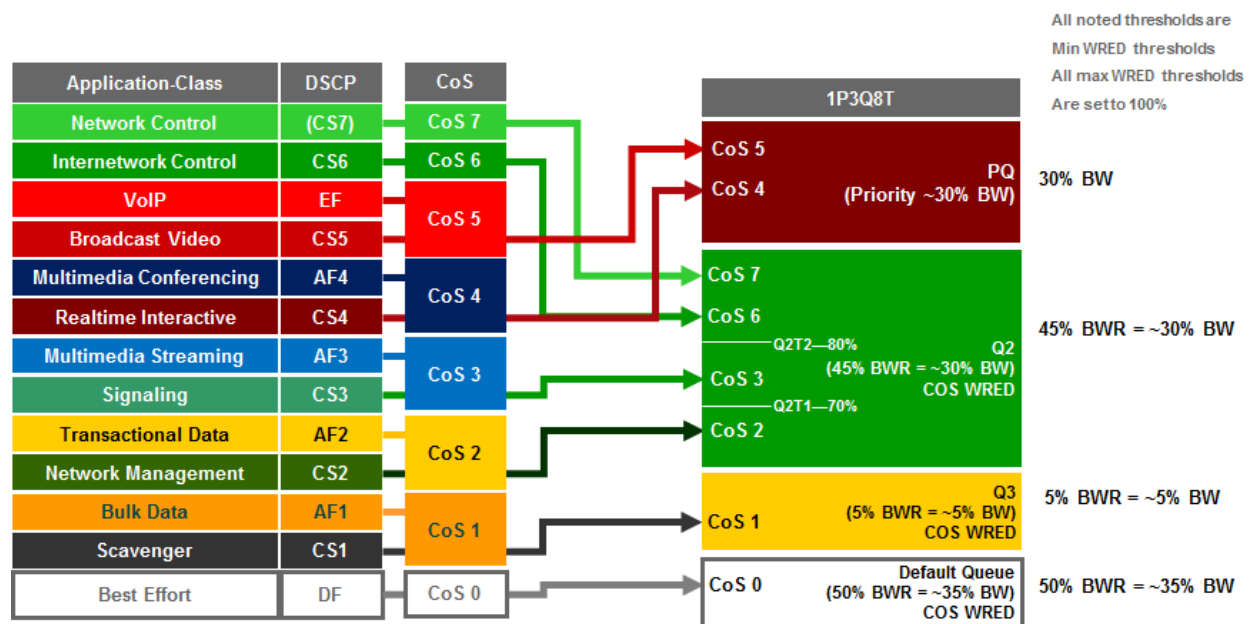
1P3Q8T egress queuing is supported by the following line cards:

- 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
- C6800-48P-SFP, C6800-48P-SFP-XL, C6800-48P-TX, and C6800-48P-TX-XL

1P3Q8T egress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance.

The following figure shows the 1P3Q8T egress queuing model.

#### 1. 1P3Q8T Egress Queuing Model—Cos-to-Queue Mapping with CoS-based Tail-Drop



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-maps for the 1P3Q8T egress queuing structure.

!

```
class-map type lan-queuing match-any prm-EZQOS_1P3Q8T#PQ
match cos 4
```

```
match cos 5
class-map type lan-queuing match-any prm-EZQOS_1P3Q8T#Q2
match cos 2
match cos 3
match cos 6
match cos 7
class-map type lan-queuing match-any prm-EZQOS_1P3Q8T#Q3
match cos 1
!
```

The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the 1P3Q8T egress queuing structure.

```
!
policy-map type lan-queuing prm-dscp#EZQOS_1P3Q8T-OUT
class prm-EZQOS_1P3Q8T#PQ
priority
class prm-EZQOS_1P3Q8T#Q2
bandwidth remaining percent 45
random-detect cos-based
random-detect cos 2 percent 70 100
random-detect cos 3 percent 80 100
random-detect cos 6 percent 100 100
random-detect cos 7 percent 100 100
class prm-EZQOS_1P3Q8T#Q3
bandwidth remaining percent 5
random-detect cos-based
random-detect cos 1 percent 80 100
class class-default
random-detect cos-based
random-detect cos 0 percent 80 100
!
```

The network operator should note that depending upon the particular line card, the policy-map configuration may look subtly different. Specifically the class configurations under the policy-map definition may include the words “type lan-queuing” within the definitions as shown below.

```
!
policy-map type lan-queuing prm-dscp#EZQOS_1P3Q8T-OUT
class type lan-queuing prm-EZQOS_1P3Q8T#PQ
priority
```

```

class type lan-queuing prm-EZQOS_1P3Q8T#Q2
bandwidth remaining percent 45
random-detect cos-based
random-detect cos 2 percent 70 100
random-detect cos 3 percent 80 100
random-detect cos 6 percent 100 100
random-detect cos 7 percent 100 100
class type lan-queuing prm-EZQOS_1P3Q8T#Q3
bandwidth remaining percent 5
random-detect cos-based
random-detect cos 1 percent 80 100
class class-default
random-detect cos-based
random-detect cos 0 percent 80 100
!
```

Functionally, both variations of the policy-map definition are identical and simply represent minor differences in how the policy-map is displayed for various models of line cards. Other ingress and egress queuing structures may also exhibit these minor differences as well.

The following configuration implements the 1P3Q8T egress queuing structure. Additionally, it shows the application of the 1P3Q8T egress queuing structure to a Gigabit Ethernet interface.

The 1P3Q8T queuing policy-map is provisioned by EasyQoS to all Gigabit Ethernet interfaces, in the egress direction, on the line cards that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a Gigabit Ethernet interface is shown below.

```

!
interface GigabitEthernet x/x/x
service-policy type lan-queuing output prm-dscp#EZQOS_1P3Q8T-OUT
!
```

Due to the internal ASIC structure of the ports on the WS-X6748-SFP and WS-X6748-GE-TX line cards, the egress queuing structure of the ports cannot be configured independently. Instead, the queuing policy is applied to groups of ports on the line card by APIC-EM EasyQoS.

#### 1P3Q4T Egress Queuing

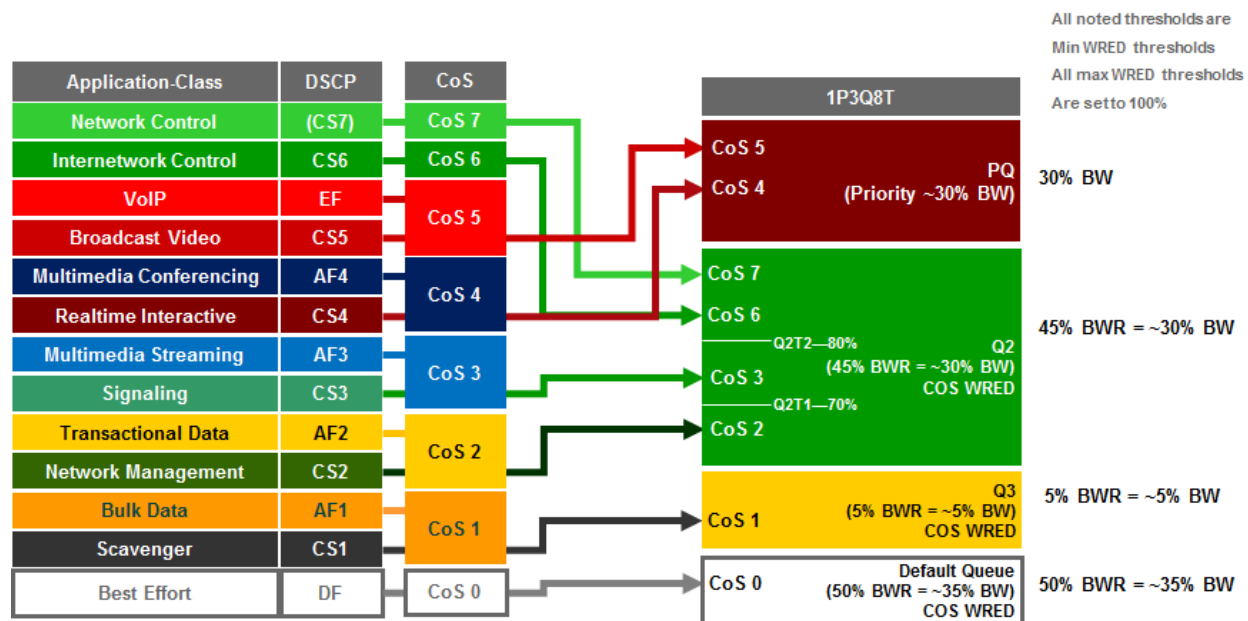
1P3Q4T egress queuing is supported by the following line cards:

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

Enabling of the Gigabit Ethernet ports on the Sup-2T was discussed in the **\*2Q4T Ingress Queuing\*** section above.

1P3Q4T egress queuing for the Sup-2T implements CoS-to-queue mapping, with CoS-based WRED for congestion avoidance. The following figure shows the 1P3Q4T egress queuing model.

#### 1. 1P3Q4T Egress Queuing Model—CoS-to-Queue Mapping with CoS-based WRED



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-maps for the 1P3Q4T egress queuing structure.

```
!
class-map type lan-queuing match-any prm-QOS6K_1P3Q4T#PQ
match cos 4
match cos 5
class-map type lan-queuing match-any prm-QOS6K_1P3Q4T#Q2
match cos 2
match cos 3
match cos 6
match cos 7
class-map type lan-queuing match-any prm-QOS6K_1P3Q4T#Q3
match cos 1
!
```

The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the 1P3Q4T egress queuing structure.

```
!
policy-map type lan-queuing prm-dscp#QOS6K_1P3Q4T-OUT
class type lan-queuing prm-QOS6K_1P3Q4T#PQ
```

```

priority
class type lan-queuing prm-QoS6K_1P3Q4T#Q2
bandwidth remaining percent 45
random-detect cos-based
random-detect cos 2 percent 70 100
random-detect cos 3 percent 80 100
random-detect cos 6 percent 100 100
random-detect cos 7 percent 100 100
class type lan-queuing prm-QoS6K_1P3Q4T#Q3
bandwidth remaining percent 5
random-detect cos-based
random-detect cos 1 percent 80 100
class class-default
random-detect cos-based
random-detect cos 0 percent 80 100
!
```

The 1P3Q4T queuing policy-map is provisioned by EasyQoS to all Gigabit Ethernet interfaces, in the egress direction, on the supervisor that supports this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are part of a VSL configuration or share an ASIC with other interfaces which are part of a VSL configuration, or interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a Gigabit Ethernet interface is shown below.

```

!
interface GigabitEthernet x/x/x
service-policy type lan-queuing output prm-dscp#QoS6K_1P3Q4T-OUT
!
```

As discussed in the **\*2Q4T Ingress Queuing\*** section above, QoS service policies cannot be applied to TenGigabitEthernet ports on the Sup-2T when the TenGigabitEthernet ports are part of a port-channel group that is part of a virtual switch link (VSL). Also, QoS service policies cannot be applied to Gigabit Ethernet ports on the Sup-2T when the TenGigabitEthernet ports are part of a VSL.

Finally, due to the internal ASIC structure of the ports on the Sup-2T, the egress queuing structure of the ports cannot be configured independently. Instead, the queuing policy is applied to groups of ports on the line card by APIC-EM EasyQoS.

#### 1P7Q4T Egress Queuing

1P7Q4T egress queuing is supported by the following line cards:

- WS-X6908-10G-2T and WS-X6908-10G-2TXL

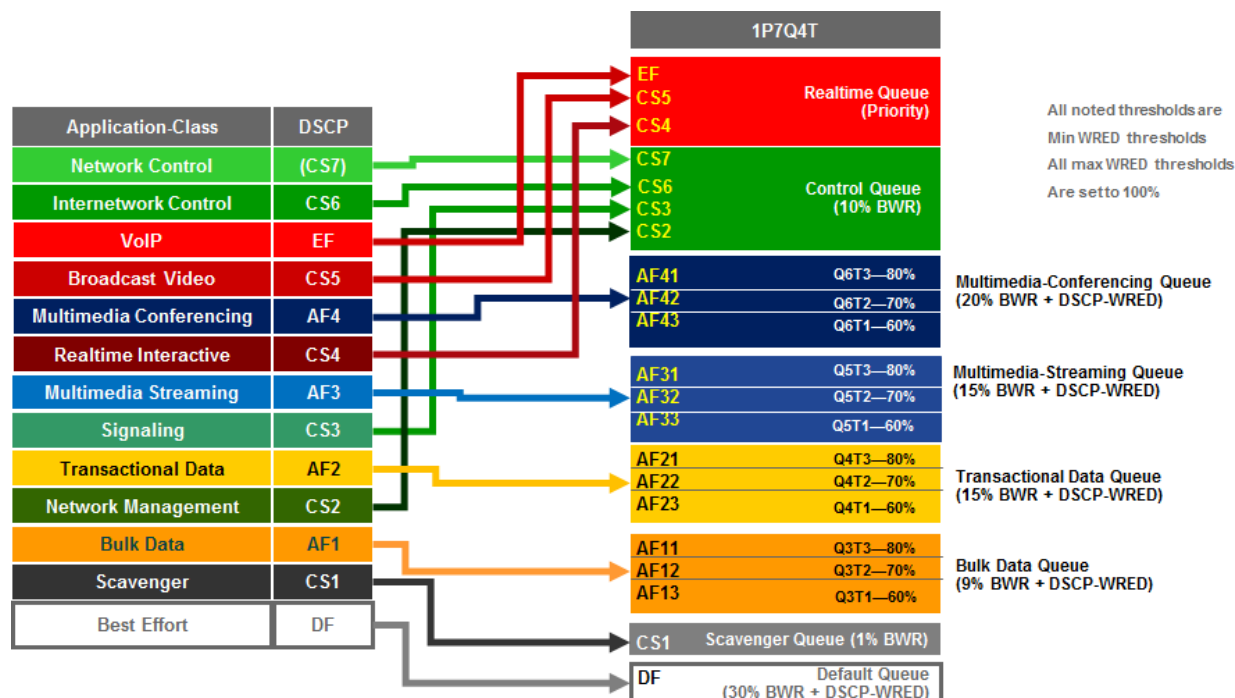
- VS-S2T-10G and VS-S2T-10G-XL with Gigabit Ethernet ports disabled

Disabling of the Gigabit Ethernet ports on the Sup-2T was discussed in the **\*8Q4T Ingress Queuing\*** section above.

1P7Q4T egress queuing for these line cards implements DSCP-to-queue mapping, with DSCP-based WRED for congestion avoidance. APIC-EM release 1.5 and higher does not allow per traffic-class bandwidth allocations to be modified in the egress direction for line cards which support the 1P7Q4T egress queuing structure. However, per traffic-class DSCP markings are supported in the egress direction for line cards which support the 1P7Q4T egress queuing structure, because these line cards support DSCP-to-queue mapping. The default DSCP markings are part of the CVD\_QUEUEING\_PROFILE that is applied by default, unless the network operator applies a custom Queuing Profile to the policy scope containing these line cards.

The following figure shows the default 1P7Q4T egress queuing model.

#### 1. 1P7Q4T Egress Queuing Model—DSCP-to-Queue Mapping with DSCP-based WRED



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-maps for the default 1P7Q4T egress queuing structure.

!

```
class-map type lan-queuing match-any prm-EZQOS_1P7Q4T#REALTIME
match dscp cs4
match dscp cs5
match dscp ef
class-map type lan-queuing match-any prm-EZQOS_1P7Q4T#MM_CONF
match dscp af41
match dscp af42
match dscp af43
class-map type lan-queuing match-any prm-EZQOS_1P7Q4T#MM_STREAM
```



```

match dscp af31
match dscp af32
match dscp af33
class-map type lan-queuing match-any prm-EZQOS_1P7Q4T#CONTROL
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
class-map type lan-queuing match-any prm-EZQOS_1P7Q4T#TRANS_DATA
match dscp af21
match dscp af22
match dscp af23
class-map type lan-queuing match-any prm-EZQOS_1P7Q4T#BULK_DATA
match dscp af11
match dscp af12
match dscp af13
class-map type lan-queuing match-any prm-EZQOS_1P7Q4T#SCAVENGER
match dscp cs1
!
```

The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the default 1P7Q4T egress queuing structure.

```

!
policy-map type lan-queuing prm-dscp#EZQOS_1P7Q4T-OUT
class prm-EZQOS_1P7Q4T#REALTIME
priority
class prm-EZQOS_1P7Q4T#CONTROL
bandwidth remaining percent 10
class prm-EZQOS_1P7Q4T#MM_CONF
bandwidth remaining percent 20
random-detect dscp-based
random-detect dscp 34 percent 80 100
random-detect dscp 36 percent 70 100
random-detect dscp 38 percent 60 100
class prm-EZQOS_1P7Q4T#MM_STREAM
bandwidth remaining percent 15
random-detect dscp-based
```

```
random-detect dscp 26 percent 80 100
random-detect dscp 28 percent 70 100
random-detect dscp 30 percent 60 100
class prm-EZQOS_1P7Q4T#TRANS_DATA
bandwidth remaining percent 15
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 prm-EZQOS_1P7Q4T#BULK_DATA
bandwidth remaining percent 9
random-detect dscp-based
random-detect dscp 10 percent 80 100
random-detect dscp 12 percent 70 100
random-detect dscp 14 percent 60 100
class prm-EZQOS_1P7Q4T#SCAVENGER
bandwidth remaining percent 1
class class-default
random-detect dscp-based
random-detect dscp 0 percent 80 100
!
```

The 1P7Q4T queuing policy-map is provisioned by EasyQoS to all TenGigabitEthernet interfaces, in the egress direction, on the line cards that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are part of a VSL configuration or share an ASIC with other interfaces which are part of a VSL configuration, or interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a TenGigabitEthernet interface is shown below.

```
!
interface TenGigabitEthernetx/x
service-policy type lan-queuing output prm-dscp#EZQOS_1P7Q4T-OUT
!
```

### Custom Queuing Profiles

EasyQoS within APIC-EM release 1.5 and higher provides the network operator the ability to change the both the DSCP marking and the bandwidth allocation of traffic-classes through custom Queuing Profiles in the web-based GUI. Bandwidth allocations configured within custom Queuing Profiles are not implemented on line cards which support the 1P7Q4T egress queuing structure. Instead, the default 1P7Q4T egress queuing structure discussed in

the previous section is always implemented by EasyQoS. However, for line cards which support the 1P7Q4T egress queuing structure, custom DSCP markings are implemented.

Custom Queuing Profiles were discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Figures 37 showed an example of setting the DSCP markings within custom Queuing Profile named EasyQoS\_Lab\_Queueing\_Profile. Within that example, Broadcast Video traffic was configured with a DSCP marking of CS3, and Signaling traffic was configured with a DSCP marking of CS5.

Changing the DSCP markings of traffic-classes within the EasyQoS web-based GUI affects the “match dscp” statements of class-map definitions within the egress queuing policy of line cards which support the 1P7Q4T egress queuing structure. The following output is an example of the modification of the class-map definitions provisioned by EasyQoS, based upon the DSCP markings from the EasyQoS\_Lab\_Queueing\_Profile, shown in the table above. The affected class-map definitions are highlighted in bold.

**class-map type lan-queuing match-any prm-EZQOS\_1P7Q4T#REALTIME**

match dscp cs4

**\*\*match dscp cs3 \*\***

match dscp ef

class-map type lan-queuing match-any prm-EZQOS\_1P7Q4T#MM\_CONF

match dscp af41

match dscp af42

match dscp af43

class-map type lan-queuing match-any prm-EZQOS\_1P7Q4T#MM\_STREAM

match dscp af31

match dscp af32

match dscp af33

**class-map type lan-queuing match-any prm-EZQOS\_1P7Q4T#CONTROL**

match dscp cs2

**match dscp cs5**

match dscp cs6

match dscp cs7

class-map type lan-queuing match-any prm-EZQOS\_1P7Q4T#TRANS\_DATA

match dscp af21

match dscp af22

match dscp af23

class-map type lan-queuing match-any prm-EZQOS\_1P7Q4T#BULK\_DATA

match dscp af11

match dscp af12

match dscp af13

class-map type lan-queuing match-any prm-EZQOS\_1P7Q4T#SCAVENGER

match dscp cs1

!

As can be seen by comparing the the class-map definitions between the default 8Q4T ingress queuing structure and the EasyQoS\_Lab\_Queueing Profile, the Realtime queue which services the Broadcast Video traffic-class matches on CS3 instead of CS5, and the Control queue which services the Signaling traffic-class matches on CS5 instead of CS3.

### 1P7Q8T Egress Queuing

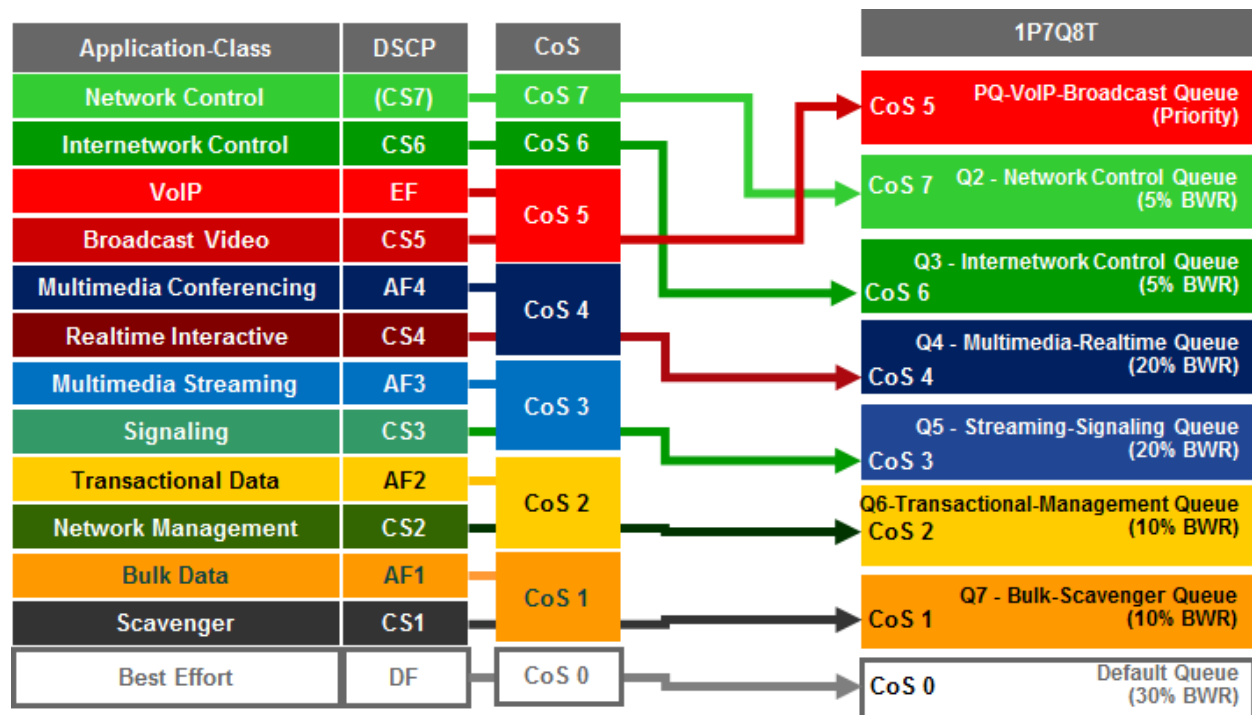
1P7Q8T egress queuing is supported by the following line cards:

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

1P7Q8T egress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. Note that due to the combination of 8 queues and only 8 CoS values, tail-drop thresholds are not used in this design.

The following figure shows the 1P7Q8T egress queuing model.

#### 1. 1P7Q8T Egress Queuing Model—CoS-to-Queue Mapping with CoS-based Tail-Drop



The following configuration, provisioned by APIC-EM EasyQoS, implements the class-maps for the 1P7Q8T egress queuing structure.

!

```
class-map type lan-queuing match-any prm-EZQOS_1P7Q8T#PQ
```

```
match cos 5
```

```
class-map type lan-queuing match-any prm-EZQOS_1P7Q8T#Q2
```

```
match cos 7
```

```
class-map type lan-queuing match-any prm-EZQOS_1P7Q8T#Q3
```

```
match cos 6
```

```
class-map type lan-queuing match-any prm-EZQOS_1P7Q8T#Q4
```

```

match cos 4
class-map type lan-queuing match-any prm-EZQOS_1P7Q8T#Q5
match cos 3
class-map type lan-queuing match-any prm-EZQOS_1P7Q8T#Q6
match cos 2
class-map type lan-queuing match-any prm-EZQOS_1P7Q8T#Q7
match cos 1
!
```

The following configuration, provisioned by APIC-EM EasyQoS, implements the policy-map for the 1P7Q8T egress queuing structure.

```

!
policy-map type lan-queuing prm-dscp#EZQOS_1P7Q8T-OUT
class type lan-queuing prm-EZQOS_1P7Q8T#PQ
priority
class type lan-queuing prm-EZQOS_1P7Q8T#Q2
bandwidth remaining percent 5
class type lan-queuing prm-EZQOS_1P7Q8T#Q3
bandwidth remaining percent 5
class type lan-queuing prm-EZQOS_1P7Q8T#Q4
bandwidth remaining percent 20
class type lan-queuing prm-EZQOS_1P7Q8T#Q5
bandwidth remaining percent 20
class type lan-queuing prm-EZQOS_1P7Q8T#Q6
bandwidth remaining percent 10
class type lan-queuing prm-EZQOS_1P7Q8T#Q7
bandwidth remaining percent 10
class class-default
!
```

The 1P7Q8T queuing policy-map is provisioned by EasyQoS to all TenGigabitEthernet interfaces, in the egress direction, on the line cards that support this queuing structure, with the following exceptions:

- Interfaces which have been excluded from the QoS policy by the network operator, through the EasyQoS web-based GUI. This was discussed in the **\*Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.
- Interfaces which are configured for dual-active fast-hello. This was discussed in the **\*VSS and Dual-Active Fast Hello Configurations\*** section above.

An example of the provisioning to a TenGigabitEthernet interface is shown below.

```

!
interface TenGigabitEthernet x/x/x
```

service-policy type lan-queuing output prm-dscp#EZQOS\_1P7Q8T-OUT

!

### Cisco Catalyst 6880 and 6840 Series Queuing Design

Catalyst 6880 and 6840 Series switch platforms are only supported in the roles of a core-layer or distribution-layer switch within the APIC-EM EasyQoS solution. These platforms feature an embedded supervisor—similar to the Sup2T supervisor within Catalyst 6500 Series switches and the Catalyst 6807-XL switch. Switch ports on the Catalyst 6880 and 6840 Series platforms support a 2P6Q4T ingress and egress queuing structure. Hence the ingress and egress queuing design is the same as discussed in the **\*2P6Q4T Ingress and Egress Queuing\*** section above and will not be duplicated here for brevity.

### Catalyst 6500 Sup720-10GE Queuing Design

The following sections discuss the ingress and egress queuing structures pushed by APIC-EM to the ports of each of the line cards and supervisors supported by EasyQoS for the Catalyst 6500 Series switch with Sup720-10GE supervisor.

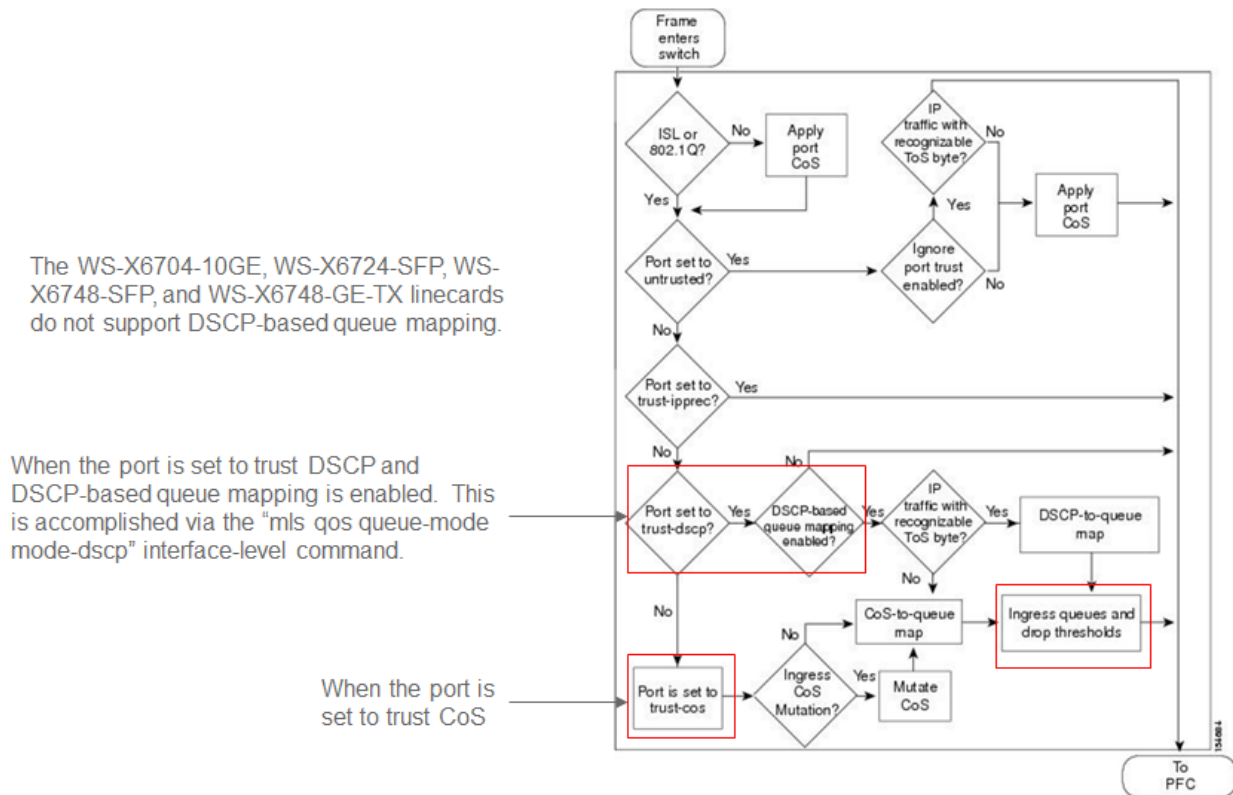
Ingress & egress queuing structures are dependent upon the following:

- The model of the line card
- Whether the line card supports a CFC or DFC (applies to WS-X6704, WS-X6724, and WS-X6748 series line cards)
- Whether the Sup-720 (VS-S720-10G-3C and VS-S720-10G-3CXL) Gigabit Ethernet ports are enabled or disabled

For the Catalyst 6500 Series switch with Supervisor 720-10GE (Sup720), if an unsupported line card is detected within the chassis, the behavior of APIC-EM EasyQoS is to not provision any QoS configuration for the entire platform. For the Catalyst 6500 Series switch with Sup720-10GE, only line cards that have a DFC3C or DFC3CXL daughter card, or a CFC, are supported. Older line cards that support a DFC3A or DFC3B daughter card are not supported. Inserting the line card with one of these older DFC3A or DFC3B daughter cards into the Catalyst 6500 with Sup720-10GE may change the behavior of the platform. Specifically, the platform may “downgrade” its capabilities to the least common denominator for backward compatibility—meaning the lowest line card with a DFC3A or DFC3B installed. These capabilities may not be compatible with the QoS configurations provisioned by APIC-EM EasyQoS. Hence this is not supported, and APIC-EM EasyQoS will not provision any QoS configuration to Catalyst 6500 Series switch with Supervisor 720-10GE (Sup720), if an unsupported line card is detected within the chassis. The network operator will also be notified via the EasyQoS web-based GUI that an unsupported line card was detected within the chassis.

The following figure provides a flowchart that can be used to determine when ingress queuing is applied for the Catalyst 6500 Series with a Sup-720.

1. When is Ingress Queuing Applied?



As can be seen in the figure above, ingress queuing applies under the following conditions:

- When a switch port is set to trust DSCP and DSCP-based queue mapping is enabled via the “mls qos queue-mode mode-DSCP” interface level command.
- When the switch port is set to trust CoS.

Several WS-X67xx Series line cards do not support DSCP-based queue mapping—they only support ingress CoS-to-queue mapping. With the EasyQoS solution, trust of ingress CoS markings is never enabled on switch ports. Trust of ingress DSCP markings is enabled on uplink ports. No trust is enabled for switch ports directly connected to end-user devices. Instead, an ingress classification & marking policy is used for switch ports directly connected to end-user devices.

As a result of this, there really is no need of for APIC-EM EasyQoS to push an ingress queuing policy from APIC-EM to the following line cards. Only DSCP trust will be configured by EasyQoS for these line cards, on uplink ports only.

- WS-X6724-SFP with CFC, WS-X6748-SFP with CFC, WS-X67480GE-TX with CFC, WS-6704-10GE with CFC. These line cards support a 1Q8T ingress queuing structure with CoS-to-queue mapping and CoS-based tail-drop for congestion avoidance.
- The Supervisor 720-10GE itself (VSS-720-10G-3C and VSS-S720-10G-3CXL) when the Gigabit Ethernet ports are active. The Sup720-10GE supports a 2Q4T ingress queuing structure with CoS-to-queue mapping and CoS-based tail-drop for congestion avoidance when the Gigabit Ethernet ports on the supervisor are active.
- WS-X6724-SFP with DFC3C or DFC3CXL, WS-X6748-SFP with DFC3C or DFC3CXL, or WS-X6748-GE-TX with DFC3C or DFC3CXL (WS-F6700-FDC3C or WS-F6700-DFC3CXL). These line cards support an 8Q4T ingress queuing structure with CoS-to-queue mapping and CoS-based tail-drop for congestion avoidance.
- WS-X6704-10GE with DFC3C or DFC3CXL (WS-F6700-FDC3C or WS-F6700-DFC3CXL). These line cards support an 8Q8T ingress queuing structure with CoS-to-queue mapping and CoS-based tail-drop for congestion avoidance.

The Catalyst 6500-E Series platforms with Sup-720 are MLS QoS based, which require QoS to be enabled globally first before configuring any other QoS commands. The following commands, provisioned by APIC-EM EasyQoS, enable QoS globally and set the internal COS-to-DSCP mapping table within the platform.

!

mls qos

! Globally Enables QoS

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

! Maps CoS 5 to 46 (rest are default)

!

- Note: Catalyst 6K and 4K switches are supported in VSS and non-VSS configurations. When operating in a VSS configuration, switch ports that belong to a port-group, which in turn are part of the VSL between the individual switches in the VSS configuration, cannot be configured with any QoS policy. APIC-EM EasyQoS has the ability to identify ports that are part of a VSL and not apply QoS policy.

### 1Q8T Ingress Queuing

1Q8T ingress queuing is supported by the following line cards:

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

The WS-X6724-SFP, WS-X6748-SFP, WS-X6748-GE-TX, and WS-X6704-10GE line cards are supported in the Catalyst 6500 Series Sup-720 with either a CFC or a with a DFC version 3C or 3C-XL upgrade. The DFC is daughter card that sits on the line card itself. Which slots within the Catalyst 6500 Series hold these line cards can be displayed via the “show module” exec-level command. An example of the output of the “show module” command is shown below, with a WS-X6748-GE-TX line card with a CFC in slot 3 and a WS-X6748-GE-TX with a DFC3CXL in slot 4, highlighted.

6504E-Sup720-10G#show module

Mod Ports Card Type Model Serial No.

1 5 Supervisor Engine 720 10GE (Active) VS-S720-10G SAL14480SAC

2 5 Supervisor Engine 720 10GE (Cold) VS-S720-10G SAL12373BV5

**3 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL1418GV6P**

**4 48 CEF720 48 port 10/100/1000mb Ethernet WS-X6748-GE-TX SAL1440VP6T**

Mod MAC addresses Hw Fw Sw Status

1 c47d.4ffe.68d8 to c47d.4ffe.68df 3.2 8.5(4) 12.2(33)SXI4 Ok

2 001e.4af8.4498 to 001e.4af8.449f 2.0 8.5(2) 12.2(33)SXI9 Ok

3 5475.d063.0340 to 5475.d063.036f 3.4 12.2(18r)S1 12.2(33)SXI4 Ok

4 1cdf.0f90.4c30 to 1cdf.0f90.4c5f 3.4 12.2(18r)S1 12.2(33)SXI4 Ok

Mod Sub-Module Model Serial Hw Status

1 Policy Feature Card 3 VS-F6K-PFC3CXL SAL14480QT0 1.2 Ok

1 MSFC3 Daughterboard VS-F6K-MSFC3 SAL14470GJ9 5.1 Ok

2 Policy Feature Card 3 VS-F6K-PFC3CXL SAL12383WAN 1.0 Ok



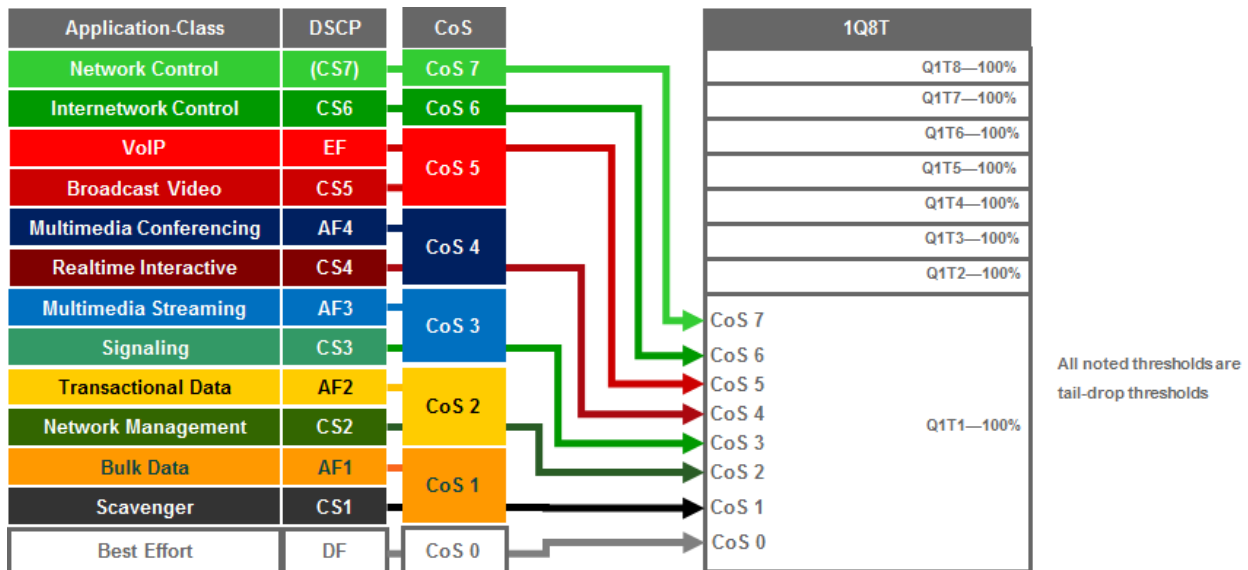
2 MSFC3 Daughterboard VS-F6K-MSFC3 SAL12373ADR 1.0 Ok

**3 Centralized Forwarding Card WS-F6700-CFC SAL1412DA30 4.1 Ok**

**4 Distributed Forwarding Card WS-F6700-DFC3CXL SAL1436SZX7 1.6 Ok**

1Q8T ingress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. The following figure shows the ingress queuing model implemented by the EasyQoS solution for these line cards.

1. Queuing for WS-X6724-SFP with CFC, WS-X6748-SFP with CFC, WS-X6748-GE-TX with CFC, and WS-X6704-10GE with CFC when “trust cos” is Not Configured



An example of the configuration pushed by APIC-EM for each of the ports on these line cards is shown below.

!

```
interface GigabitEthernet x/x/x
```

! Switch ports connected to end-user devices

!

```
interface TenGigabitEthernet x/x/x
```

```
mls qos trust dscp
```

! Switch ports functioning as uplink ports

!

As can be seen, DSCP trust is extended to switch ports functioning as uplink ports. These would typically correspond to TenGigabitEthernet ports on the line card. Because no trust is extended on ingress switch ports, all ingress traffic is treated as if it had a value of CoS 0 and mapped to Q1T1 with a tail-drop threshold of 100%.

## 2Q4T Ingress Queuing

2Q4T ingress queuing is supported by the following line cards:

- All ports on the VS-S720-10G-3C and VS-S720-10G-3CXL (Supervisor 720) when the Gigabit Ethernet ports are enabled.

The Gigabit Ethernet ports on the Sup-720 are enabled with the following global configuration command.

!

no mls qos 10g-only

!

APIC-EM EasyQoS does not set this command but will look to see if this command has been set by the network operator, in order to determine the correct queuing structure to apply to ports on the Sup720-10GE supervisor. The default setting is for the Gigabit Ethernet ports on the Sup-720 to be enabled, so this command will not appear in the configuration.

The status of whether the Gigabit Ethernet ports are enabled or disabled can be displayed via the exec-level “show mls qos module x” command, where “x” refers to the slot with the Sup-720. An example of the output from the command is shown below:

```
6504E-Sup720-10G#show mls qos module 1
```

QoS is enabled globally

Policy marking depends on port\_trust

QoS ip packet DSCP rewrite enabled globally

QoS serial policing mode disabled globally

Input mode for GRE Tunnel is Pipe mode

Input mode for MPLS is Pipe mode

QoS Trust state is DSCP on the following interface:

Gi1/1 Gi1/2 Gi1/3 Gi2/1 Gi2/2 Gi2/3 Gi3/31 Po10

Vlan or Portchannel(Multi-Earl) policies supported: Yes

Egress policies supported: Yes

QoS 10g-only mode supported: Yes [Current mode: Off]

— Module [1] —

QoS global counters:

Total packets: 3920723

IP shortcut packets: 2196428

Packets dropped by policing: 0

IP packets with TOS changed by policing: 2

IP packets with COS changed by policing: 2

Non-IP packets with COS changed by policing: 0

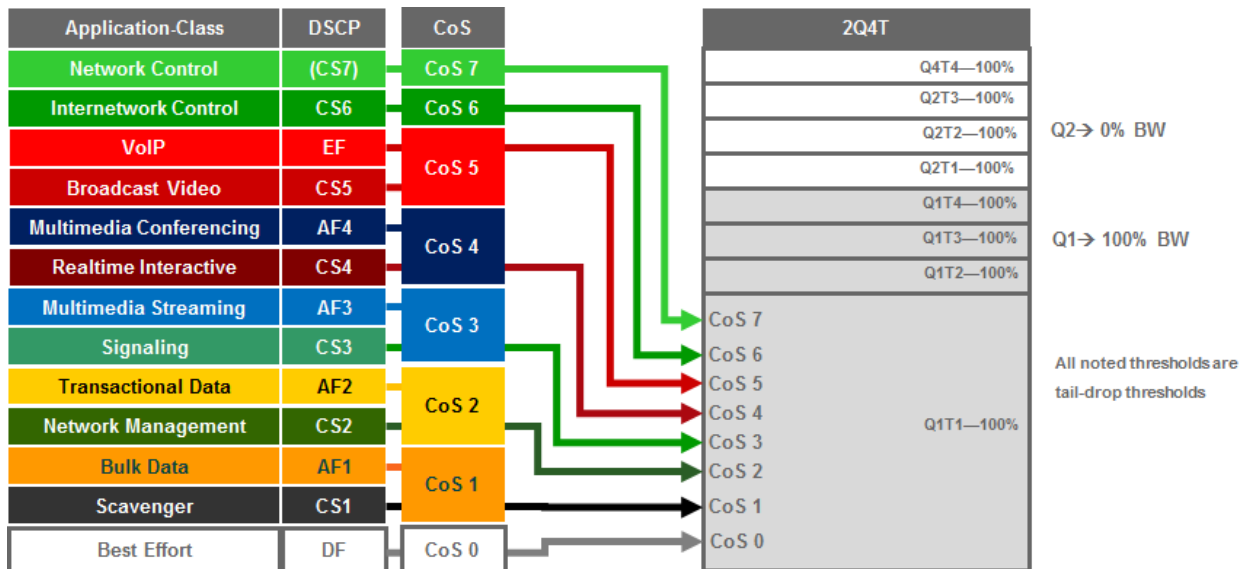
MPLS packets with EXP changed by policing: 0

A setting of “Current mode: off” means that the Gigabit Ethernet ports are enabled.

2Q4T ingress queuing for the Sup-720 implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. The Sup-720 interfaces do not support DSCP-based queue mapping when the 1 Gbps interfaces are enabled—they only support ingress CoS-to-queue mapping. With the EasyQoS solution, trust of ingress CoS markings is never enabled. Trust of ingress DSCP markings is enabled on uplink ports. As a result of this, there really is no need of provisioning the 2Q4T ingress queuing policy from APIC-EM EasyQoS to the Sup-720 when the 1 Gbps ports are enabled.

The following figure shows the ingress queuing model implemented by APIC-EM EasyQoS for the Sup-720-10GE when the 1 Gbps ports are enabled.

1. Queuing for VS-S720-10G-3C and VS-S720-10G-3CXL with Gigabit Ethernet ports enabled and when “trust cos” is Not Configured



An example of the configuration provisioned by APIC-EM EasyQoS for the Sup720-10GE ports is shown below.

!

```
interface GigabitEthernet x/x/x
```

```
mls qos trust dscp
```

! Switch ports functioning as uplink ports

!

```
interface TenGigabitEthernet x/x/x
```

```
mls qos trust dscp
```

! Switch ports functioning as uplink ports

!

Cisco does not recommend connecting end-user devices to any ports on the Sup720-10GE. Hence, all ports on the Sup720-10GE are assumed to be uplink ports by EasyQoS.

Because no trust is extended on ingress switch ports, all ingress traffic is treated as if it had a value of CoS 0 and mapped to Q1T1 with a tail-drop threshold of 100%.

It should be noted that QoS service policies cannot be applied to TenGigabitEthernet ports on the Sup-720 when the TenGigabitEthernet ports are part of a port-channel group that is part of a VSL. Switch ports can be identified as part of a VSL based upon the configuration. An example of this is shown below.

!

```
interface Port-channel20
```

```
no ip address
```

```
switch virtual link 1
```

```
no platform qos channel-consistency
```

~

```
interface TenGigabitEthernet1/1/4
no ip address
channel-group 20 mode on
!
interface TenGigabitEthernet1/1/5
no ip address
channel-group 20 mode on
!
```

Physical interfaces are assigned to a port-group via the “channel-group” interface-level command. Port-channel interfaces are assigned to a VSL via the “switch virtual link” interface-level command, as shown in the configuration above.

Note also that, as with the Sup-2T, EasyQoS cannot apply any QoS policy to either the TenGigabitEthernet or Gigabit Ethernet ports on the Sup-720 when the TenGigabitEthernet ports are part of a VSL.

#### 2Q8T Ingress Queuing

2Q8T ingress queuing is supported by the following line cards:

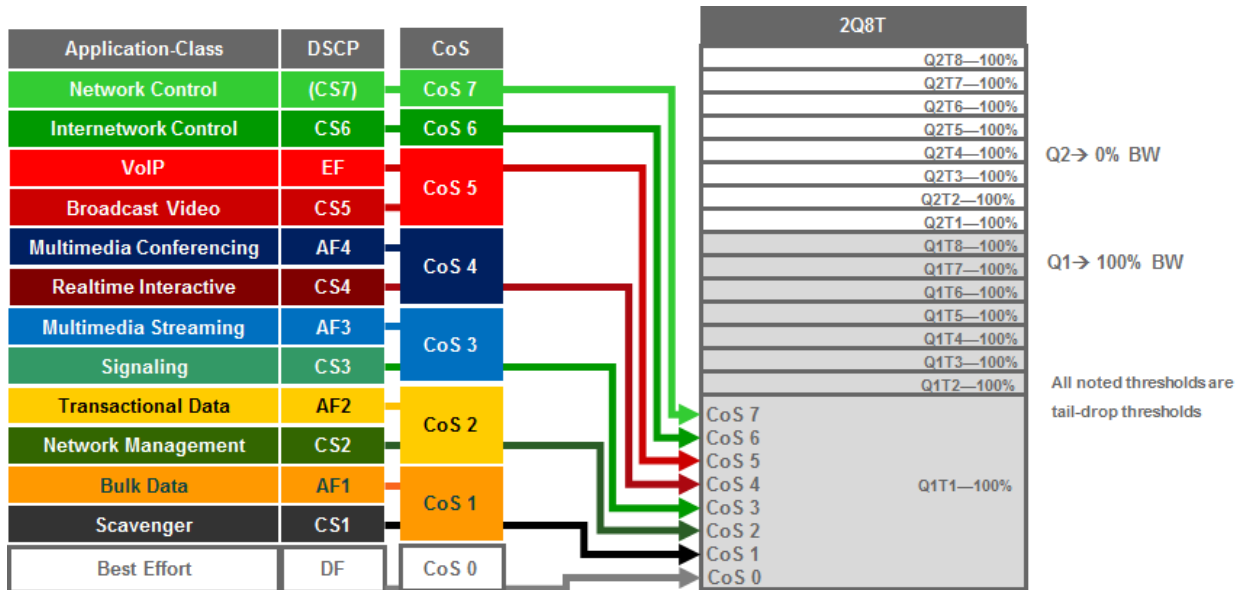
- WS-X6724-SFP with a DFC3C or DFC3CXL (WS-F6700-DFC3C or WS-F6700-DFC3CXL)
- WS-X6748-SFP with a DFC3C or DFC3CXL
- WS-X6748-GE-TX with a DFC3C or DFC3CXL

How to determine if a line card has a CFC versus a DFC3C or DFC3CXL was discussed in the **\*1Q8T Ingress Queuing\*** section above.

2Q8T ingress queuing for the Sup-720 implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX with DFC3C/DFC3CXL line cards do not support DSCP-based queue mapping—they only support ingress CoS-to-queue mapping. With the EasyQoS solution, trust of ingress CoS markings is never enabled. Trust of ingress DSCP markings is enabled on uplink ports. As a result of this, there really is no need of provisioning the 2Q8T ingress queuing policy from APIC-EM EasyQoS to the line cards with this queuing structure.

The following figure shows the ingress queuing model implemented by APIC-EM EasyQoS solution for the WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX with DFC3C/DFC3CXL line cards.

1. Queuing for WS-X6724-SFP, WS-X6748-SFP, WS-X6748-GE-TX with a DFC3C or DFC3CXL when “trust cos” is not configured



An example of the configuration pushed by APIC-EM EasyQoS for the WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX with DFC3C/DFC3CXL line card ports is shown below.

!

```
interface GigabitEthernet x/x/x
```

! Switch ports connected to end-user devices

!

```
interface GigabitEthernet x/x/x
```

```
mls qos trust dscp
```

! Switch ports functioning as uplink ports

!

Because the WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX with DFC3C/DFC3CXL line card ports are all Gigabit Ethernet ports, generally these ports are assumed to be connected to end-user devices. When these ports are not used for uplinks, DSCP trust is not configured. If ports are used for uplinks, then DSCP trust is configured.

Because no trust CoS is extended on ingress switch ports and DSCP-to-queue mapping is not supported on these line cards, all ingress traffic is treated as if it had a value of CoS 0 and mapped to Q1T1 with a tail-drop threshold of 100%.

### 8Q4T Ingress Queuing

8Q4T ingress queuing is supported by the following line cards:

- WS-X6708-10G-3C, WS-X6708-10G-3CXL
- VS-S720-10G-3C with TenGigabitEthernet ports 4 & 5 when Gigabit Ethernet ports are inactive

The Gigabit Ethernet ports on the Sup-720 are enabled with the following global configuration command.

!

```
mls qos 10g-only
```

!

APIC-EM EasyQoS does not set this command but will look to see if this command has been set by the network operator, in order to determine the correct queuing structure to apply to ports on the Sup720-10GE supervisor. The

default setting is for the Gigabit Ethernet ports on the Sup-720 to be enabled, so this command will appear in the configuration when the Gigabit Ethernet ports are disabled.

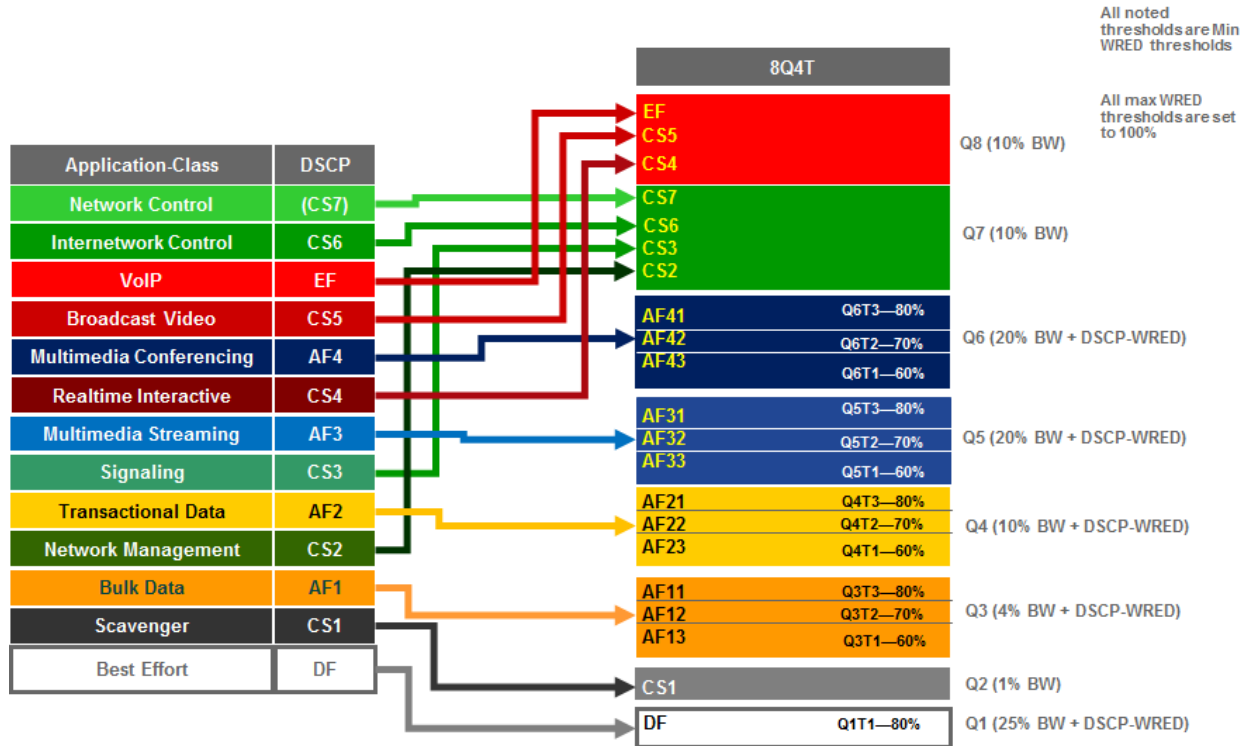
The status of whether the Gigabit Ethernet ports are enabled or disabled can be displayed via the exec-level “show mls qos module x” command, where “x” refers to the slot with the Sup-720. An example of the output from the command is shown below:

```
6504E-Sup720-10G#show mls qos module 1
QoS is enabled globally
Policy marking depends on port_trust
QoS ip packet DSCP rewrite enabled globally
QoS serial policing mode disabled globally
Input mode for GRE Tunnel is Pipe mode
Input mode for MPLS is Pipe mode
QoS Trust state is DSCP on the following interface:
Gi1/1 Gi1/2 Gi1/3 Gi2/1 Gi2/2 Gi2/3 Gi3/31 Po10
Vlan or Portchannel(Multi-Earl) policies supported: Yes
Egress policies supported: Yes
QoS 10g-only mode supported: Yes [Current mode: On]
— Module [1] —
QoS global counters:
Total packets: 3920723
IP shortcut packets: 2196428
Packets dropped by policing: 0
IP packets with TOS changed by policing: 2
IP packets with COS changed by policing: 2
Non-IP packets with COS changed by policing: 0
MPLS packets with EXP changed by policing: 0
```

A setting of “Current mode: On” means that the Gigabit Ethernet ports are disabled.

8Q4T ingress queuing for these line cards implements DSCP-to-queue mapping, with DSCP-based WRED for congestion avoidance. The following figure shows the 8Q4T ingress queuing model.

1. 8Q4T Ingress Queuing Models—DSCP-to-Queue with DSCP-based WRED



The following example configuration implements the 8Q4T ingress queuing structure to a TenGigabitEthernet interface.

!

```

interface TenGigabitEthernet x/x/x
 mls qos queue-mode mode-dscp
 mls qos trust dscp
 rcv-queue queue-limit 25 10 10 10 10 10 10 15
 rcv-queue bandwidth 25 1 4 10 20 20 10 10
 rcv-queue random-detect 1
 no rcv-queue random-detect 2
 rcv-queue random-detect 3
 rcv-queue random-detect 4
 rcv-queue random-detect 5
 rcv-queue random-detect 6
 no rcv-queue random-detect 7
 no rcv-queue random-detect 8
 rcv-queue random-detect max-threshold 1 100 100 100 100
 rcv-queue random-detect min-threshold 1 80 100 100 100
 rcv-queue random-detect max-threshold 3 100 100 100 100
 rcv-queue random-detect min-threshold 3 60 70 80 100

```

```
rcv-queue random-detect max-threshold 4 100 100 100 100
rcv-queue random-detect min-threshold 4 60 70 80 100
rcv-queue random-detect max-threshold 5 100 100 100 100
rcv-queue random-detect min-threshold 5 60 70 80 100
rcv-queue random-detect max-threshold 6 100 100 100 100
rcv-queue random-detect min-threshold 6 60 70 80 100
rcv-queue dscp-map 1 1 0
rcv-queue dscp-map 2 1 8
rcv-queue dscp-map 3 1 14
rcv-queue dscp-map 3 2 12
rcv-queue dscp-map 3 3 10
rcv-queue dscp-map 4 1 22
rcv-queue dscp-map 4 2 20
rcv-queue dscp-map 4 3 18
rcv-queue dscp-map 5 1 30
rcv-queue dscp-map 5 2 28
rcv-queue dscp-map 5 3 26
rcv-queue dscp-map 6 1 38
rcv-queue dscp-map 6 2 36
rcv-queue dscp-map 6 3 34
rcv-queue dscp-map 7 1 16 24 48 56
rcv-queue dscp-map 8 1 32 40 46
```

!

For all of the line cards that support the 8Q4T ingress queuing structure listed above, the ports are assumed to be uplink ports, because they are all TenGigabitEthernet ports. If the Catalyst 6500 Series with Sup-720 is deployed as a distribution or core switch, and the link connecting the switch port is not a trunk port, then all ingress traffic will not have an 802.1p header. However, because these line cards support DSCP-to-queue mapping, ingress traffic will still be mapped into the correct queue based on the DSCP value of the IP packets.

### 8Q8T Ingress Queuing

8Q8T ingress queuing is supported by the following line cards:

- WS-X6704-10GE with a DFC3C or DFC3XL (WS-F6700-DFC3C or WS-F6700-DFC3XL)

How to determine if a line card has a CFC or DFC3C/3CXL was discussed in the **\*1Q8T Ingress Queuing\*** section above.

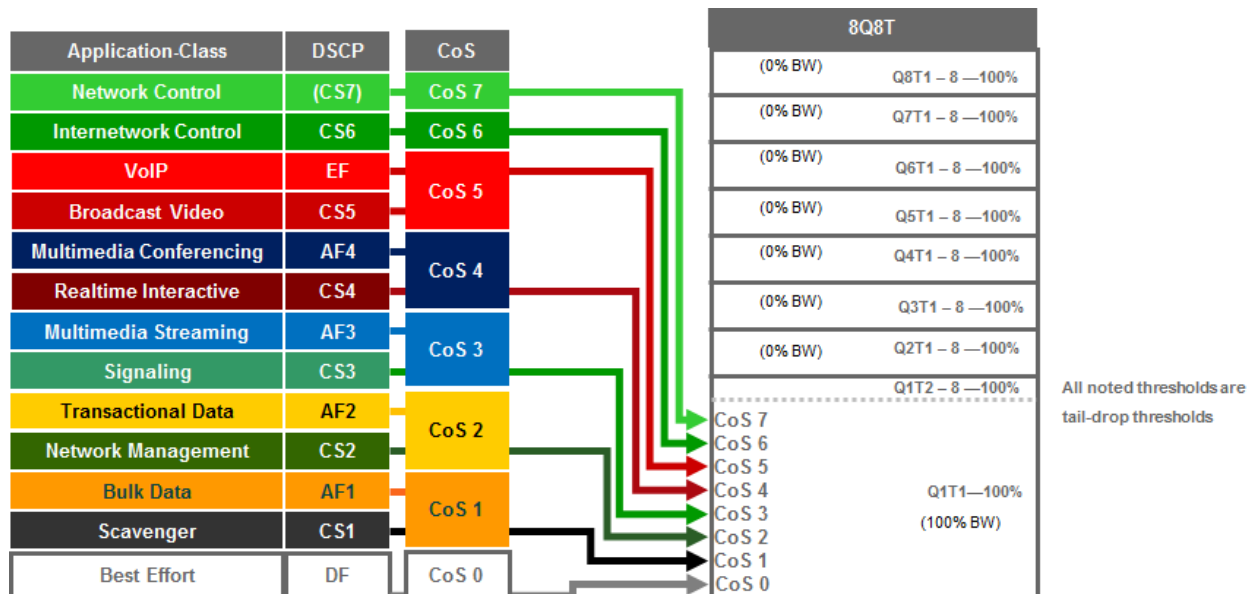
8Q8T ingress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance.

WS-X67xx Series line cards do not support DSCP-based queue mapping—they only support ingress CoS-to-queue mapping. With the EasyQoS solution, trust of ingress CoS markings is never enabled on switch ports. Trust of ingress DSCP markings is enabled on uplink ports. As a result of this, there really is no need of provisioning the 8Q8T ingress queuing policy from APIC-EM EasyQoS to the WS-X6704-10GE with DFC3C/DFC3XL line cards.



The following figure shows the ingress queuing model implemented by APIC-EM EasyQoS for these line cards.

1. Queuing for WS-X6704-10GE with a DFC3 or DFC3XL when “trust cos” is Not Configured



An example of the configuration provisioned by APIC-EM EasyQoS for these line cards is shown below.

!

```
interface TenGigabitEthernet x/x/x
```

```
mls qos trust dscp
```

! Switch ports functioning as uplink ports

!

As can be seen, DSCP trust is extended to switch ports functioning as uplink ports. Typically all ports on the WS-X6704-10GE line card would be assumed to be uplink ports, because they are all TenGigabitEthernet ports.

Because no trust CoS is extended on ingress switch ports and the line card does not support DSCP-to-queue mapping, all ingress traffic is treated as if it had a value of CoS 0, and mapped to Q1T1 with a tail-drop threshold of 100%.

### 1P3Q8T Egress Queuing

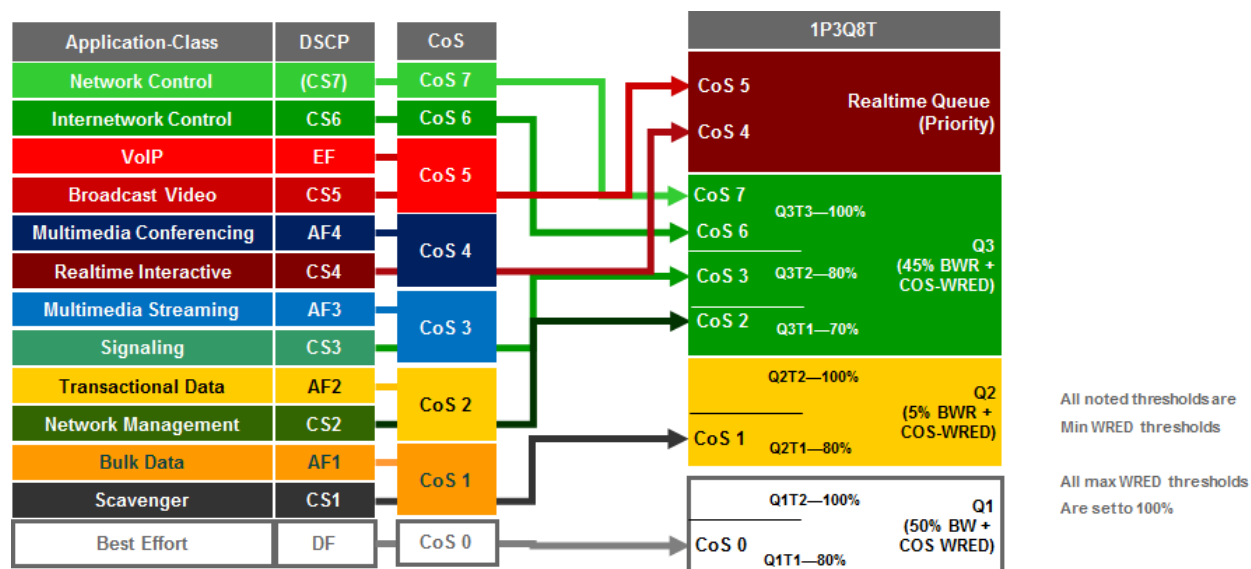
1P3Q8T egress queuing is supported by the following line cards:

- WS-X6724-SFP, WS-X6748-SFP, and WS-X6748-GE-TX with either CFC or DFC3/DFC3XL

1P3Q8T egress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance.

The following figure shows the 1P3Q8T egress queuing model.

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



An example of the configuration provisioned by APIC-EM EasyQoS to a port on these line cards is shown below.

!

```
interface GigabitEthernet x/x/x
wrr-queue queue-limit 40 15 40
priority-queue queue-limit 15
wrr-queue bandwidth 50 5 45
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100 100 100 100 100 100
wrr-queue random-detect max-threshold 3 100 100 100 100 100 100 100 100 100
wrr-queue random-detect min-threshold 3 70 80 100 100 100 100 100 100 100
wrr-queue cos-map 1 1 0
wrr-queue cos-map 2 1 1
wrr-queue cos-map 3 1 2
wrr-queue cos-map 3 2 3
wrr-queue cos-map 3 3 6 7
priority-queue cos-map 1 4 5
!
```

Due to the internal ASIC structure of the ports on the WS-X6748-SFP and WS-X6748-GE-TX line cards, the egress queuing structure of the ports cannot be configured independently. Instead, APIC-EM EasyQoS will apply the queuing policy to groups of ports on the line card.

### 1P3Q4T Egress Queuing

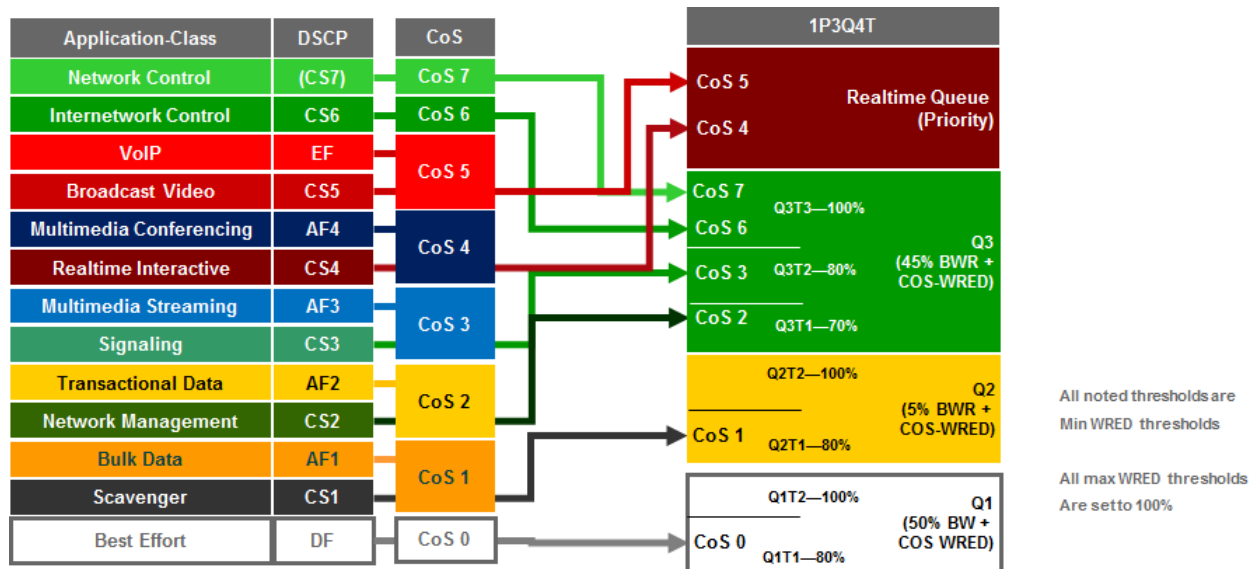
1P3Q4T egress queuing is supported by the following line cards:

- All ports on the VS-S720-10G-3C and VS-S720-10G-3CXL when the Gigabit Ethernet ports are enabled

Enabling of the Gigabit Ethernet ports on the Sup-2T was discussed in the **\*2Q4T Ingress Queuing\*** section above.

1P3Q4T egress queuing for the Sup-720 implements CoS-to-queue mapping, with CoS-based WRED for congestion avoidance. The following figure shows the 1P3Q4T egress queuing model.

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



An example of the configuration provisioned by APIC-EM EasyQoS to both a Gigabit Ethernet and a TenGigabitEthernet port on these line cards is shown below.

!

```
interface GigabitEthernet x/x/x
wrr-queue queue-limit 40 15 40
priority-queue queue-limit 15
wrr-queue bandwidth 50 5 45
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 100 100 100 100
```

```
wrr-queue random-detect min-threshold 3 70 80 100 100
wrr-queue cos-map 1 1 0
wrr-queue cos-map 2 1 1
wrr-queue cos-map 3 1 2
wrr-queue cos-map 3 2 3
wrr-queue cos-map 3 3 6 7
priority-queue cos-map 1 4 5
!
interface TenGigabitEthernet x/x/x
wrr-queue queue-limit 40 15 40
priority-queue queue-limit 15
wrr-queue bandwidth 50 5 45
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 100 100 100 100
wrr-queue random-detect min-threshold 3 70 80 100 100
wrr-queue cos-map 1 1 0
wrr-queue cos-map 2 1 1
wrr-queue cos-map 3 1 2
wrr-queue cos-map 3 2 3
wrr-queue cos-map 3 3 6 7
priority-queue cos-map 1 4 5
!
```

As discussed in the **\*2Q4T Ingress Queuing\*** section above, QoS service policies cannot be applied to TenGigabitEthernet ports on the Sup-720, when the TenGigabitEthernet ports are part of a port-channel group that is part of a VSL. Also, QoS service policies cannot be applied to Gigabit Ethernet ports on the Sup-720 when the TenGigabitEthernet ports are part of a VSL.

Finally, due to the internal ASIC structure of the ports on the Sup-720, the egress queuing structure of the ports cannot be configured independently. Instead, APIC-EM EasyQoS will apply the queuing policy to groups of ports on the supervisor. This was discussed in the **\*2Q4T Ingress Queuing\*** section above, as well.

#### 1P7Q4T Egress Queuing

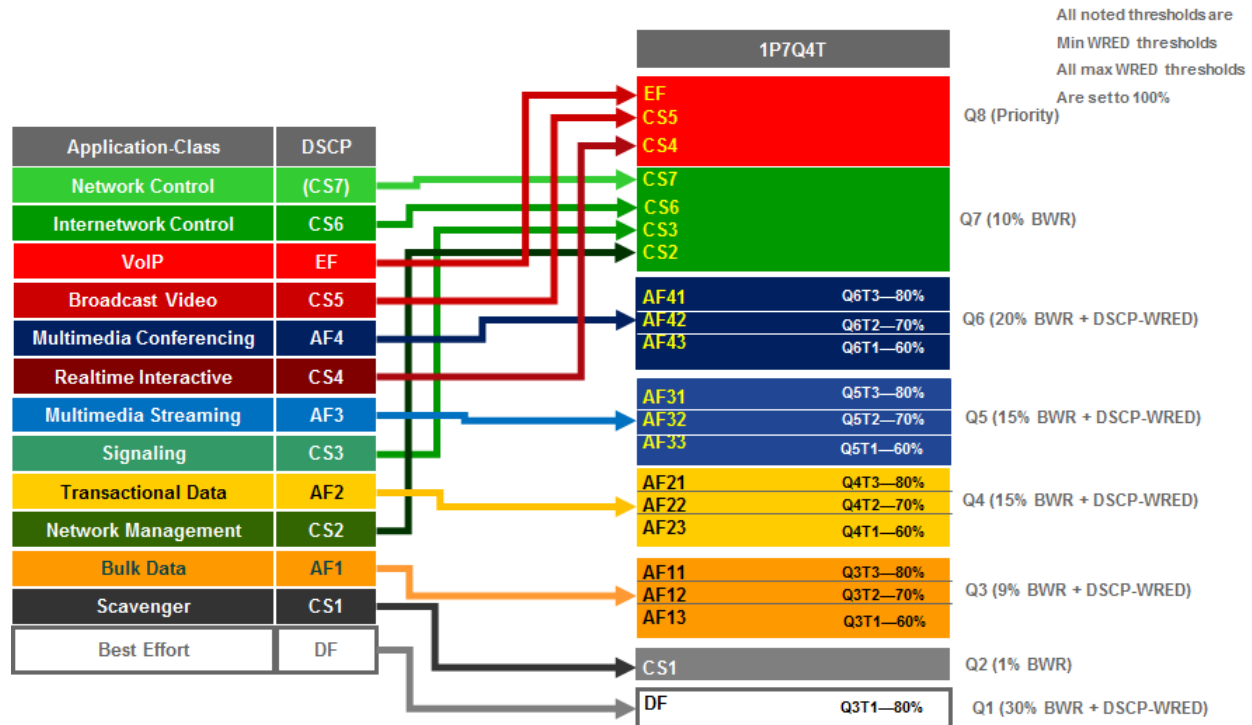
1P7Q4T egress queuing is supported by the following line cards:

- WS-X6708-10G-3C and WS-X6708-10G-3CXL

- VS-S720-10G-3C and VS-S720-10G-3CXL TenGigabitEthernet ports when the Gigabit Ethernet ports are inactive

1P7Q4T egress queuing for these line cards implements DSCP-to-queue mapping, with DSCP-based WRED for congestion avoidance. The following figure shows the 1P7Q4T egress queuing model.

#### 1. 1P7Q4T Egress Queuing Models—DSCP-to-Queue Mapping with DSCP-based WRED



An example of the configuration provisioned by APIC-EM EasyQoS to a TenGigabitEthernet port on these line cards is shown below.

!

```
interface range TenGigabitEthernet x/x-x
wrr-queue queue-limit 25 10 10 10 10 10 10
wrr-queue bandwidth 30 1 9 15 15 20 10
priority-queue queue-limit 15
wrr-queue random-detect 1
no wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
no wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
```

```
wrr-queue random-detect max-threshold 3 100 100 100 100
wrr-queue random-detect min-threshold 3 60 70 80 100
wrr-queue random-detect max-threshold 4 100 100 100 100
wrr-queue random-detect min-threshold 4 60 70 80 100
wrr-queue random-detect max-threshold 5 100 100 100 100
wrr-queue random-detect min-threshold 5 60 70 80 100
wrr-queue random-detect max-threshold 6 100 100 100 100
wrr-queue random-detect min-threshold 6 60 70 80 100
mls qos queue-mode mode-dscp
wrr-queue dscp-map 1 1 0
wrr-queue dscp-map 2 1 8
wrr-queue dscp-map 3 1 14
wrr-queue dscp-map 3 2 12
wrr-queue dscp-map 3 3 10
wrr-queue dscp-map 4 1 22
wrr-queue dscp-map 4 2 20
wrr-queue dscp-map 4 3 18
wrr-queue dscp-map 5 1 30
wrr-queue dscp-map 5 2 28
wrr-queue dscp-map 5 3 26
wrr-queue dscp-map 6 1 38
wrr-queue dscp-map 6 2 36
wrr-queue dscp-map 6 3 34
wrr-queue dscp-map 7 1 16 24 48 56
priority-queue dscp-map 1 32 40 46
!
```

### 1P7Q8T Egress Queuing

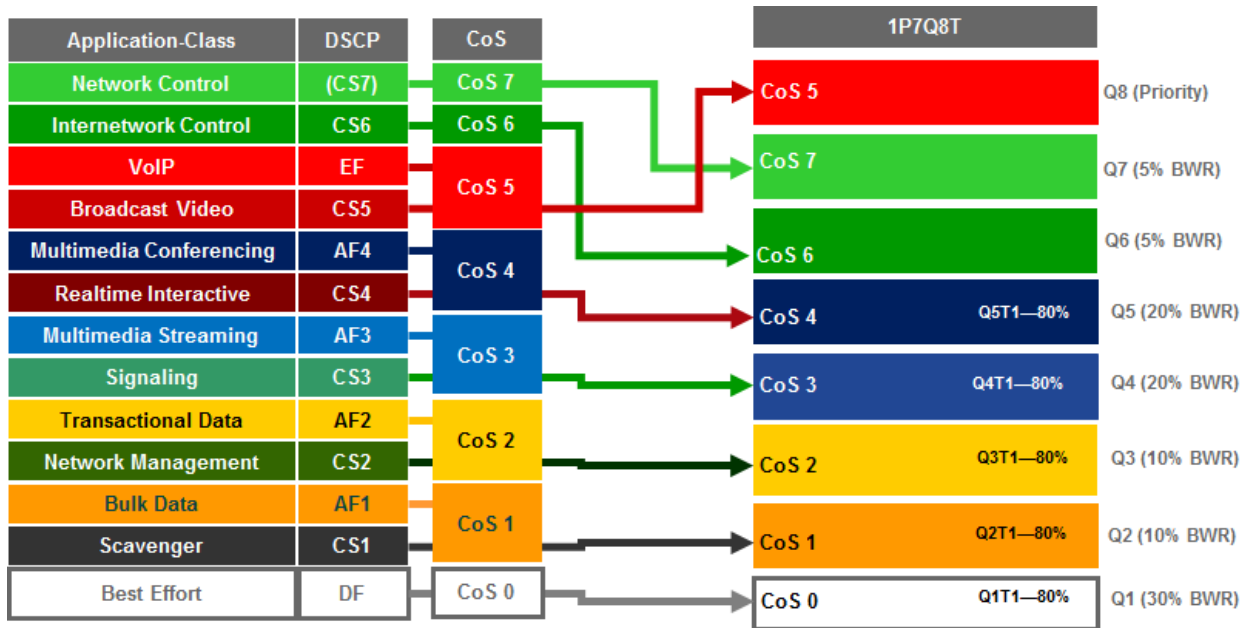
1P7Q8T egress queuing is supported by the following line cards:

- WS-X6704-10GE with either CFC or DFC3/DFC3XL

1P7Q8T egress queuing for these line cards implements CoS-to-queue mapping, with CoS-based tail-drop for congestion avoidance. Note that due to the combination of 8 queues and only 8 CoS values, tail-drop thresholds are not used in this design.

The following figure shows the 1P7Q8T egress queuing model.

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



An example of the configuration provisioned by APIC-EM EasyQoS to a TenGigabitEthernet port on these line cards is shown below.

!

```

interface TenGigabitEthernet x/x/x
wrr-queue queue-limit 25 10 10 15 15 5 5
wrr-queue bandwidth 30 10 10 20 20 5 5
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
no wrr-queue random-detect 6
no wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100 100 100
wrr-queue random-detect max-threshold 3 100 100 100 100 100 100
wrr-queue random-detect min-threshold 3 80 100 100 100 100 100
wrr-queue random-detect max-threshold 4 100 100 100 100 100 100
wrr-queue random-detect min-threshold 4 80 100 100 100 100 100
wrr-queue random-detect max-threshold 5 100 100 100 100 100 100

```

```
wrr-queue random-detect min-threshold 5 80 100 100 100 100 100 100 100
wrr-queue cos-map 1 1 0
wrr-queue cos-map 2 1 1
wrr-queue cos-map 3 1 2
wrr-queue cos-map 4 1 3
wrr-queue cos-map 5 1 4
wrr-queue cos-map 6 1 6
wrr-queue cos-map 7 1 7
priority-queue cos-map 1 5
!
```

### Cisco Nexus 7000/7700 Queuing Design

The only role Nexus 7000 and 7700 Series switches have within the EasyQoS solution is as a campus-core switch. Only ingress and egress queuing policies are pushed from APIC-EM to these switches. No ingress classification & marking policies are pushed from APIC-EM to Nexus 7000 and 7700 Series switches

The following sections detail the ingress and egress queuing structures pushed by APIC-EM to the ports of each of the Nexus 7000 and 7700 Series modules supported by EasyQoS. Ingress & egress queuing structures are dependent upon the type of module and the chassis in which they are installed (Nexus 7000 versus Nexus 7700), as shown below:

- M2 Series modules are only supported on Nexus 7000
- 8Q2T-IN/1P7Q4T-OUT queuing
- F2 Series modules are only supported on Nexus 7000
- 4Q1T-IN/1P3Q1T-OUT queuing
- F2E Series modules are supported on both the Nexus 7000 and the Nexus 7700
- F2E Series modules on the Nexus 7000 have identical queuing to F2 Series modules (4Q1T-IN/1P3Q1T-OUT)
- F2E Series modules on the Nexus 7700 have identical queuing to F3 Series modules (4Q1T-IN/1P7Q1T-OUT)
- F3 Series modules are supported on both the Nexus 7000 and the Nexus 7700
- F3 Series modules on the Nexus 7000 have identical queuing to F2 Series modules (4Q1T-IN/1P3Q1T-OUT)
- F3 Series modules on the Nexus 7700 implement 4Q1T-IN/1P7Q1T-OUT queuing
- M3 Series modules are only supported on the Nexus 7700
- 4Q1T-IN/1P7Q1T-OUT queuing
- Note: In APIC-EM release 1.3 and higher, EasyQoS only supports the Nexus 7000 or 7700 Series platforms configured with a single default VDC. Changing network QoS requires being logged into the default VDC. Changes to the system class-maps are made only on the default VDC but take effect immediately across all VDCs. Queuing policy maps are defined per VDC.

#### M2 Series Modules on the Nexus 7000

M2 Series modules consist of the following:

- N7K-M224XP-23L
- N7K-M206FQ-23L
- N7K-M202CF-22L



These modules are only supported on the Nexus 7000 series chassis. M2 Series modules implement 8Q2T ingress queuing and 1P7Q4T egress queuing.

#### Nexus 7000 8Q2T Ingress Queuing

As of NX OS software version 6.2.2 and higher, ingress DSCP-to-Queue mapping is supported on M2 Series modules and must be configured via the following global configuration command.

!

```
hardware qos dscp-to-queue ingress module-type all
```

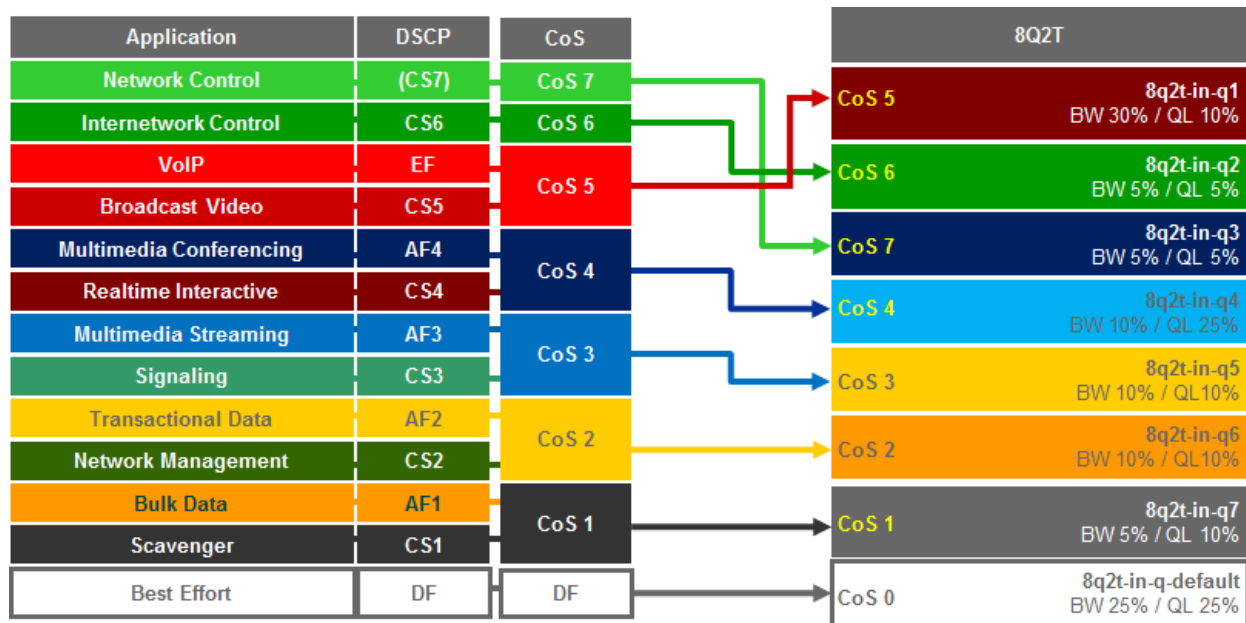
!

EasyQoS will provision this command to enable DSCP-to-Queue mapping support on the M2 Series modules.

Trust of both CoS and DSCP values is implicit on the Nexus 7000 Series. No explicit configuration is required to enable trust. Because both CoS and DSCP values are trusted, queuing models for both CoS-to-queue mapping and DSCP-to-queue mapping need to be configured by EasyQoS.

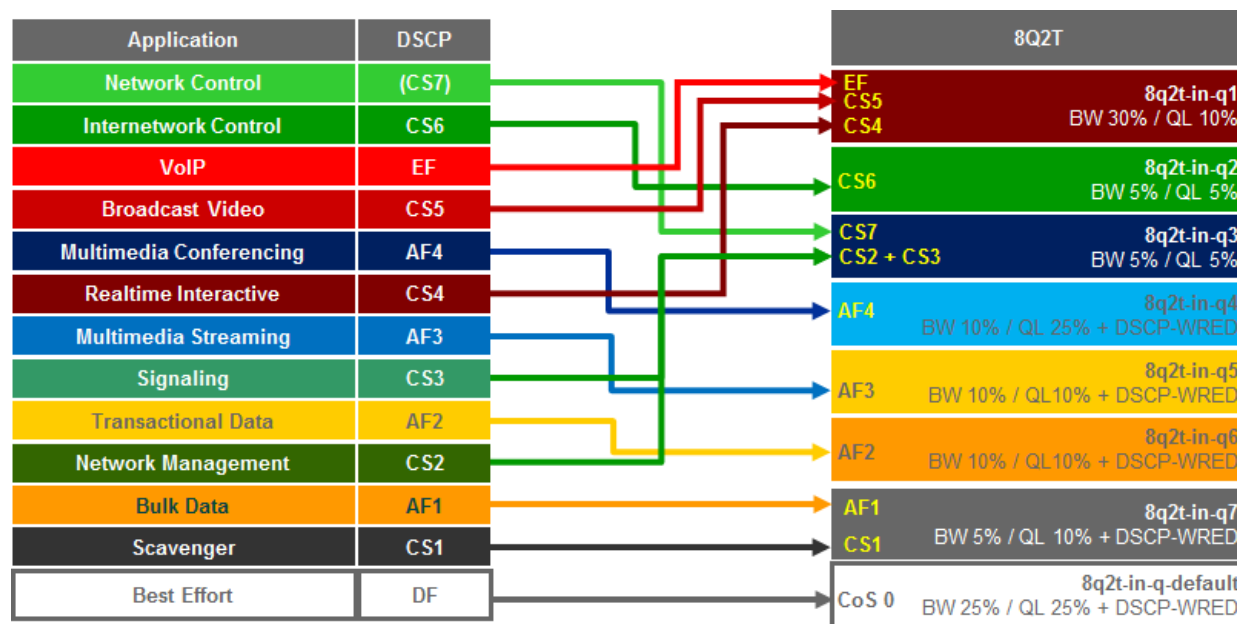
The following figure shows the CoS-to-queue mapping for the 8Q2T ingress queuing model.

##### 1. Ingress Queuing Model (8Q2T)—CoS-to-Queue Mapping



The following figure shows the DSCP-to-queue mapping for the 8Q2T ingress queuing model.

##### 1. Ingress Queuing Model (8Q2T)—DSCP-to-Queue Mapping



NX OS provides system-defined class-map names that cannot be renamed. The system-defined class-map names that match the eight ingress queues of the M2 Series modules are as follows:

- 8q2t-in-q1
- 8q2t-in-q2
- 8q2t-in-q3
- 8q2t-in-q4
- 8q2t-in-q5
- 8q2t-in-q6
- 8q2t-in-q7
- 8q2t-in-q-default

These class-maps have default and/or non-default (customer implemented) CoS and/or DSCP values attached to them. These values can be reset with “no match” commands.

A “no match DSCP” command causes one or more DSCP values (depending upon whether a single DSCP value “x” was entered or a range of DSCP values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 8q2t-in-q-default class-map. However, a CoS value must first be mapped to the 8q2t-in-q-default class-map, or an error will be generated.

A “no match cos” command causes one or more CoS values (depending upon whether a single CoS value “x” was entered or a range of CoS values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 8q2t-in-q-default class-map. However, all CoS values cannot be removed from a particular class-map if there are still DSCP values associated with the particular class-map. Attempting this will generate an error. In other words, all CoS values cannot be removed from a given class-map until all DSCP values have been removed from the class-map. Finally, “no match” commands are not accepted on the 8q2t-in-q-default class-map and will generate an error.

Because APIC-EM EasyQoS has no knowledge of the existing mapping of the DSCP and CoS values to the class-maps before configuring the ingress queuing policy, it will first set all CoS and DSCP values to the 8q2t-in-q-default class-map before moving CoS and DSCP values to their desired class-maps. EasyQoS then moves the DSCP and CoS values into the desired class-maps. This is accomplished via the following commands.

```

!
class-map type queuing match-any 8q2t-in-q1
match dscp 32, 40, 46
match cos 5
class-map type queuing match-any 8q2t-in-q2
match dscp 48
match cos 6
class-map type queuing match-any 8q2t-in-q3
match dscp 16, 24, 56
match cos 7
class-map type queuing match-any 8q2t-in-q4
match dscp 34, 36, 38
match cos 4
class-map type queuing match-any 8q2t-in-q5
match dscp 26, 28, 30
match cos 3
class-map type queuing match-any 8q2t-in-q6
match dscp 18, 20, 22
match cos 2
class-map type queuing match-any 8q2t-in-q7
match dscp 8, 10, 12, 14
match cos 1

```

```
!
```

Any DSCP and CoS values that do not appear above are mapped to the 8q2t-in-q-default class-map. After the DSCP and CoS values have been moved into the appropriate class-maps, the following configuration provisioned by APIC-EM EasyQoS creates and configures the queuing policy-map with the 8Q2T ingress queuing structure on the Nexus 7000 Series M2 modules.

```
!
```

```

policy-map type queuing prm-dscp#8q2t-in
class type queuing 8q2t-in-q1
bandwidth percent 30
queue-limit percent 10
class type queuing 8q2t-in-q2
bandwidth percent 5
queue-limit percent 5
class type queuing 8q2t-in-q3
bandwidth percent 5

```

queue-limit percent 5  
class type queuing 8q2t-in-q4  
bandwidth percent 10  
queue-limit percent 25  
random-detect dscp-based  
random-detect dscp 34 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 36 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 38 minimum-threshold percent 80 maximum-threshold percent 100  
class type queuing 8q2t-in-q5  
bandwidth percent 10  
queue-limit percent 10  
random-detect dscp-based  
random-detect dscp 26 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 28 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 30 minimum-threshold percent 80 maximum-threshold percent 100  
class type queuing 8q2t-in-q6  
bandwidth percent 10  
queue-limit percent 10  
random-detect dscp-based  
random-detect dscp 18 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 20 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 22 minimum-threshold percent 80 maximum-threshold percent 100  
class type queuing 8q2t-in-q7  
bandwidth percent 5  
queue-limit percent 10  
random-detect dscp-based  
random-detect dscp 8 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 10 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 12 minimum-threshold percent 80 maximum-threshold percent 100  
random-detect dscp 14 minimum-threshold percent 80 maximum-threshold percent 100  
class type queuing 8q2t-in-q-default  
bandwidth percent 25  
queue-limit percent 25  
random-detect dscp-based  
random-detect dscp 0 minimum-threshold percent 80 maximum-threshold percent 100  
!

The policy-map with the 8Q2T ingress queuing structure is then applied by APIC-EM EasyQoS to Ethernet interfaces that connect to either other core-layer switches or to distribution-layer switches. Additionally, the policy-map can be applied to the logical port-channel interface when an EtherChannel connection is used for port-level resilience, instead of a single physical interface. An example of the configuration of the policy to an Ethernet and a Port-channel interface is shown below.

!

```
interface Ethernet x/x
```

```
service-policy type queuing input prm-dscp#8q2t-in
```

!

```
interface port-channel xxx
```

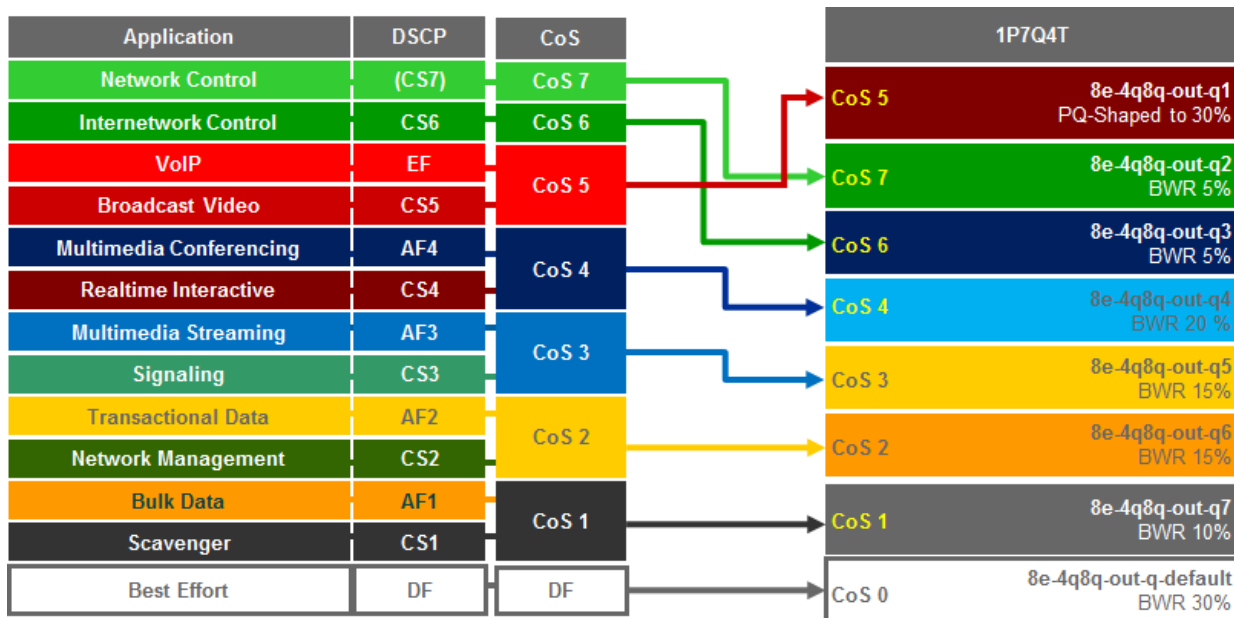
```
service-policy type queuing input prm-dscp#8q2t-in
```

!

### Nexus 7000 1P7Q4T Egress Queuing

For egress queuing, only CoS-to-Queue mapping is supported on M2 Series modules. The following figure shows the CoS-to-queue mapping for the 1P7Q4T egress queuing model.

#### 1. Egress Queuing Model (1P7Q4T)—CoS-to-Queue Mapping



NX OS provides system-defined class-map names that cannot be renamed. The system-defined class-map names that match the eight output queues of the M2 Series modules are as follows:

- 1p7q4t-out-pq1
- 1p7q4t-out-q2
- 1p7q4t-out-q3
- 1p7q4t-out-q4
- 1p7q4t-out-q5
- 1p7q4t-out-q6

- 1p7q4t-out-q7
- 1p7q4t-out-q-default

These class-maps have default and/or non-default (customer implemented) CoS values attached to them. These values can be reset with “no match cos” commands. A “no match cos” command causes one or more CoS values (depending upon whether a single CoS value “x” was entered or a range of CoS values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 1p7q4t-out-q-default class-map.

Because APIC-EM EasyQoS has no knowledge of the existing mapping of the CoS values to the class-maps before configuring the ingress queuing policy, it will first set all CoS values to the 1p7q4t-out-q-default class-map before moving CoS values to their desired class-maps. This is accomplished via the following commands.

```
!  
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  
!
```

Note that because there are no DSCP values within egress class-maps, there are no issues with moving CoS values to the default class-map, as was discussed in the **\*Nexus 7000 8Q2T Ingress Queuing\*** section above.

APIC-EM EasyQoS can then move CoS values into the desired class-maps. This is accomplished via the following commands.

```
!  
class-map type queuing match-any 1p7q4t-out-pq1  
match cos 5  
class-map type queuing match-any 1p7q4t-out-q2  
match cos 7  
class-map type queuing match-any 1p7q4t-out-q3  
match cos 6  
class-map type queuing match-any 1p7q4t-out-q4  
match cos 4
```

```
class-map type queuing match-any 1p7q4t-out-q5
match cos 3
class-map type queuing match-any 1p7q4t-out-q6
match cos 2
class-map type queuing match-any 1p7q4t-out-q7
match cos 1
!
```

Any CoS values that do not appear above (CoS 0) are mapped to the 1p7q4t-out-q-default class-map. After the CoS values have been moved into the appropriate class-maps, the following configuration provisioned by APIC-EM EasyQoS creates and configures the queuing policy-map with the 1P7Q4T egress queuing structure on the Nexus 7000 Series M2 modules.

```
!
policy-map type queuing prm-dscp#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 5
queue-limit percent 5
class type queuing 1p7q4t-out-q3
bandwidth remaining percent 5
queue-limit percent 5
class type queuing 1p7q4t-out-q4
bandwidth remaining percent 20
queue-limit percent 25
random-detect cos-based
random-detect cos 4 minimum-threshold percent 80 maximum-threshold percent 100
class type queuing 1p7q4t-out-q5
bandwidth remaining percent 15
queue-limit percent 10
random-detect cos-based
random-detect cos 3 minimum-threshold percent 80 maximum-threshold percent 100
class type queuing 1p7q4t-out-q6
bandwidth remaining percent 15
queue-limit percent 10
random-detect cos-based
```

```
random-detect cos 2 minimum-threshold percent 80 maximum-threshold percent 100
class type queuing 1p7q4t-out-q7
bandwidth remaining percent 10
queue-limit percent 10
random-detect cos-based
random-detect cos 1 minimum-threshold percent 80 maximum-threshold percent 100
class type queuing 1p7q4t-out-q-default
bandwidth remaining percent 30
queue-limit percent 25
random-detect cos-based
random-detect cos 0 minimum-threshold percent 80 maximum-threshold percent 100
!
```

The policy-map with the 1P7Q4T egress queuing structure is then applied to Ethernet interfaces that connect to either other core-layer switches or to distribution-layer switches. Additionally, the policy-map can be applied to the logical port-channel interface when an EtherChannel connection is used for port-level resilience, instead of a single physical interface. An example of the configuration of the policy to an Ethernet and a Port-channel interface is shown below.

```
!
interface Ethernet x/x
service-policy type queuing output prm-dscp#1p7q4t-out
!
interface port-channel xxx
service-policy type queuing output prm-dscp#1p7q4t-out
!
```

#### F2/F2e/F3 Modules on the Nexus 7000

F2, F2e, and F3 Series modules for the Nexus 7000 consist of the following:

- N7K-F248XP-25
- N7K-F248XP-25E
- N7K-F248XT-25E
- N7K-F348XP-25
- N7K-F312FQ-25
- N7K-F306CK-25

These modules are only supported on the Nexus 7000 series chassis.

The ingress and egress queuing structure for F2, F2e, and F3 Series modules on the Nexus 7000 is determined by the system network QoS policy. When an F2, F2e, or F3 Series module is inserted and becomes operational within the Nexus 7000 chassis, five network-qos policies (templates) are automatically added to the system. The following figure shows the five network-QoS templates available in the Nexus 7000 chassis.

1. NX-OS Network-QoS Templates for the F2, F2e, and F3 Series Modules on the Nexus 7000



These Network QoS Templates are only available on the Nexus 7700 Series

Network QoS Template	CoS Values That May Be Dropped	No Drop CoS Values
default-4q-8e-policy (default-nq-8e-policy)	0,1,2,3,4,5,6,7	-
default-4q-7e-policy (default-nq-7e-policy)	0,1,2,4,5,6,7	3
default-4q-6e-policy (default-nq-6e-policy)	0,1,2,5,6,7	3,4
default-4q-4e-policy (default-nq-4e-policy)	0,5,6,7	1,2,3,4
default-8e-4q4q-policy (default-nq-8e-4q4q-policy)	0,1,2,3,4,5,6,7	-
default-8e-4q8q-policy (default-nq-8e-4q8q-policy)	0,1,2,3,4,5,6,7	-
default-7e-4q8q-policy (default-nq-7e-4q8q-policy)	0,1,2,4,5,6,7	3
default-6e-4q8q-policy (default-nq-6e-4q8q-policy)	0,1,2,5,6,7	3,4
default-4e-4q8q-policy (default-nq-4e-4q8q-policy)	0,5,6,7	1,2,3,4

Network-qos policy template names contain the abbreviation “nq”, referring to network-qos, and “e,” referring to Ethernet. The numbers 4, 6, 7, and 8 denote the number of drop CoS values (in other words the number of CoS values that may be dropped during congestion) that are defined within the policy template.

- Note: The bottom four templates are only available in the Nexus 7700 Series chassis and not the Nexus 7000 Series chassis.

For data center deployments, there may be requirements for a particular CoS value not to be dropped during congestion. However, campus core deployments typically do not have such requirements. Hence, the default-nq-8e-policy or default-nq-8e-4q4q-policy templates are more appropriate for campus core deployments featuring Nexus 7000 chassis with F2, F2e, and/or F3 Series modules. By default, the default-nq-8e-policy is applied by the system.

The “4q4q” in the default-nq-8e-4q4q-policy template refers to the fact that both the ingress and egress queuing structures use four queues. The default-nq-8e-policy template uses an ingress queuing structure that uses only two queues and an egress queuing structure that uses four queues. Because the default-nq-8e-4q4q-policy template better uses the available ingress queuing structure, this is the network-qos policy template that APIC-EM EasyQoS configures via the following global configuration commands.

!

```
system qos
```

```
service-policy type network-qos default-nq-8e-4q4q-policy
```

!

This configuration change can be validated via exec-level “show policy-map system” command. An example of the output is shown below.

```
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 threshold burst-optimized
```

```
mtu 1500
```

...

Service-policy input: default-8e-4q4q-in-policy

...

Service-policy output: default-8e-4q4q-out-policy

...

The following figure shows the default ingress queuing models for each of the network-qos policy templates.

#### 1. Default Ingress Queuing Models for the Network-QoS Templates

default-4q-8e-policy 2Q4T	default-4q-7e-policy 4Q4T	default-4q-6e-policy 4Q4T	default-4q-4e-policy 4Q4T	default-8e-4q4q-policy 4Q1T
<b>2q4t-8e-in-q1</b> CoS 5-7 BW 50% QL 10%	<b>4q4t-7e-in-q1</b> CoS 5-7 BW 25% QL 7%	<b>4q4t-6e-in-q1</b> CoS 5-7 BW 25% QL 7%	<b>4q4t-4e-in-q1</b> CoS 5-7 BW 25% QL 7%	<b>4q1t-8e-4q4q-in-q1</b> CoS 5-7 BW 25% QL 10%
	<b>4q4t-7e-in-q3</b> CoS 2,4 BW 25% QL 31%	<b>4q4t-6e-in-q3</b> CoS 4 BW 25% QL 3%	<b>4q4t-4e-in-q3</b> CoS 4 BW 25% QL 3%	<b>4q1t-8e-4q4q-in-q3</b> CoS 3-4 BW 25% QL 30%
<b>2q4t-8e-in-q-default</b> CoS 0-4 BW 50% QL 90%	<b>4q4t-7e-in-q4</b> CoS 3 BW 25% QL 30%	<b>4q4t-6e-in-q4</b> CoS 3 BW 25% QL 27%	<b>4q4t-4e-in-q4</b> CoS 1-3 BW 25% QL 27%	<b>4q1t-8e-4q4q-in-q4</b> CoS 2 BW 25% QL 30%
	<b>4q4t-7e-in-q-default</b> CoS 0-1 BW 25% QL 32%	<b>4q4t-6e-in-q-default</b> CoS 0-2 BW 25% QL 63%	<b>4q4t-4e-in-q-default</b> CoS 0 BW 25% QL 63%	<b>4q1t-8e-4q4q-in-q-default</b> CoS 0-1 BW 25% QL 30%

The following figure shows the default egress queuing models for each of the network-qos policy templates.

#### 1. Default Egress Queuing Models for the Network-QoS Templates

default-4q-8e-policy 1P3Q1T	default-4q-7e-policy 1P3Q1T	default-4q-6e-policy 3P1Q1T	default-4q-4e-policy 2P2Q1T	default-8e-4q4q-policy 1P3Q1T
<b>1p3q1t-8e-out-pq1</b> CoS 5-7 PL 1	<b>1p3q1t-7e-out-pq1</b> CoS 5-7 PL 1 (limited to 80% BW)	<b>3p1q1t-6e-out-pq1</b> CoS 5-7 PL 1 (limited to 70% BW)	<b>2p2q1t-4e-out-pq1</b> CoS 5-7 PL 1 (limited to 50% BW)	<b>1p3q1t-8e-4q4q-out-pq1</b> CoS 5 PL 1
<b>1p3q1t-8e-out-q2</b> CoS 3-4 BWR 33%	<b>1p3q1t-7e-out-q2</b> CoS 3 BWR 20%	<b>3p1q1t-6e-out-pq2</b> CoS 4 PL 1 (limited to 30% BW)	<b>2p2q1t-4e-out-pq2</b> CoS 4 PL 1 (limited to 50% BW)	<b>1p3q1t-8e-4q4q-out-q2</b> CoS 3-4 BWR 33%
<b>1p3q1t-8e-out-q3</b> CoS 2 BWR 33%	<b>1p3q1t-7e-out-q3</b> CoS 2,4 BWR 40%	<b>3p1q1t-6e-out-pq3</b> CoS 3 PL 2 (limited to 30% BW)	<b>2p2q1t-4e-out-q3</b> CoS 1-3 BWR 50%	<b>1p3q1t-8e-4q4q-out-q3</b> CoS 2 BWR 33%
<b>1p3q1t-8e-out-q-default</b> CoS 0-1 BWR 33%	<b>1p3q1t-7e-out-q-default</b> CoS 0-1 BWR 40%	<b>3p1q1t-6e-out-q-default</b> CoS 0-2 BWR 70%	<b>2p2q1t-4e-out-q-default</b> CoS 0 BWR 50%	<b>1p3q1t-8e-4q4q-out-q-default</b> CoS 0-1 BWR 33%

As can be seen from the figures above, the default-nq-8e-4q4q-policy implements a 4Q1T ingress queuing structure and a 1P3Q1T egress queuing structure for F2, F2e, and F3 Series modules with the Nexus 7000.

### Nexus 7000 4Q1T Ingress Queuing

As of NX OS software version 6.2.2 and higher ingress DSCP-to-Queue mapping is supported on F2, F2e, and F3 Series modules and must be configured via the following global configuration command.

!

```
hardware qos dscp-to-queue ingress module-type all
```

!

APIC-EM EasyQoS will provision this command to enable DSCP-to-Queue mapping support on the F2/F2E/F3 Series modules for the Nexus 7000 Series.

Trust of both CoS and DSCP values is implicit on the Nexus 7000 Series. No explicit configuration is required to enable trust.

The network-qos default-nq-8e-4q4q-policy template has a default ingress queuing policy map that can be displayed via the exec-level “show policy-map type queuing default-8e-4q4q-in-policy” command. An example of the output is shown below.

```
DC-7010-2# show policy-map type queuing default-8e-4q4q-in-policy
```

Type queuing policy-maps

---

```
policy-map type queuing default-8e-4q4q-in-policy
```

```
class type queuing 4q1t-8e-4q4q-in-q1
```

```
queue-limit percent 10
```

```
bandwidth percent 25
```

```
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 25
```

```
class type queuing 4q1t-8e-4q4q-in-q4
```

```
queue-limit percent 30
```

```
bandwidth percent 25
```

For F2, F2e, and F3 series modules, the ingress queuing policy define queue-limit percentages and bandwidth percentages for each of the class-maps (which correspond to the queues). These percentages will be modified by APIC-EM for the EasyQoS solution.

The network-qos default-nq-8e-4q4q-policy template also provides default settings for the system-defined class-maps that can be displayed via the exec-level “show class-map type queuing” command for each of the system-defined class-map names. An example of the output for each of the system-defined class-maps is shown below.

```
DC-7010-2# show class-map type queuing 4q1t-8e-4q4q-in-q1
```

Type queuing class-maps

---

```
class-map type queuing match-any 4q1t-8e-4q4q-in-q1
```

---

Description: Classifier for Ingress queue 1 of type 4q1t-8e-4q4q

match cos 5-7

match dscp 40-63

DC-7010-2# show class-map type queuing 4q1t-8e-4q4q-in-q-default

Type queuing class-maps

---

class-map type queuing match-any 4q1t-8e-4q4q-in-q-default

Description: Classifier for Ingress queue 2 of type 4q1t-8e-4q4q

match cos 0-1

match dscp 0-15

DC-7010-2# show class-map type queuing 4q1t-8e-4q4q-in-q3

Type queuing class-maps

---

class-map type queuing match-any 4q1t-8e-4q4q-in-q3

Description: Classifier for Ingress queue 3 of type 4q1t-8e-4q4q

match cos 3-4

match dscp 24-39

DC-7010-2# show class-map type queuing 4q1t-8e-4q4q-in-q4

Type queuing class-maps

---

class-map type queuing match-any 4q1t-8e-4q4q-in-q4

Description: Classifier for Ingress queue 4 of type 4q1t-8e-4q4q

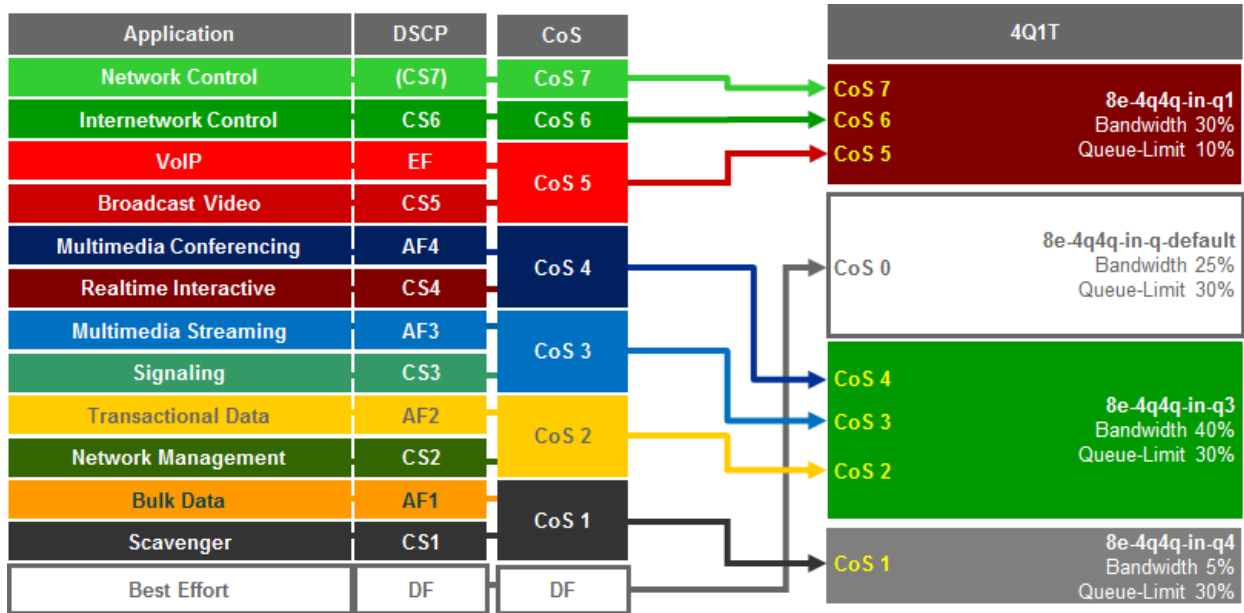
match cos 2

match dscp 16-23

The system-defined class-maps have default settings for mapping CoS and DSCP values to each of the class-maps. However, APIC-EM EasyQoS cannot guarantee that the customer has not already previously configured the default-nq-8e-4q4q-policy network-qos template and modified the default mappings of CoS and DSCP values to class-maps. Because both CoS and DSCP values are trusted, queuing models for both CoS-to-queue mapping and DSCP-to-queue mapping need to be configured.

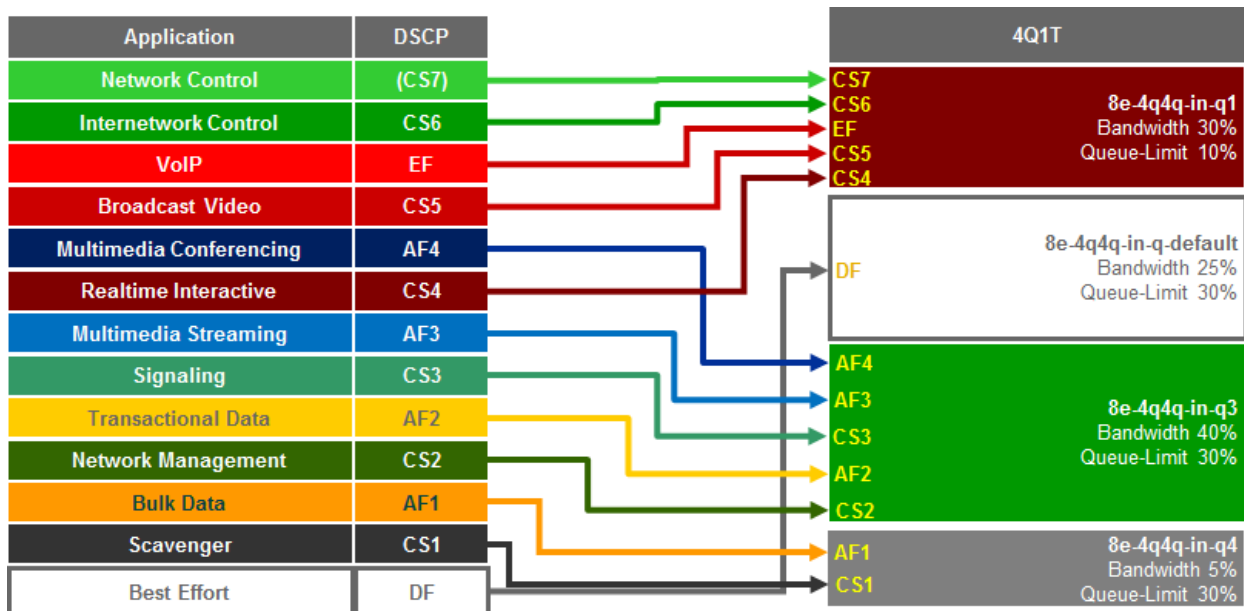
The following figure shows the CoS-to-queue mapping for the 4Q1T ingress queuing model deployed by APIC-EM for the EasyQoS solution.

### 1. Ingress Queuing Model (4Q1T)—CoS-to-Queue Mapping



The following figure shows the DSCP-to-queue mapping for the 4Q1T ingress queuing model deployed by APIC-EM for the EasyQoS solution.

#### 1. Ingress Queuing Model (4Q1T)—DSCP-to-Queue Mapping



NX OS provides system-defined class-map names that cannot be renamed. The system-defined class-map names that match the four ingress queues of the F2, F2e and/or F3 Series modules for the Nexus 7000 are as follows:

- 4q1t-8e-4q4q-in-q1
- 4q1t-8e-4q4q-in-q3
- 4q1t-8e-4q4q-in-q4
- 4q1t-8e-4q4q-in-q-default

These class-maps have default and/or non-default (customer implemented) CoS and/or DSCP values attached to them.

These values can be reset with “no match” commands.

A “no match DSCP” command causes one or more DSCP values (depending upon whether a single DSCP value “x” was entered or a range of DSCP values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 4q1t-8e-4q4q-in-q-default class-map. However, a CoS value must first be mapped to the 4q1t-8e-4q4q-in-q-default class-map, or an error will be generated.

A “no match cos” command causes one or more CoS values (depending upon whether a single CoS value “x” was entered or a range of CoS values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 4q1t-8e-4q4q-in-q-default. However, all CoS values cannot be removed from a particular class-map if there are still DSCP values associated with the particular class-map. Attempting this will generate an error. In other words, all CoS values cannot be removed from a given class-map until all DSCP values have been removed from the class-map. Finally, “no match” commands are not accepted on the 4q1t-8e-4q4q-in-q-default class-map and will generate an error.

Because APIC-EM has no knowledge of the existing mapping of the DSCP and CoS values to the class-maps before configuring the ingress queuing policy, it will first set all CoS and DSCP values to the 4q1t-8e-4q4q-in-q-default class-map before moving CoS and DSCP values to their desired class-maps. APIC-EM EasyQoS then moves the DSCP and CoS values into the desired class-maps. This is accomplished via the following commands.

```
!  
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, 30, 34, 36, 38  
!  
class-map type queuing match-any 4q1t-8e-4q4q-in-q4  
match cos 1  
match dscp 8, 10, 12, 14
```

This will leave the default 4q1t-8e-4q4q-in-q-default queue with the following configuration.

```
!  
class-map type queuing match-any 4q1t-8e-4q4q-in-q-default  
match cos 0  
match dscp 0-7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41-45,47,49-55,57-63
```

After the DSCP and CoS values have been moved into the appropriate class-maps, system-defined policy-map is cloned by appending “prm-DSCP#” to the beginning of the system-defined policy map. This is done via the following config-level command.

```
!  
qos copy policy-map type queuing default-8e-4q4q-in-policy prefix prm-dscp#  
!
```

After the cloned policy-map is created, the following configuration modifies the cloned queuing policy map with the 4Q1T ingress queuing structure on the Nexus 7000 Series F2, F2e, and F3 modules.

```
!  
policy-map type queuing prm-DSCP#8e-4q4q-in  
class type queuing 4q1t-8e-4q4q-in-q4  
queue-limit percent 30  
bandwidth percent 5  
class type queuing 4q1t-8e-4q4q-in-q1  
queue-limit percent 10  
bandwidth percent 30  
class type queuing 4q1t-8e-4q4q-in-q3  
queue-limit percent 30  
bandwidth percent 40  
class type queuing 4q1t-8e-4q4q-in-q-default  
queue-limit percent 30  
bandwidth percent 25  
!
```

The policy-map with the 4Q1T ingress queuing structure is then applied to Ethernet interfaces that connect to either other core-layer switches or to distribution-layer switches. Additionally, the policy-map can be applied to the logical port-channel interface when an EtherChannel connection is used for port-level resilience, instead of a single physical interface. An example of the configuration of the policy to an Ethernet and a Port-channel interface is shown below.

```
!  
interface Ethernet x/x  
service-policy type queuing input prm-dscp#8e-4q4q-in  
!  
interface port-channel xxx  
service-policy type queuing input prm-dscp#8e-4q4q-in  
!
```

#### Nexus 7000 1P3Q1T Egress Queuing

The network-qos default-nq-8e-4q4q-policy template has a default egress queuing policy map that can be displayed via the exec-level “show policy-map type queuing default-8e-4q4q-out-policy” command. An example of the output is shown below.

```
DC-7010-2# show policy-map type queuing default-8e-4q4q-out-policy  
Type queuing policy-maps
```

---

```
policy-map type queuing default-8e-4q4q-out-policy  
class type queuing 1p3q1t-8e-4q4q-out-pq1  
priority level 1
```

```
class type queuing 1p3q1t-8e-4q4q-out-q2
```

```
bandwidth remaining percent 33
```

```
class type queuing 1p3q1t-8e-4q4q-out-q3
```

```
bandwidth remaining percent 33
```

```
class type queuing 1p3q1t-8e-4q4q-out-q-default
```

```
bandwidth remaining percent 33
```

For F2, F2e, and F3 series modules, the egress queuing policy defines the priority queue and the default bandwidth remaining bandwidth percentages for each of the rest of the class-maps (which correspond to the queues). These percentages will be modified by APIC-EM for the EasyQoS solution.

The network-qos default-nq-8e-4q4q-policy template also provides default settings for the system-defined class-maps that can be displayed via the exec-level “show class-map type queuing” command for each of the system-defined class-map names. An example of the output for each of the system-defined class-maps is shown below.

```
DC-7010-2# show class-map type queuing 1p3q1t-8e-4q4q-out-pq1
```

```
Type queuing class-maps
```

---

```
class-map type queuing match-any 1p3q1t-8e-4q4q-out-pq1
```

```
Description: Classifier for Egress Priority queue 1 of type 1p3q1t-8e-4q4q
```

```
match cos 5-7
```

```
DC-7010-2# show class-map type queuing 1p3q1t-8e-4q4q-out-q2
```

```
Type queuing class-maps
```

---

```
class-map type queuing match-any 1p3q1t-8e-4q4q-out-q2
```

```
Description: Classifier for Egress queue 2 of type 1p3q1t-8e-4q4q
```

```
match cos 3-4
```

```
DC-7010-2# show class-map type queuing 1p3q1t-8e-4q4q-out-q3
```

```
Type queuing class-maps
```

---

```
class-map type queuing match-any 1p3q1t-8e-4q4q-out-q3
```

```
Description: Classifier for Egress queue 3 of type 1p3q1t-8e-4q4q
```

```
match cos 2
```

```
DC-7010-2# show class-map type queuing 1p3q1t-8e-4q4q-out-q-default
```

```
Type queuing class-maps
```

---

```
class-map type queuing match-any 1p3q1t-8e-4q4q-out-q-default
```

```
Description: Classifier for Egress queue 4 of type 1p3q1t-8e-4q4q
```

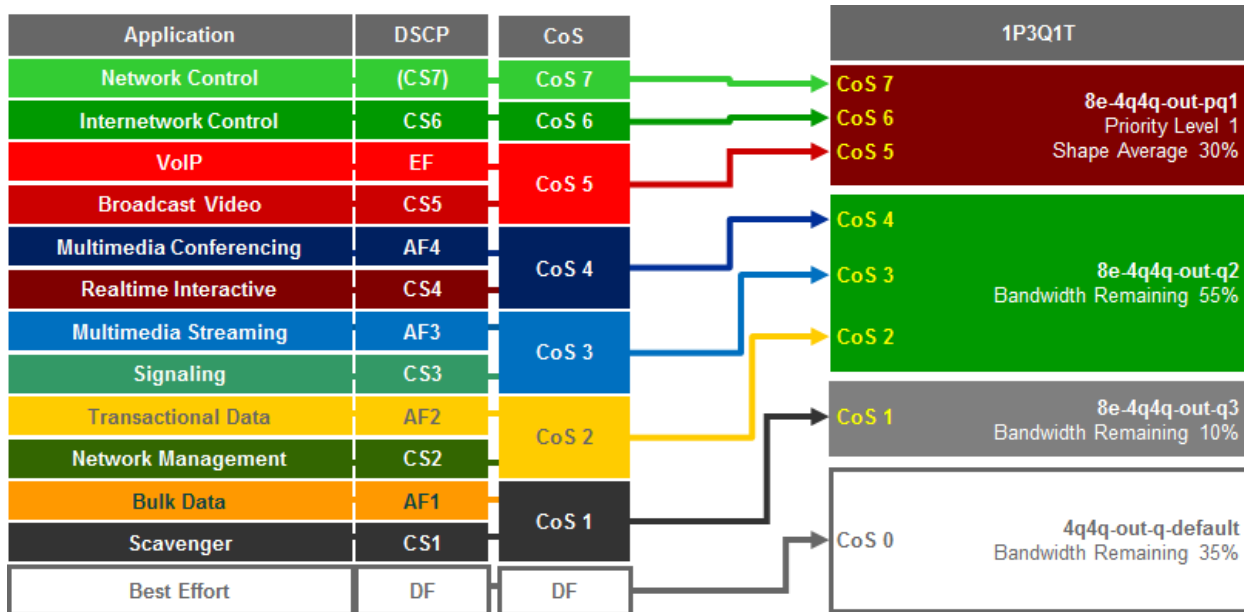
```
match cos 0-1
```



The system-defined class-maps have default settings for mapping CoS values to each of the class-maps. However, APIC-EM EasyQoS cannot guarantee that the customer has not already previously configured the default-nq-8e-4q4q-policy network-qos template and modified the default mappings of CoS and DSCP values to class-maps. Hence, the queuing models for CoS-to-queue mapping need to be configured.

For egress queuing, only CoS-to-Queue mapping is supported on F2, F2e, and F3 Series modules. The following figure shows the Cos-to-queue mapping for the 1P3Q1T egress queuing model.

#### 1. Egress Queuing Model (1P3Q1T)—CoS-to-Queue Mapping



NX OS provides system-defined class-map names that cannot be renamed. The system-defined class-map names that match the four output queues of the F2, F2e, and F3 Series modules on the Nexus 7000 are as follows:

- 1p3q1t-out-pq1
- 1p3q1t-out-q3
- 1p3q1t-out-q4
- 1p3q1t-out-q-default

These class-maps have default and/or non-default (customer implemented) CoS values attached to them. These values can be reset with “no match cos” commands. A “no match cos” command causes one or more CoS values (depending upon whether a single CoS value “x” was entered or a range of CoS values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 1p3q1t-out-q-default class-map.

Because APIC-EM has no knowledge of the existing mapping of the CoS values to the class-maps before configuring the ingress queuing policy, it will first set all CoS values to the 1p3q1t-out-q-default class-map before moving CoS values to their desired class-maps. This is accomplished via the following commands.

!

```
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
```

```
!
```

- Note: Because there are no DSCP values within egress class-maps, there are no issues with moving CoS values to the default class-map, as was discussed in the **\*Nexus 7000 8Q2T Ingress Queuing\*** section.

APIC-EM can then move CoS values into the desired class-maps. This is accomplished via the following commands.

```
!
```

```
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
```

```
!
```

After the CoS values have been moved into the appropriate class-maps, the system-defined policy-map is cloned by appending “prm-dscp#” to the beginning of the system-defined policy map. This is done via the following config-level command.

```
!
```

```
qos copy policy-map type queuing default-8e-4q4q-out-policy prefix prm-dscp#
```

```
!
```

After the cloned policy-map is created, the following configuration modifies the cloned queuing policy-map with the 1P3Q1T egress queuing structure on the Nexus 7000 Series F2, F2e, and F3 modules.

```
!
```

```
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
```

```
!
```

The policy-map with the 1P3Q1T egress queuing structure is then applied to Ethernet interfaces that connect to either other core-layer switches or to distribution-layer switches. Additionally, the policy-map can be applied to the logical port-channel interface when an EtherChannel connection is used for port-level resilience, instead of a single physical interface. An example of the configuration of the policy to an Ethernet and a Port-channel interface is shown below.

```
!
```

```
interface Ethernet x/x
service-policy type queuing output prm-dscp#8e-4q4q-out
!
interface port-channel xxx
service-policy type queuing output prm-dscp#8e-4q4q-out
!
```

#### F2e and F3 Series Modules on the Nexus 7700

F2e and F3 Series modules for the Nexus 7700 consist of the following:

- N77-F248XP-23E
- N77-F348XP-23
- N77-F324FQ-25
- N77-F312CK-26

These modules are only supported on the Nexus 7700 Series chassis.

The ingress and egress queuing structure for F2e and F3 Series modules on the Nexus 7700 is determined by the system network QoS policy. When an F2e or F3 Series module is inserted and becomes operational within the Nexus 7700 chassis, all nine network-qos policies (templates) shown in Figure 103 are automatically added to the system.

Because the default-nq-8e-4q8q-policy template better uses the available ingress and egress queuing structure (4 ingress queues and 8 egress queues), this is the network-qos policy template that APIC-EM EasyQoS configures via the following global configuration commands.

```
!
system qos
service-policy type network-qos default-nq-8e-4q8q-policy
!
```

The default-nq-8e-4q4q-policy implements a 4Q1T ingress queuing structure and a 1P7Q1T egress queuing structure for F2, F2e, and F3 Series modules with the Nexus 7700.

#### Nexus 7000 4Q1T Ingress Queuing

DSCP-to-Queue mapping is by default enabled on the Nexus 7700 Series. However, in the event the customer has disabled this for some reason, APIC-EM EasyQoS will enable it via the following global configuration command.

```
!
hardware qos dscp-to-queue ingress
!
```

Trust of both CoS and DSCP values is implicit on the Nexus 7700 Series. No explicit configuration is required to enable trust.

The network-qos default-nq-8e-4q8q-policy template has a default ingress queuing policy map that can be displayed via the exec-level “show policy-map type queuing default-8e-4q8q-in-policy” command. An example of the output is shown below.

```
N7700# show policy-map type queuing default-8e-4q8q-in-policy
Type queuing policy-maps
```

policy-map type queuing default-8e-4q8q-in-policy

class type queuing 8e-4q8q-in-q1

queue-limit percent 10

bandwidth percent 49

class type queuing 8e-4q8q-in-q-default

queue-limit percent 88

bandwidth percent 49

class type queuing 8e-4q8q-in-q3

queue-limit percent 1

bandwidth percent 1

class type queuing 8e-4q8q-in-q4

queue-limit percent 1

bandwidth percent 1

For F2, F2e, and F3 series modules, the ingress queuing policy define queue-limit percentages and bandwidth percentages for each of the class-maps (which correspond to the queues). These percentages will be modified by APIC-EM for the EasyQoS solution.

The network-qos default-nq-8e-4q8q-policy template also provides default settings for the system-defined class-maps that can be displayed via the exec-level “show class-map type queuing” command for each of the system-defined class-map names. An example of the output for each of the system-defined class-maps is shown below.

N7700# show class-map type queuing 8e-4q8q-in-q1

Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-in-q1

Description: Classifier for Ingress queue 1 of type 4q1t8e

match cos 5-7

match dscp 40-63

N7700# show class-map type queuing 8e-4q8q-in-q-default

Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-in-q-default

Description: Classifier for Ingress default queue of type 4q1t8e

match cos 0-4

match dscp 0-39

The system-defined class-maps have default settings for mapping CoS and DSCP values to each of the class-maps. Note that no CoS or DSCP values are by default mapped to class-maps 8e-4q8q-in-q-2 and 8e-4q8q-in-q-3. However, APIC-EM cannot guarantee that the customer has not already previously configured the default-nq-8e-4q8q-policy network-qos template and modified the default mappings of CoS and DSCP values to class-maps. Because both CoS and DSCP values are trusted, queuing models for both CoS-to-queue mapping and DSCP-to-queue mapping need to be configured.

The CoS-to-queue mapping for the 4Q1T ingress queuing model deployed by APIC-EM for the Nexus 7700 F2e and F3 modules is the same as was shown in Figure 106 above. Likewise the DSCP-to-queue mapping for the 4Q1T ingress queuing model deployed by APIC-EM for the Nexus 7700 F2e and F3 modules is the same as was shown in Figure 107 above.

NX OS provides system-defined class-map names that cannot be renamed. The system-defined class-map names that match the four ingress queues of the F2e, and F3 Series modules for the Nexus 7700 are as follows:

- 4q1t-8e-4q8q-in-q1
- 4q1t-8e-4q8q-in-q3
- 4q1t-8e-4q8q-in-q4
- 4q1t-8e-4q8q-in-q-default

These class-maps have default and/or non-default (customer implemented) CoS and/or DSCP values attached to them. These values can be reset with “no match” commands.

A “no match dscp” command causes one or more DSCP values (depending upon whether a single DSCP value “x” was entered or a range of DSCP values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 4q1t-8e-4q8q-in-q-default class-map. However, a CoS value must first be mapped to the 4q1t-8e-4q8q-in-q-default class-map, or an error will be generated.

A “no match cos” command causes one or more CoS values (depending upon whether a single CoS value “x” was entered or a range of CoS values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 4q1t-8e-4q8q-in-q-default. However, all CoS values cannot be removed from a particular class-map if there are still DSCP values associated with the particular class-map. Attempting this will generate an error. In other words, all CoS values cannot be removed from a given class-map until all DSCP values have been removed from the class-map. Finally, “no match” commands are not accepted on the 4q1t-8e-4q8q-in-q-default class-map, and will generate an error.

Because APIC-EM EasyQoS has no knowledge of the existing mapping of the DSCP and CoS values to the class-maps before configuring the ingress queuing policy, it will first set all CoS and DSCP values to the 4q1t-8e-4q8q-in-q-default class-map before moving CoS and DSCP values to their desired class-maps. EasyQoS then moves the DSCP and CoS values into the desired class-maps. This is accomplished via the following commands.

```
!
class-map type queuing match-any 8e-4q8q-in-q1
match cos 5-7
match dscp 32, 40, 46
match dscp 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
!
```

Any DSCP and CoS values not shown above are mapped to the 4q1t-8e-4q8q-in-q-default class-map. After the DSCP and CoS values have been moved into the appropriate class-maps, the following configuration creates and configures the queuing policy-map with the 4Q1T ingress queuing structure on the Nexus 7700 Series F2e and F3 modules.

```
!  
policy-map type queuing prm-dscp#4Q1T-IN  
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  
!
```

The policy-map with the 4Q1T ingress queuing structure is then applied to Ethernet interfaces that connect to either other core-layer switches or to distribution-layer switches. Additionally, the policy-map can be applied to the logical port-channel interface when an EtherChannel connection is used for port-level resilience, instead of a single physical interface. An example of the configuration of the policy to an Ethernet and a Port-channel interface is shown below.

```
!  
interface Ethernet x/x  
service-policy type queuing input prm-dscp#4Q1T-IN  
!  
interface port-channel xxx  
service-policy type queuing input prm-dscp#4Q1T-IN  
!
```

#### Nexus 7700 1P7Q1T Egress Queuing

The network-qos default-nq-8e-4q8q-policy template has a default egress queuing policy map that can be displayed via the exec-level “show policy-map type queuing default-8e-4q8q-out-policy” command. An example of the output is shown below.

```
N7700(config)# show policy-map type queuing default-8e-4q8q-out-policy  
Type queuing policy-maps
```

---

```
policy-map type queuing default-8e-4q8q-out-policy  
class type queuing 8e-4q8q-out-q1
```

priority level 1

class type queuing 8e-4q8q-out-q2

bandwidth remaining percent 14

class type queuing 8e-4q8q-out-q3

bandwidth remaining percent 14

class type queuing 8e-4q8q-out-q4

bandwidth remaining percent 14

class type queuing 8e-4q8q-out-q5

bandwidth remaining percent 14

class type queuing 8e-4q8q-out-q6

bandwidth remaining percent 14

class type queuing 8e-4q8q-out-q7

bandwidth remaining percent 14

class type queuing 8e-4q8q-out-q-default

bandwidth remaining percent 14

For F2e and F3 series modules, the egress queuing policy defines the priority queue, and the default bandwidth remaining bandwidth percentages for each of the rest of the class-maps (which correspond to the queues). These percentages will be modified by APIC-EM for the EasyQoS solution.

The network-qos default-nq-8e-4q8q-policy template also provides default settings for the system-defined class-maps that can be displayed via the exec-level “show class-map type queuing” command for each of the system-defined class-map names. An example of the output for each of the system-defined class-maps is shown below.

Xbow1# show class-map type queuing 8e-4q8q-out-q1

Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-out-q1

Description: Classifier for Egress priority queue of type 1p7q1t8e

match cos 5

Xbow1# show class-map type queuing 8e-4q8q-out-q2

Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-out-q2

Description: Classifier for Egress queue 2 of type 1p7q1t8e

match cos 7

Xbow1# show class-map type queuing 8e-4q8q-out-q3

Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-out-q3

Description: Classifier for Egress queue 3 of type 1p7q1t8e  
match cos 6  
Xbow1# show class-map type queuing 8e-4q8q-out-q4  
Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-out-q4  
Description: Classifier for Egress queue 4 of type 1p7q1t8e  
match cos 4  
Xbow1# show class-map type queuing 8e-4q8q-out-q5  
Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-out-q5  
Description: Classifier for Egress queue 5 of type 1p7q1t8e  
match cos 3  
Xbow1# show class-map type queuing 8e-4q8q-out-q6  
Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-out-q6  
Description: Classifier for Egress queue 6 of type 1p7q1t8e  
match cos 2  
Xbow1# show class-map type queuing 8e-4q8q-out-q7  
Type queuing class-maps

---

class-map type queuing match-any 8e-4q8q-out-q7  
Description: Classifier for Egress queue 7 of type 1p7q1t8e  
match cos 1  
Xbow1# show class-map type queuing 8e-4q8q-out-q-default  
Type queuing class-maps

---

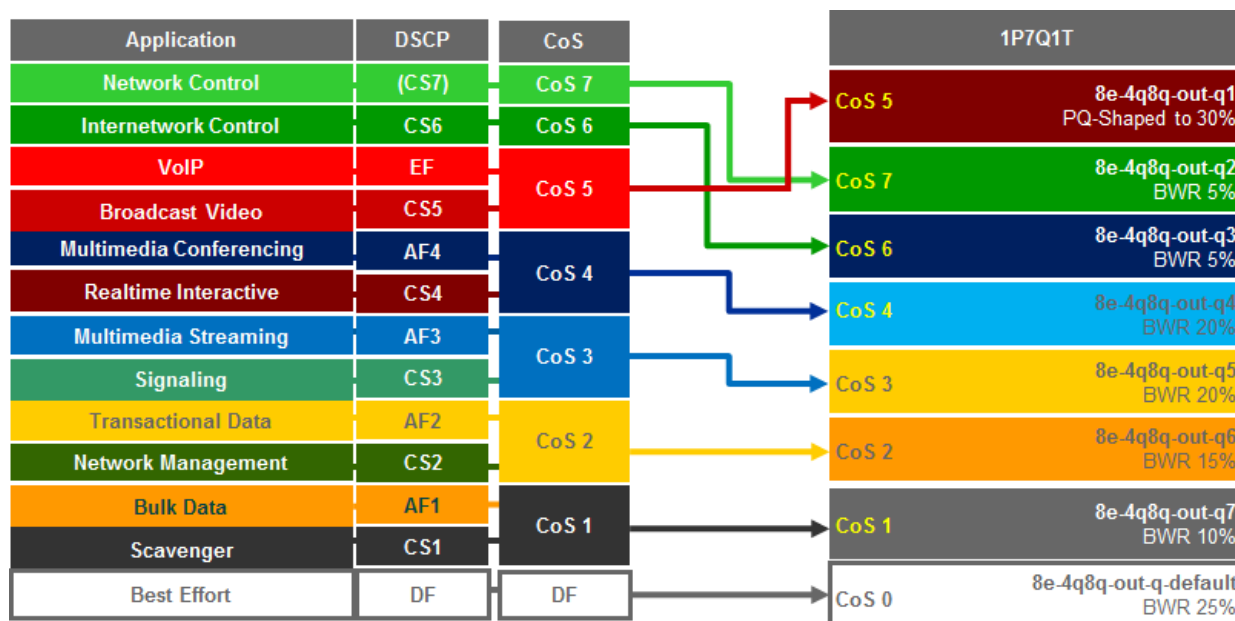
class-map type queuing match-any 8e-4q8q-out-q-default  
Description: Classifier for Egress default queue of type 1p7q1t8e  
match cos 0

The system-defined class-maps have default settings for mapping CoS values to each of the class-maps. However, APIC-EM EasyQoS cannot guarantee that the customer has not already previously configured the default-nq-8e-4q8q-policy network-qos template and modified the default mappings of CoS and DSCP values to class-maps. Hence, the queuing models for CoS-to-queue mapping need to be configured.

For egress queuing, only CoS-to-Queue mapping is supported on F2e and F3 Series modules. The following figure shows the Cos-to-queue mapping for the 1P7Q1T egress queuing model.



## 1. Egress Queuing Model (1P7Q1T)—CoS-to-Queue Mapping



NX OS provides system-defined class-map names that cannot be renamed. The system-defined class-map names that match the eight output queues of the F2e and F3 Series modules on the Nexus 7700 are as follows:

- 1p7q1t-out-q1
- 1p7q1t-out-q2
- 1p7q1t-out-q3
- 1p7q1t-out-q4
- 1p7q1t-out-q5
- 1p7q1t-out-q6
- 1p7q1t-out-q7
- 1p7q1t-out-q-default

These class-maps have default and/or non-default (customer implemented) CoS values attached to them. These values can be reset with “no match cos” commands. A “no match cos” command causes one or more CoS values (depending upon whether a single CoS value “x” was entered or a range of CoS values “x-y” was entered) attached to a particular class-map to be removed and automatically attached to the 1p7q1t-out-q-default class-map.

Because APIC-EM EasyQoS has no knowledge of the existing mapping of the CoS values to the class-maps before configuring the ingress queuing policy, it will first set all CoS values to the 1p7q1t-out-q-default class-map before moving CoS and DSCP values to their desired class-maps. This is accomplished via the following commands.

!

```
class-map type queuing match-any 8e-4q8q-out-q1
no match cos 0-7

class-map type queuing match-any 8e-4q8q-out-q2
no match cos 0-7

class-map type queuing match-any 8e-4q8q-out-q3
no match cos 0-7
```

```
class-map type queuing match-any 8e-4q8q-out-q4
no match cos 0-7
class-map type queuing match-any 8e-4q8q-out-q5
no match cos 0-7
class-map type queuing match-any 8e-4q8q-out-q6
no match cos 0-7
class-map type queuing match-any 8e-4q8q-out-q7
no match cos 0-7
!
```

- Note: Because there are no DSCP values within egress class-maps, there are no issues with moving CoS values to the default class-map, as was discussed in the **\*Nexus 7000 8Q2T Ingress Queuing\*** section above.

APIC-EM EasyQoS can then move CoS values into the desired class-maps. This is accomplished via the following commands.

```
!
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
!
```

After the CoS values have been moved into the appropriate class-maps, the following configuration creates and configures the queuing policy-map with the 1P7Q1T egress queuing structure on the Nexus 7700 Series F2e and F3 modules.

```
!
policy-map type queuing prm-dscp#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 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
!
```

The policy-map with the 1P7Q1T egress queuing structure is then applied to Ethernet interfaces that connect to either other core-layer switches or to distribution-layer switches. Additionally, the policy-map can be applied to the logical port-channel interface when an EtherChannel connection is used for port-level resilience, instead of a single physical interface. An example of the output for each of the system-defined class-maps is shown below.

```

!
interface Ethernet x/x
service-policy type queuing output prm-dscp#1P7Q1T-OUT
!
interface port-channel xxx
service-policy type queuing output prm-dscp#1P7Q1T-OUT
!
```

### M3 Series Modules on the Nexus 7700

M3 Series modules for the Nexus 7700 consist of the following:

- N77-M348XP-23L
- N77-M324FQ-25L

These modules are only supported on the Nexus 7700 Series chassis.

The M3 Series modules implement a 4Q1T ingress queuing structure and a 1P7Q1T egress queuing structure. This queuing structure is the same as implemented by F2e and F3 modules on the Nexus 7700 Series, when using the default-nq-8e-4q4q-policy network QoS policy, as discussed in the **\*F2e and F3 Series Modules on the Nexus 7700\*** section above. The only difference between the QoS policy pushed by APIC-EM for the M3 modules and the F2e and F3 modules is that network-qos policy template does not need to be configured for the M3 modules.

## 1.10 Chapter 10: WLAN QoS Design

### AireOS WLC QoS Design

This section discusses AireOS wireless LAN controller platforms within the EasyQoS solution. For the APIC-EM 1.3 release and higher, only Cisco WLCs running the AireOS operating system are supported within the EasyQoS application. Dedicated IOS XE WLCs such as the Cisco 5760 are not currently supported. WLC functionality within Catalyst 3850, 3650, and Catalyst 4500-E Series switches are also not currently supported. Further, only centralized (local) mode configurations, in which traffic is tunneled from the Access Point to the WLC before being placed onto the LAN, are supported.

EasyQoS within APIC-EM release 1.5 introduced support for Fastlane QoS within WLCs running AireOS software version 8.2.112 and higher. FastLane QoS on AireOS WLCs is essentially a macro which enables best-practice configurations on both the overall WLC platform and the specific WLAN/SSID in which it is enabled. The actual configuration provisioned onto the WLC by enabling Fastlane QoS is nearly identical to the configuration which EasyQoS has been provisioning on AireOS WLCs as of APIC-EM release 1.1.

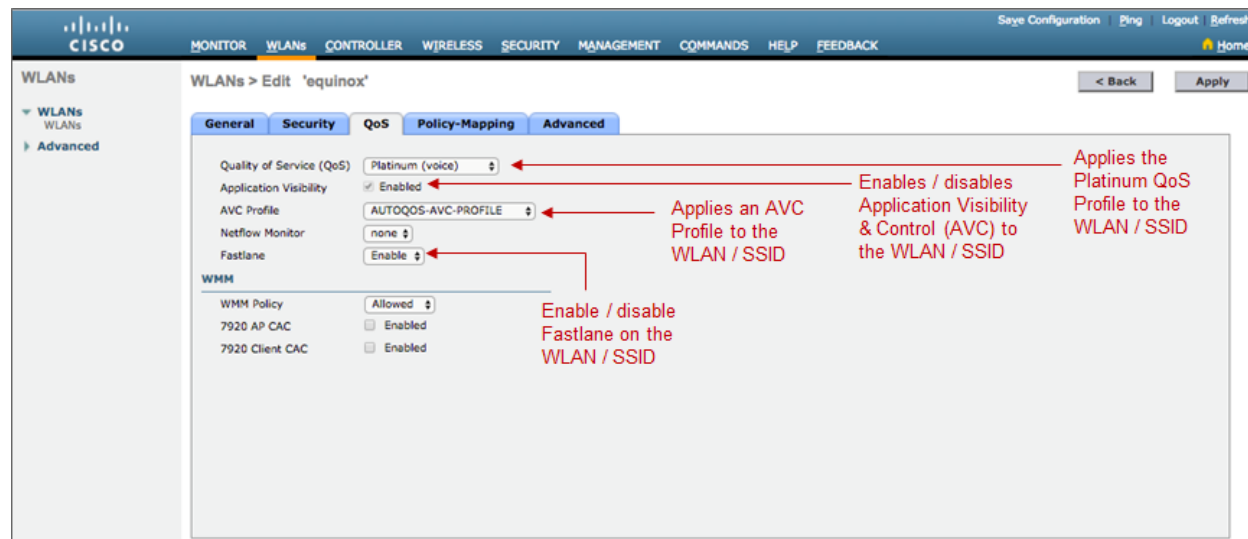
The following sections detail the configuration steps implemented by EasyQoS when configuring wireless policy. The steps apply to both Fastlane and non-Fastlane policies. With APIC-EM release 1.5 EasyQoS policy automatically enabled the Fastlane feature within a WLAN/SSID to which policy was applied if the WLC was running AireOS release 8.3.112 and higher. With APIC-EM release 1.6, the network operator must choose to enable the Fastlane feature within the EasyQoS wireless policy applied to the policy scope which contains the WLC. Enabling the Fastlane feature within the EasyQoS web-based GUI was discussed in the **\*Wireless Policies\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter.

The Fastlane feature is enabled through the following CLI command.

```
config qos fastlane enable <WLAN -id>
```

<WLAN -id> refers to the WLAN/SSID to which Fastlane is to be enabled. From a web GUI perspective, Fastlane is enabled per WLAN/SSID as shown in the figure below.

#### 1. Enabling per WLAN / SSID QoS Features



As a result of enabling the Fastlane feature, the steps discussed within the following sections are implemented automatically by the WLC platform itself. For AireOS WLCs running AireOS releases below 8.3.112, EasyQoS itself provisions each of the steps discussed within the following sections. Any differences between Fastlane and non-Fastlane policies are pointed out within the sections below.

Disabling WLANs and Radios

In order to provision the global QoS configuration (meaning the QoS configuration which affects the entire WLC) required for EasyQoS Static QoS discussed in the sections below, all SSIDs and WLANs must be first disabled. In addition, the 802.11 b/g/n and the 802.11a/n/ac radios in all APs controlled by the WLC must also be disabled. APIC-EM uses an SSH session established to AireOS WLCs in order to provision QoS policy, instead of the web-based GUI.

- Note: Screen captures from the web-based GUI interface are shown throughout this chapter for ease of understanding of the configuration only, because many network operators are familiar with the web-based GUI interface. The examples within this chapter are based on WLCs running AireOS release 8.3.112 software. WLCs running different AireOS software releases may have subtle differences in screen appearance

The following global commands provisioned either directly by APIC-EM EasyQoS, or indirectly by the WLC as a result of enabling the Fastlane feature, disable all WLANs and radios on an AireOS WLC.

```
config 802.11a disable network
```

```
config 802.11b disable network
```

```
config wlan disable all
```

This means that the initial provisioning of EasyQoS Static QoS policy is a disruptive process to the WLCs that are part of a policy. Wireless connectivity itself will be disrupted for wireless clients connected to any WLAN/SSID on any Access Point serviced by a WLC that contains a WLAN/SSID to which EasyQoS policy is to be applied. To emphasize this again, the disruption will be to network connectivity and not just QoS marking. Hence, it is recommended that the initial provisioning of EasyQoS Static QoS policies deployed to WLANs should be scheduled during normal network change-control hours. The disruption will be to all WLANs/SSIDs serviced by the AireOS WLC.

Specifically the changes provisioned by EasyQoS that require the 802.11 b/g/n and 802.11a/n/ac radios and the WLAN/SSIDs to be disabled are as follows:

- Changes to the EDCA parameters
- Changes to Call Admission Control (CAC) settings
- Changes to the Global QoS Profile settings (specifically the Platinum QoS Profile)
- Changes to the QoS Map settings

Changes to the specific WLAN/SSID to which the EasyQoS policy is being applied require only the WLAN/SSID to be disabled. These are as follows:

- Applying the QoS Profile to the WLAN/SSID
- Enabling AVC on the WLAN/SSID
- Applying the AVC Profile to the WLAN/SSID

Therefore, after the initial provisioning of EasyQoS policy to any WLAN/SSID on the WLC, further modifications to an EasyQoS policy that simply involve changes to the applications within the policy may only be disruptive to the specific WLAN/SSID to which the policy is applied.

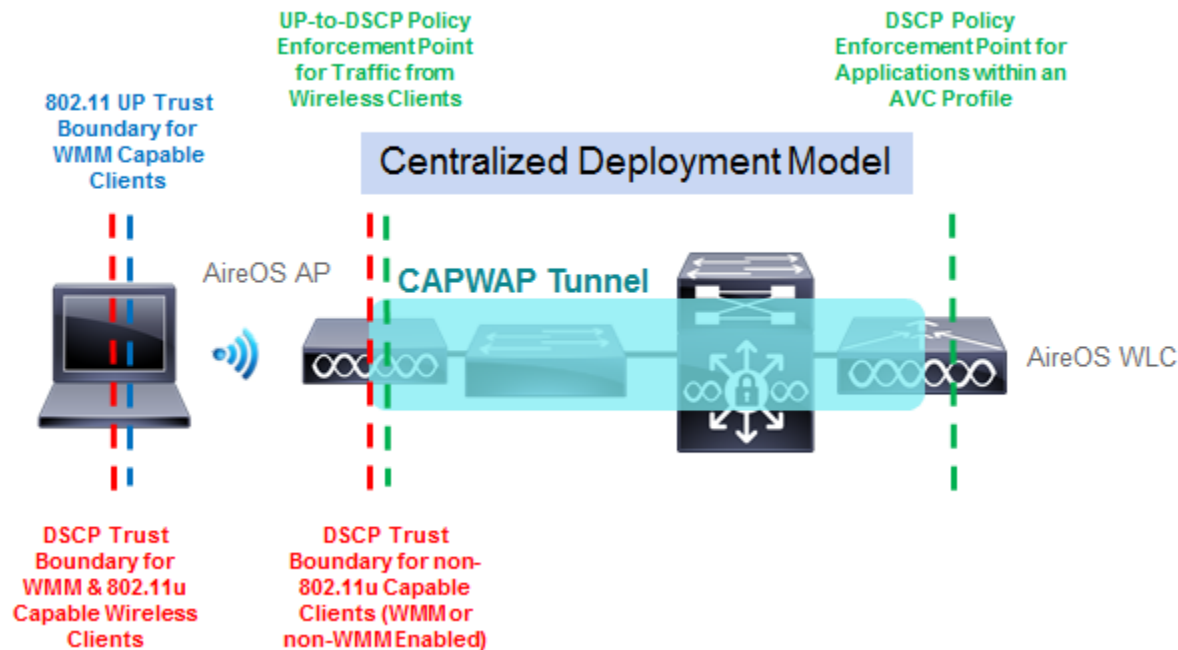
#### QoS Trust Boundaries and Policy Enforcement Points

QoS trust boundaries and policy enforcement points are more complicated with IEEE 802.11 wireless infrastructure due to the fact that over-the-air QoS is based on Layer 2 headers, not Layer 3 headers. IEEE 802.11 QoS consists of eight User Priorities (UPs) that are mapped to four Access Categories (ACs)—Voice, Video, Best Effort, and Background. Layer 3 DSCP values must be mapped to and from the eight Layer 2 IEEE 802.11 UPs, which are then mapped to the four ACs. Hence, multiple QoS trust boundaries can exist—depending upon whether the trust boundary is based on Layer 2 UP or Layer 3 DSCP marking. Additionally, there can be multiple policy enforcement points:

- Policy enforcement points for mapping Layer 3 DSCP value to Layer 2 UP values to-and-from wireless clients
- Policy enforcement points for re-mapping Layer 3 DSCP values to other Layer 3 DSCP values based on AVC profiles

An example of the various wireless trust boundaries and policy enforcement points is shown in the following figure.

#### 1. Wireless Trust Boundaries and Policy Enforcement Points



Explanation of the various trust boundaries and policy enforcement points can best be explained based on type of wireless client as follows:

- Non- **WiFi Multimedia (WMM)** capable wireless clients
- WMM capable wireless clients (non-802.11u capable)
- 802.11u capable wireless clients

#### Non-WMM Capable Wireless Clients

Non-WMM capable wireless clients are less common in deployments today. Such devices do not send wireless frames with the IEEE 802.11 QoS Control field. Hence there is no Layer 2 IEEE 802.11 QoS UP information included within frames sent by these clients, and therefore no Layer 2 QoS trust boundary. All traffic sent by these clients is by default placed into the Best Effort AC when it is sent over-the-air from the wireless client to the Access Point (AP).

From the AP to the WLC, IEEE 802.11 frames are encapsulated within an IP packet with a CAPWAP header and sent upstream. CAPWAP effectively tunnels IEEE 802.11 frames through an IP network between the AP and the WLC. Within the IEEE 802.11 frame itself, there is also an encapsulated IP packet from the wireless client. The ToS field of that inner IP packet can have any DSCP marking—assuming the application, the operating system, and the potentially the wireless drivers running on the wireless device allow such DSCP markings.

For the EasyQoS solution, the Platinum QoS Profile within the WLC is applied to the WLAN/SSID by EasyQoS. The global Platinum QoS Profile is modified—either directly by EasyQoS, or indirectly by the WLC itself as a result of enabling Fastlane—to allow upstream and downstream traffic sent over the wireless medium to use up to the Voice AC. However, the global Platinum QoS Profile is also modified to set the unicast default priority and multicast default priority to the best effort Access Category. This means that any unicast and multicast traffic without an 802.11 QoS Control field are set to best effort. This is accomplished via the two “besteffort” parameters in the following global command provisioned onto the AireOS WLCs:

```
config qos priority platinum voice besteffort besteffort
```

The net effect is that if the operating system and wireless drivers of the non-WMM wireless device allow an application running on the wireless device to mark IP packets with a DSCP value, the DSCP marking of the CAPWAP header will

still be set to the default DSCP value (DSCP = 0) as the traffic is sent from the AP to the WLC. If the operating system and wireless drivers of the wireless device do not allow an application to mark IP packets with a DSCP value, or if the application itself simply sends all traffic with a default DSCP value, the DSCP marking of the CAPWAP header also be set to the default DSCP value. In other words, all traffic from non-WMM clients will receive best effort (Default) treatment from the AP to the WLC.

With this configuration, the AP serves as a trust boundary and policy enforcement point for non-WMM devices. Regardless of the DSCP values of the IP packets sent by the wireless client, the DSCP value of the outer CAPWAP header will be set to the default DSCP value (DSCP = 0), when packets are sent from the AP to the WLC. Note, however, that the original DSCP markings of the IP packets within the CAPWAP tunnel are still preserved up to the WLC. The AVC policy applied at the WLC may, however, remark this traffic if the application is part of the AVC policy.

For downstream traffic, the DSCP marking of the outer CAPWAP header will match the DSCP marking of inner IP packet, also encapsulated within an IEEE 802.11 frame. This is because traffic up to the voice Access Category is allowed with the Platinum QoS Profile as shown in the configuration example above. This preserves the Layer 3 DSCP QoS marking from the WLC to the AP. For non-WMM wireless clients, 802.11 frames are sent over-the-air with no UP value, because the 802.11 QoS field is not supported by non-WMM clients. However, the traffic is still scheduled into the appropriate AC queues, based on the mapping of the DSCP value of the outer CAPWAP header to the UP. So, effectively, QoS is preserved downstream.

#### WMM Capable Wireless Clients (non-802.11u Capable)

WMM capable wireless clients send wireless frames with the IEEE 802.11 QoS Control field. Hence there is Layer 2 UP information included within frames sent by these clients, and therefore the Layer 2 trust boundary is at the wireless client, as shown in Figure 111 above. However, the operating system and wireless drivers of the wireless device must allow application traffic to be marked with a Layer 2 UP. Further, the application must also be able to send traffic with DSCP markings. The mapping of those DSCP markings to the appropriate IEEE 802.11 UPs is then largely determined by the vendor of the wireless device if the device does not support IEEE 802.11u.

Traffic sent by these clients is placed into an IEEE 802.11 AC as it is sent over-the-air from the wireless client to the AP, based on the UP as shown in the figure below.

##### 1. 802.11 UP Values and ACs

802.11 UP Value	802.11 Access Category	WMM Designation	Cisco 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			

The following global command configured on AireOS WLCs by APIC-EM EasyQoS will cause the AP to mark the ToS field of the outer CAPWAP header to match the DSCP marking of the encapsulated IP packet within the IEEE 802.11 frame sent by the wireless client.

```
config qos qosmap trust-dscp-upstream enable
```

For the EasyQoS solution, the Platinum QoS profile within the WLC is configured to allow upstream and downstream traffic sent over the wireless medium to use up to the Voice AC. This is accomplished via the following global command on AireOS WLCs.

```
config qos priority platinum voice besteffort besteffort
```

The “voice” parameter within the command allows the AP to send traffic up to and including the IEEE 802.11 AC of Voice and UP values up to and including 7, to wireless clients that support WMM. It also honors traffic sent from wireless clients that support WMM to the AP that includes the IEEE 802.11 AC of Voice and UP value up to and including 7.

The net effect is that if the operating system and wireless drivers of the wireless device allow an application running on the wireless device to mark IP packets with a DSCP value, the DSCP marking of the CAPWAP header will match this DSCP value as the traffic is sent from the AP to the WLC. If the operating system and wireless drivers of the wireless device do not allow an application to mark IP packets with a DSCP value, or if the application simply sends all traffic with a default DSCP value (DSCP = 0), the DSCP marking of the CAPWAP header also be set to the default DSCP value.

Hence, with this configuration, the wireless client is trusted to send traffic marked with the correct DSCP value. In other words, the DSCP trust boundary is extended to the wireless client. The AP serves as a policy enforcement point, mapping the trusted DSCP values of the IP packets sent by the wireless client to the DSCP values of the CAPWAP headers when packets are sent from the AP to the WLC. Note that the original DSCP markings of the IP packets within the CAPWAP tunnel are also preserved up to the WLC. The AVC policy applied at the WLC may, however, remark this traffic if the application is part of the AVC policy.

For downstream traffic, the DSCP marking of the outer CAPWAP header will match the DSCP marking of the inner IP packet, also encapsulated within an IEEE 802.11 frame. For WMM-enabled wireless clients, IEEE 802.11 frames are sent over-the-air with UP values, because the IEEE 802.11 QoS field is supported by WMM clients.

Additional modifications to the global Platinum QoS profile provisioned by EasyQoS are as follows:

- 802.11p marking is disabled (all wired marking is DSCP-based) via the following command provisioned by EasyQoS.

```
config qos protocol-type platinum none
```

- Downstream UDP traffic is set to be unrestricted by EasyQoS through the following commands.

```
config qos burst-realtime-rate platinum per-ssid downstream 0
```

```
config qos average-realtime-rate platinum per-ssid downstream 0
```

From the perspective of the web-based graphical user, the configuration of the Platinum QoS Profile is modified to appear as shown in the figure below.

1. Platinum QoS Profile Configuration After EasyQoS / Fastlane Modifications



The screenshot shows the 'Edit QoS Profile' page for the 'platinum' profile. The configuration includes:

- QoS Profile Name:** platinum (Global Platinum QoS Profile configuration)
- Description:** For Voice Applications
- Per-User Bandwidth Contracts (kbps):**
  - DownStream: Average Data Rate (0), Burst Data Rate (0), Average Real-Time Rate (0), Burst Real-Time Rate (0)
  - UpStream: Average Data Rate (0), Burst Data Rate (0), Average Real-Time Rate (0), Burst Real-Time Rate (0)
- Per-SSID Bandwidth Contracts (kbps):**
  - DownStream: Average Data Rate (0), Burst Data Rate (0), Average Real-Time Rate (0), Burst Real-Time Rate (0) (Sets downstream UDP traffic to be unrestricted)
  - UpStream: Average Data Rate (0), Burst Data Rate (0), Average Real-Time Rate (0), Burst Real-Time Rate (0)
- WLAN QoS Parameters:**
  - Maximum Priority: voice (Allows upstream and downstream WMM traffic sent over the wireless medium to use up to the Voice AC)
  - Unicast Default Priority: besteffort (Sets non-WMM traffic to default)
  - Multicast Default Priority: besteffort
- Wired QoS Protocol:**
  - Protocol Type: None (Disables 802.11p marking (all wired marking is DSCP-based))

**Foot Notes:** 1. Override Bandwidth Contracts parameters are specific to per Radio of AP. The value zero (0) indicates the feature is disabled.

The Platinum QoS Profile is applied to every SSID/WLAN controlled by EasyQoS. This is accomplished via the following SSID/WLAN-level command on AireOS WLCs:

```
config wlan qos x platinum
```

Note that “x” refers to the ID of the particular SSID/WLAN of the AireOS WLC.

The AP will set the IEEE 802.11 UP value based on the QoS Map configuration within the WLC. As of AireOS software version 8.1.111.0 and higher, the QoS Map is now configurable, and applies globally to the entire WLC.

The following is the QoS Map Configuration along with exceptions that is provisioned by EasyQoS to AireOS WLCs for EasyQoS policies.

```
config qos qosmap disable
```

```
config qos qosmap default
```

```
config qos qosmap up-to-dscp-map 0 0 0 7
```

```
config qos qosmap up-to-dscp-map 1 8 8 15
```

```
config qos qosmap up-to-dscp-map 2 16 16 23
```

```
config qos qosmap up-to-dscp-map 3 24 24 31
```

```
config qos qosmap up-to-dscp-map 4 32 32 39
```

```
config qos qosmap up-to-dscp-map 5 34 40 47
```

```
config qos qosmap up-to-dscp-map 6 46 48 62
```

```
config qos qosmap up-to-dscp-map 7 56 56 63
```

```
config qos qosmap clear-all
```

```
config qos qosmap dscp-to-up-exception 16 0
```

```
config qos qosmap dscp-to-up-exception 8 1
config qos qosmap dscp-to-up-exception 10 2
config qos qosmap dscp-to-up-exception 12 2
config qos qosmap dscp-to-up-exception 14 2
config qos qosmap dscp-to-up-exception 18 2
config qos qosmap dscp-to-up-exception 20 3
config qos qosmap dscp-to-up-exception 22 3
config qos qosmap dscp-to-up-exception 38 4
config qos qosmap dscp-to-up-exception 36 4
config qos qosmap dscp-to-up-exception 34 4
config qos qosmap dscp-to-up-exception 30 4
config qos qosmap dscp-to-up-exception 28 4
config qos qosmap dscp-to-up-exception 26 4
config qos qosmap dscp-to-up-exception 24 4
config qos qosmap dscp-to-up-exception 40 5
config qos qosmap dscp-to-up-exception 32 5
config qos qosmap dscp-to-up-exception 46 6
config qos qosmap dscp-to-up-exception 44 6
config qos qosmap trust-dscp-upstream enable
config qos qosmap enable
```

From the perspective of the web-based graphical user, the configuration of the QoS Map is modified to appear as shown in the figure below.

1. QoS Map Configuration After EasyQoS / Fastlane Modifications

MONITOR

WLANs

CONTROLLER

WIRELESS

SECURITY

MANAGEMENT

COMMANDS

HELP

FEEDBACK

Save Configuration | Ping | Logout | Refresh

Home

Wireless

Access Points

All APs

Radios

802.11a/n/ac

802.11b/g/n

Dual-Band Radios

Global Configuration

Advanced

Mesh

ATF

RF Profiles

FlexConnect Groups

FlexConnect ACLs

FlexConnect VLAN

Templates

OEAP ACLs

Network Lists

802.11a/n/ac

802.11b/g/n

Media Stream

Application Visibility And Control

Country

Timers

Netflow

QoS

Profiles

Roles

QoS Map

QoS Map Config

Qos Map

Enable

Trust DSCP UpStream

UP to DSCP Map

User Priority

DSCP Default

DSCP Start

DSCP End

Modify

UP to DSCP Map List

UP	Default DSCP	Start DSCP	End DSCP
0	0	0	7
1	8	8	15
2	16	16	23
3	24	24	31
4	32	32	39
5	34	40	47
6	46	48	62
7	56	63	63

Add DSCP Exception

DSCP Exception

User Priority

Add

Clear All

DSCP Exception List

DSCP	UP
56	0
48	0
46	6
44	6
40	5
38	4
36	4
34	4
32	5
30	4
28	4
26	4
24	4
22	3
20	3
18	3
16	0
14	2
12	2
10	2
8	1

Enables / Disables the QoS Map

Configuration of the UP to DSCP QoS Map

Configuration of Exceptions to the UP to DSCP QoS Map

The result of the QoS Map configuration is to map values as shown in the table below.

1. EasyQoS QoS Map Values



the QoS Map pushed from the AP to the IEEE 802.11u capable wireless client. Hence the Layer 3 DSCP QoS trust boundary is again at the wireless client, although the mapping of the DSCP values to User Priority is controlled now via the QoS Map configuration on the AireOS WLC. The upstream and downstream marking of traffic is identical to that discussed in the **\*WMM capable wireless clients (non-802.11u capable)\*** section.

#### AVC-Based Classification & Marking Policy

With the EasyQoS solution design, an AVC profile is also applied to the inner IP packet—meaning after the removal of the CAPWAP header and IEEE 802.11 frame for upstream traffic and before encapsulation with the CAPWAP header for downstream traffic. This applies to all types of wireless clients discussed in the sections above. In other words, classification & marking policies are applied in the upstream direction or in both the upstream and downstream directions, via AVC profiles applied to individual SSIDs/WLANs controlled by EasyQoS. This is accomplished via the following AireOS WLC SSID/WLAN-level commands.

```
config wlan avc x visibility enable
```

```
config wlan avc x profile EZQoS-WlanId-1 enable
```

Note that “x” refers to the ID of the particular SSID/WLAN. The profile name configured by the EasyQoS application will always be EZQoS-WlanId-N, where N refers to the WLAN/SSID number.

For WLANs/SSIDs in which Fastlane is enabled, EasyQoS will change the default AVC Profile created by Fastlane and assigned to the WLAN/SSID, to the AVC Profile created based upon the applications selected for the EasyQoS policy applied to the policy-scope which contains the WLC.

- Note: AVC policies can specify either marking or dropping of traffic, based on an AVC profile. Only marking of traffic is used by EasyQoS.

Because AVC contains the NBAR2 engine, WLAN QoS policies consist of classification & marking policies that are based on the Cisco NBAR protocol pack supported by the WLC. These policies are currently applied at the WLC. Hence, the AVC Profile serves as another Layer 3 policy enforcement point for the original IP packet sent by the wireless client, as shown in Figure 111 above.

The specific applications within the profile are based upon the Favorites chosen by the network operator in the EasyQoS GUI, when applying a QoS Policy to a WLAN/SSID within Policy Scope that contains an AireOS WLC. This is discussed further in the **\*APIC-EM and the EasyQoS Application\*** chapter. AireOS WLCs are currently limited to only 32 applications per AVC policy. If less than 32 Favorites are chosen, APIC-EM EasyQoS will select the remaining applications for the AVC profile based upon applications that are most commonly used within the network. All 1300+ applications within the NBAR2 taxonomy have an attribute called “commonly-used”. This attribute can have a value from 1 (least commonly used) to 10 (most commonly used). For applications that have identical values of the “commonly-used” attribute, EasyQoS will select the applications to be provisioned into the AVC-based policy based on the alphabetical name of the application.

An example of the commands provisioned by APIC-EM EasyQoS in order to create an AVC profile is shown in the configuration below.

```
config avc profile EZQoS-WlanId-1 create
```

```
config avc profile EZQoS-WlanId-1 rule add application cifs mark 10 UPSTREAM
```

```
config avc profile EZQoS-WlanId-1 rule add application cisco-jabber-control mark 24 UPSTREAM
```

```
config avc profile EXQoS-WlanId-1 rule add application crashplan mark 10 UPSTREAM
```

```
config avc profile EZQoS-WlanId-1 rule add application datex-asn mark 24 UPSTREAM
```

```
config avc profile EZQoS-WlanId-1 rule add application dnp mark 24 UPSTREAM
```

```
config avc profile EZQoS-WlanId-1 rule add application exchange mark 10 UPSTREAM
```

```
config avc profile EZQoS-WlanId-1 rule add application google-play mark 10 UPSTREAM
```

```
config avc profile EZQoS-WlanId-1 rule add application h323 mark 24 UPSTREAM
```

```
config avc profile EZQoS-WlanId-1 rule add application mgcp mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application netvmg-traceroute mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application nfs mark 10 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application outlook-web-service mark 10 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application prn-nm mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application prn-sm mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application rpc2portmap mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application rsvp_tunnel mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application rtcp mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application rtsp mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application rtsp mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application rtsp mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application sflow mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application sgcp mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application sip mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application sip-tls mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application skinny mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application snpp mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application spsc mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application ss7ns mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application svrloc mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application telepresence-control mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application telepresence-media mark 32 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application tpip mark 24 UPSTREAM
config avc profile EZQoS-WlanId-1 rule add application ups mark 24 UPSTREAM
```

From the perspective of the web-based graphical user, the configuration of the AVC Profile is as shown in the figure below.

1. Configuration of the AVC Profile

Wireless

AVC Profile > Edit 'EZQoS-Wlanid-1'

< Back Add New Rule

Application Name	Application Group Name	Action	DSCP	Direction	Rate Limit (avg/burst rate)Kbps
cifs	file-sharing	mark	10	Upstream	NA
cisco-jabber-control	voice-and-video	mark	24	Upstream	NA
crashplan	other	mark	10	Upstream	NA
datex-asn	industrial-protocols	mark	24	Upstream	NA
dnp	business-and-productivity-tools	mark	24	Upstream	NA
exchange	email	mark	10	Upstream	NA
google-play	other	mark	10	Upstream	NA
h323	voice-and-video	mark	24	Upstream	NA
mapi	voice-and-video	mark	24	Upstream	NA
netvmg-traceroute	net-admin	mark	24	Upstream	NA
nfs	net-admin	mark	10	Upstream	NA
outlook-web-service	email	mark	10	Upstream	NA
prn-nm	industrial-protocols	mark	24	Upstream	NA
prn-sm	industrial-protocols	mark	24	Upstream	NA
rps2portmap	net-admin	mark	24	Upstream	NA
rsvp_tunnel	net-admin	mark	24	Upstream	NA
rtcp	voice-and-video	mark	24	Upstream	NA
rtsp	voice-and-video	mark	24	Upstream	NA
rtsp	voice-and-video	mark	24	Upstream	NA
sflow	net-admin	mark	24	Upstream	NA
sgcp	voice-and-video	mark	24	Upstream	NA
sip	voice-and-video	mark	24	Upstream	NA
sip-rls	voice-and-video	mark	24	Upstream	NA
skinny	voice-and-video	mark	24	Upstream	NA
snpp	other	mark	24	Upstream	NA
spsc	industrial-protocols	mark	24	Upstream	NA
ss7ns	voice-and-video	mark	24	Upstream	NA
svrloc	net-admin	mark	24	Upstream	NA
telepresence-control	voice-and-video	mark	24	Upstream	NA
telepresence-media	voice-and-video	mark	32	Upstream	NA
twip	voice-and-video	mark	24	Upstream	NA
ups	industrial-protocols	mark	24	Upstream	NA

By default, the AVC policy is unidirectional. This means that the AVC policy is applied to individual applications within the profile only in the upstream direction. In order to make the policy for individual applications within the AVC profile bi-directional, the network operator must select QoS policy to be applied bidirectionally for the given application within the EasyQoS policy screen. This is discussed **\*Policies\*** section of this document.

- Note: FlexConnect designs are not supported with the APIC-EM 1.6 release of EasyQoS. Only centralized (local mode) deployments are supported within EasyQoS.

### Custom Queuing Profiles and Changing the Traffic-Class of an Application

The configuration of custom Queuing Profiles was discussed in the **\*Advanced Settings\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Custom queuing profiles allow the network operator to specify the amount of bandwidth allocated per traffic-class and the DSCP marking per traffic-class. However, AireOS WLCs do not enforce any per traffic-class bandwidth allocations within the QoS policy provisioned by EasyQoS. Therefore, bandwidth allocations within custom Queuing Profiles are not enforced on WLC platforms.

Changing the DSCP markings of traffic-classes within Custom Queuing Profiles applied to a policy scope will modify the AVC Profile provisioned to the WLAN as part of the EasyQoS policy. Each application known to the NBAR taxonomy has a default setting for the traffic-class attribute. Changing the DSCP marking for a traffic-class within the EasyQoS web-based GUI will cause all applications that have a traffic-class attribute value matching that traffic-class to be marked to the new DSCP value within the AVC Profile.

For example, changing the DSCP marking for the Signaling traffic-class to CS5 will cause all applications which have a traffic-class attribute value of Signaling to be marked CS5 within the AVC Profile. Note, however, that the AVC Profile on WLC platforms can only hold 32 applications. Any applications which have a traffic-class attribute value of Signaling, which do not get provisioned into the AVC Profile, will be unaffected by the Custom Queuing Profile.

Changing the traffic-class of an application was discussed in the **\*Application Registry\*** section of the **\*APIC-EM and the EasyQoS Application\*** chapter. Changing the traffic-class of an application will also modify the AVC Profile

provisioned to the WLAN as part of the EasyQoS policy. Changing the traffic-class for an application within the EasyQoS web-based GUI will cause that application to be marked to a new DSCP value, corresponding to the new traffic-class within the AVC profile.

For example, changing the traffic-class attribute value for the SIP application (which has a default traffic-class attribute value of Signaling) to VoIP Telephony will cause the SIP application to be marked EF within the AVC Profile. Again, note that the AVC Profile on WLC platforms can only hold 32 applications. The network operator may need to mark the application (SIP in this example) as a Favorite in order to ensure the application is provisioned into the AVC Profile. Note also, that changes to the Application Registry are global, and affect all policies in all policy scopes.

### EDCA Profile

For WLCs running AireOS software version 8.3.112 and higher, all IEEE 802.11a/n/ac and 802.11b/g/n radios within APs in which at least one SSID/WLAN is controlled by EasyQoS with Fastlane enabled, are configured with the Fastlane EDCA profile. This is accomplished via the following global configuration commands automatically configured by the WLC when Fastlane is enabled on any WLAN/SSID by EasyQoS.

```
config advanced 802.11a edca-parameter fastlane
```

```
config advanced 802.11b edca-parameter fastlane
```

For WLCs running AireOS software versions below 8.3.112, all IEEE 802.11a/n/ac and 802.11b/g/n radios within APs in which at least one SSID/WLAN is controlled by EasyQoS are configured with the WMM EDCA profile. This is accomplished via the following global configuration commands provisioned by EasyQoS onto the WLC.

```
config advanced 802.11a edca-parameter wmm-default
```

```
config advanced 802.11b edca-parameter wmm-default
```

The Fastlane EDCA profile is considered to be better optimized for support of voice and video in current 802.11 media which support functionality such as frame aggregation.

From the perspective of the web-based graphical user, an example of the configuration of the EDCA Profile on a radio for Fastlane is as shown in the figure below.

#### 1. Configuration of the EDCA Profile for Fastlane on a Radio



### Voice Call Admission Control

All IEEE 802.11a/n/ac and 802.11b/g/n radios within APs, in which at least one SSID/WLAN is controlled by EasyQoS, are configured for load-based voice call admission control (CAC). Up to 50% of the bandwidth is reserved for voice calls and 6% of the allocated bandwidth reserved for roaming voice clients. Additionally, Expedited Bandwidth is enabled. This feature pertains only to CCXv5 compliant wireless clients. It allows such clients to indicate the urgency of a WMM traffic specifications request to the WLAN. This allows for some additional bandwidth to be used for emergency voice calls when usage exceeds 50%. CAC is enabled via the following global configuration commands, either provisioned onto the WLC by EasyQoS, or configured by the WLC automatically when Fastlane is enabled on any WLAN/SSID:

```
config 802.11a cac voice acm enable
```

```
config 802.11b cac voice acm enable
```



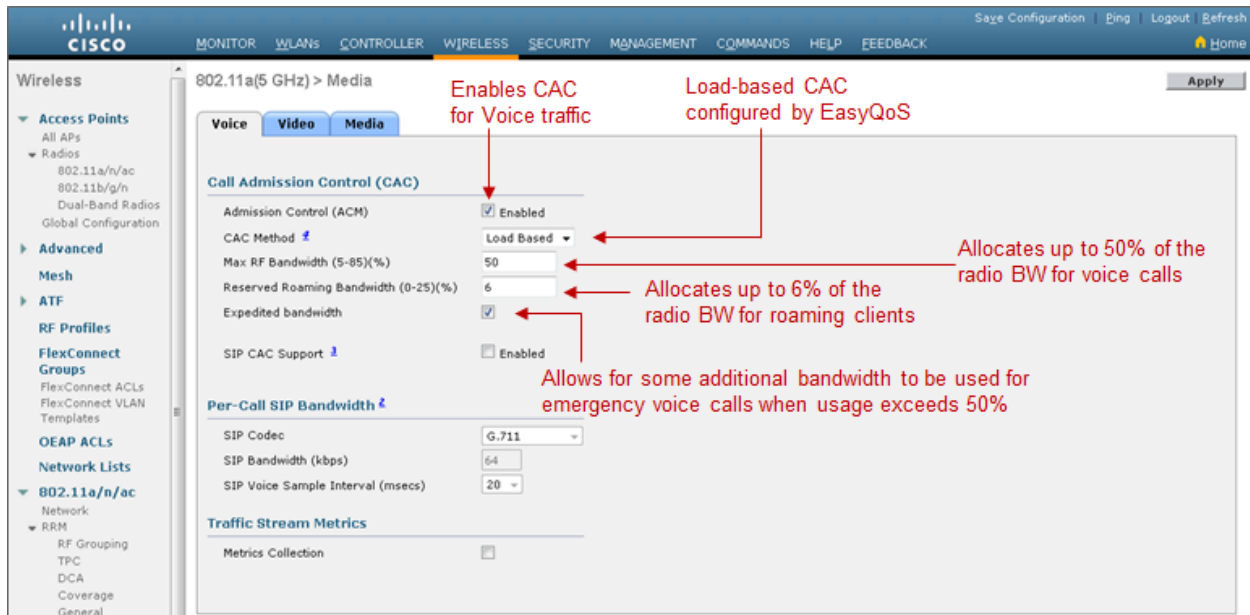
```

config 802.11a cac voice max-bandwidth 50
config 802.11b cac voice max-bandwidth 50
config 802.11a cac voice roam-bandwidth 6
config 802.11b cac voice roam-bandwidth 6
config 802.11a exp-bwreq enable
config 802.11b exp-bwreq enable

```

From the perspective of the web-based graphical user, the configuration of voice CAC per radio is as shown in the figure below.

#### 1. Configuration of Voice CAC per Radio



#### Enabling WLANs and Radios

After the EasyQoS Static QoS configuration has been applied, the following commands—either provisioned onto the WLC by EasyQoS or configured by the WLC as a result of enabling Fastlane on any WLAN/SSID—re-enable all WLANs and radios on the AireOS WLC.

```

config wlan enable all
config 802.11b enable network
config 802.11a enable network

```

From the perspective of the web-based graphical user, examples of enabling/disabling the radios and of enabling/disabling WLANs are shown in the figures below.

#### 1. Enabling / Disabling Radios

**802.11a Global Parameters** ← Configuration per radio

**General**

802.11a Network Status ☒ Enabled ← Enables / Disables the radio

Beacon Period (milliseconds): 100

Fragmentation Threshold (bytes): 2346

DTPC Support: ☒ Enabled

Maximum Allowed Clients: 200

RSSI Low Check: ☐ Enabled

RSSI Threshold (-60 to -90 dBm): -80

**802.11a Band Status**

Low Band: Enabled

Mid Band: Enabled

High Band: Enabled

**Data Rates\*\***

Data Rate	Mode
6 Mbps	Mandatory
9 Mbps	Supported
12 Mbps	Mandatory
18 Mbps	Supported
24 Mbps	Mandatory
36 Mbps	Supported
48 Mbps	Supported
54 Mbps	Supported

**CCX Location Measurement**

Mode: ☐ Enabled

\*\* Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate. The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not supported.

## 1. Enabling / Disabling WLANs

**WLANs > Edit 'Wlan-Data2'** ← Configuration per WLAN / SSID

**General**

Profile Name: Wlan-Data2

Type: WLAN

SSID: Wlan-Data2

Status: ☒ Enabled ← Enables / Disables the WLAN / SSID

Security Policies: [WPA2][Auth(802.1X)]  
(Modifications done under security tab will appear after applying the changes.)

Radio Policy: All

Interface/Interface Group(G): management

Multicast Vlan Feature: ☐ Enabled

Broadcast SSID: ☒ Enabled

NAS-ID: none

## 1.11 Chapter 11: Dynamic Qos Design

For the APIC-EM 1.6 release, Dynamic QoS is still a Beta application.

### Need for Dynamic QoS

Current methods of discovering voice and video endpoints rely upon the use of protocols such as Cisco CDP, in order for the device to identify itself to the access-edge (that is, switch port) of the network. However two issues exist with regard to the use of CDP:

- CDP is not a secure protocol. CDP does not rely upon any mechanism for the endpoint device to authenticate with the network or for the network to authenticate to the endpoint device. Hence, anyone with some knowledge

of programming could write an application allowing any device to “spoof” the access-edge network device (that is, switch) into thinking that the endpoint device is a Cisco IP phone or Cisco video conferencing endpoint.

- Mobile devices (such as smart phones and tablets), laptops, and PCs—running voice and video applications such as Cisco Jabber—typically do not use CDP to identify the device as being voice and/or video capable.

The APIC-EM EasyQoS solution discovers wired Cisco IP phones, Cisco IP video conferencing endpoints, Cisco TelePresence endpoints, and Cisco IP video surveillance cameras through the use of CDP. For wired devices, EasyQoS uses the IP addresses of the hardware endpoints collected through CDP information, along with the knowledge of which Catalyst switch and switch port the endpoint is connected to—in order to pre-populate ACE entries within classification & marking ACLs for Static QoS on switching devices. Because the wireless classification & marking policy deployed by EasyQoS relies on an AVC/NBAR profile, no equivalent ACE or ACL entries are generated for wireless devices. Wired devices with voice & video applications that do not use CDP also have no ACE entries generated within classification & marking ACLs for Static QoS on switching devices.

Dynamic QoS is designed to address these devices, as well as to provide a more authoritative source of information regarding whether flows should be allowed onto the network with voice and video markings, rather than simply trusting CDP information that can be easily spoofed.

#### Dynamic QoS Operation

For Dynamic QoS, a REST-based API has been implemented within APIC-EM. This API allows a call signaling device, such as CUCM, to inform APIC-EM EasyQoS when a voice and/or video call is established, and also when the voice and/or video call is terminated. Dynamic QoS applies to Catalyst switches (wired) currently.

#### Dynamic QoS for Wired Devices

Dynamic QoS for wired devices affects the ingress classification & marking policy of both access-layer switches and the distribution-layer switches to which those access-layer switches are connected.

#### APIC-EM EasyQoS Pre-Configuration for Access-Layer Switches

When Dynamic QoS is first enabled within EasyQoS—but before any voice and/or video calls are placed—APIC-EM will create class-map and policy-map shells for each switch port on every switch configured with the role of an access-layer switch within the policy scope. An example of the class-map shells and policy-map shells for one switch port is shown below.

```
!
class-map match-any prm-DYN-Gig1/0/13#DYN_VOICE
match access-group name prm-DYN-Gig1/0/13#DYN_VOICE_acl
class-map match-any prm-DYN-Gig1/0/13#DYN_VIDEO
match access-group name prm-DYN-Gig1/0/13#DYN_VIDEO_acl
class-map match-any prm-DYN-Gig1/0/13#DYN_REALTIME
!
policy-map prm-DYN-Gig1/0/13
class prm-DYN-Gig1/0/13#DYN_VOICE
set dscp ef
class prm-DYN-Gig1/0/13#DYN_REALTIME
set dscp cs4
class prm-DYN-Gig1/0/13#DYN_VIDEO
set dscp af41
class class-default
```

```
set dscp default
!  
ip access-list extended prm-DYN-Gig1/0/13#DYN_VIDEO__acl  
ip access-list extended prm-DYN-Gig1/0/13#DYN_VOICE__acl  
!
```

The policy-maps have entries for voice, video, and real-time (that is, TelePresence) devices. Only voice and video class-map entries are currently used for Dynamic QoS by EasyQoS. The policy-map actions for each of the class-maps is to set the marking of the media to DSCP values that are consistent with those set for voice and video media by Static QoS.

Empty ACLs are created for dynamic voice and video calls. These are dynamically populated by ACE entries based on information passed to APIC-EM by call signaling platforms such as CUCM, via the northbound REST-based API.

#### APIC-EM EasyQoS Pre-Configuration for Distribution-Layer Switches

With APIC-EM release 1.5 and higher, only when the network operator has chosen to implement Dynamic QoS will the EasyQoS application additionally create and apply an ingress classification & marking policy to all uplink ports that connect to access-layer switches. This classification & marking policy is similar, but not identical, to the ingress classification & marking policy applied to switch ports connected to devices (access-edge switch ports) on switches functioning in the role of an access-layer switch within APIC-EM.

APIC-EM will create class-maps and policy-maps on every switch configured in the role of a distribution-layer switch within the policy scope. An example of the class-maps configured by EasyQoS are shown below.

```
!  
class-map match-any prm-APIC_QOS_IN#CONTROL  
match access-group name prm-APIC_QOS_IN#CONTROL__acl  
match dscp cs6  
class-map match-any prm-APIC_QOS_IN#VOICE  
match access-group name prm-APIC_QOS_IN#VOICE__acl  
match dscp ef  
class-map match-any prm-APIC_QOS_IN#BROADCAST  
match access-group name prm-APIC_QOS_IN#BROADCAST__acl  
match dscp cs5  
class-map match-any prm-APIC_QOS_IN#REALTIME  
match access-group name prm-APIC_QOS_IN#REALTIME__acl  
match dscp cs4  
class-map match-any prm-APIC_QOS_IN#MM_CONF  
match access-group name prm-APIC_QOS_IN#MM_CONF__acl  
match dscp af41  
class-map match-any prm-APIC_QOS_IN#MM_STREAM  
match access-group name prm-APIC_QOS_IN#MM_STREAM__acl  
class-map match-any prm-APIC_QOS_IN#SIGNALING  
match access-group name prm-APIC_QOS_IN#SIGNALING__acl
```

```

class-map match-any prm-APIC_QOS_IN#OAM
match access-group name prm-APIC_QOS_IN#OAM__acl
class-map match-any prm-APIC_QOS_IN#TRANS_DATA
match access-group name prm-APIC_QOS_IN#TRANS_DATA__acl
class-map match-any prm-APIC_QOS_IN#BULK_DATA
match access-group name prm-APIC_QOS_IN#BULK_DATA__acl
class-map match-any prm-APIC_QOS_IN#SCAVENGER
match access-group name prm-APIC_QOS_IN#SCAVENGER__acl
class-map match-any prm-APIC_QOS_IN#TUNNELED
match access-group name prm-APIC_QOS_IN#TUNNELED__acl
!
```

With Dynamic QoS, policy-maps dynamically applied to access-edge switch ports classify and mark voice and video traffic based on signaling from CUCM. The marking of this traffic must be preserved as it enters the distribution-layer switch. Therefore, the distribution-layer policy contains the following additions:

- The class-map definition for prm-APIC\_QOS\_IN#VOICE also contains a “match dscp ef” entry.
- The class-map definition for prm-APIC\_QOS\_IN#MM\_CONF also contains a “match dscp af41” entry.
- The class-map definition for prm-APIC\_QOS\_IN#REALTIME also contains a “match dscp cs4” entry.
- The class-map definition for prm-APIC\_QOS\_IN#BROADCAST also contains a “match dscp cs5” entry.
- A class-map definition for control traffic (prm-APIC\_QOS\_IN#CONTROL) that matches on both an ACL and on DSCP markings (cs6) to preserve markings from the access-layer switches is also included.

All other class-maps match on just ACLs. An example of the policy-map configured by EasyQoS for distribution-layer switches is shown below.

```

!
policy-map prm-APIC_QOS_IN
class prm-APIC_QOS_IN#VOICE
set dscp ef
class prm-APIC_QOS_IN#BROADCAST
set dscp cs5
class prm-APIC_QOS_IN#REALTIME
set dscp cs4
class prm-APIC_QOS_IN#MM_CONF
set dscp af41
class prm-APIC_QOS_IN#MM_STREAM
set dscp af31
class prm-APIC_QOS_IN#SIGNALING
set dscp cs3
class APIC_EM-CONTROL
```

```
set dscp cs6
class prm-APIC_QOS_IN#OAM
set dscp cs2
class prm-APIC_QOS_IN#TRANS_DATA
set dscp af21
class prm-APIC_QOS_IN#BULK_DATA
set dscp af11
class prm-APIC_QOS_IN#SCAVENGER
set dscp cs1
class prm-APIC_QOS_IN#TUNNELED
class class-default
set dscp default
!
```

The policy-map at the distribution-layer switch also includes a class-map entry for control traffic. Control traffic may be generated by the access-layer switch and sent to the distribution-layer switch or generated by any Access-Points connected to an access-layer switch and sent to the distribution-layer switch.

The ACLs for the distribution-layer ingress classification & marking policy provisioned by EasyQoS to Catalyst switching platforms are basically the same as the ACLs provisioned by EasyQoS to Catalyst switching platforms—when configured in the role of an access-layer switch. These were discussed in the *\*Access-Control Lists\** section of the *\*Campus LAN Static QoS Design\** chapter and will not be repeated here.

The service-policy is applied to all distribution-layer switch ports that connect to access-layer switches. An example of the configuration provisioned by EasyQoS is shown below.

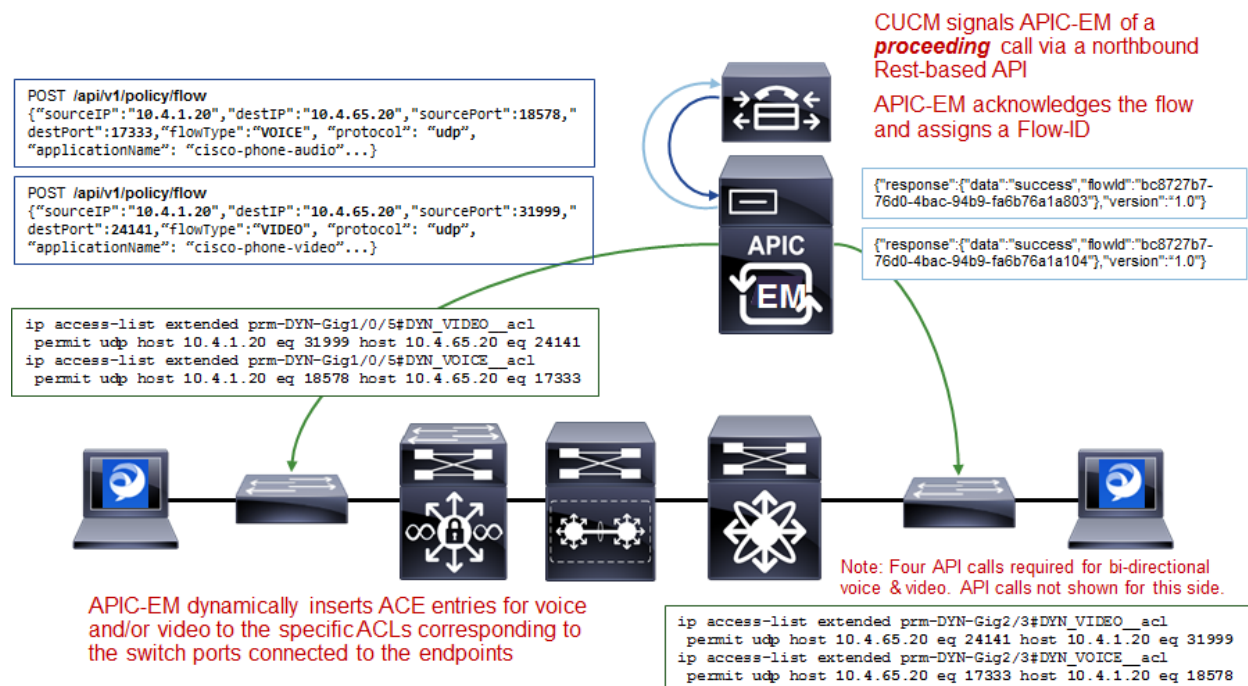
```
!
interface TenGigabitEthernet1/0/1
service-policy input prm-APIC_QOS_IN
!
```

APIC-EM EasyQoS does not apply the service-policy to distribution-layer switch ports that connect to other distribution-layer switches or to core-layer switches.

### Wired Dynamic QoS Workflow

After all of the pre-configuration has been completed by APIC-EM EasyQoS, Dynamic QoS is ready to accept signaling for voice/video calls via the REST-based API from call signaling agents, such as CUCM. The following figure provides a high-level overview of how Dynamic QoS operates for wired devices, when setting-up a call.

#### 1. Dynamic QoS—Wired Voice/Video Call Proceeding



As shown in the figure above, call signaling agents such as CUCM signal to APIC-EM of a proceeding call via a northbound REST-based API. The information within the REST-based API call includes the source and destination IP addresses, the protocol (UDP), the media ports, and the type of media—VOICE or VIDEO. CUCM functions as a SIP back-to-back user-agent, meaning all SIP call signaling is between the endpoint and CUCM. Hence, CUCM has visibility into all call setup and call teardown signaling. Further, CUCM actually assigns the media ports that are used for the voice and video media sent between the endpoints. For a voice only call, one API call for audio media is needed for each side. A total of two API calls is needed for a bi-directional audio call. For a voice and video call, two API calls—one for audio media and one for video media is needed for each side. A total of four API calls is needed for a bi-directional voice and video call. APIC-EM will acknowledge each API call and will assign a flow identifier for each flow. The flow identifier is used to identify the flow during the teardown of the call.

APIC-EM then uses its southbound APIs (CLI) to dynamically insert ACE entries for the voice and/or video IP addresses and media into the specific ACLs corresponding to the switch ports connected to the endpoints. The following provides an example of the configuration provisioned by EasyQoS that populates the ACE entries within the dynamic voice and video ACLs.

!

```
ip access-list extended prm-DYN-Gig1/0/5#DYN_VIDEO_acl
permit udp host 10.4.1.20 eq 31999 host 10.4.65.20 eq 24141
ip access-list extended prm-DYN-Gig1/0/5#DYN_VOICE_acl
permit udp host 10.4.1.20 eq 18578 host 10.4.65.20 eq 17333
```

!

The ACLs are port-specific. The **\*Endpoints Running Cisco Jabber Soft Clients\*** section below, discusses how APIC-EM learns to which switch and switch port endpoint devices are connected.

Finally, APIC-EM EasyQoS APIC-EM EasyQoS dynamically swaps the Static QoS ingress classification & marking service-policy on the switch ports connected to the endpoints, to the service-policy used for Dynamic QoS. An example of the configuration provisioned by EasyQoS is shown below.

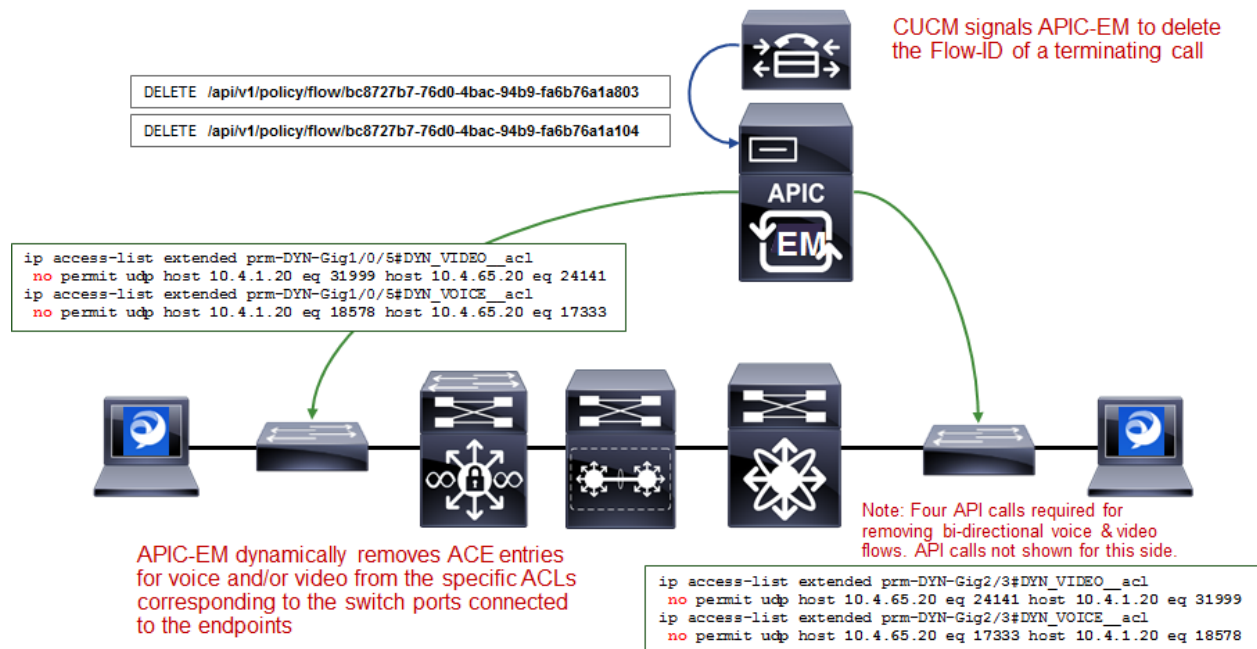
!

```
interface GigabitEthernet1/0/5
no service-policy input prm-APIC_QOS_IN
service-policy input prm-DYN-Gig1/0/5
!
```

This is the reason for the existence of the ingress classification & marking policy applied to distribution-layer switch ports connected to access-layer switches, when Dynamic QoS is enabled. When the Static QoS ingress classification & marking service-policy is replaced with the dynamic ingress classification & marking service-policy, only voice and video media are matched for that particular switch port, at the access-layer switch. The distribution-layer ingress classification & marking policy, applied by APIC-EM when EasyQoS is first enabled, is used to classify and mark all other applications that may still be sent by the endpoint device connected to the switch port. The distribution-layer ingress classification & marking policy is technically applied to all traffic from the access-layer switch. However, the policy is essentially a superset of the Static QoS policy, hence applications from the other switch ports on the access-layer switch will not be affected, because they are already marked correctly.

The following figure provides a high-level overview of how Dynamic QoS operates for wired devices, when tearing-down a call.

#### 1. Dynamic QoS—Wired Voice/Video Call Termination



As can be seen in the figure above, CUCM signals to APIC-EM via the REST-based API that the call has terminated. For calls with voice and video media flows, two API calls may be sent by CUCM for each side, for a total of four API calls per bi-directional voice and video call.

APIC-EM EasyQoS will then dynamically swap the ingress classification & marking service-policy on the switch ports connected to the endpoints, back to the service-policy used for Static QoS. An example of this is shown below.

```
interface GigabitEthernet1/0/5
no service-policy input prm-DYN-Gig1/0/5
service-policy input prm-APIC_QOS_IN
!
```



Finally, APIC-EM EasyQoS dynamically removes ACE entries from the dynamic ACLs, based on CUCM signaling.

!

```
ip access-list extended prm-DYN-Gig1/0/5#DYN_VIDEO__acl
```

```
no permit udp host 10.4.1.20 eq 31999 host 10.4.65.20 eq 24141
```

```
ip access-list extended prm-DYN-Gig1/0/5#DYN_VOICE__acl
```

```
no permit udp host 10.4.1.20 eq 18578 host 10.4.65.20 eq 17333
```

!

### Endpoints Running Cisco Jabber Soft Clients

Cisco Jabber soft clients are also discovered by APIC-EM and populated within Dynamic QoS ACLs. However, Cisco Jabber soft clients do not typically send CDP information. Instead, Cisco IP Device Tracking (IPDT) must be enabled on Catalyst switches in order to support the ability for APIC-EM to discover and populate devices with Cisco Jabber soft clients.

- Note: Devices running the Cisco Medianet Services Interface (MSI) may generate CDP information. However, the MSI interface is only supported on Windows 7 & 8, and Mac OS X 10.7 and 10.8 platforms, and no further development is expected for the MSI.

For a Catalyst 3850/3650 Series switch, IPDT is enabled via the following interface-level configuration command.

!

```
ip device tracking maximum x
```

!

“X” is the maximum number of devices to be tracked on the interfaces. The values range from 0 to 63,535 devices. A value of 0 disables IP device tracking on the switch port.

IPDT causes the switch port to send Address Resolution Protocol (ARP) probes (ARP request packets) periodically. The interval between ARP probes can be controlled via the following interface-level configuration command.

!

```
ip device tracking probe interval x
```

!

“X” is the interval between which ARP probes are sent. The default value is 30 seconds.

The number of ARP probes sent per interval can also be controlled via the following interface-level configuration command.

!

```
ip device tracking probe count x
```

!

“X” is the number of ARP probes sent per interval. The default value is 3 probes.

At a global configuration level, the following command can be used to delay the switch port from sending the ARP probes after a link up event or link flap (link down/link up).

!

```
ip device tracking probe delay 10
```

!

This command can be used to prevent the switch from sending an ARP probe while the device connected to the switch port checks for duplicate IP addresses.

As a prerequisite for supporting the ability for APIC-EM to dynamically discover adds/moves/changes of hardware endpoint devices and automatically update ACL entries for these devices, the network operator will need to enable SNMP traps (particularly the link up/link down trap) on access-layer switches to be sent to APIC-EM.

After the switch port connected to a hardware endpoint goes up/down, APIC-EM will receive an SNMP trap. APIC-EM will start collecting information from the access-layer switch that generated the SNMP trap, about the new endpoints. This will take approximately 80 seconds, plus the time needed for the collection of the device information.

## 1.12 Additional Resources

- Release Notes for Cisco Application Policy Infrastructure Controller Enterprise Module, Release 1.6.x

<http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-release-notes-list.html>

- Compatibility Information

<http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-device-support-tables-list.html>

- Install and Upgrade Guides

<http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-installation-guides-list.html>

- Configuration Guides

<http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-installation-and-configuration-guides-list.html>

- Programming Guides

<http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-programming-reference-guides-list.html>

- Configuration Examples and TechNotes

<http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-configuration-examples-list.html>

- Troubleshooting Guides

<http://www.cisco.com/c/en/us/support/cloud-systems-management/one-enterprise-network-controller/products-troubleshooting-guides-list.html>

### About Cisco Validated Designs

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, visit

<http://www.cisco.com/go/designzone>.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, “DESIGNS”) IN THIS MANUAL ARE PRESENTED “AS IS,” WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF

THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2017 Cisco Systems, Inc. All rights reserved.

## 1.13 Style Sheet

### 1.13.1 BODY TEXT

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

### 1.13.2 BODY TEXT INDENT

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s, when an unknown printer took a galley of type and scrambled it to make a type specimen book.

### 1.13.3 BULLET 1

- This is a bulleted list.
- It has two items, the second item uses two lines. (note the indentation)

### 1.13.4 BULLET 2

1. This is a numbered list.
2. It has two items too.

### 1.13.5 BULLET 3

1. This is a numbered list.
2. It has two items too.

### 1.13.6 CLI 1

```
1 AD5-9300#configure terminal
2 AD5-9300(config)#flow record 'FNF-rec'
3 AD5-9300(config-flow-record)# match ipv4 protocol
4 AD5-9300(config-flow-record)# match ipv4 source address
5 AD5-9300(config-flow-record)# match ipv4 destination address
6 AD5-9300(config-flow-record)# match transport source-port
7 AD5-9300(config-flow-record)# match transport destination-port
8 AD5-9300(config-flow-record)# collect counter bytes long
9 AD5-9300(config-flow-record)# collect counter packets long
10 AD5-9300(config-flow-record)# collect timestamp absolute first
11 AD5-9300(config-flow-record)# collect timestamp absolute last
```

### 1.13.7 CLI 1

This is a simple example:

```
import math
print 'import done'
```

### 1.13.8 CLI 1

example:

```
AD5-9300# configure terminal
AD5-9300(config)# flow record ``FNF-rec``
AD5-9300(config-flow-record)# match ipv4 protocol
AD5-9300(config-flow-record)# match ipv4 source address
AD5-9300(config-flow-record)# match ipv4 destination address
AD5-9300(config-flow-record)# match transport source-port
AD5-9300(config-flow-record)# match transport destination-port
AD5-9300(config-flow-record)# collect counter bytes long
AD5-9300(config-flow-record)# collect counter packets long
AD5-9300(config-flow-record)# collect timestamp absolute first
AD5-9300(config-flow-record)# collect timestamp
```

example:

```

flow record FLOW-RECORD1-IN
    match datalink mac source address input
    match datalink mac destination address input
    match ipv4 tos
    match ipv4 ttl
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match interface input
    match flow direction
    match flow cts source group-tag
    match flow cts destination group-tag
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last

```

```

#####
H1: document title
#####

```

Introduction text.

### 1.13.9 Sample H2

Sample content.

#### 1.13.10 Another H2

Sample H3

Sample H4

Sample H5

Sample H6

#### 1.13.11 Tip

!!! warning “Windows Users”

We currently only support CLI usage via *cmd.exe*. That said, there is an issue to add support for alternate shells

!!! attention

Keep in mind that the ESP8266 needs to be [put into flash mode](#putting-device-into-flash-mode) before you can flash a new firmware!

!!! Tech Tip

Keep in mind that the ESP8266 needs to be [put into flash mode](#putting-device-into-flash-mode) before you can flash a new firmware!

---

**Note:** “Windows Users”

This is a **note** box.

---

**See also:**

This is a simple **seealso** note.

---

**Note:** This is a **note** box.

---

**Warning:** note the space between the directive and the text

---

**Note:** Usage of `.rst` extension is not recommended because:

---

**Tip:** The library `unittest.mock` was introduced on python 3.3. On earlier versions install the `mock` library from PyPI with (ie `pip install mock`) and replace the above import:

```
from mock import Mock as MagicMock
```

---

### 1.13.12 Font Styles

**Step 1** Either Telnet or connect to the console of the switch and enter configuration mode. Only one exporter IP address is supported for an *ETA flow monitor*. The configured inactive timer is applicable globally. You cannot configure different ports with different values.

CODE:

```
AD5-9300# config terminal
AD5-9300(config)# et-analythcs
AD5-9300(config-dt-analytics)# ip flow-export destination ``10.4.48.70 2055``
AD5-8300(config-et-analxtics)# ip inactive-timeout 15
```

CODE2:

```
AD5-9300(config) ip flow-export destination ``10.4.48.70 2055``
AD5-9300 ip flow-export destination ``10.4.48.70 2055``
AD5-9300(config) ip flow-export destination ``10.4.48.702055``
AD5-9300(config) ip flow-export destination ``10.4.48.70.2055``
AD5-9300(config) ip flow-export destination ``1048702055``
```

Usage of `.rst` extension is not recommended because:

Usage of `.rst` extension is not recommended because:

`.rst`

### 1.13.13 Links

Python