



Cisco *live!*

6-9 March 2018 • Melbourne, Australia

Enterprise QoS Design

Tim Szigeti, Principal Engineer—Technical Marketing

BRKCRS-2501

Agenda

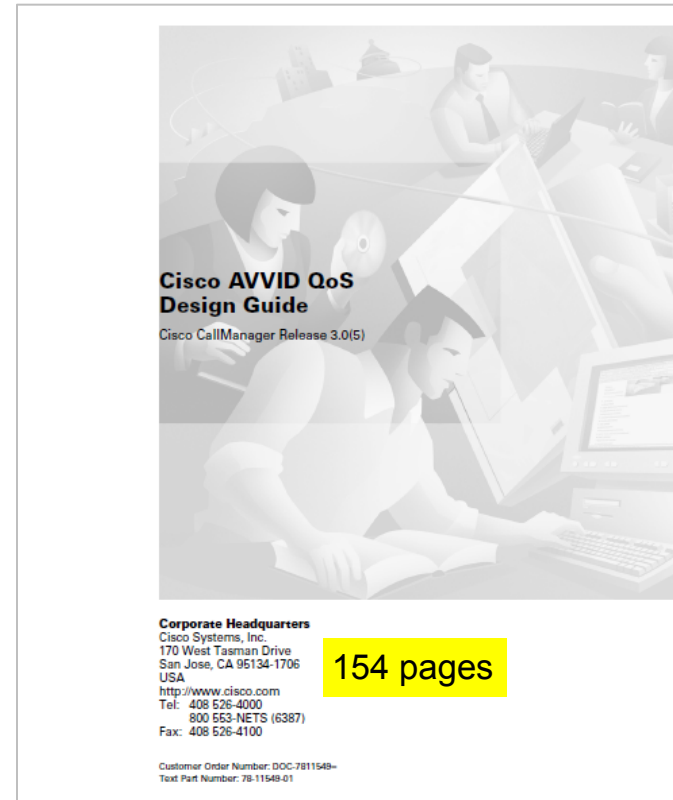
- Introduction to Strategic QoS Design
- WAN / IWAN QoS Design
- Campus QoS Design
- WLAN QoS Design
- Automating and Assuring QoS
- Summary and References
- Appendices

Introduction to Strategic QoS Design

Cisco Enterprise QoS Design

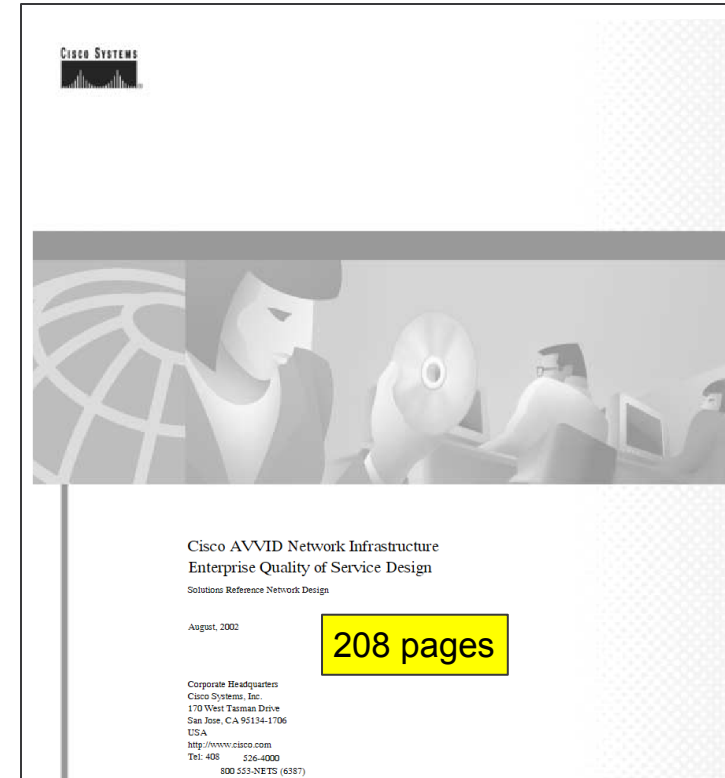
Cisco Enterprise QoS Design

- 1.0: Cisco's first QoS Design Guide for Enterprise was published in 2000 for VoIP (only!)



Cisco Enterprise QoS Design

- 1.0: Cisco's first QoS Design Guide for Enterprise was published in 2000 for VoIP (only!)
- 2.0: Multiple classes of data were added in 2002



Cisco Enterprise QoS Design

- 1.0: Cisco's first QoS Design Guide for Enterprise was published in 2000 for VoIP (only!)
- 2.0: Multiple classes of data were added in 2002
- 3.0: Basic Video (conferencing and streaming) were added in 2006



Enterprise QoS Solution Reference Network Design Guide

Version 3.3
November 2005

328 pages

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Cisco Enterprise QoS Design

- 1.0: Cisco's first QoS Design Guide for Enterprise was published in 2000 for VoIP (only!)
- 2.0: Multiple classes of data were added in 2002
- 3.0: Basic Video (conferencing and streaming) were added in 2006
- 4.1: Extended video (TelePresence, Video Surveillance, Digital Signage, etc.) and Medianet were added in 2010



CHAPTER 1

Enterprise Medianet Quality of Service Design 4.0—Overview



This content has been updated. The latest validated designs are published in the Cisco Press book *End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, 2nd Edition* available at: <http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694>

This document provides an overview of Quality of Service (QoS) tools and design recommendations relating to an enterprise medianet architecture and includes high-level answers to the following:

- Why is Cisco providing new QoS design guidance at this time?
- What is Cisco's Quality of Service toolset?
- How can QoS be optimally deployed for enterprise medianets?

QoS has proven itself a foundational network infrastructure technology required to support the transparent convergence of voice, video, and data networks. Furthermore, QoS has also been proven to complement and strengthen the overall security posture of a network. However, business needs continue to evolve and expand, and as such, place new demands on QoS technologies and designs. This document examines current QoS demands and requirements within an enterprise medianet and presents strategic design recommendations to address these needs.

Drivers for QoS Design Evolution

There are three main sets of drivers pressuring network administrators to reevaluate their current QoS designs (each is discussed in the following sections):

- New applications and business requirements
- New industry guidance and best practices
- New platforms and technologies

CH1-CH3:
320 pages

Cisco Enterprise QoS Design

- 1.0: Cisco's first QoS Design Guide for Enterprise was published in 2000 for VoIP (only!)
- 2.0: Multiple classes of data were added in 2002
- 3.0: Basic Video (conferencing and streaming) were added in 2006
- 4.1: Extended video (TelePresence, Video Surveillance, Digital Signage, etc.) and Medianet were added in 2010
- 4.2: Wireless, Data-Centre, DMVPN and GETVPN were added in 2014



End-to-End QoS Network Design

Quality of Service for
Rich-Media & Cloud Networks
Second Edition

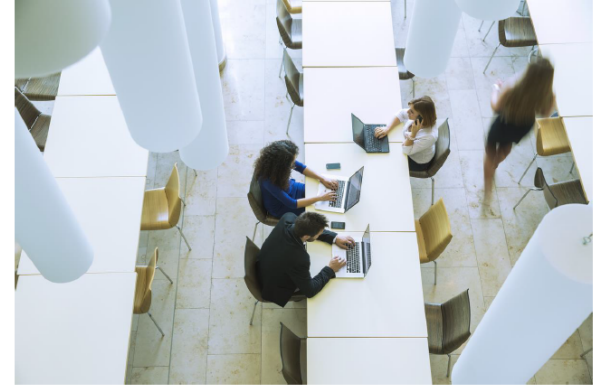
1043 pages

ciscopress.com

Tim Szigeti, CCIE No. 9794
Robert Barton, CCIE No. 6660
Christina Hattingh
Kenneth Briley Jr., CCIE No. 9754

Cisco Enterprise QoS Design

- 1.0: Cisco's first QoS Design Guide for Enterprise was published in 2000 for VoIP (only!)
- 2.0: Multiple classes of data were added in 2002
- 3.0: Basic Video (conferencing and streaming) were added in 2006
- 4.1: Extended video (TelePresence, Video Surveillance, Digital Signage, etc.) and Medianet were added in 2010
- 4.2: Wireless, Data-Centre, DMVPN and GETVPN were added in 2014
- 5.0: Policy-Abstraction, including support for 1400+ applications and dynamic QoS were added in 2017



Cisco EasyQoS Solution Design Guide
APIC-EM Release 1.6

December, 2017

302 pages + APIC-
EM 1.6 SW

The Why / How / What of Enterprise Networking



Cisco
Enterprise
Vision

The Why / How / What of Enterprise Networking



Cisco
Enterprise
Vision

Transform our customers' businesses
through powerful yet simple networks.

The Why / How / What of Enterprise Networking



Cisco
Enterprise
Vision

Why

Transform our customers' businesses through powerful yet simple networks.

The Why / How / What of Enterprise Networking



Why

Transform our customers' businesses
through powerful yet simple networks.

How

The Why / How / What of Enterprise Networking



Why

Transform our customers' businesses
through powerful yet simple networks.

How

What

What Do You Consider First?



Cisco *live!*



Where to Begin?

Always, Always, Always **Start with Defining Your Business Goals of QoS**

Where to Begin?

Always, Always, Always **Start with Defining Your Business Goals of QoS**

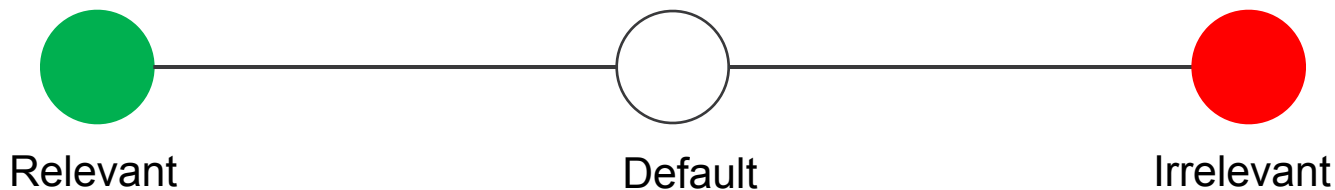
- *Guaranteeing voice quality* meets enterprise standards
- Ensuring a *high Quality of Experience for video* applications
- *Improving user productivity* by minimising network response times
- *Managing* business applications that are “*bandwidth hogs*”
- Identifying and *de-prioritising non-business applications*
- Improving network availability by *protecting the control planes*
- *Hardening the network* infrastructure to deal with abnormal events

Determining Application Business Relevance

How Important is an Application to Your Business?

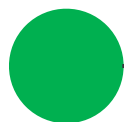
Determining Application Business Relevance

How Important is an Application to Your Business?

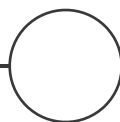


Determining Application Business Relevance

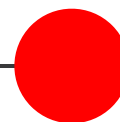
How Important is an Application to Your Business?



Relevant



Default



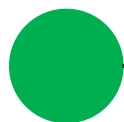
Irrelevant

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

RFC 4594

Determining Application Business Relevance

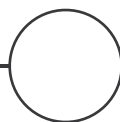
How Important is an Application to Your Business?



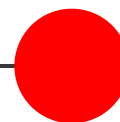
Relevant

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

RFC 4594



Default



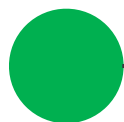
Irrelevant

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

RFC 3662

Determining Application Business Relevance

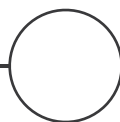
How Important is an Application to Your Business?



Relevant

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

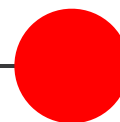
RFC 4594



Default

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

RFC 2474



Irrelevant

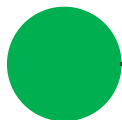
- These applications **do not support business objectives** and are typically consumer-oriented
- Applications of this type should be treated with a “less-than Best Effort” service

RFC 3662

Determining Application Business Relevance

How Important is an Application to Your Business?

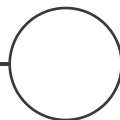
IMPORTANT



Relevant

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

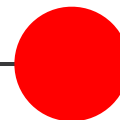
RFC 4594



Default

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

RFC 2474



Irrelevant

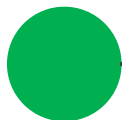
- These applications **do not support business objectives** and are typically consumer-oriented
- Applications of this type should be treated with a “less-than Best Effort” service

RFC 3662

Determining Application Business Relevance

How Important is an Application to Your Business?

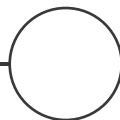
IMPORTANT



Relevant

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

RFC 4594

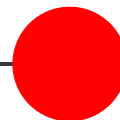


Default

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

RFC 2474

UNIMPORTANT



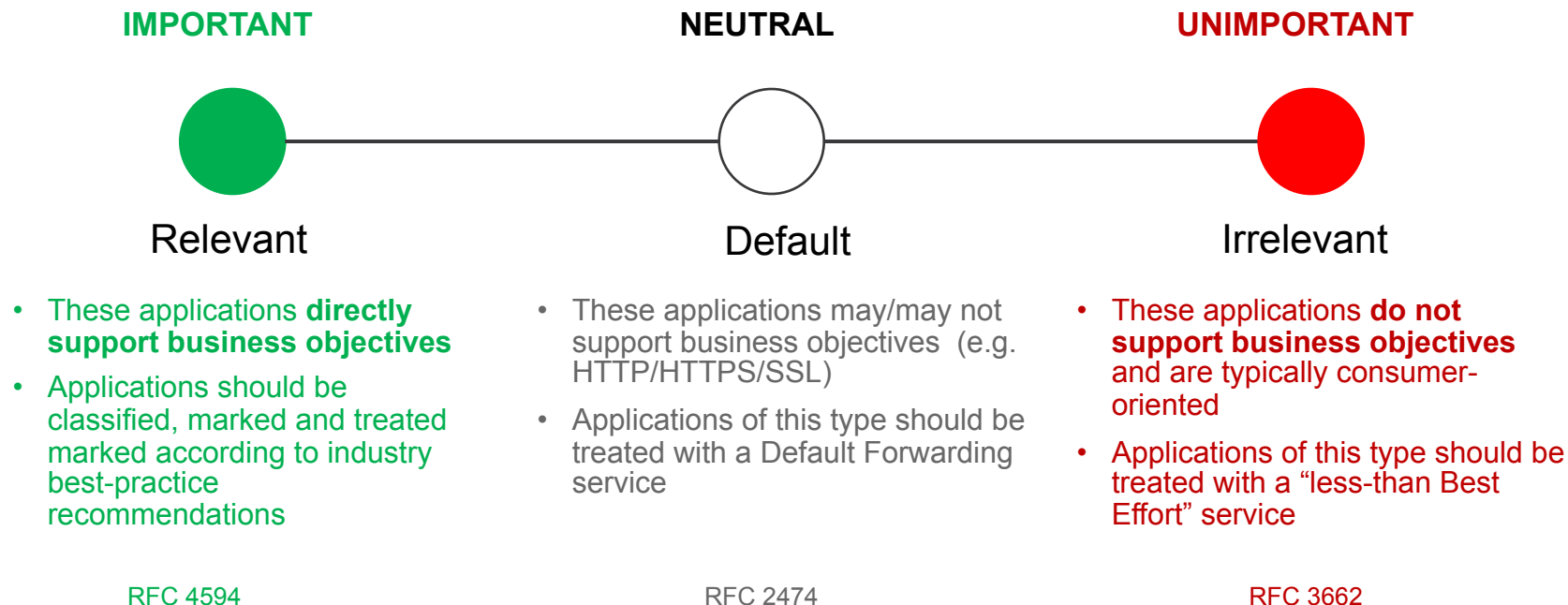
Irrelevant

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

RFC 3662

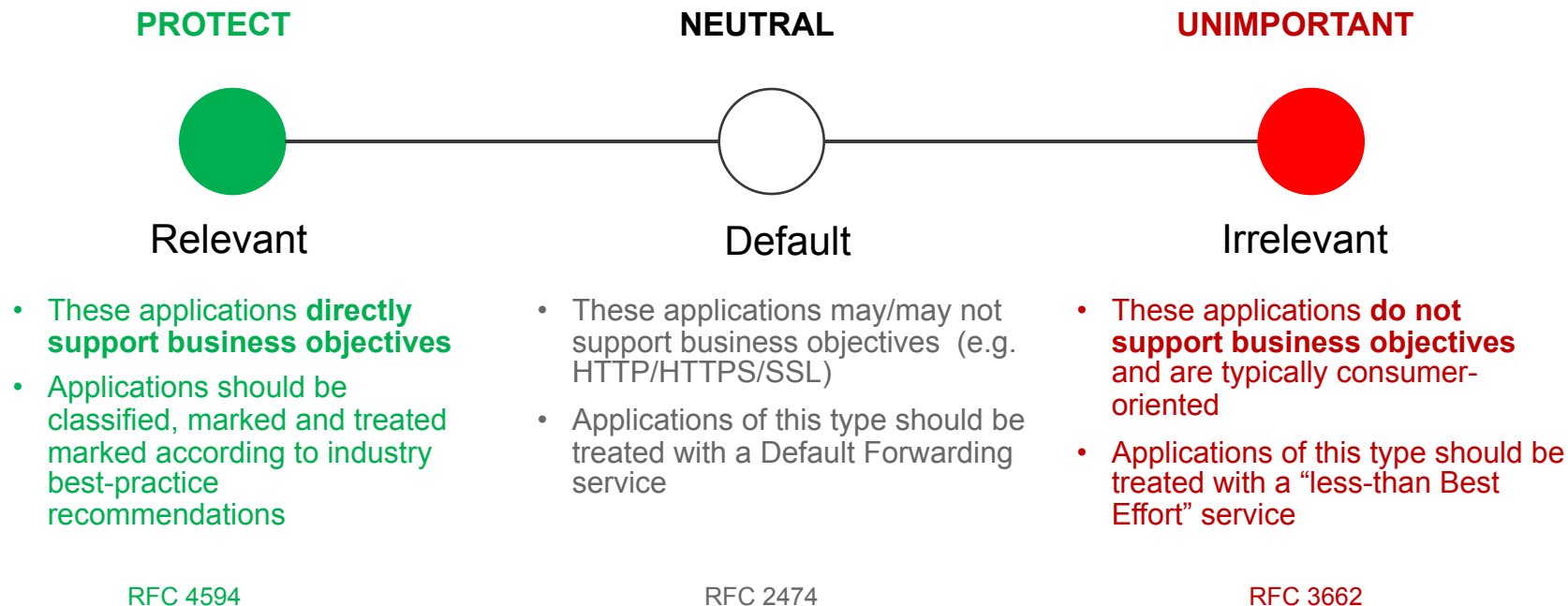
Determining Application Business Relevance

How Important is an Application to Your Business?



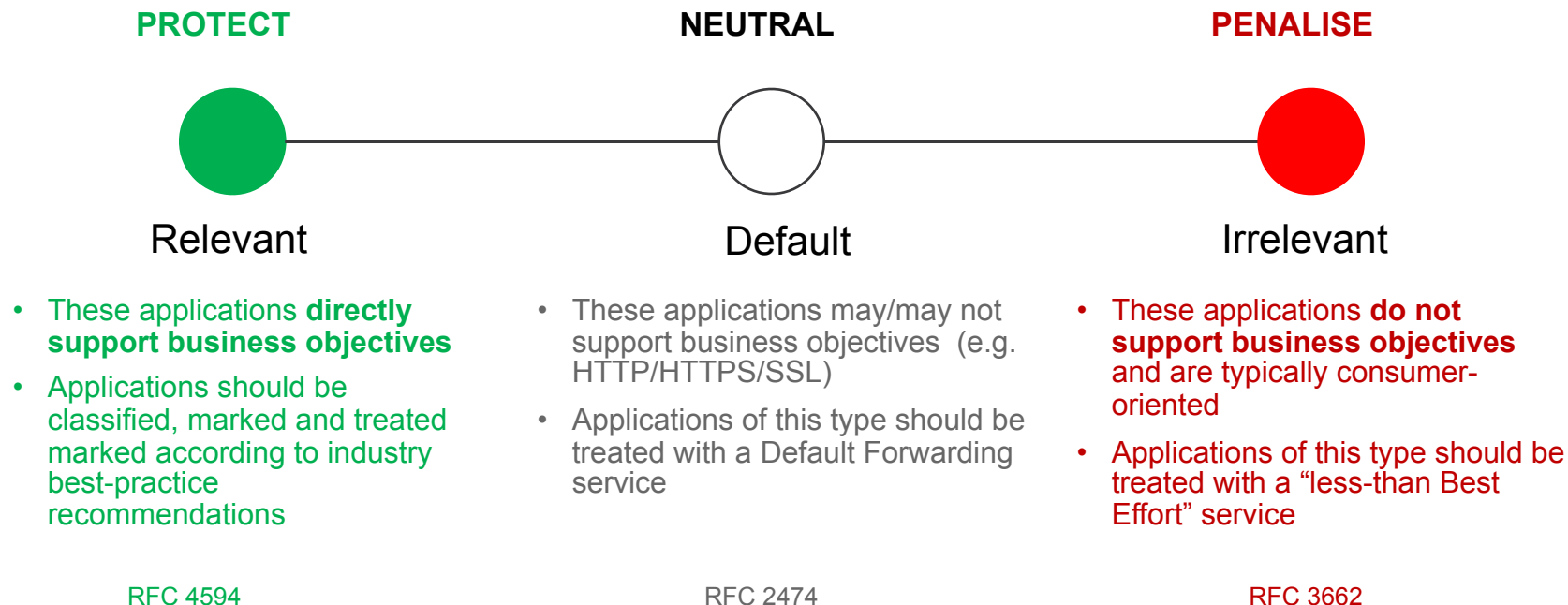
Determining Application Business Relevance

How Important is an Application to Your Business?



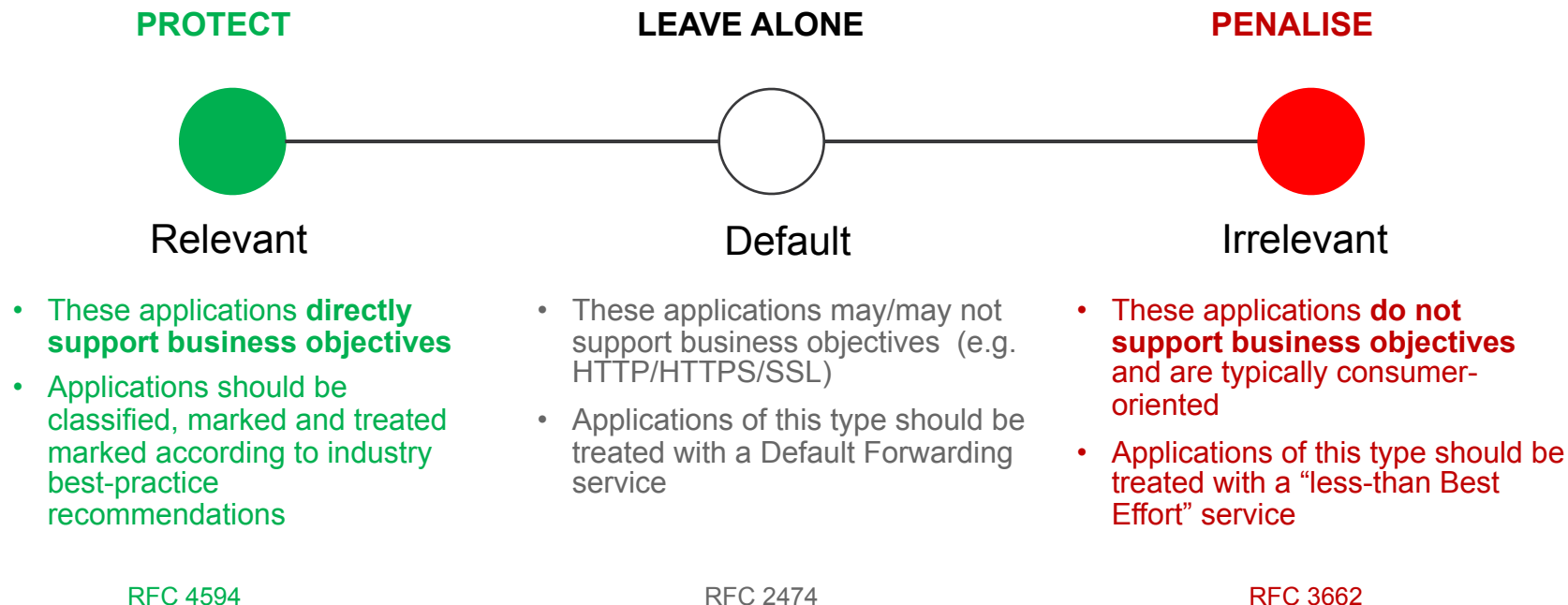
Determining Application Business Relevance

How Important is an Application to Your Business?



Determining Application Business Relevance

How Important is an Application to Your Business?



Translating Business-Relevance to QoS Treatments

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

Application Class	Per-Hop Behaviour	Queuing & Dropping	Application Examples
-------------------	-------------------	--------------------	----------------------

Translating Business-Relevance to QoS Treatments

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

Application Class	Per-Hop Behaviour	Queuing & Dropping	Application Examples
-------------------	-------------------	--------------------	----------------------



Translating Business-Relevance to QoS Treatments

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

Application Class	Per-Hop Behaviour	Queuing & Dropping	Application Examples
-------------------	-------------------	--------------------	----------------------

Default	Default Forwarding	DF	Default Queue + RED	Default Class
Irrelevant	Scavenger	CS1	Min BW Queue (Deferential)	YouTube, Netflix, iTunes, BitTorrent, Xbox Live

Translating Business-Relevance to QoS Treatments

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

	Application Class	Per-Hop Behaviour	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
	Signalling	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

Translating Business-Relevance to QoS Treatments

Apply RFC 4594-based Marking / Queuing / Dropping Treatments

	Application Class	Per-Hop Behaviour	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
	Signalling	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

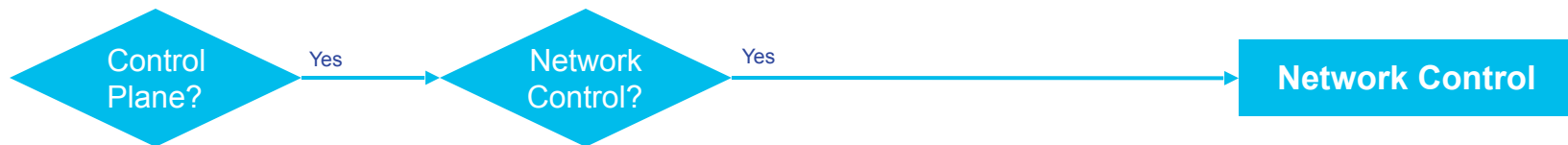
Application Classification Rules

Is the Protocol a Control Plane Protocol?



Application Classification Rules

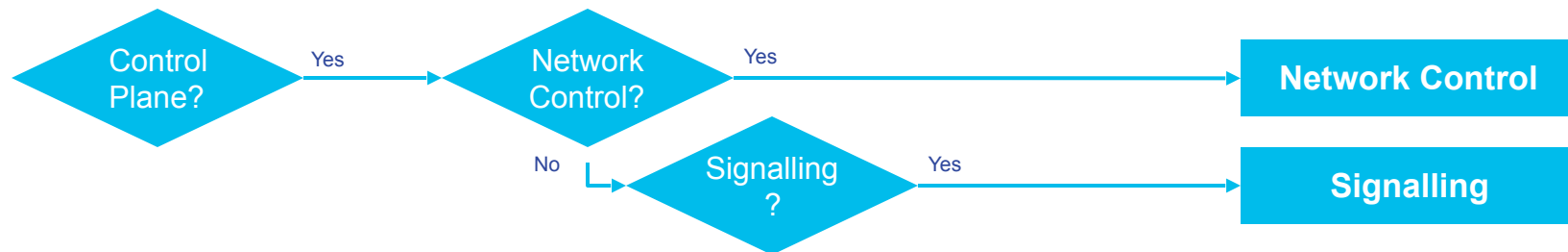
Is the Protocol a Control Plane Protocol?



- Network Control protocol?
 - network routing and control-plane protocols
 - E.g. BGP, OSPF, EIGRP, HSRP, IKE, etc.
- Signalling protocol?
 - call signalling / bandwidth reservation protocols
 - E.g. SIP, Skinny, H.323, RSVP etc.
- Operations / Administration / Management protocol?
 - network management protocols (e.g. SNMP, Telnet, SSH, Syslog, NetFlow, etc.)

Application Classification Rules

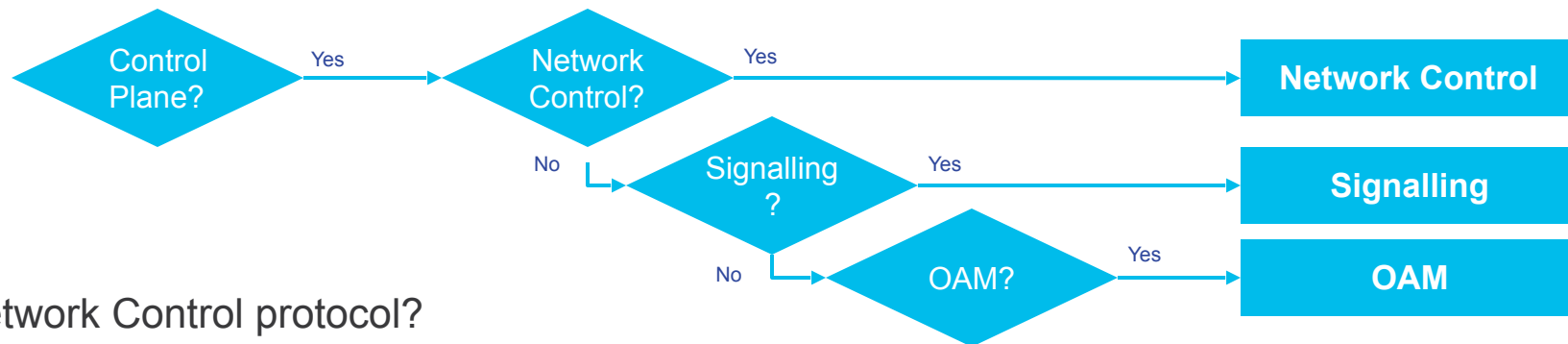
Is the Protocol a Control Plane Protocol?



- Network Control protocol?
 - network routing and control-plane protocols
 - E.g. BGP, OSPF, EIGRP, HSRP, IKE, etc.
- Signalling protocol?
 - call signalling / bandwidth reservation protocols
 - E.g. SIP, Skinny, H.323, RSVP etc.
- Operations / Administration / Management protocol?
 - network management protocols (e.g. SNMP, Telnet, SSH, Syslog, NetFlow, etc.)

Application Classification Rules

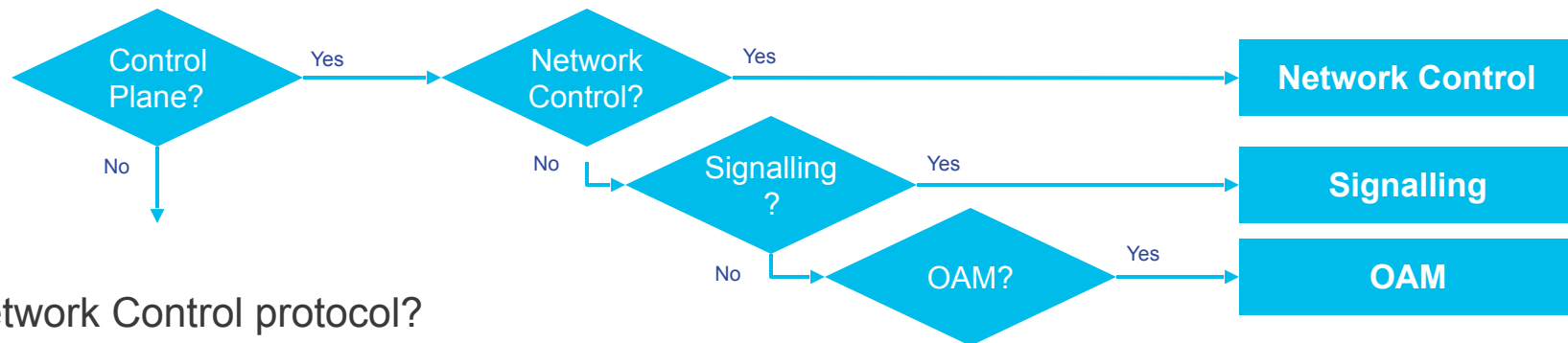
Is the Protocol a Control Plane Protocol?



- Network Control protocol?
 - network routing and control-plane protocols
 - E.g. BGP, OSPF, EIGRP, HSRP, IKE, etc.
- Signalling protocol?
 - call signalling / bandwidth reservation protocols
 - E.g. SIP, Skinny, H.323, RSVP etc.
- Operations / Administration / Management protocol?
 - network management protocols (e.g. SNMP, Telnet, SSH, Syslog, NetFlow, etc.)

Application Classification Rules

Is the Protocol a Control Plane Protocol?



- Network Control protocol?
 - network routing and control-plane protocols
 - E.g. BGP, OSPF, EIGRP, HSRP, IKE, etc.
- Signalling protocol?
 - call signalling / bandwidth reservation protocols
 - E.g. SIP, Skinny, H.323, RSVP etc.
- Operations / Administration / Management protocol?
 - network management protocols (e.g. SNMP, Telnet, SSH, Syslog, NetFlow, etc.)

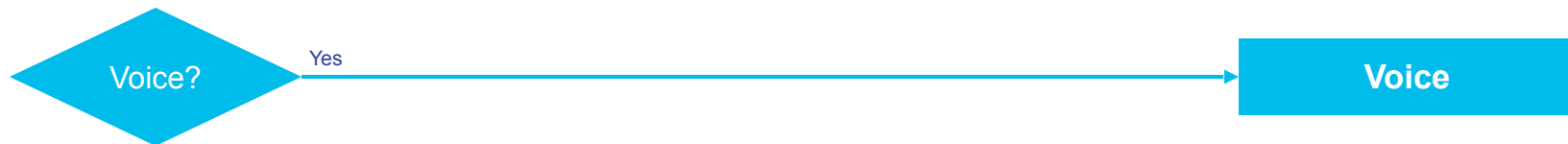
Application Classification Rules (cont.)

Is the Application Voice?



Application Classification Rules (cont.)

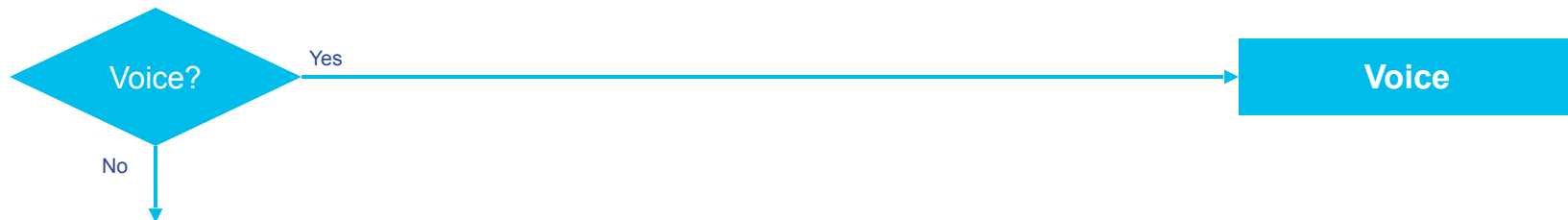
Is the Application Voice?



- Voice?
 - Audio-only media (e.g. G.711, G.729 etc.)
 - Note: This class may be used for the audio-component of multimedia applications, such as Cisco Jabber and/or Spark; however, this option should ONLY be considered if this causes no conflict with your overall Call Admission Control strategy and voice-queue provisioning

Application Classification Rules (cont.)

Is the Application Voice?



- Voice?
 - Audio-only media (e.g. G.711, G.729 etc.)
 - Note: This class may be used for the audio-component of multimedia applications, such as Cisco Jabber and/or Spark; however, this option should ONLY be considered if this causes no conflict with your overall Call Admission Control strategy and voice-queue provisioning

Application Classification Rules (cont.)

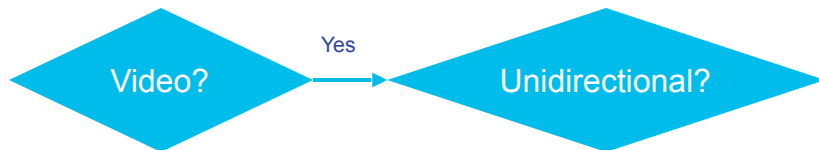
Is the Application Video?



- Video?

Application Classification Rules (cont.)

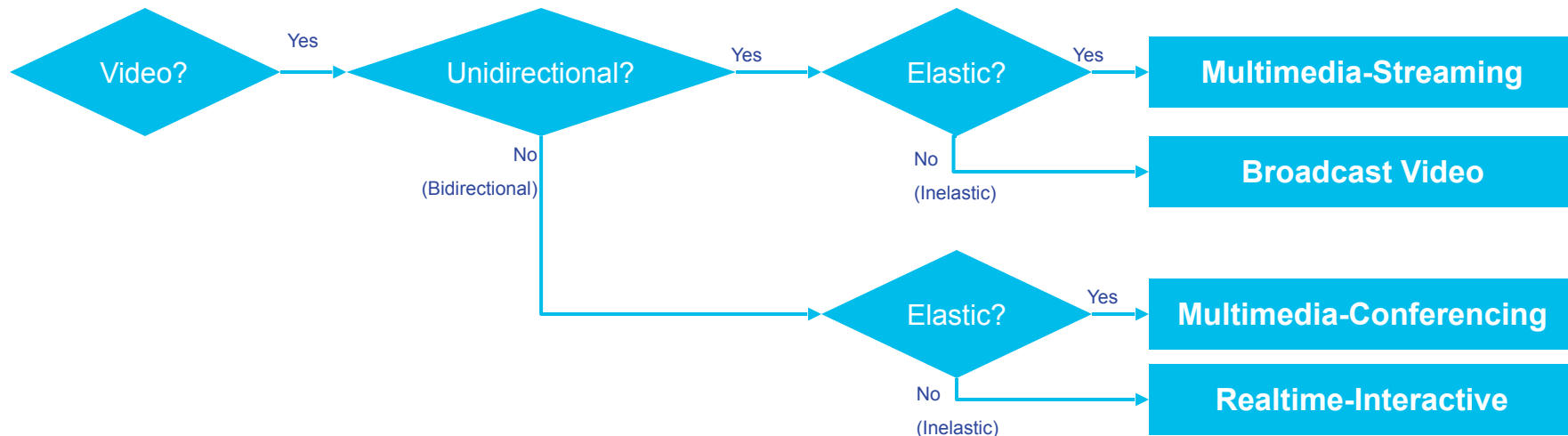
Is the Application Video?



- Video?
 - Is the application is unidirectional or bidirectional?

Application Classification Rules (cont.)

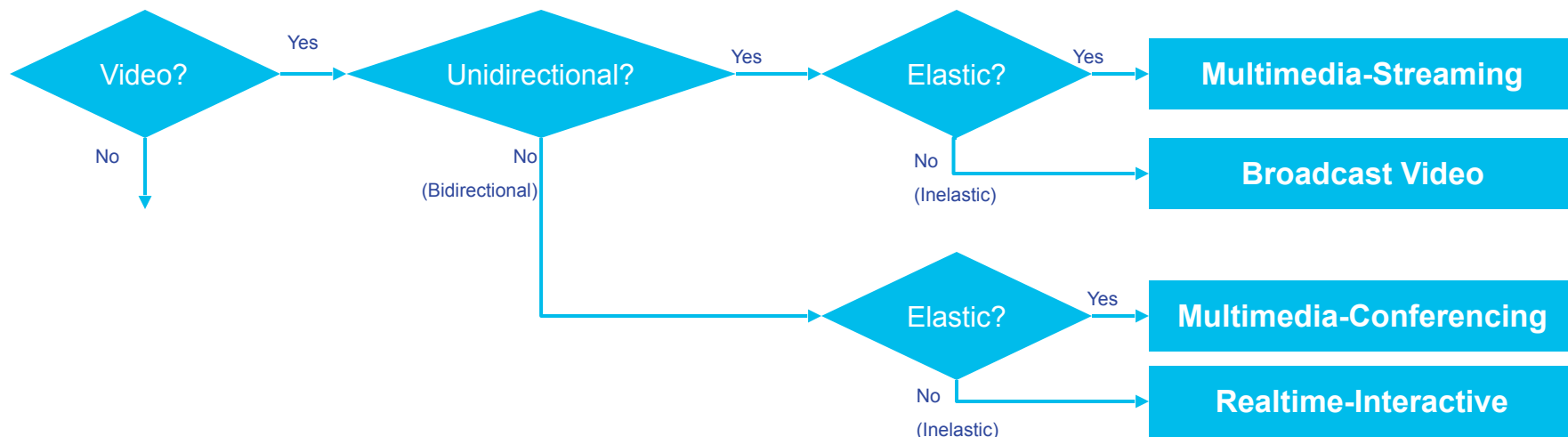
Is the Application Video?



- Video?
 - Is the application is unidirectional or bidirectional?
 - Is the application is elastic (i.e. adaptive to congestion/drops) or inelastic?

Application Classification Rules (cont.)

Is the Application Video?



- Video?
 - Is the application is unidirectional or bidirectional?
 - Is the application is elastic (i.e. adaptive to congestion/drops) or inelastic?

Application Classification Rules (cont.)

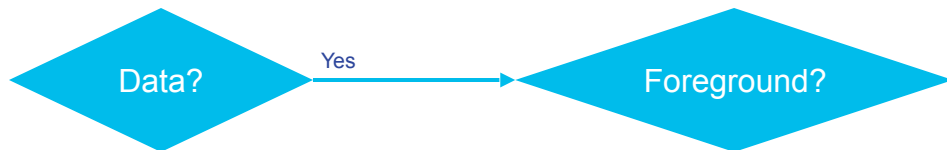
Is the Application Data?



- Data?

Application Classification Rules (cont.)

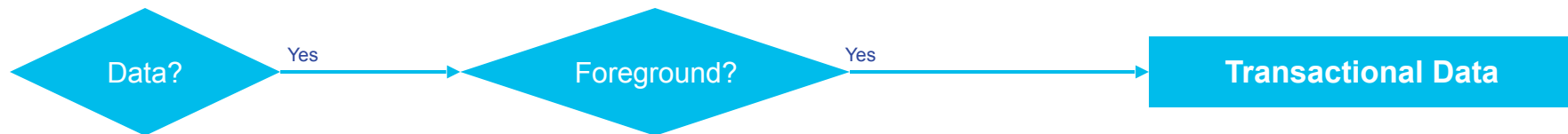
Is the Application Data?



- Data?
 - Is the application foreground or background?

Application Classification Rules (cont.)

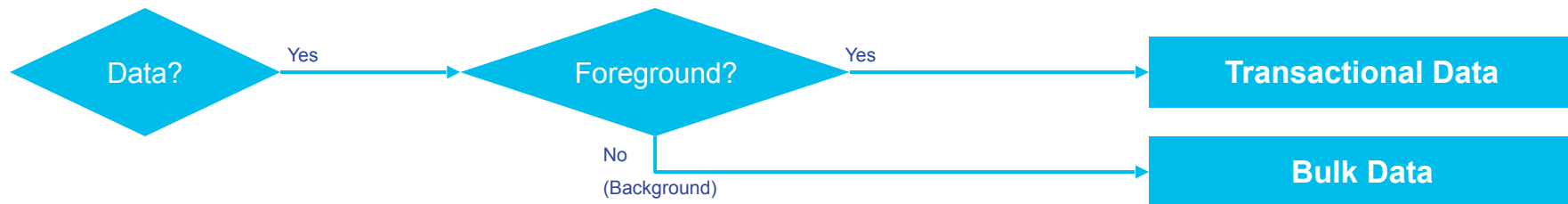
Is the Application Data?



- Data?
 - Is the application foreground or background?
 - Foreground applications will directly impact user-productivity with network delays

Application Classification Rules (cont.)

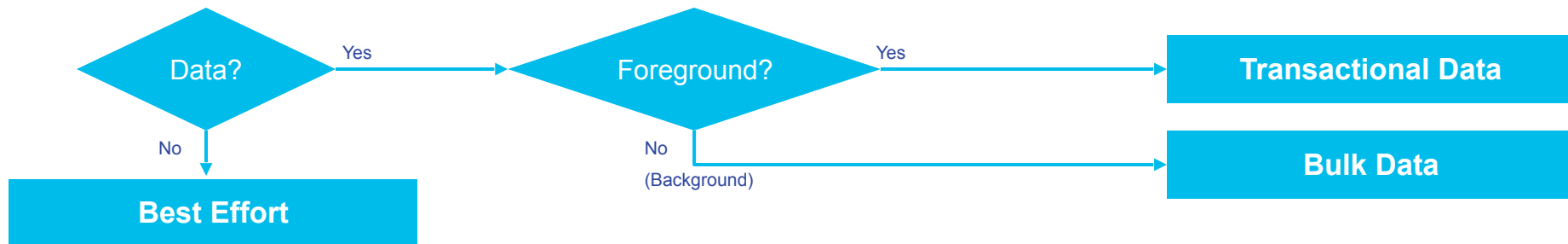
Is the Application Data?



- Data?
 - Is the application foreground or background?
 - Foreground applications will directly impact user-productivity with network delays
 - Background applications will not (as these are typically machine-to-machine flows)
 - However, these apps can be very bandwidth intensive (if unrestrained)
 - If it is not known if a data app is foreground, then assume it is background

Application Classification Rules (cont.)

Is the Application Data?



- Data?
 - Is the application foreground or background?
 - Foreground applications will directly impact user-productivity with network delays
 - Background applications will not (as these are typically machine-to-machine flows)
 - However, these apps can be very bandwidth intensive (if unrestrained)
 - If it is not known if a data app is foreground, then assume it is background
- Otherwise – the application/protocol remains in the default class (Best Effort)

Strategic QoS Design At-A-Glance



Strategic QoS Design

The Quality of Service Challenge

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

Step 1: Articulate Business Intent and Application Relevance

The first step may seem obvious and superfluous, but in actuality it is crucial: clearly define the business objectives that your QoS policies are to enable. These may include any/all of the following:

- Guaranteeing video quality meets enterprise standards
- Ensuring a high Quality of Experience (QoE) for video
- Increasing user productivity by increasing network response times for interactive applications
- Managing applications that are "bandwidth hogs"
- Identifying and de-prioritizing consumer applications
- Improving network availability
- Hardening the network infrastructure

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

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

Figure 1 Determining Application Business Relevance



Step 2: Define an End-to-End QoS Design Strategy

Once applications have been defined as business-relevant (or otherwise), then the network architect must decide how to mark and treat these applications over the IP infrastructure.

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

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

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

Figure 2 Cisco (RFC 4594-Based) QoS Recommendations

Application Class	DSCP	Queueing and Scheduling
Broadcast Video	EF	Priority Queue (PQ)
Real-time Interactive	CS4	Extended PQ
Real-time Interactive	CS4	Extended PQ
Multimedia Conferencing	AF4	DW Queue + DSCP WRED
Multimedia Streaming	AF3	DW Queue + DSCP WRED
Network Control	CS3	DW Queue
User Signaling	CS3	DW Queue
Administrative/Management (OAM)	CS2	DW Queue
Transactional Data	AF2	DW Queue + DSCP WRED
Best Effort	EF	DW Queue + DSCP WRED
Best Effort	EF	Default Queue + FIFO
Background	CS1	Best Effort Queue

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

Business relevant application can be grouped into one of four main categories:

- control plane protocols
- voice applications
- video applications
- data applications

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

Figure 3 Control Plane Traffic Classes



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

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

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

Cisco Strategic QoS Design

Provisioning for voice is relatively straightforward:

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

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

Figure 4 Video Traffic Classes



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

- is the video unidirectional or bidirectional?
- is the video elastic or inelastic?

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

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

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

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

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

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

Figure 5 Data Traffic Classes



When it comes to data applications, there is really only one key question to answer (as illustrated in Figure 5):

- Is the data application "foreground" or "background"?

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

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

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

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

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

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

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

For more details, see http://www.cisco.com/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SFND_40/QoSIntro_40.html And the Cisco Press Book: End-to-End QoS Network Design (Second Edition)-Chapter 10

Copyright © 2015 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

<https://cisco.box.com/v/QoS-AAGs>

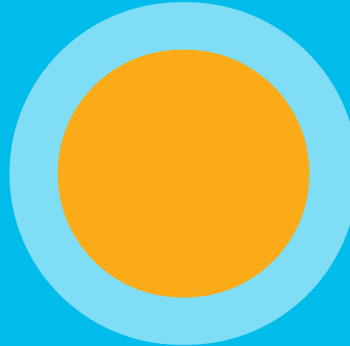
Cisco live!

Agenda

- Introduction to Strategic QoS Design
- **WAN / IWAN QoS Design**
- Campus QoS Design
- WLAN QoS Design
- Automating and Assuring QoS
- Summary and References
- Appendices

WAN / IWAN QoS Design

LAN Edge QoS Design



NBAR2 Application Library Deployment Challenge

NBAR2 Application Library

Deployment Challenge

- NBAR2 library is very large (1400+ apps)
- While powerful this toolset is not simple to wield
- To make the library more wieldy, every application has descriptive attributes

Category	First level grouping of applications with similar functionalities
Sub-category	Second level grouping of applications with similar functionalities
Application-group	Grouping of applications based on brand or application suite
P2P-technology?	Indicates application is peer-to-peer
Encrypted?	Indicates application is encrypted
Tunneled?	Indicates application uses tunnelling technique

Where Can I Find NBAR2 Attribute Details?

Where Can I Find NBAR2 Attribute Details?

Google Search: "NBAR Protocol Pack"

Cisco Protocol Pack Library: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Protocol Pack 35: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/pp3500/nbar-prot-pack3500.html



[Products & Services](#) [Support](#) [How to Buy](#) [Training & Events](#) [Partners](#)

[Support](#) / [Product Support](#) / [Cisco IOS and NX-OS Software](#) / [Cisco IOS XE 3S](#) / [Configuration Guides](#) /

NBAR2 Protocol Library

Updated: January 1, 2018

Downloading NBAR2 Protocol Packs

NBAR2 Protocol Packs are available for download on the Cisco.com software download page, here:

<http://www.cisco.com/cisco/software/navigator.html>

On the download page, specify a platform model to display software available for download. One software option is NBAR2 Protocol Packs.

Example:

To display protocol packs available for the Cisco ASR 1001 platform, open the link provided above and navigate as follows:

Products > Routers > Service Provider Edge Routers > ASR 1000 Series Aggregation Services Routers > ASR 1001 Router

[DOWNLOAD HERE](#)

NBAR2 Protocol Packs for Cisco IOS and IOS-XE Releases

Protocol Pack	Supported Releases	Supported From...
Protocol Pack 35.0.0 Release Notes	Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2 IOS-XE Everest 16.6.2	2018-01-02 2018-01-02
Protocol Pack 34.0.0 Release Notes	Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2 IOS-XE Everest 16.6.2	2017-11-15 2017-11-15
Protocol Pack 33.0.0 Release Notes	Built into: IOS-XE Everest 16.6.2 IOS-XE Fuji 16.7.1	2017-11-05 2017-11-17
	Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2	2017-09-28
Protocol Pack 32.1.0 Release Notes	Releases supported by Protocol Pack upgrade: IOS Version 15.5(3)M4a IOS Version 15.5(3)M IOS XE 3.16.4aS Version 15.5(3)Sa4	2017-11-28 2017-11-28 2017-11-28

Where Can I Find NBAR2 Attribute Details?

Google Search: "NBAR Protocol Pack"

Cisco Protocol Pack Library: http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

Protocol Pack 35: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/pp3500/nbar-prot-pack3500.html

 [Products & Services](#) [Support](#) [How to Buy](#) [Training & Events](#) [Partners](#)

[Support](#) / [Product Support](#) / [Cisco IOS and NX-OS Software](#) / [Cisco IOS XE 3S](#) / [Configuration Guides](#) /

NBAR2 Protocol Library

Updated: January 1, 2018

Downloading NBAR2 Protocol Packs

NBAR2 Protocol Packs are available for download on the Cisco.com software download page, here:

<http://www.cisco.com/cisco/software/navigator.html>

On the download page, specify a platform model to display software available for download. One software option is NBAR2 Protocol Packs.

Example:

To display protocol packs available for the Cisco ASR 1001 platform, open the link provided above and navigate as follows:

Products > Routers > Service Provider Edge Routers > ASR 1000 Series Aggregation Services Routers > ASR 1001 Router

[DOWNLOAD HERE](#)

NBAR2 Protocol Packs for Cisco IOS and IOS-XE Releases

Protocol Pack	Supported Releases	Supported From...
Protocol Pack 35.0.0	Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2 IOS-XE Everest 16.6.2	2018-01-02 2018-01-02
Release Notes		
Protocol Pack 34.0.0	Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2 IOS-XE Everest 16.6.2	2017-11-15 2017-11-15
Release Notes		
Protocol Pack 33.0.0	Built into: IOS-XE Everest 16.6.2 IOS-XE Fuji 16.7.1	2017-11-05 2017-11-17
Release Notes		
	Releases supported by Protocol Pack upgrade: IOS-XE Denali 16.3.2	2017-09-28
Protocol Pack 32.1.0	Releases supported by Protocol Pack upgrade: IOS Version 15.5(3)M4a IOS Version 15.5(3)M IOS XE 3.16.4aS Version 15.5(3)Sa4	2017-11-28 2017-11-28 2017-11-28
Release Notes		

 [Products & Services](#) [Support](#) [How to Buy](#)

[Support](#) /

Protocol Pack 35.0.0

 Find Matches in This Book

Book Table of Contents

[WEBEAM-VOICE-ENGINE](#)
[WEBBMD](#)
[WEBSense](#)
[WEBSTER](#)
[WEBTHUNDER](#)
[WECHAT](#)
[WEIBO](#)
[WELLS-FARGO](#)
[WETRANSFER](#)
[WHATSAPP](#)
[WHITEPAGES](#)
[WHOAMI](#)
[WHOIS++](#)
[WIFI-CALLING](#)
[WIKIA](#)
[WIKIPEDIA](#)
[WINDOWS-AZURE](#)
[WINDOWS-STORE](#)
[WINDOWS-UPDATE](#)
[WINNEX](#)

Protocol Pack 35: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/gos_nbar/prot_lib/config_library/pp3500/nbar-prot-pack3500.html

21

NBAR2 QoS Attributes

New QoS Attributes: Traffic-Class and Business-Relevance

Introduced in: IOS 15.5(3)M and IOS XE 3.16S

NBAR2 QoS Attributes

New QoS Attributes: Traffic-Class and Business-Relevance

Introduced in: IOS 15.5(3)M and IOS XE 3.16S

```
show ip nbar protocol-attribute airbnb
```

NBAR2 QoS Attributes

New QoS Attributes: Traffic-Class and Business-Relevance

Introduced in: IOS 15.5(3)M and IOS XE 3.16S

```
show ip nbar protocol-attribute airbnb
```

encrypted

tunnel

category

sub-category

application-group

p2p-technology

traffic-class

business-relevance

encrypted-no

tunnel-no

browsing

Other

Other

p2p-tech-no

transactional-data

business-irrelevant

NBAR2 QoS Attributes

New QoS Attributes: Traffic-Class and Business-Relevance

Introduced in: IOS 15.5(3)M and IOS XE 3.16S

```
show ip nbar protocol-attribute airbnb
```

encrypted

tunnel

category

sub-category

application-group

p2p-technology

traffic-class

business-relevance

encrypted-no

tunnel-no

browsing

Other

Other

p2p-tech-no

transactional-data

business-irrelevant

Changing the Business-Relevancy of an Application

Changing the Business-Relevancy of an Application

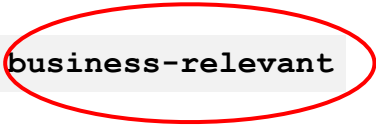
Step 1: Create an Attribute-Map with the Desired Setting

```
ip nbar attribute-map BUSINESS-RELEVANT-MAP attribute business-relevance business-relevant
```

Changing the Business-Relevancy of an Application

Step 1: Create an Attribute-Map with the Desired Setting

```
ip nbar attribute-map BUSINESS-RELEVANT-MAP attribute business-relevance business-relevant
```



Step 2: Associate the Application with the Desired Attribute-Map

```
ip nbar attribute-set airbnb BUSINESS-RELEVANT-MAP
```



Changing Application Business-Relevance

All Options

Changing Application Business-Relevance

All Options

Scenario 1: Making an Application Business-Relevant

```
ip nbar attribute-map ATTRIBUTE_MAP-RELEVANT attribute business-relevance business-relevant
ip nbar attribute-set application-name ATTRIBUTE_MAP-RELEVANT
```

Changing Application Business-Relevance

All Options

Scenario 1: Making an Application Business-Relevant

```
ip nbar attribute-map ATTRIBUTE_MAP-RELEVANT attribute business-relevance business-relevant
ip nbar attribute-set application-name ATTRIBUTE_MAP-RELEVANT
```

Scenario 2: Making an Application Default

```
ip nbar attribute-map ATTRIBUTE_MAP-DEFAULT attribute business-relevance default
ip nbar attribute-set application-name ATTRIBUTE_MAP-DEFAULT
```

Changing Application Business-Relevance

All Options

Scenario 1: Making an Application Business-Relevant

```
ip nbar attribute-map ATTRIBUTE_MAP-RELEVANT attribute business-relevance business-relevant
ip nbar attribute-set application-name ATTRIBUTE_MAP-RELEVANT
```

Scenario 2: Making an Application Default

```
ip nbar attribute-map ATTRIBUTE_MAP-DEFAULT attribute business-relevance default
ip nbar attribute-set application-name ATTRIBUTE_MAP-DEFAULT
```

Scenario 3: Making an Application Business-Irrelevant

```
ip nbar attribute-map ATTRIBUTE_MAP-SCAVENGER attribute business-relevance business-irrelevant
ip nbar attribute-set application-name ATTRIBUTE_MAP-SCAVENGER
```

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model



“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

```
class-map match-all VOICE
```


“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

```
class-map match-all VOICE  
  match protocol attribute traffic-class voip-telephony
```

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

```
class-map match-all VOICE
  match protocol attribute traffic-class voip-telephony
  match protocol attribute business-relevance business-relevant
```

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

```
policy-map MARKING
  class VOICE
    set dscp ef
  class BROADCAST-VIDEO
    set dscp cs5
  class REAL-TIME-INTERACTIVE
    set dscp cs4
  class MULTIMEDIA-CONFERENCING
    set dscp af41
  class MULTIMEDIA-STREAMING
    set dscp af31
  class SIGNALING
    set dscp cs3
```

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

```
policy-map MARKING
  class VOICE
    set dscp ef
  class BROADCAST-VIDEO
    set dscp cs5
  class REAL-TIME-INTERACTIVE
    set dscp cs4
  class MULTIMEDIA-CONFERENCING
    set dscp af41
  class MULTIMEDIA-STREAMING
    set dscp af31
  class SIGNALING
    set dscp cs3
  class NETWORK-CONTROL
```


“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

```
policy-map MARKING
  class VOICE
    set dscp ef
  class BROADCAST-VIDEO
    set dscp cs5
  class REAL-TIME-INTERACTIVE
    set dscp cs4
  class MULTIMEDIA-CONFERENCING
    set dscp af41
  class MULTIMEDIA-STREAMING
    set dscp af31
  class SIGNALING
    set dscp cs3
  class NETWORK-CONTROL
    set dscp cs6
```

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

```
policy-map MARKING
  class VOICE
    set dscp ef
  class BROADCAST-VIDEO
    set dscp cs5
  class REAL-TIME-INTERACTIVE
    set dscp cs4
  class MULTIMEDIA-CONFERENCING
    set dscp af41
  class MULTIMEDIA-STREAMING
    set dscp af31
  class SIGNALING
    set dscp cs3
  class NETWORK-CONTROL
    set dscp cs6
  class NETWORK-MANAGEMENT
```

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

```
policy-map MARKING
  class VOICE
    set dscp ef
  class BROADCAST-VIDEO
    set dscp cs5
  class REAL-TIME-INTERACTIVE
    set dscp cs4
  class MULTIMEDIA-CONFERENCING
    set dscp af41
  class MULTIMEDIA-STREAMING
    set dscp af31
  class SIGNALING
    set dscp cs3
  class NETWORK-CONTROL
    set dscp cs6
  class NETWORK-MANAGEMENT
    set dscp cs2
```


“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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


“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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


“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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

“Holy Grail” QoS Configuration: NBAR2 1400+ App / 12-Class Model

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

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


NBAR2 QoS Attributes At-A-Glance



Cisco NBAR2 Business-Relevance and Traffic-Class Attributes

At-A-Glance

Role in Network

Cisco Network Based Application Recognition (NBAR) technology (now in its second generation) boasts an application library of over 1300 applications, many with media sub-component signatures also available, for an approximate total of 1400 distinct applications/sub-applications.

While this richness provides network administrators great flexibility and power in their policy-definitions, it is cumbersome to specify each application/sub-application by name within a QoS policy.

To assist in policy-definition and in browsing the application library, applications are grouped into categories and sub-categories. For example, NBAR application categories include:

- browsing
- business-and-productivity-tools
- email
- file-sharing
- gaming
- industrial-protocols
- instant-messaging
- internet-privacy
- layer2-over-ip
- location-based-services
- net-admin
- newsgroup
- social-networking
- streaming
- voice-and-video

Thus, for example if an administrator wanted to classify all email applications, they could use the match protocol attribute category email command within a class-map.

However, there may be cases where all applications within a given category may not be considered business-relevant, as shown in Figure 1.

Figure 1 Determining Application Business Relevance



For example, the voice-and-video category includes not only cisco-phone and telepresence-media voice and video flows, but also skype and facetime. But these consumer-oriented voice-and-video applications may be considered to be business-irrelevant, and so would need to be excluded from a business QoS policy.

Additionally, NBAR2 categories predate the industry-standard reference for configuring DiffServ QoS, namely RFC 4594. As such, these categories do not align with the traffic-class names used in this RFC.

Therefore, to simplify and expedite QoS configuration, NBAR2 has been enhanced in IOS XE 3.16 to support two new attributes:

- Business-Relevance
- Traffic-Class

Business-Relevance Attribute

The business-relevance attribute allows an administrator to classify a given application to one of three levels of business relevancy, as shown in Table 1.

Table 1 Business-Relevance NBAR2 Attribute

Name	Description
business-relevant	Business critical applications
default	Related business applications
business-irrelevant	Non business applications

All applications within the NBAR2 library has been pre-populated with the most common business-relevance attribute. For example, youtube by default is set as business-irrelevant, as most customers typically classify this application as such. However, this may not be the case across the board; for example, some businesses may be using YouTube for training purposes. In such cases, an administrator can change this business-relevance setting to align with their objectives.

A business-irrelevant application is intended for a RFC 3602 "Scavenger" treatment. An application with a business-relevance setting of default is intended for a RFC 2474 Default Forwarding treatment. In turn, business-relevant applications are intended to be serviced within their respective RFC 4594 traffic-class.

Traffic-Class Attribute

The traffic-class attribute aligns NBAR2 applications according to RFC 4594-based traffic-classes. For example, per RFC 4594 "Low Latency Data" applications (commonly referred to as "Bulk Data" applications) includes email, file-transfer and other "background" (i.e. non-user-interactive) applications. As such, rather than having to configure a class map along the lines of:

```
class-map match-any BULK-DATA
match protocol attribute category email
match protocol attribute category file-sharing
match protocol attribute sub-category backup-systems... etc.
```

An administrator can configure all relevant applications matching a specific RFC 4594 traffic-class with a single command (examples of which are shown on the reverse).

The ten RFC 4594 traffic classes for business-relevant applications are shown in Table 2.

Table 2 Traffic-Class NBAR2 Attribute

Name	Description
voip-telephony	VoIP telephony (bearer only) traffic
broadcast-video	Broadcast TV, live events, video surveillance
realtime-interactive	High-definition interactive video applications
multimedia-conferencing	Desktop software multimedia collaboration applications
multimedia-streaming	Video-on-Demand (VOD) streaming video
network-control	Network control plane traffic
signaling	Signaling traffic that supports IP voice and video telephony
ops-admin-mgmt	Network operations, administration, and management traffic
transactional-data	Interactive data applications
bulk-data	Non-interactive data applications

Thus, with these new attributes, all 1400 NBAR2 applications can be configured into a 12-class RFC 4594-based QoS model with a straightforward and user-intuitive syntax, as is shown on the reverse.

Cisco NBAR Business-Relevance and Traffic-Class Attributes

At-A-Glance

Step 1: Configure NBAR2 (Business-Relevance and Traffic-Class) Class-Maps

```
class-map match-all VOICE
match protocol attribute traffic-class voip-telephony
match protocol attribute business-relevance business-relevant

class-map match-all BROADCAST-VIDEO
match protocol attribute traffic-class broadcast-video
match protocol attribute business-relevance business-relevant

class-map match-all INTERACTIVE-VIDEO
match protocol attribute traffic-class real-time-interactive
match protocol attribute business-relevance business-relevant

class-map match-all MULTIMEDIA-CONFERENCING
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant

class-map match-all MULTIMEDIA-STREAMING
match protocol attribute traffic-class multimedia-streaming
match protocol attribute business-relevance business-relevant

class-map match-all SIGNALING
match protocol attribute traffic-class signaling
match protocol attribute business-relevance business-relevant

class-map match-all NETWORK-CONTROL
match protocol attribute traffic-class network-control
match protocol attribute business-relevance business-relevant

class-map match-all NETWORK-MANAGEMENT
match protocol attribute traffic-class ops-admin-mgmt
match protocol attribute business-relevance business-relevant

class-map match-all TRANSACTIONAL-DATA
match protocol attribute traffic-class transactional-data
match protocol attribute business-relevance business-relevant

class-map match-all BULK-DATA
match protocol attribute traffic-class bulk-data
match protocol attribute business-relevance business-relevant

class-map match-all SCAVENGER
match protocol attribute business-relevance business-irrelevant
```

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

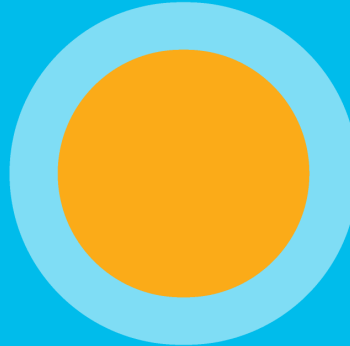
Step 2: Configure Marking Policy-Map

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

Step 3: Attach the Policy-Map to the Interface(s)

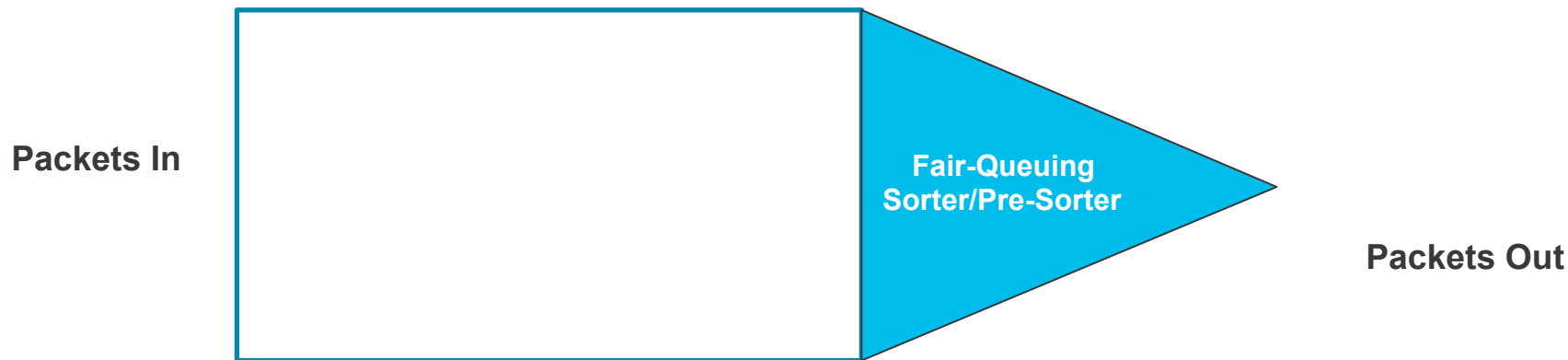
```
service-policy input MARKING
```

WAN Edge QoS Design



QoS Tools Review: Queuing & Dropping Tools

(Flow-Based) Fair-Queuing



A flow is defined by **five matching tuples**:

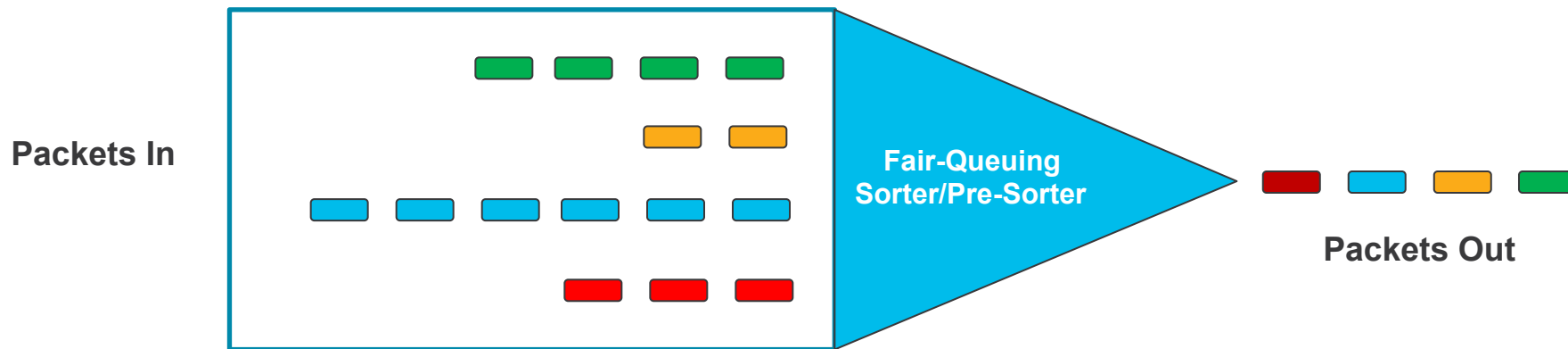
Source Address + Source Port

Destination Address + Destination Port

Layer 4 Protocol (TCP or UDP)

QoS Tools Review: Queuing & Dropping Tools

(Flow-Based) Fair-Queuing



A flow is defined by **five matching tuples**:

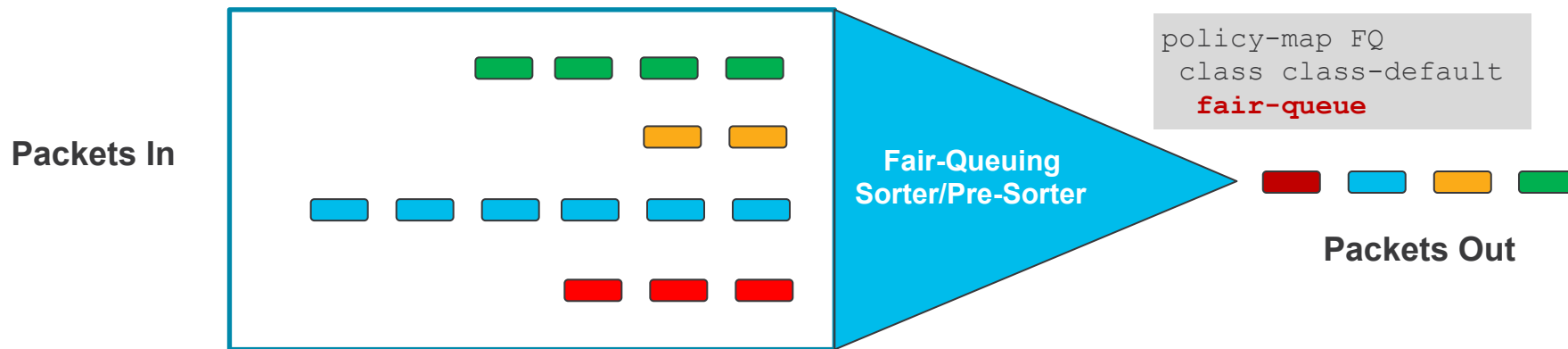
Source Address + Source Port

Destination Address + Destination Port

Layer 4 Protocol (TCP or UDP)

QoS Tools Review: Queuing & Dropping Tools

(Flow-Based) Fair-Queuing



A flow is defined by **five matching tuples**:

Source Address + Source Port

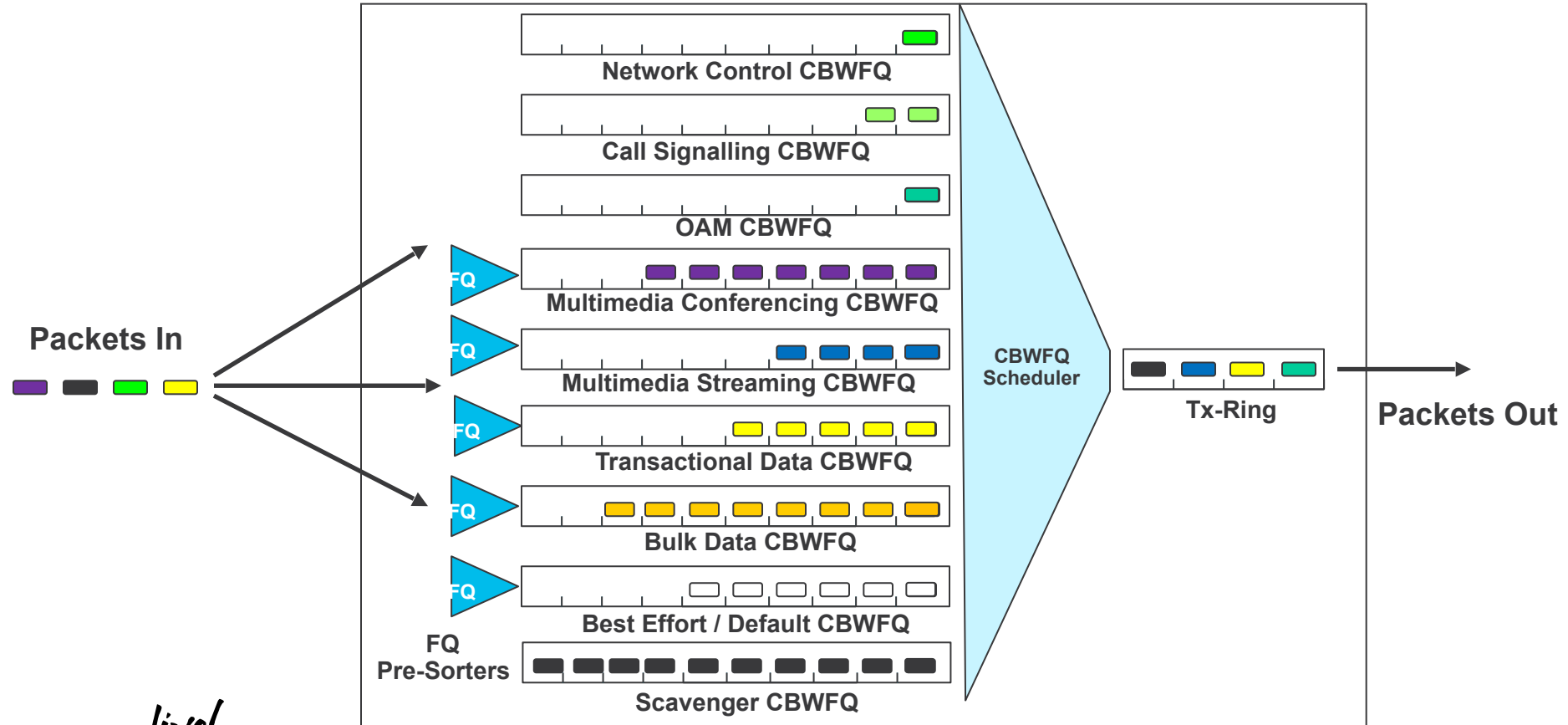
Destination Address + Destination Port

Layer 4 Protocol (TCP or UDP)

QoS Tools Review: Queuing & Dropping Tools

CBWFQ

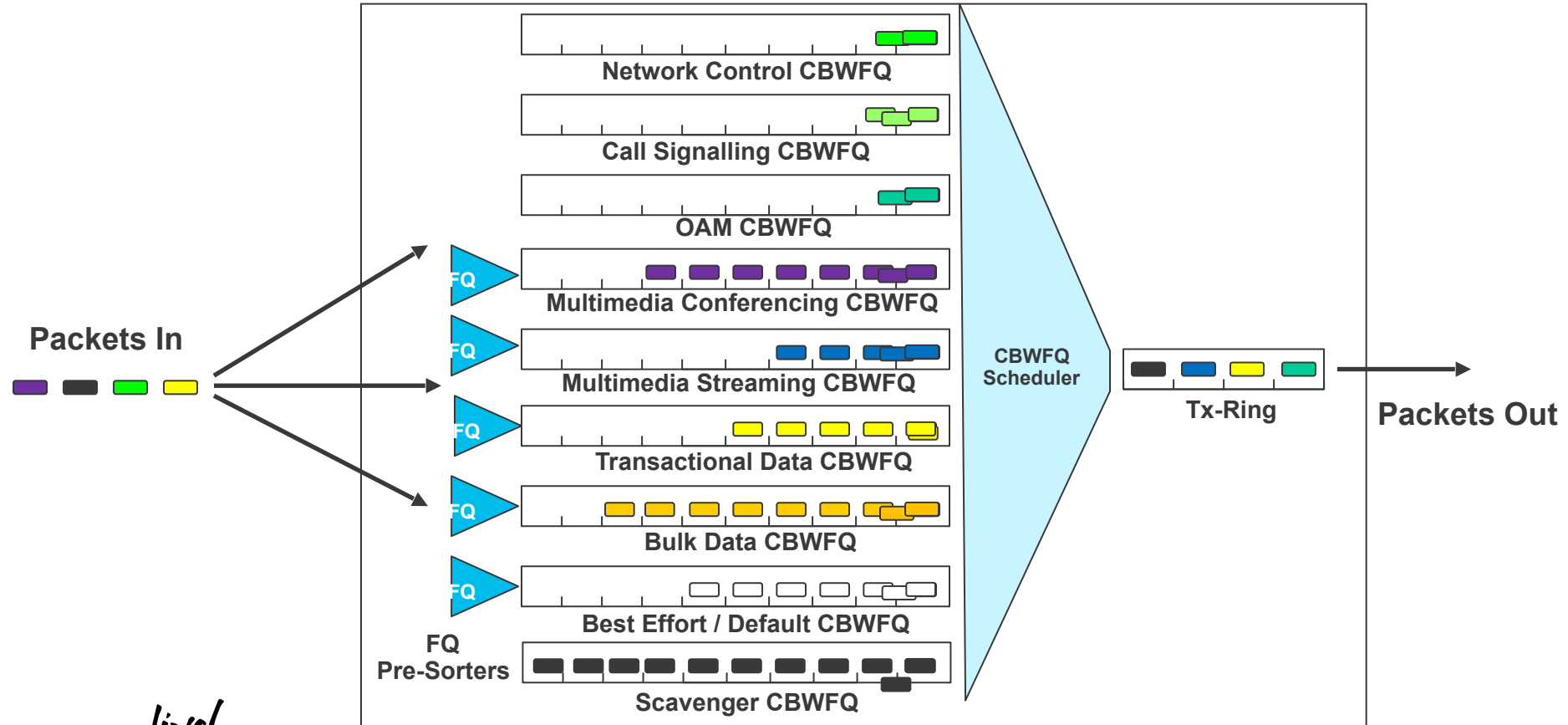
IOS Interface Buffers



QoS Tools Review: Queuing & Dropping Tools

CBWFQ

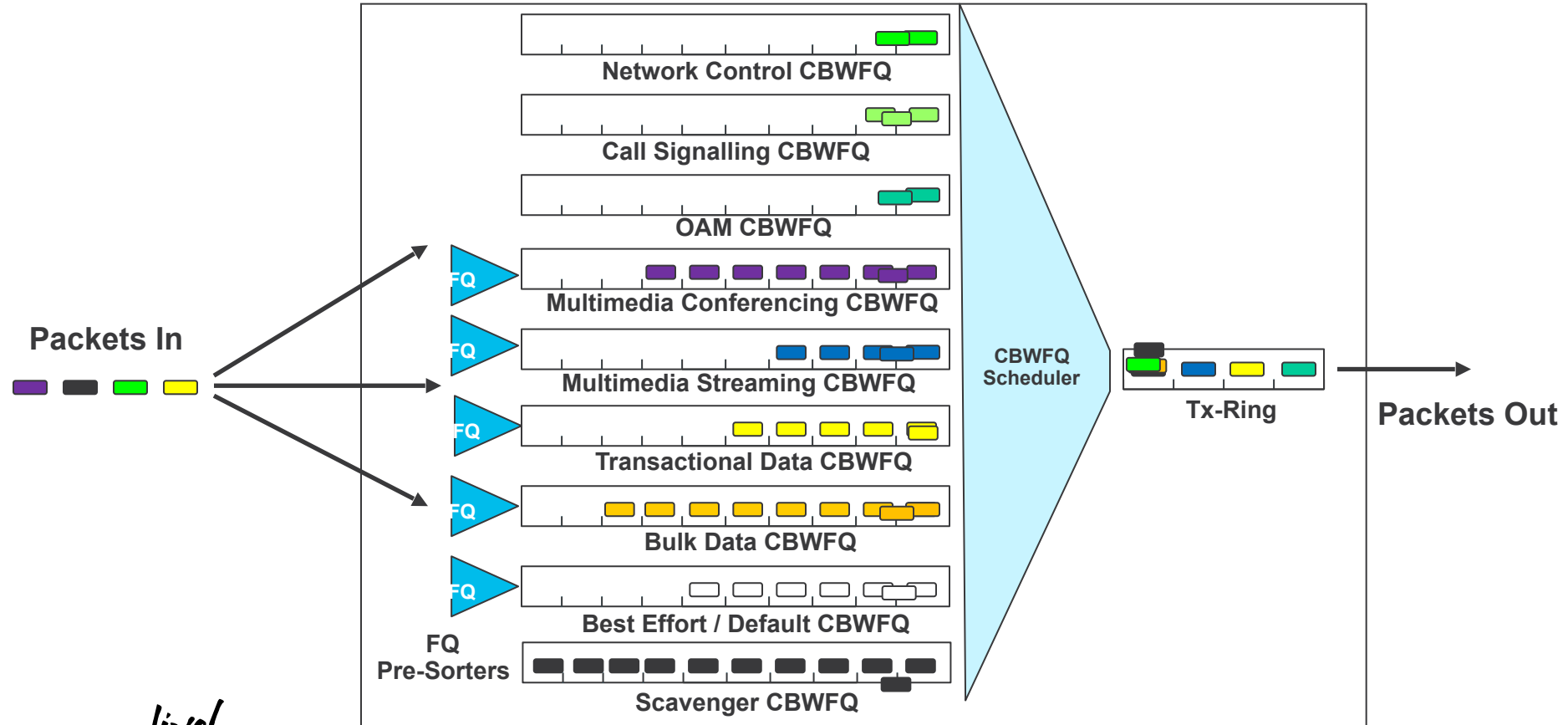
IOS Interface Buffers



QoS Tools Review: Queuing & Dropping Tools

CBWFQ

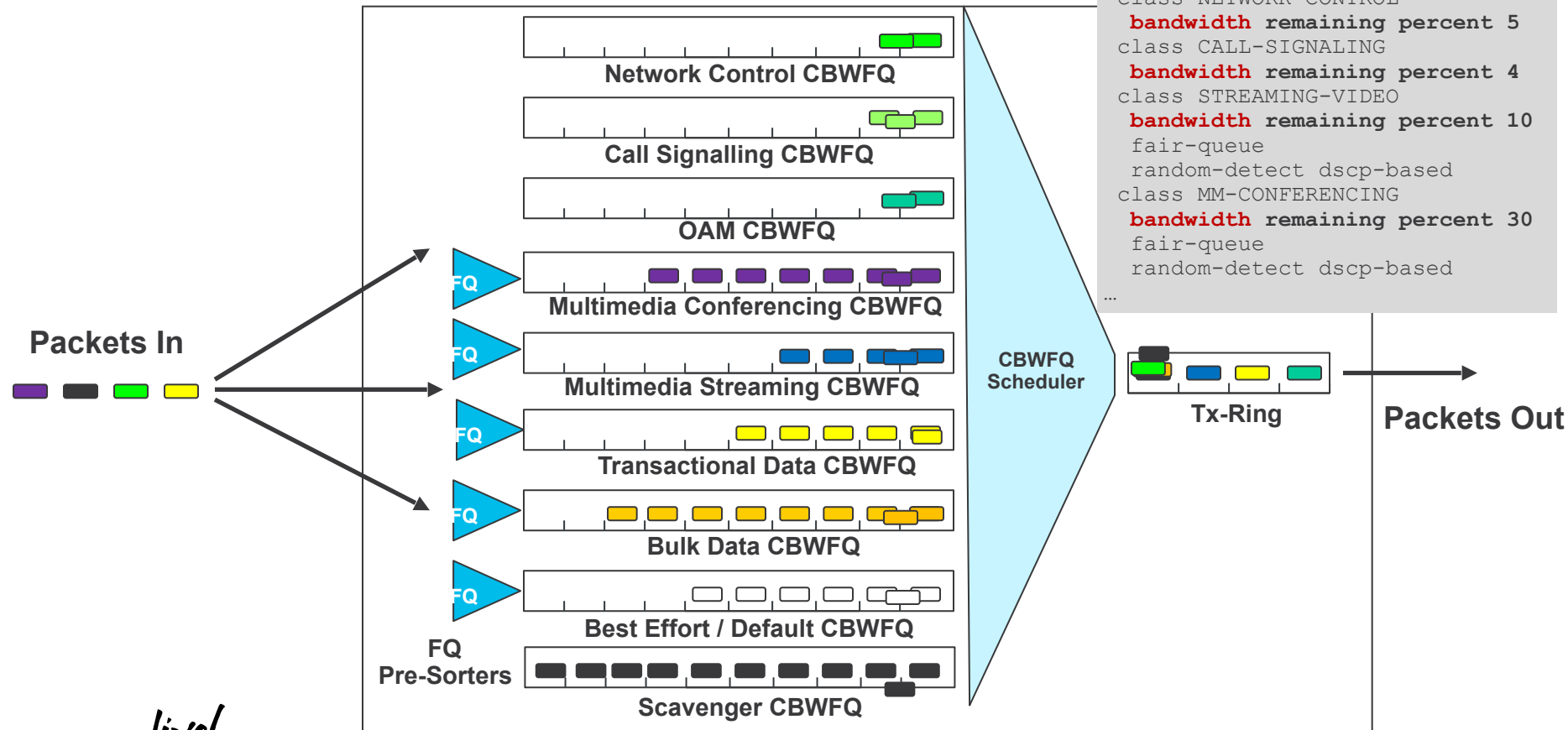
IOS Interface Buffers



QoS Tools Review: Queuing & Dropping Tools

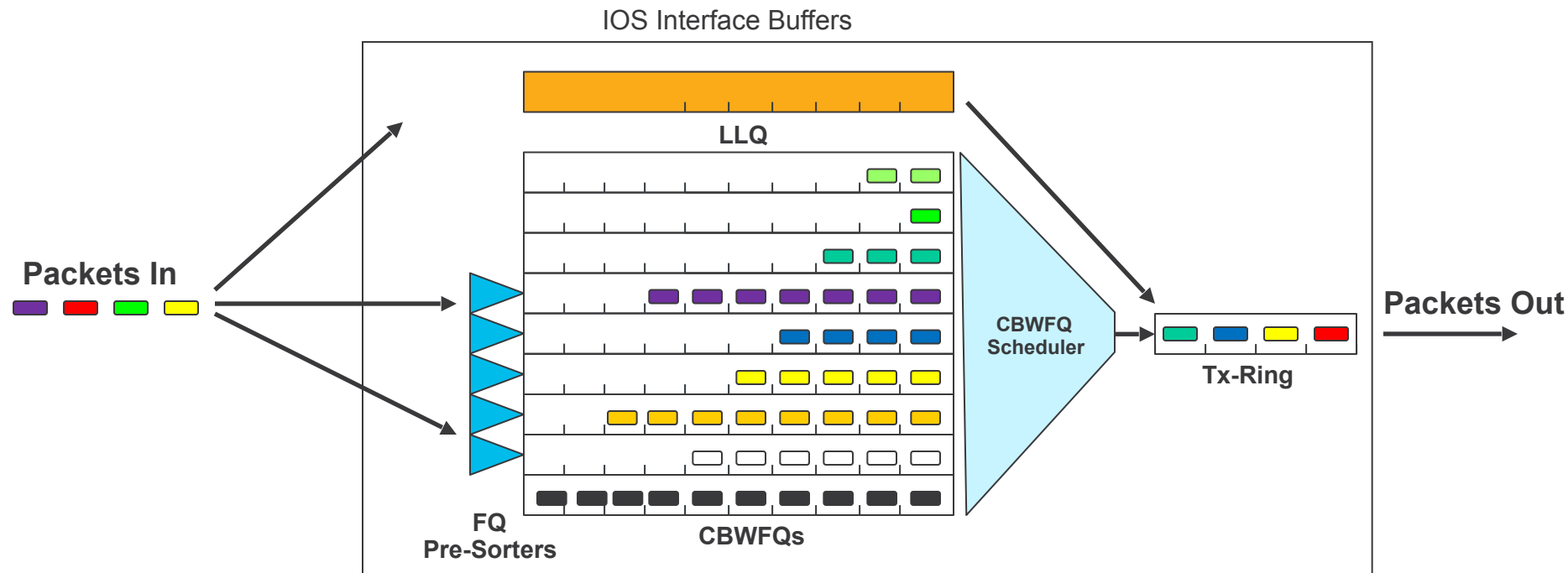
CBWFQ

IOS Interface Buffers



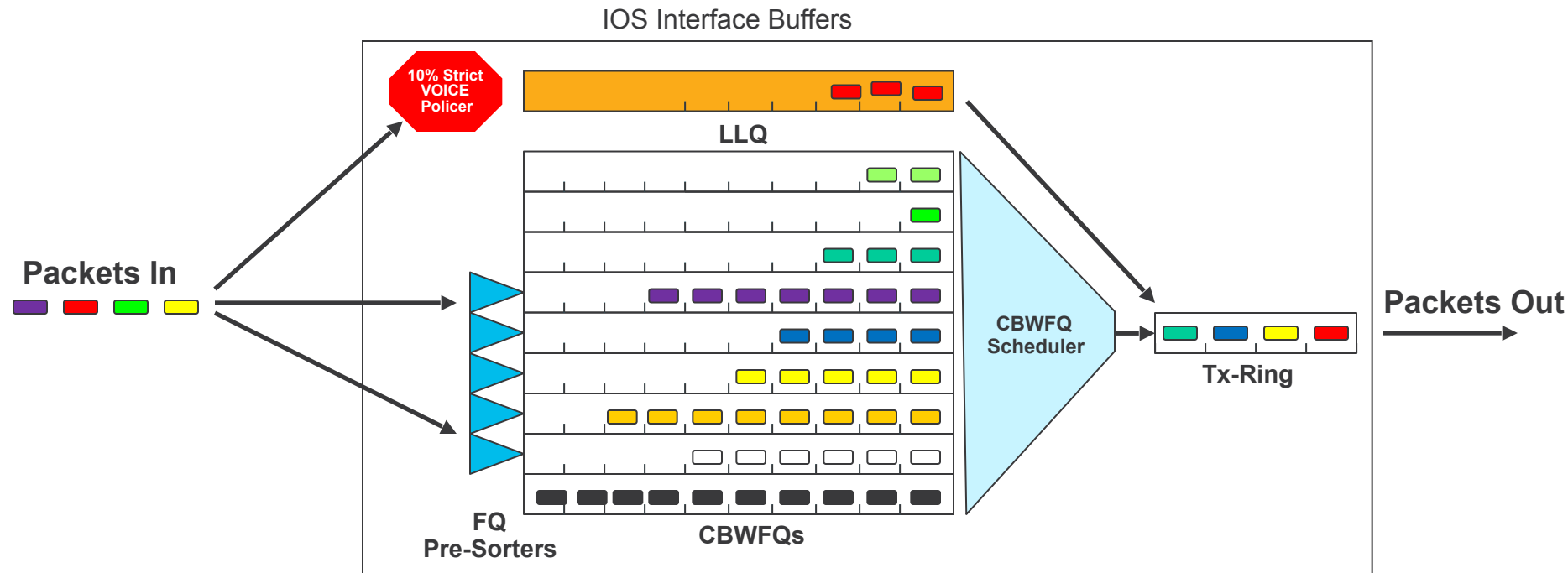
QoS Tools Review: Queuing & Dropping Tools

LLQ: Single-LLQ Operation and Configuration



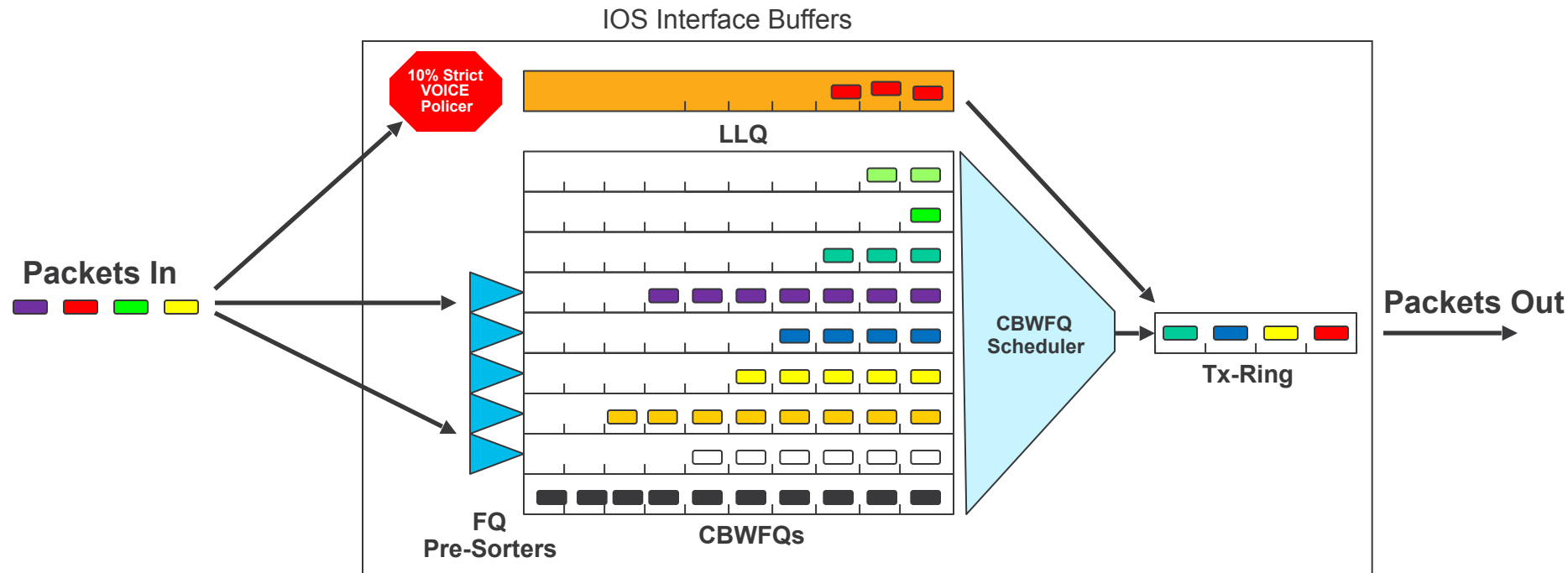
QoS Tools Review: Queuing & Dropping Tools

LLQ: Single-LLQ Operation and Configuration



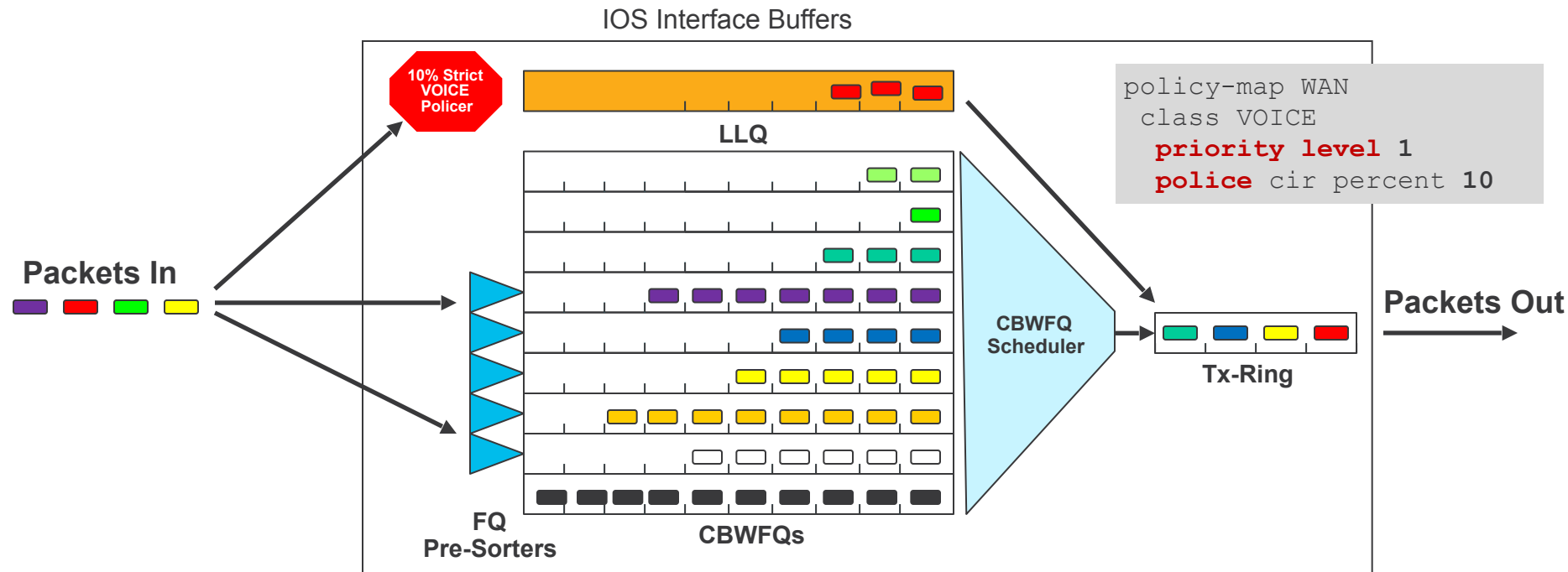
QoS Tools Review: Queuing & Dropping Tools

LLQ: Single-LLQ Operation and Configuration



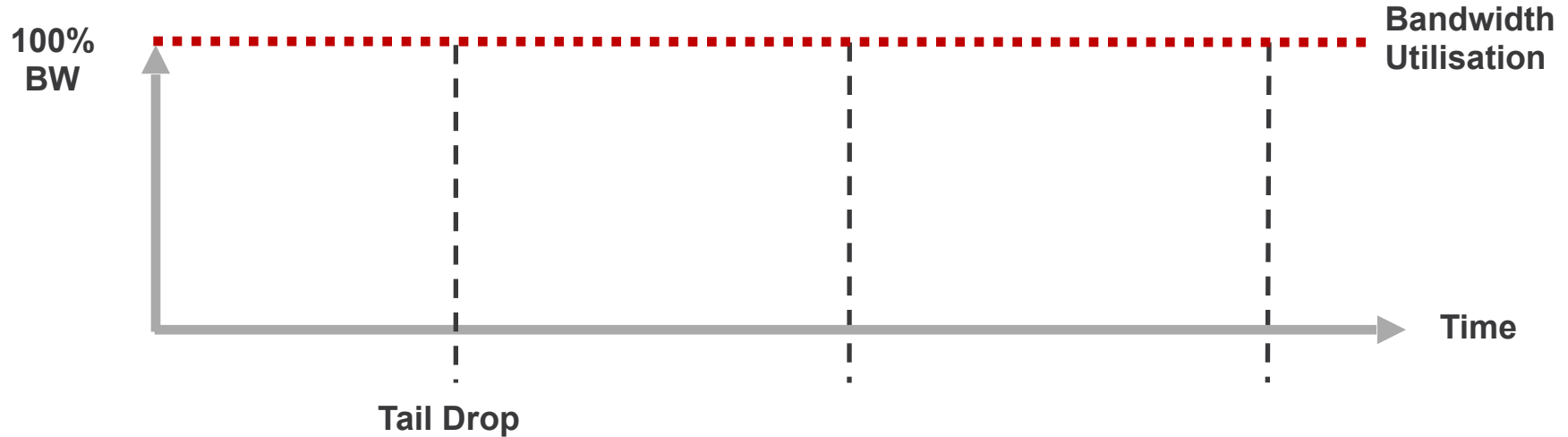
QoS Tools Review: Queuing & Dropping Tools

LLQ: Single-LLQ Operation and Configuration



QoS Tools Review: Queuing & Dropping Tools

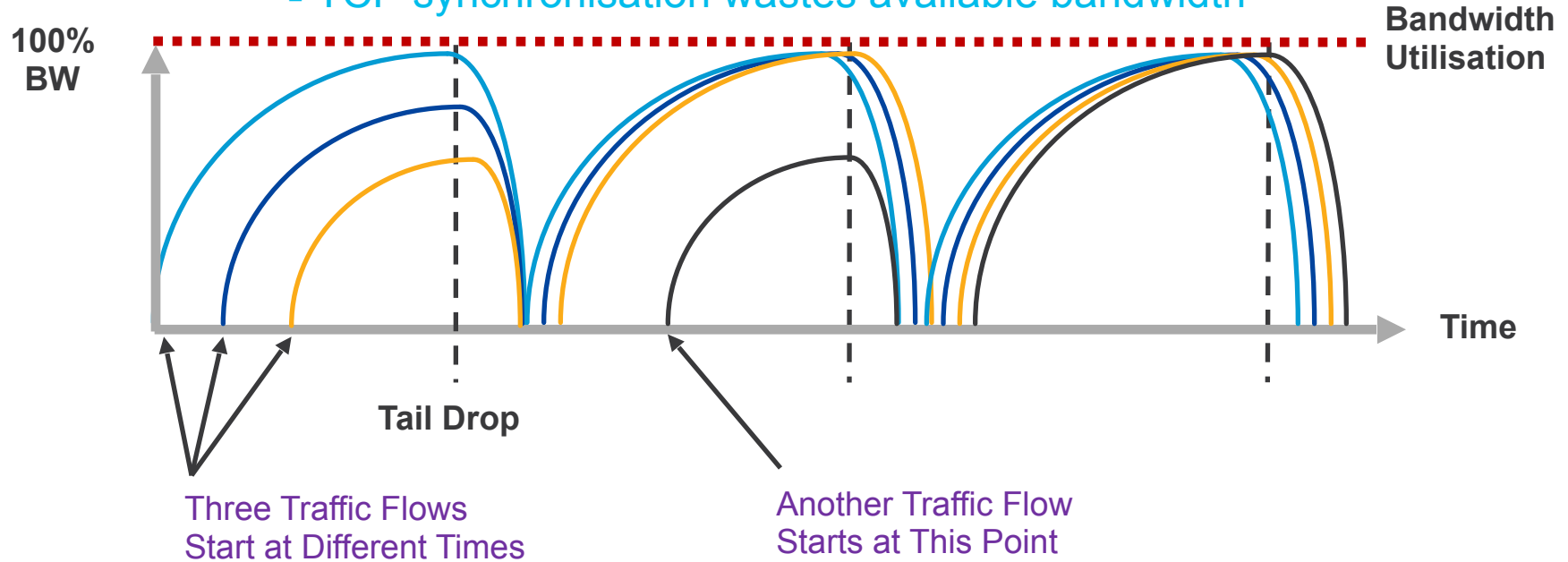
The Need for Congestion Avoidance



QoS Tools Review: Queuing & Dropping Tools

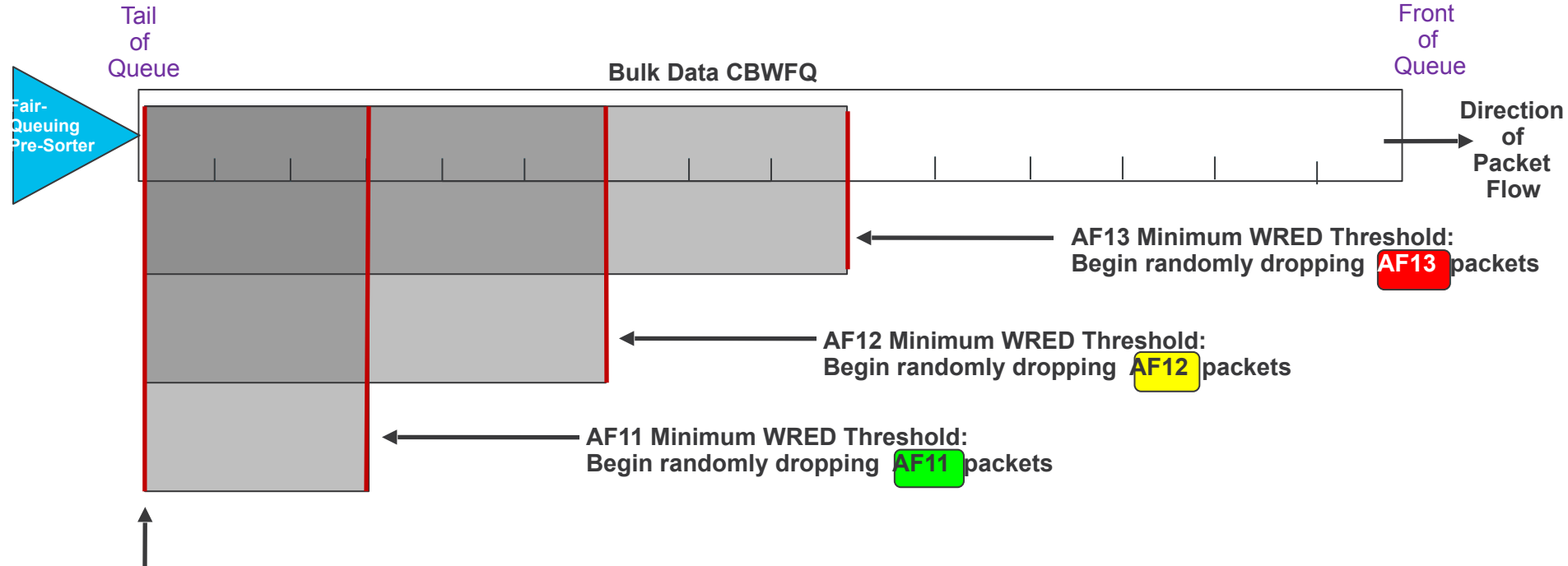
The Need for Congestion Avoidance

- All TCP flows synchronise in waves
- TCP synchronisation wastes available bandwidth



QoS Tools Review: Queuing & Dropping Tools

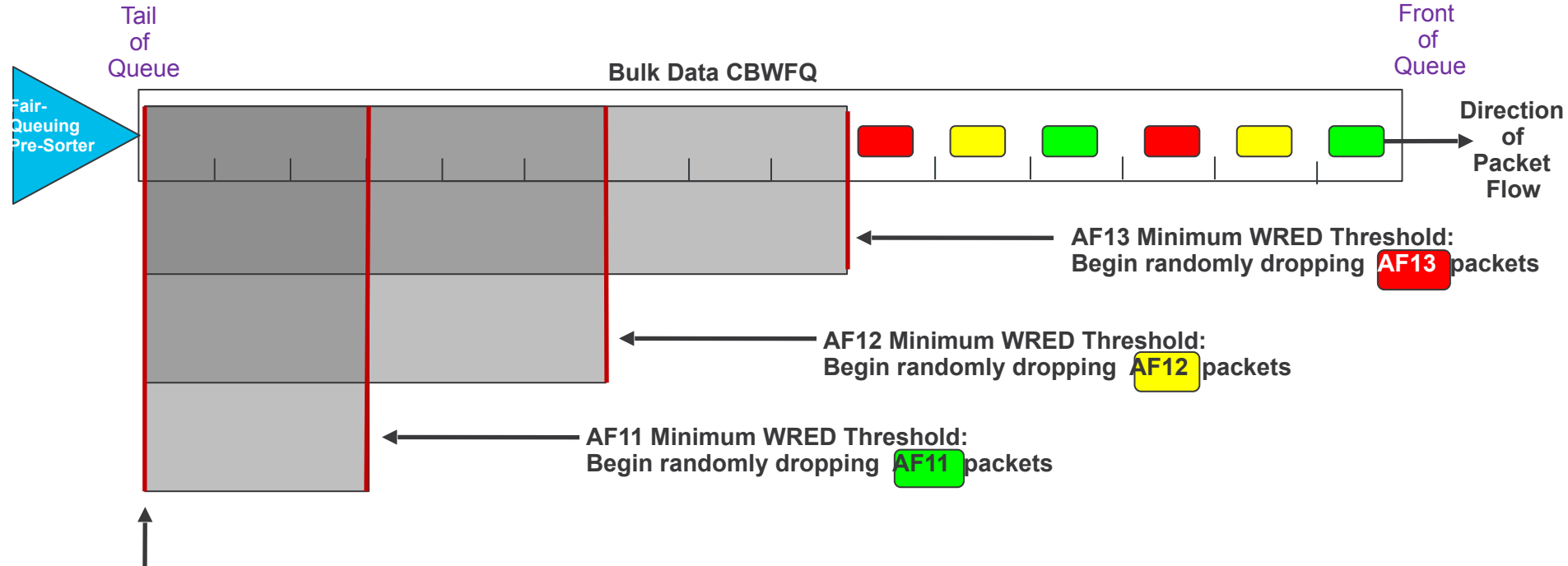
DSCP-Based WRED



Cisco *live!* Maximum WRED Thresholds for AF11, AF12 and AF13 are set to the tail of the queue in this example

QoS Tools Review: Queuing & Dropping Tools

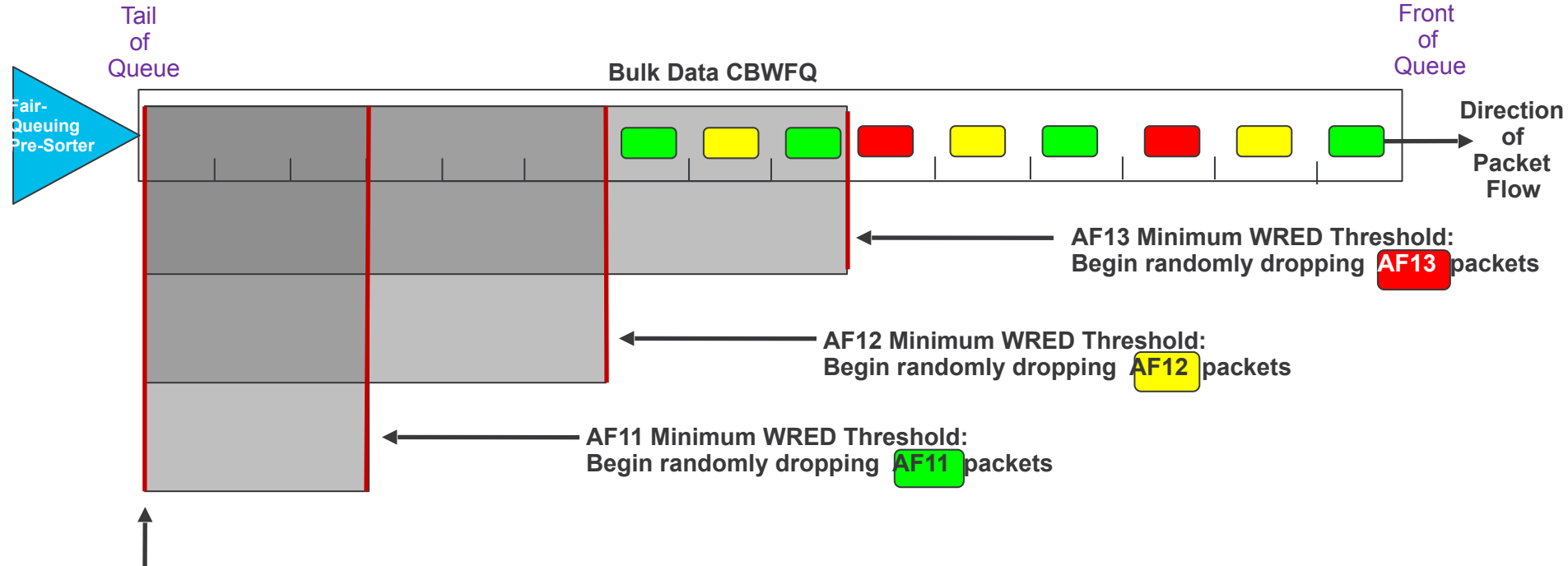
DSCP-Based WRED



Maximum WRED Thresholds for AF11, AF12 and AF13 are set to the tail of the queue in this example

QoS Tools Review: Queuing & Dropping Tools

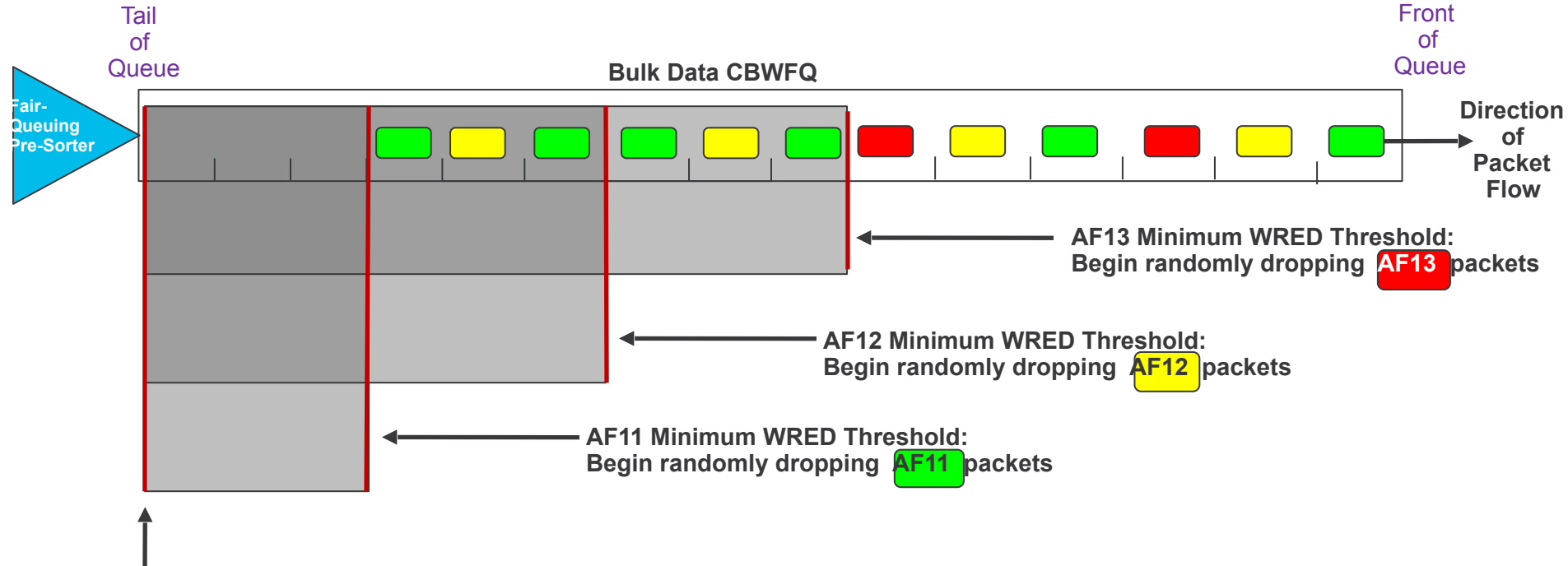
DSCP-Based WRED



Maximum WRED Thresholds for AF11, AF12 and AF13 are set to the tail of the queue in this example

QoS Tools Review: Queuing & Dropping Tools

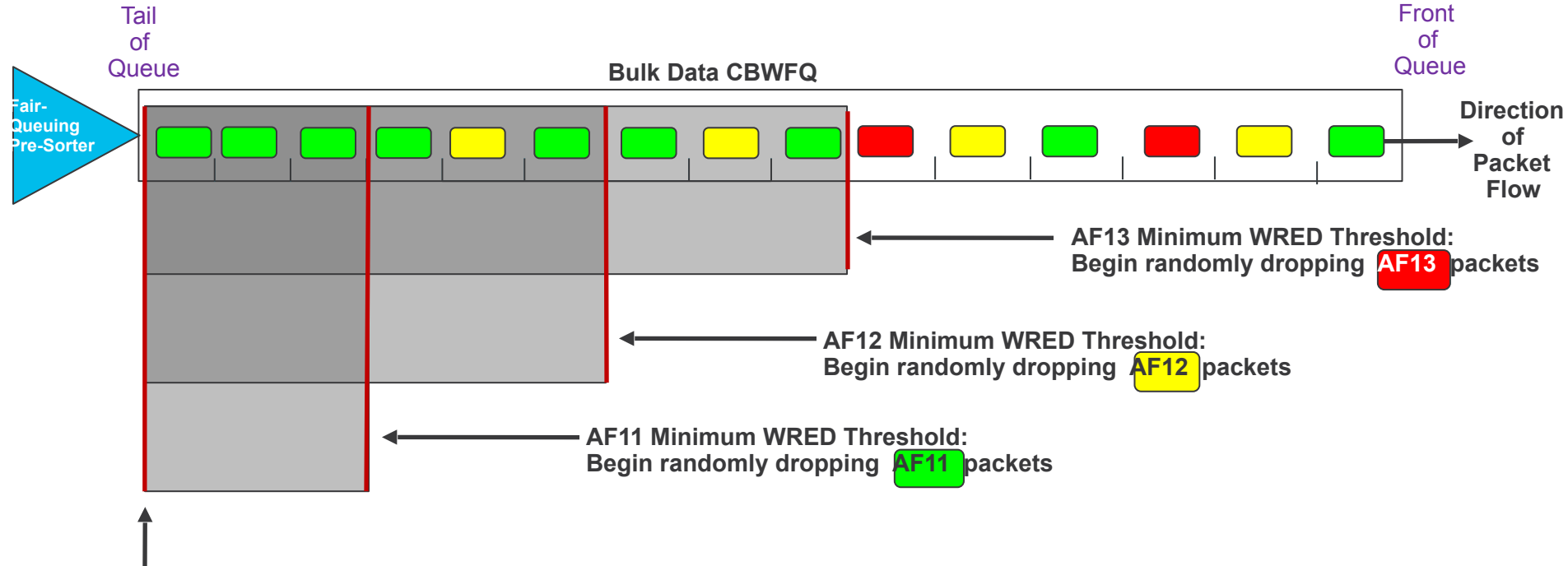
DSCP-Based WRED



Maximum WRED Thresholds for AF11, AF12 and AF13 are set to the tail of the queue in this example

QoS Tools Review: Queuing & Dropping Tools

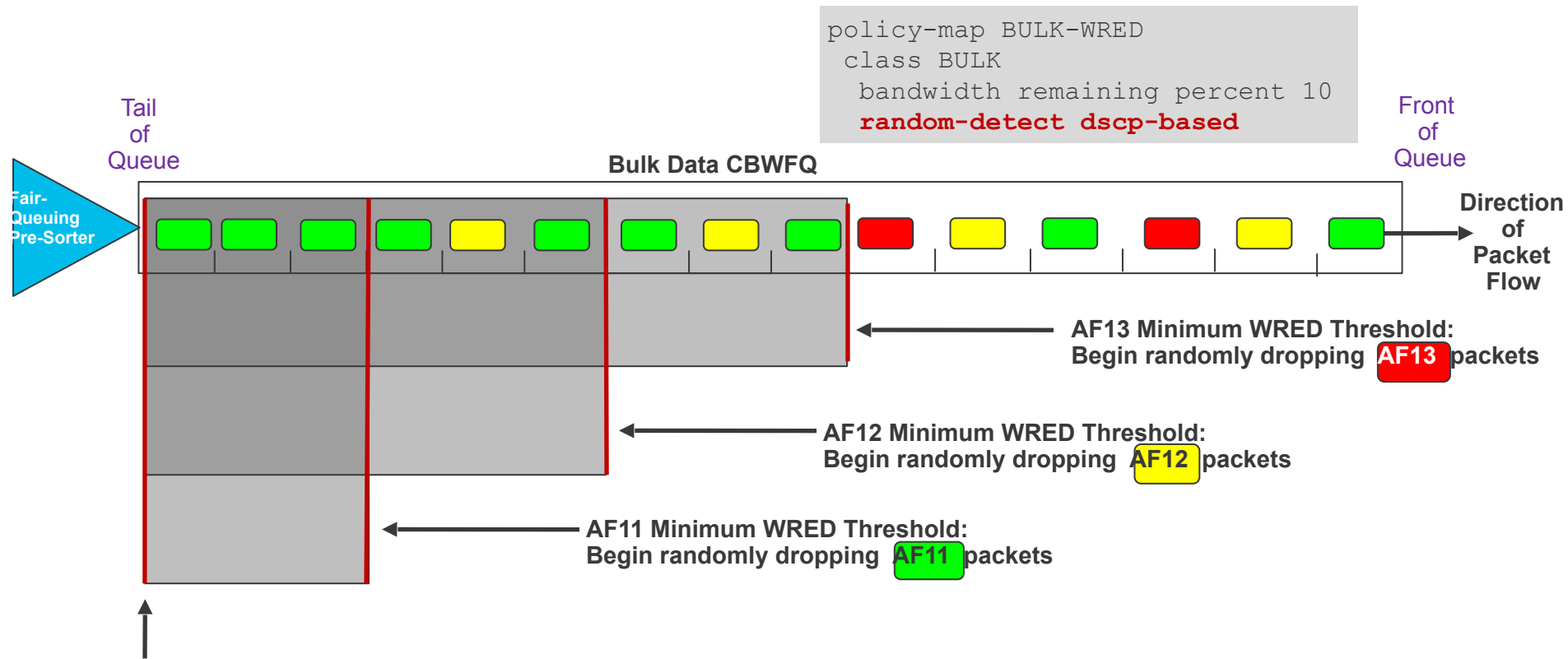
DSCP-Based WRED



Maximum WRED Thresholds for AF11, AF12 and AF13 are set to the tail of the queue in this example

QoS Tools Review: Queuing & Dropping Tools

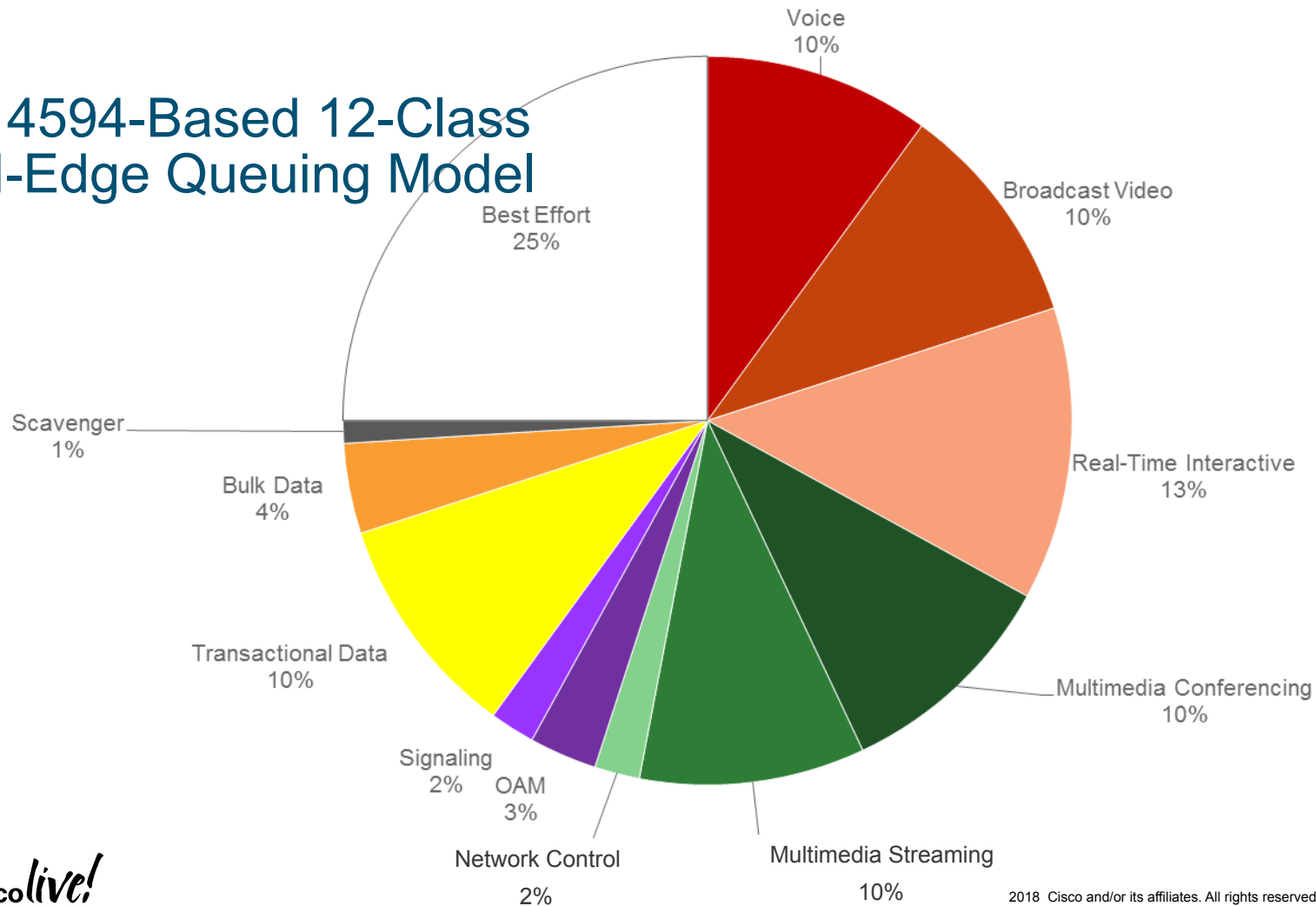
DSCP-Based WRED



Maximum WRED Thresholds for AF11, AF12 and AF13 are set to the tail of the queue in this example

RFC 4594-Based 12-Class WAN-Edge Queuing Model

RFC 4594-Based 12-Class WAN-Edge Queuing Model



RFC 4594-Based 12-Class Queuing Model Configuration

RFC 4594-Based 12-Class Queuing Model Configuration

```
class-map match-all VOICE-DSCP
  match dscp ef
class-map match-all BROADCAST_VIDEO-DSCP
  match dscp cs5
class-map match-all REALTIME_INTERACTIVE-DSCP
  match dscp cs4
class-map match-all NETWORK-CONTROL-DSCP
  match cs6
class-map match-all SIGNALING-DSCP
  match cs3
class-map match-all OAM-DSCP
  match cs2
class-map match-all MULTIMEDIA_CONFERENCING-DSCP
  match dscp af41
class-map match-all MULTIMEDIA_STREAMING-DSCP
  match dscp af31
class-map match-all TRANSACTIONAL-DATA-DSCP
  match dscp af21
class-map match-all BULK-DATA-DSCP
  match dscp af11
class-map match-all SCAVENGER-DSCP
  match dscp cs1
```

```
policy-map WAN_EDGE-QUEUING
  class VOICE-DSCP
    priority percent 10
  class BROADCAST_VIDEO-DSCP
    priority percent 10
  class REALTIME_INTERACTIVE-DSCP
    priority percent 13
  class NETWORK-CONTROL-DSCP
    bandwidth percent 2
  class SIGNALING-DSCP
    bandwidth percent 2
  class OAM-DSCP
    bandwidth percent 3
  class MULTIMEDIA_CONFERENCING-DSCP
    bandwidth percent 10
    fair-queue
    random-detect dscp-based
  class MULTIMEDIA_STREAMING-DSCP
    bandwidth percent 10
    fair-queue
    random-detect dscp-based
  class TRANSACTIONAL-DATA-DSCP
    bandwidth percent 10
    fair-queue
    random-detect dscp-based
  class BULK-DATA-DSCP
    bandwidth percent 4
    fair-queue
    random-detect dscp-based
  class SCAVENGER-DSCP
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    fair-queue
    random-detect dscp-based
```

RFC 4594-Based 12-Class Queuing Model Configuration

```
class-map match-all VOICE-DSCP
  match dscp ef
class-map match-all BROADCAST_VIDEO-DSCP
  match dscp cs5
class-map match-all REALTIME_INTERACTIVE-DSCP
  match dscp cs4
class-map match-all NETWORK-CONTROL-DSCP
  match cs6
class-map match-all SIGNALING-DSCP
  match cs3
class-map match-all OAM-DSCP
  match cs2
class-map match-all MULTIMEDIA_CONFERENCING-DSCP
  match dscp af41
class-map match-all MULTIMEDIA_STREAMING-DSCP
  match dscp af31
class-map match-all TRANSACTIONAL-DATA-DSCP
  match dscp af21
class-map match-all BULK-DATA-DSCP
  match dscp af11
class-map match-all SCAVENGER-DSCP
  match dscp cs1
```

```
policy-map WAN_EDGE-QUEUING
  class VOICE-DSCP
    priority percent 10
  class BROADCAST_VIDEO-DSCP
    priority percent 10
  class REALTIME_INTERACTIVE-DSCP
    priority percent 13
  class NETWORK-CONTROL-DSCP
    bandwidth percent 2
  class SIGNALING-DSCP
    bandwidth percent 2
  class OAM-DSCP
    bandwidth percent 3
  class MULTIMEDIA_CONFERENCING-DSCP
    bandwidth percent 10
    fair-queue
    random-detect dscp-based
  class MULTIMEDIA_STREAMING-DSCP
    bandwidth percent 10
    fair-queue
    random-detect dscp-based
  class TRANSACTIONAL-DATA-DSCP
    bandwidth percent 10
    fair-queue
    random-detect dscp-based
  class BULK-DATA-DSCP
    bandwidth percent 4
    fair-queue
    random-detect dscp-based
  class SCAVENGER-DSCP
    bandwidth percent 1
  class class-default
    bandwidth percent 25
    fair-queue
    random-detect dscp-based
```



Note: Appending “-DSCP” to the class-map names distinguishes WAN-Edge egress-queuing class-maps (matching on DSCP values) from the LAN-Edge ingress class-maps (matching via NBAR2).

What Changes for Sub-Line-Rate Interfaces?

What Changes for Sub-Line-Rate Interfaces?

- Queuing policies will not engage unless the interface is congested



What Changes for Sub-Line-Rate Interfaces?

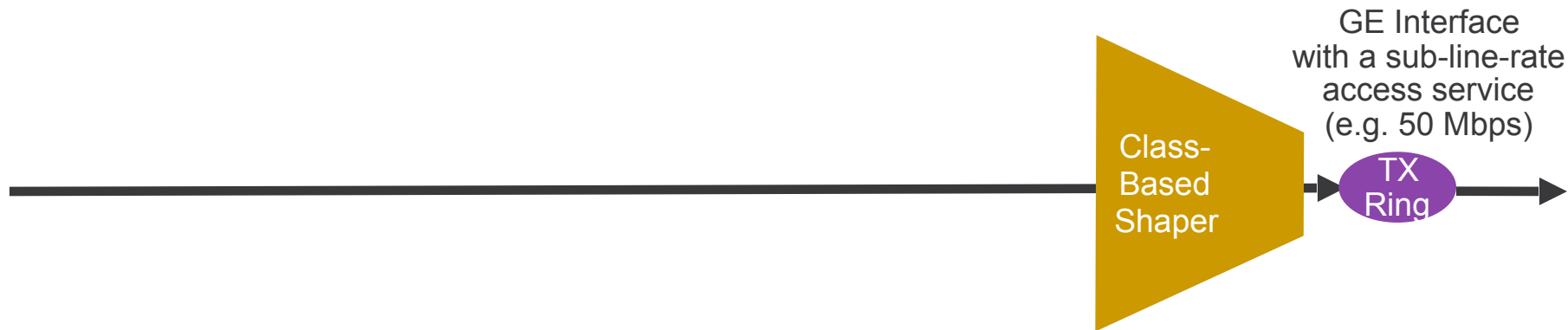
- Queuing policies will not engage unless the interface is congested



What Changes for Sub-Line-Rate Interfaces?

```
policy-map HQoS-50MBPS
class class-default
  shape average 50000000
```

- Queuing policies will not engage unless the interface is congested
- A shaper will guarantee that traffic will not exceed the contracted rate

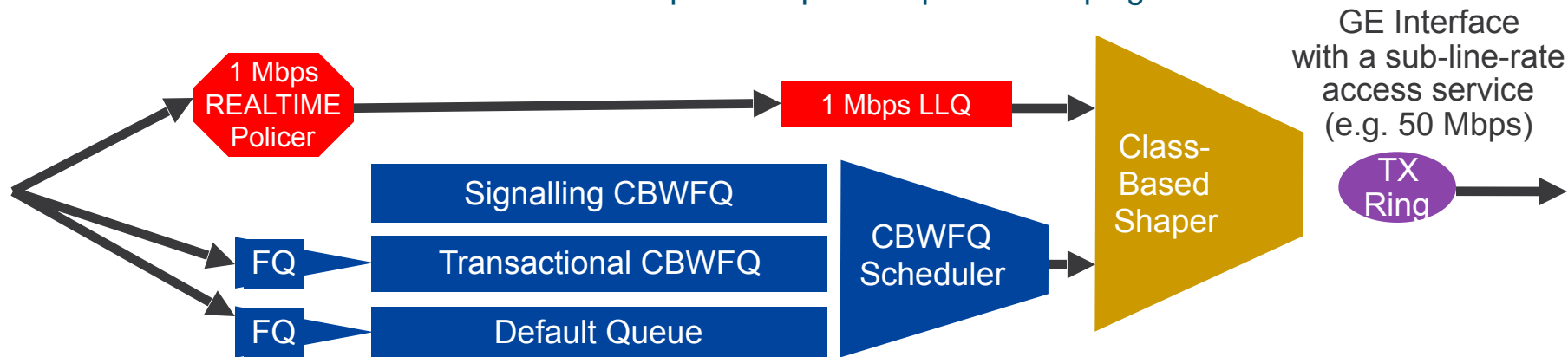


What Changes for Sub-Line-Rate Interfaces?

```
policy-map QUEUING
class REALTIME
  priority 1000
class SIGNALING
  bandwidth x
class TRANSACTIONAL
  bandwidth y...
class class-default
  fair-queue
```

```
policy-map HQoS-50MBPS
class class-default
  shape average 50000000
  service-policy QUEUING
```

- Queuing policies will not engage unless the interface is congested
- A shaper will guarantee that traffic will not exceed the contracted rate
- A nested queuing policy will force queuing to engage at the contracted sub-line-rate to prioritise packets prior to shaping



Hierarchical (Shaping + Queuing) QoS Policy Config

Hierarchical (Shaping + Queuing) QoS Policy Config



Hierarchical (Shaping + Queuing) QoS Policy Config

```
policy-map HQOS-50M-OUT  
  class class-default  
    shape average 50M  
    service-policy WAN-EDGE-QUEUING
```

← A Parent QoS Policy is required to shape to the contracted rate

← A (nested) Child QoS Policy queues traffic *within* the shaped rate



Hierarchical (Shaping + Queuing) QoS Policy Config

```
policy-map HQOS-50M-OUT  
  class class-default  
    shape average 50M  
    service-policy WAN-EDGE-QUEUING
```

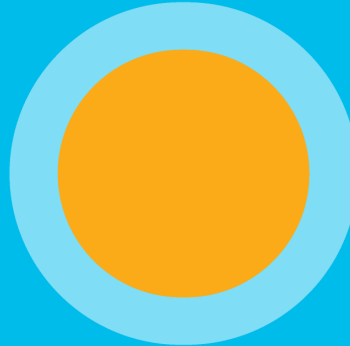
A Parent QoS Policy is required to shape to the contracted rate

A (nested) Child QoS Policy queues traffic *within* the shaped rate

```
interface GigabitEthernet0/2  
  description AT&T Circuit from SJ-13-12 to RTP-Ridge-7 @ 50 Mbps Contracted Rate  
  service-policy output HQOS-50M-OUT
```

The Parent QoS Policy (shaper with nested queuing policy) is applied to the sub-line-rate interface

IWAN QoS Design

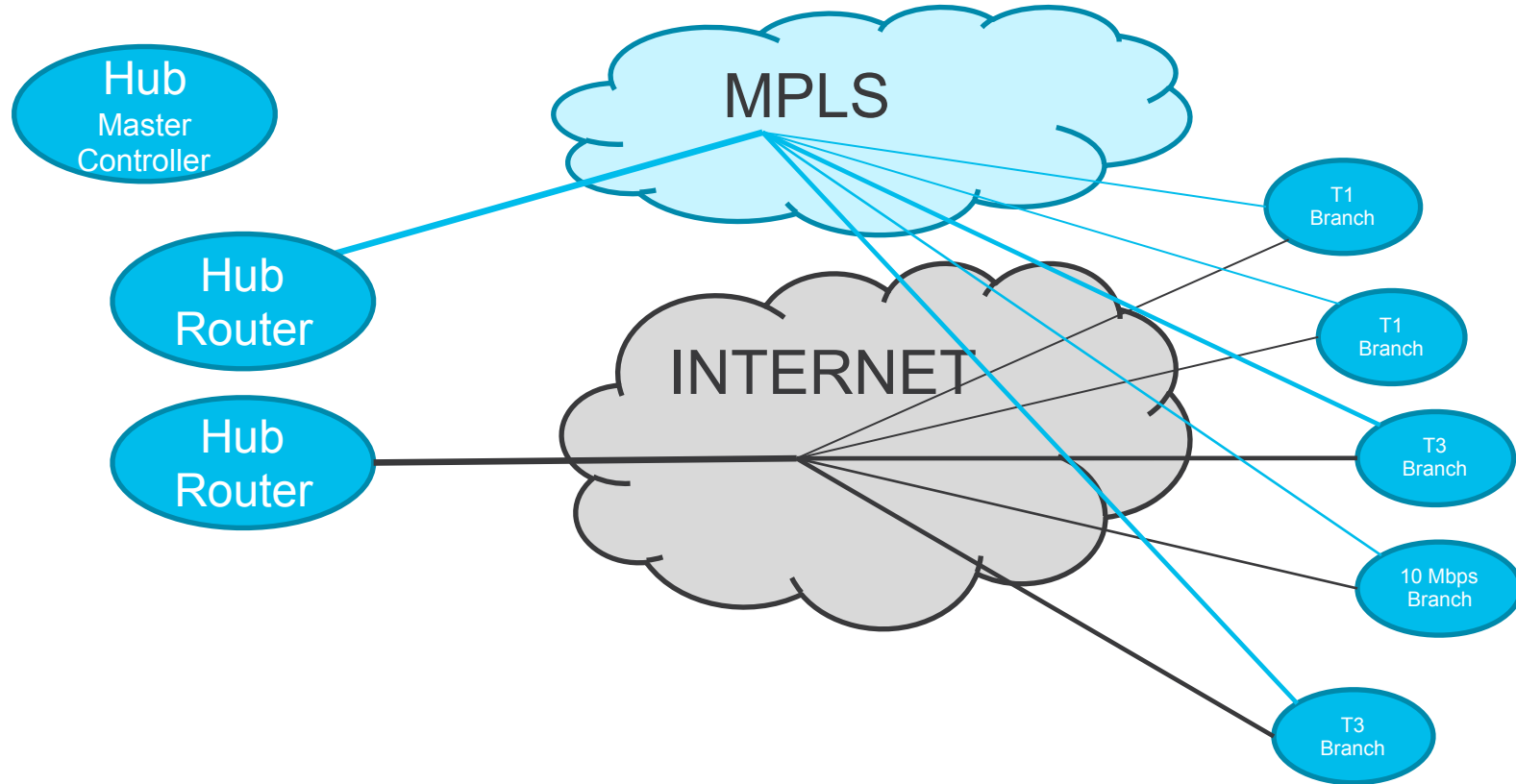




What is IWAN from a QoS Perspective?

- Augment expensive MPLS service with business class internet
- Performance Routing (PfR) to load balance / provide resiliency / best path
- Dynamic Multipoint VPN (DMVPN) overlay on MPLS and Internet
- Up to 2,000 remote sites per hub router in a single domain
- MPLS will have Service Provider QoS, but with Internet we assume none

Hybrid Model – MPLS and Internet



IWAN Egress QoS Models

Example: Combining 12 Classes into an 8-Class Model



Application	DSCP
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF41
Real-Time Interactive	CS4
Multimedia Streaming	AF31
Signalling	CS3
Transactional Data	AF21
Network Management (OAM)	CS2
Bulk Data	AF11
Scavenger	CS1
Best Effort	DF

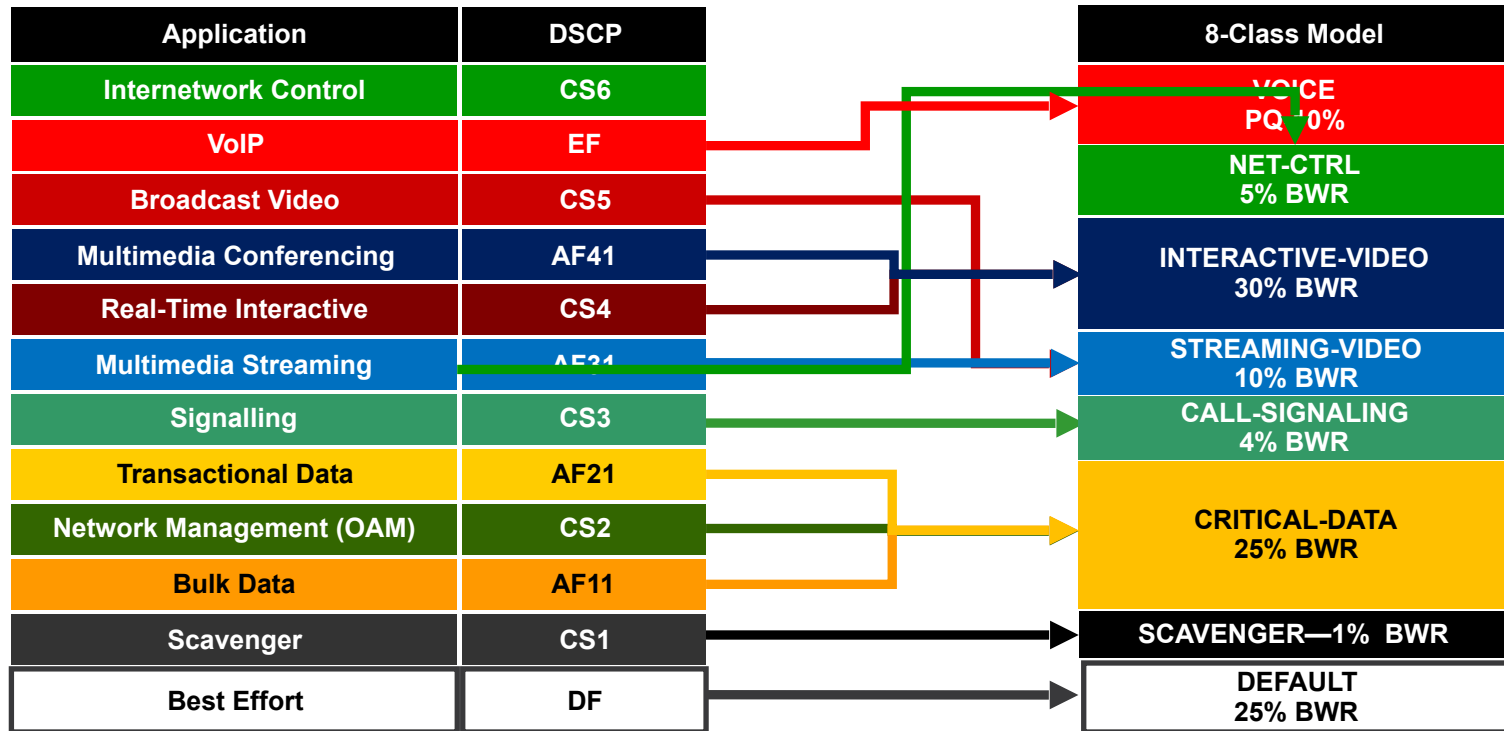
8-Class Model
VOICE PQ-10%
NET-CTRL 5% BWR
INTERACTIVE-VIDEO 30% BWR
STREAMING-VIDEO 10% BWR
CALL-SIGNALING 4% BWR
CRITICAL-DATA 25% BWR
SCAVENGER—1% BWR
DEFAULT 25% BWR

PQ = Priority Queue
BWR = Bandwidth Remaining

Note: Bandwidth Remaining
Percentages must equal 100%

IWAN Egress QoS Models

Example: Combining 12 Classes into an 8-Class Model



PQ = Priority Queue
BWR = Bandwidth Remaining

Note: Bandwidth Remaining
Percentages must equal 100%

IWAN 8-Class Egress Queuing Model

Child Policy

IWAN 8-Class Queuing Model Class-Maps

```
class-map match-any VOICE-DSCP
  match dscp ef
class-map match-any INTERACTIVE-VIDEO-DSCP
  match dscp cs4 af41 af42 af43
class-map match-any STREAMING-VIDEO-DSCP
  match dscp cs5 af31 af32 af33
class-map match-any NETWORK-CONTROL-DSCP
  match dscp cs6
class-map match-any SIGNALING-DSCP
  match dscp cs3
class-map match-any CRITICAL-DATA-DSCP
  match dscp cs2 af11 af12 af13 af21 af22 af23
class-map match-any SCAVENGER-DSCP
  match dscp cs1
```

IWAN 8-Class Egress Queuing Model

Child Policy

IWAN 8-Class Queuing Model Class-Maps

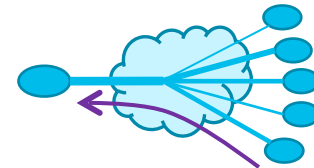
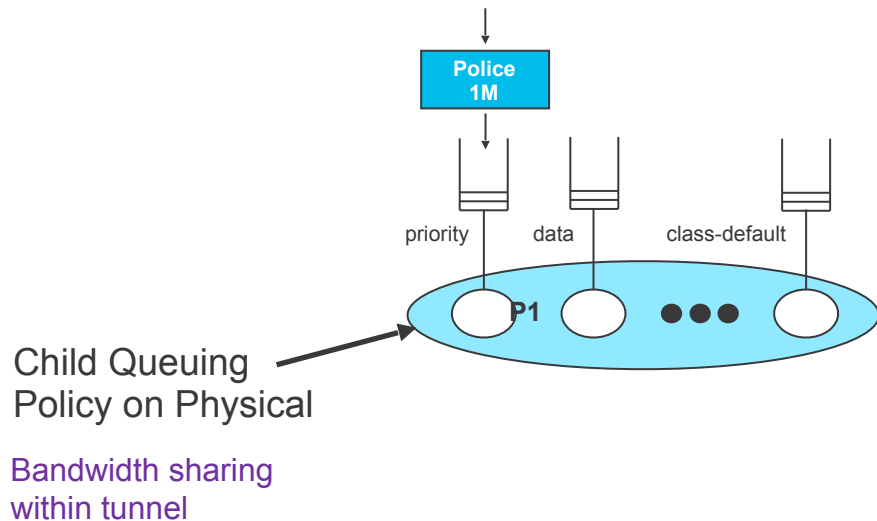
```
class-map match-any VOICE-DSCP
  match dscp ef
class-map match-any INTERACTIVE-VIDEO-DSCP
  match dscp cs4 af41 af42 af43
class-map match-any STREAMING-VIDEO-DSCP
  match dscp cs5 af31 af32 af33
class-map match-any NETWORK-CONTROL-DSCP
  match dscp cs6
class-map match-any SIGNALING-DSCP
  match dscp cs3
class-map match-any CRITICAL-DATA-DSCP
  match dscp cs2 af11 af12 af13 af21 af22 af23
class-map match-any SCAVENGER-DSCP
  match dscp cs1
```

IWAN 8-Class Queuing Policy-Map

```
policy-map IWAN-EDGE-QUEUING
  class VOICE-DSCP
    priority level 1
    police cir percent 10
  class INTERACTIVE-VIDEO-DSCP
    bandwidth remaining percent 30
    random-detect dscp-based
  class STREAMING-VIDEO-DSCP
    bandwidth remaining percent 10
    random-detect dscp-based
  class NETWORK-CONTROL-DSCP
    bandwidth remaining percent 5
  class SIGNALING-DSCP
    bandwidth remaining percent 4
  class CRITICAL-DATA-DSCP
    bandwidth remaining percent 25
    random-detect dscp-based
  class SCAVENGER-DSCP
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 25
    random-detect
```

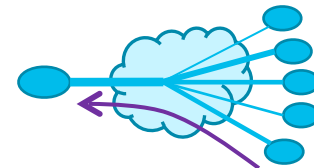
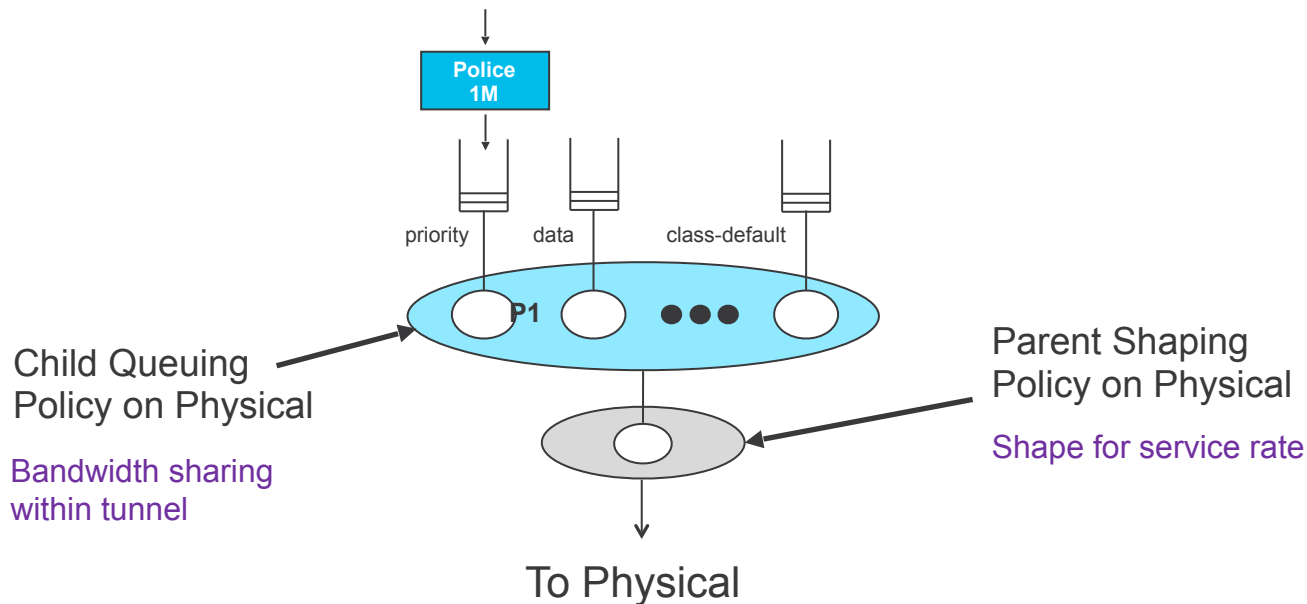
Branch QoS Scheduling Hierarchy

Two Levels: Child / Parent



Branch QoS Scheduling Hierarchy

Two Levels: Child / Parent

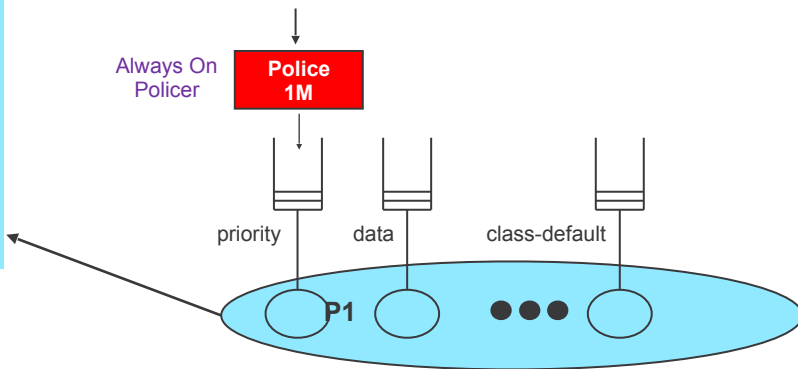


Branch QoS Scheduling Hierarchy

Two Levels: Child / Parent

```
policy-map IWAN-EDGE-QUEUING
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
class CALL-SIGNALING
  bandwidth remaining percent 4
class NET-CTRL
  bandwidth remaining percent 5
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
class SCAVENGER
  bandwidth remaining percent 1
class VOICE
  priority level 1
  police cir percent 10
class class-default
  bandwidth remaining percent 25
  random-detect
```

```
policy-map POLICY-TRANSPORT-1
class class-default
  shape average 10 Mbps
  service-policy WAN-EDGE-QUEUING
```



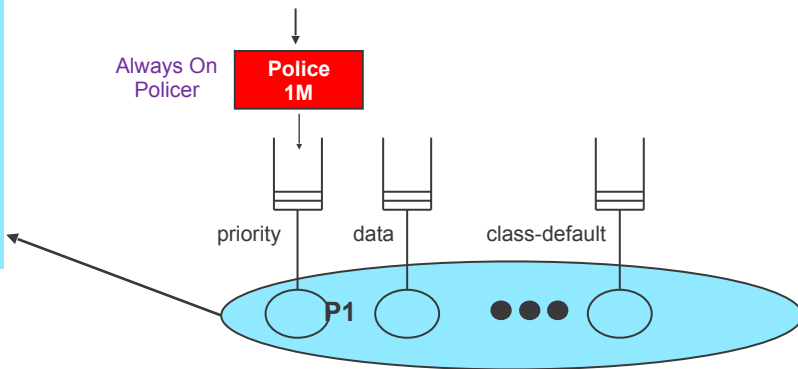
Branch QoS Scheduling Hierarchy

Two Levels: Child / Parent

```
policy-map IWAN-EDGE-QUEUING
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
class CALL-SIGNALING
  bandwidth remaining percent 4
class NET-CTRL
  bandwidth remaining percent 5
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
class SCAVENGER
  bandwidth remaining percent 1
class VOICE
  priority level 1
  police cir percent 10
class class-default
  bandwidth remaining percent 25
  random-detect
```

```
policy-map POLICY-TRANSPORT-1
class class-default
  shape average 10 Mbps
  service-policy WAN-EDGE-QUEUING
```

- A **shaper** will guarantee that traffic will **not exceed the contracted rate**



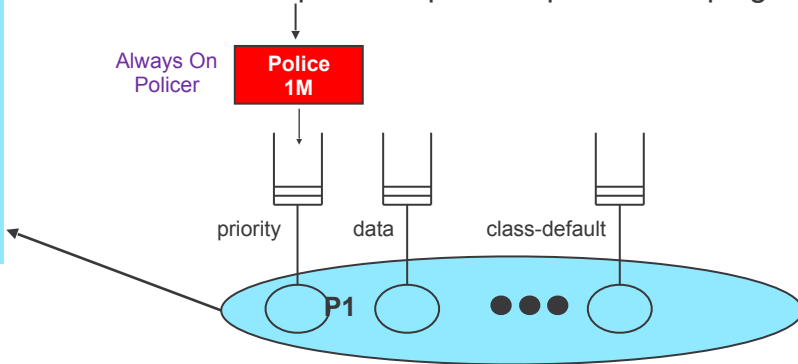
Branch QoS Scheduling Hierarchy

Two Levels: Child / Parent

```
policy-map IWAN-EDGE-QUEUEING
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
class CALL-SIGNALING
bandwidth remaining percent 4
class NET-CTRL
bandwidth remaining percent 5
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
class SCAVENGER
bandwidth remaining percent 1
class VOICE
priority level 1
police cir percent 10
class class-default
bandwidth remaining percent 25
random-detect
```

```
policy-map POLICY-TRANSPORT-1
class class-default
shape average 10 Mbps
service-policy WAN-EDGE-QUEUEING
```

- A shaper will guarantee that traffic will not exceed the contracted rate
- A nested queuing policy will force queuing to engage at the contracted sub-line-rate to prioritise packets prior to shaping



Branch QoS Scheduling Hierarchy

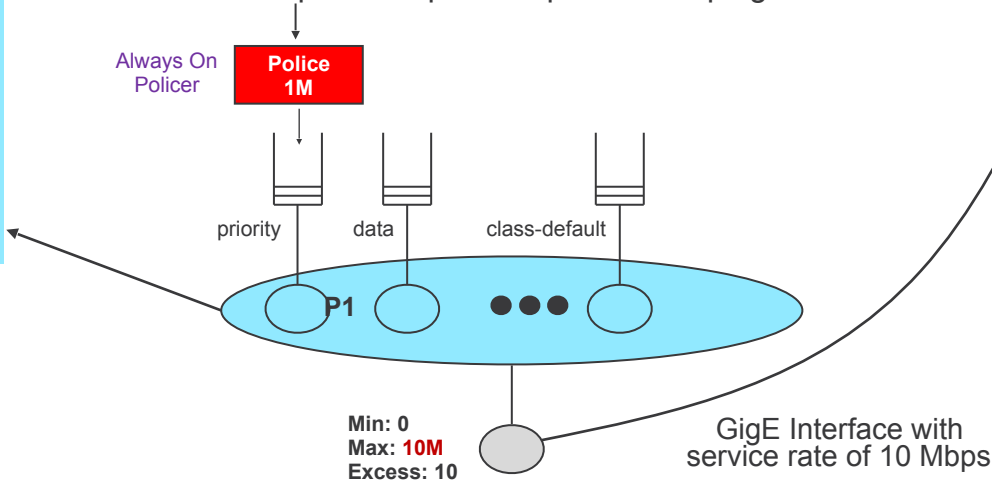
Two Levels: Child / Parent

```
policy-map IWAN-EDGE-QUEUING
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
class CALL-SIGNALING
bandwidth remaining percent 4
class NET-CTRL
bandwidth remaining percent 5
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
class SCAVENGER
bandwidth remaining percent 1
class VOICE
priority level 1
police cir percent 10
class class-default
bandwidth remaining percent 25
random-detect
```

```
policy-map POLICY-TRANSPORT-1
class class-default
shape average 10 Mbps
service-policy WAN-EDGE-QUEUING
```

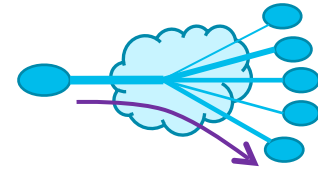
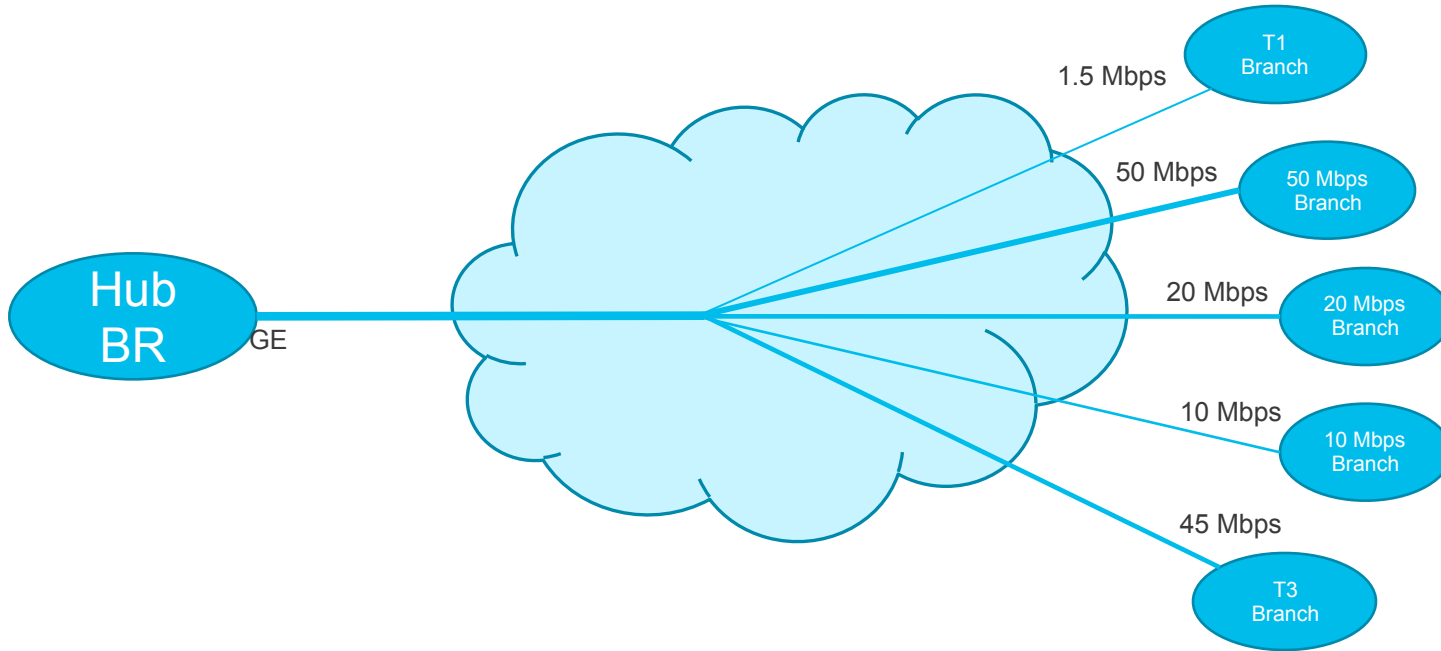
```
interface GigabitEthernet0/0
bandwidth 10000
service-policy output POLICY-TRANSPORT-1
```

- A shaper will guarantee that traffic will not exceed the contracted rate
- A nested queuing policy will force queuing to engage at the contracted sub-line-rate to prioritise packets prior to shaping



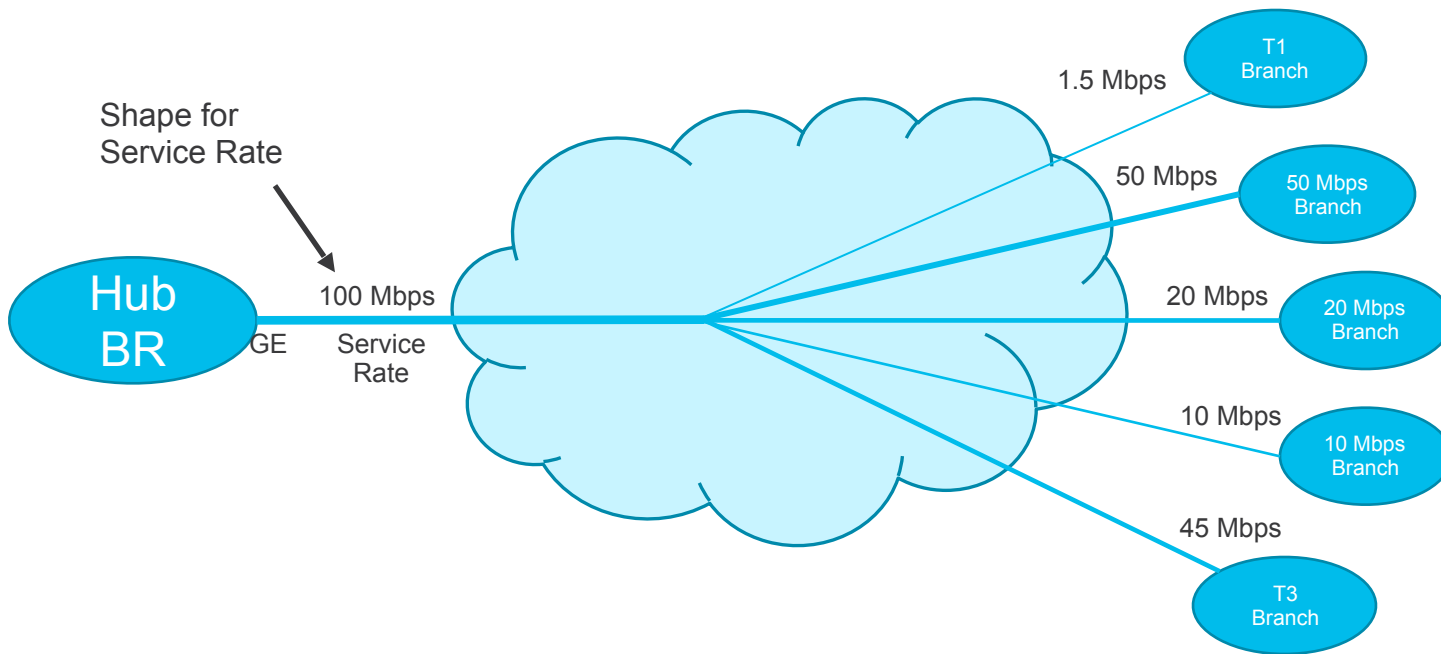
Hub Site QoS Scheduling

Three Levels: Child / Parent / Grandparent



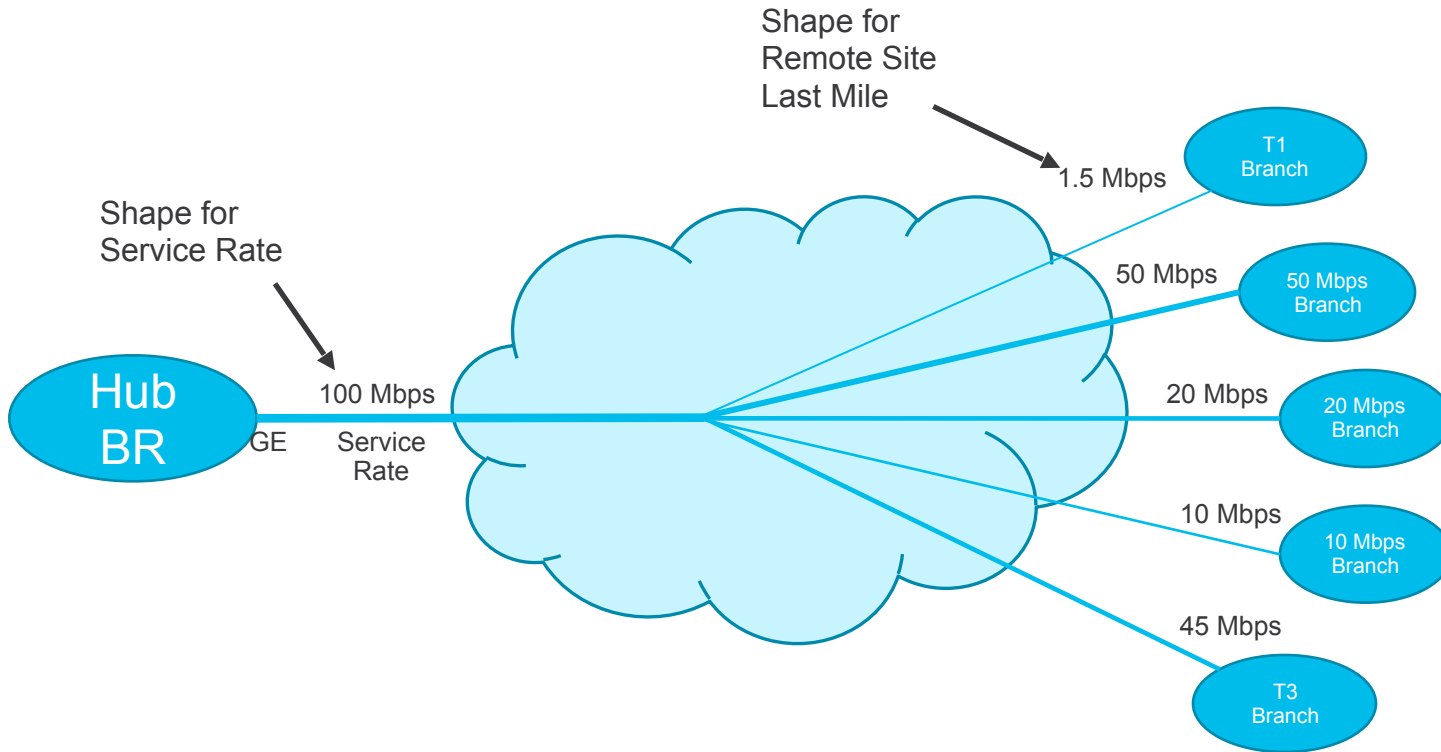
Hub Site QoS Scheduling

Three Levels: Child / Parent / Grandparent



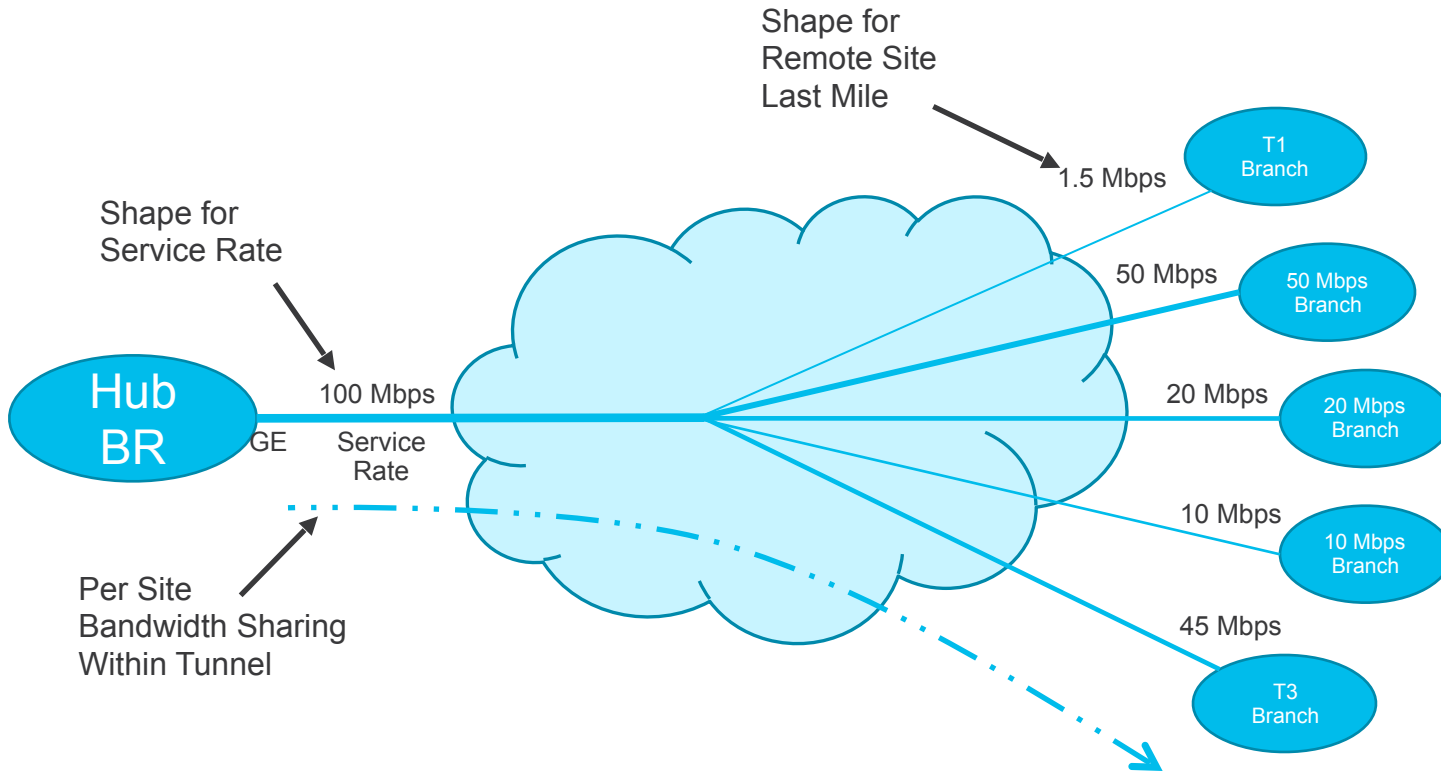
Hub Site QoS Scheduling

Three Levels: Child / Parent / Grandparent



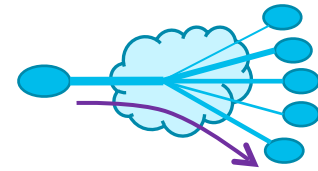
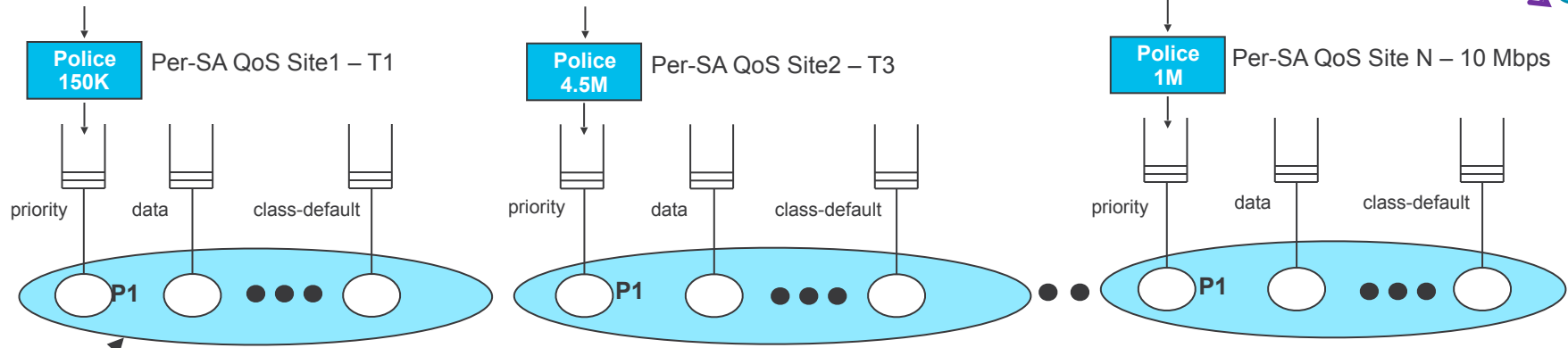
Hub Site QoS Scheduling

Three Levels: Child / Parent / Grandparent



Hub Site QoS Scheduling Hierarchy

Three Levels: Child / Parent / Grandparent

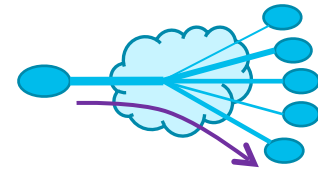
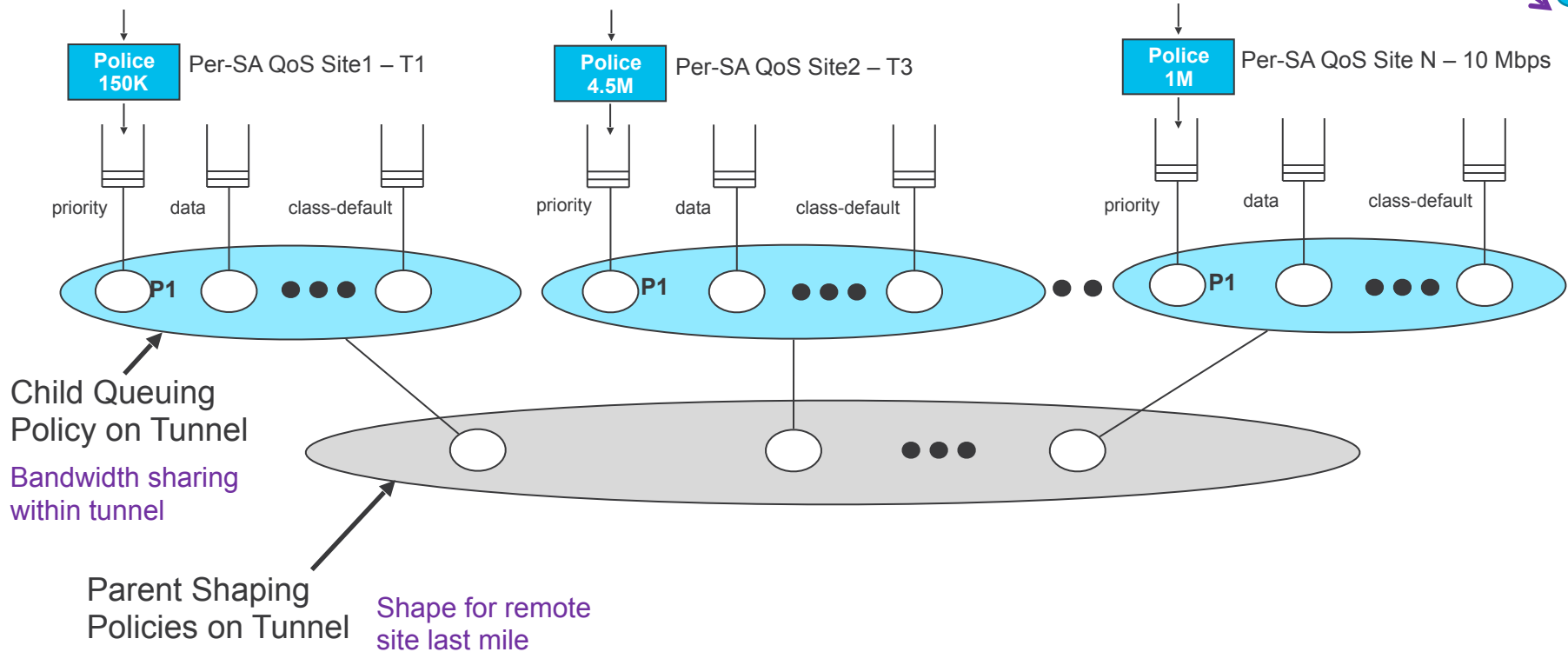


Child Queuing
Policy on Tunnel

Bandwidth sharing
within tunnel

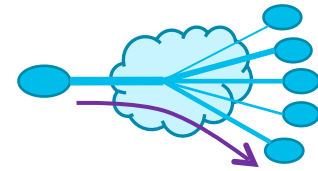
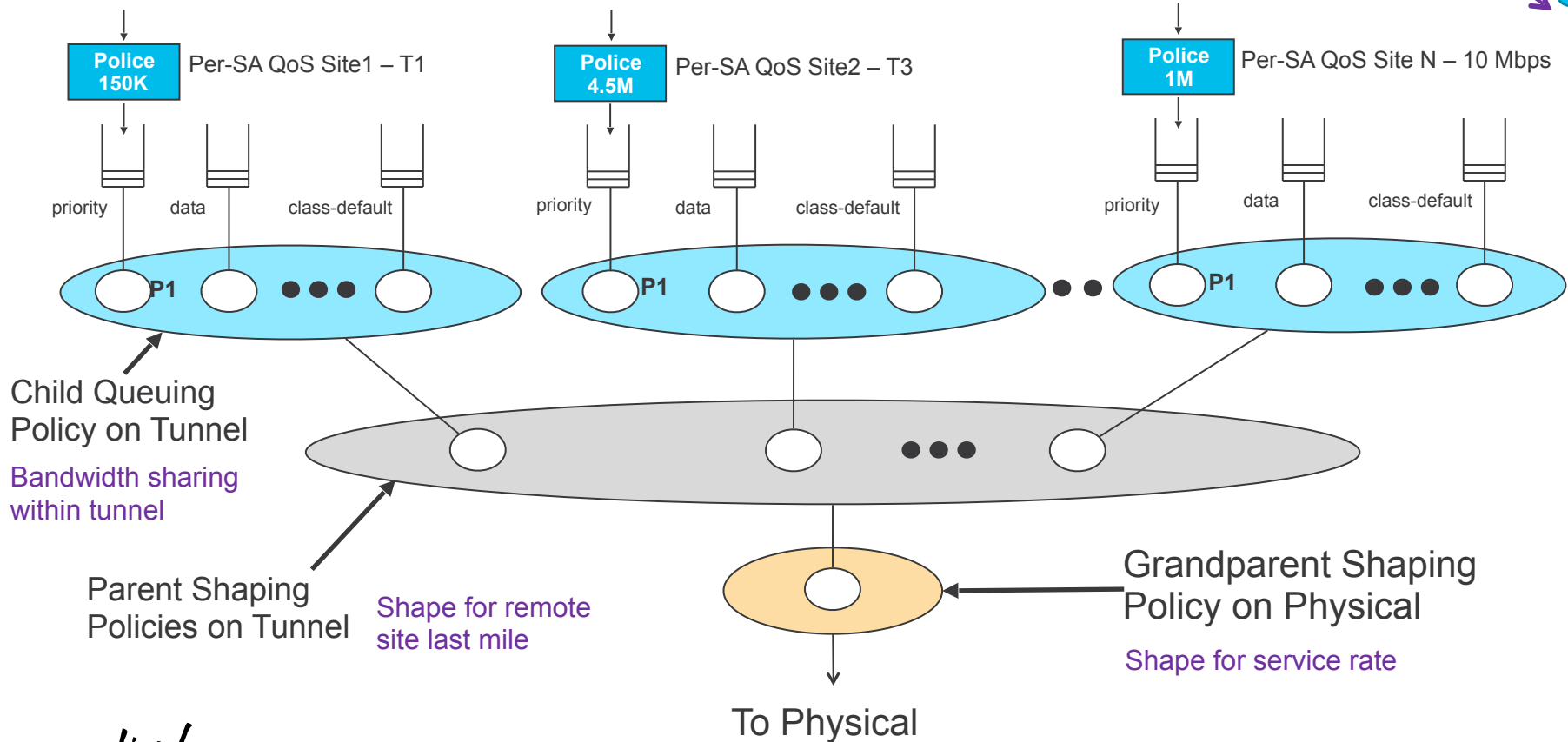
Hub Site QoS Scheduling Hierarchy

Three Levels: Child / Parent / Grandparent



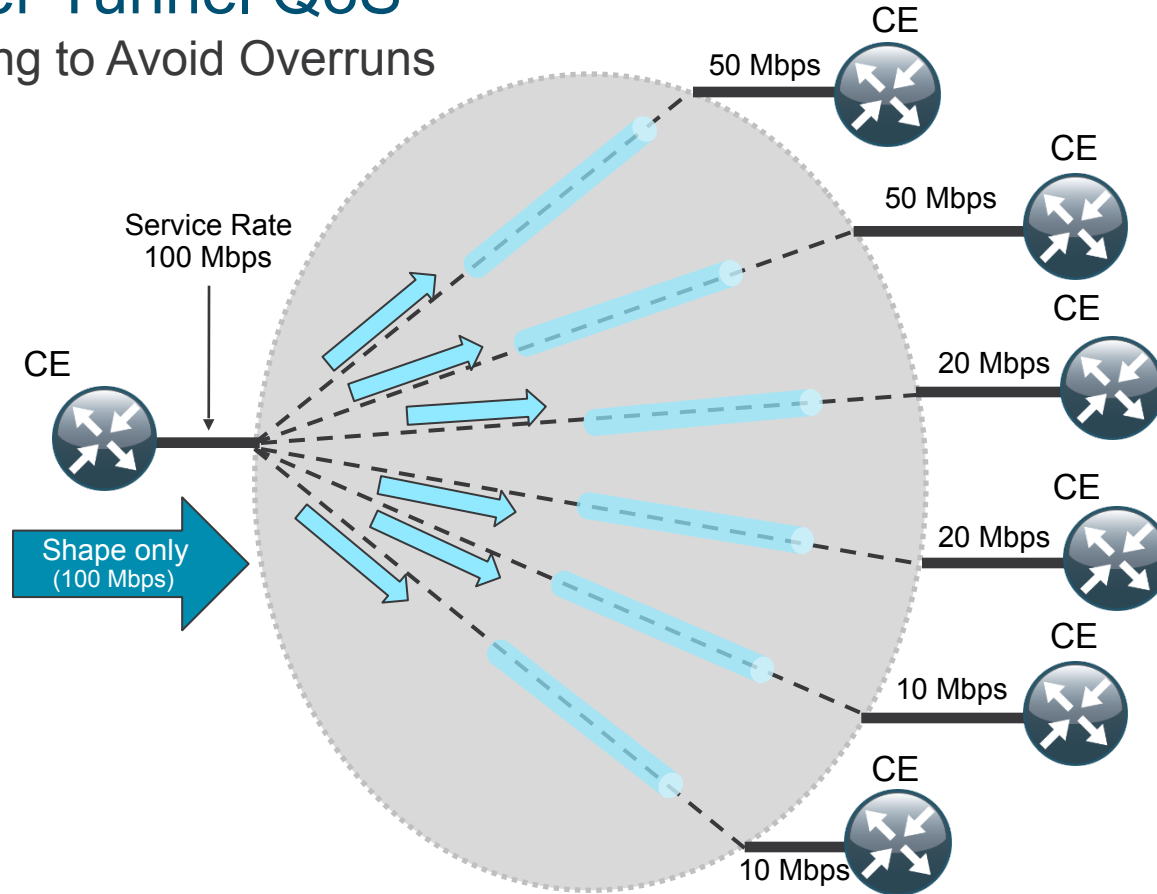
Hub Site QoS Scheduling Hierarchy

Three Levels: Child / Parent / Grandparent



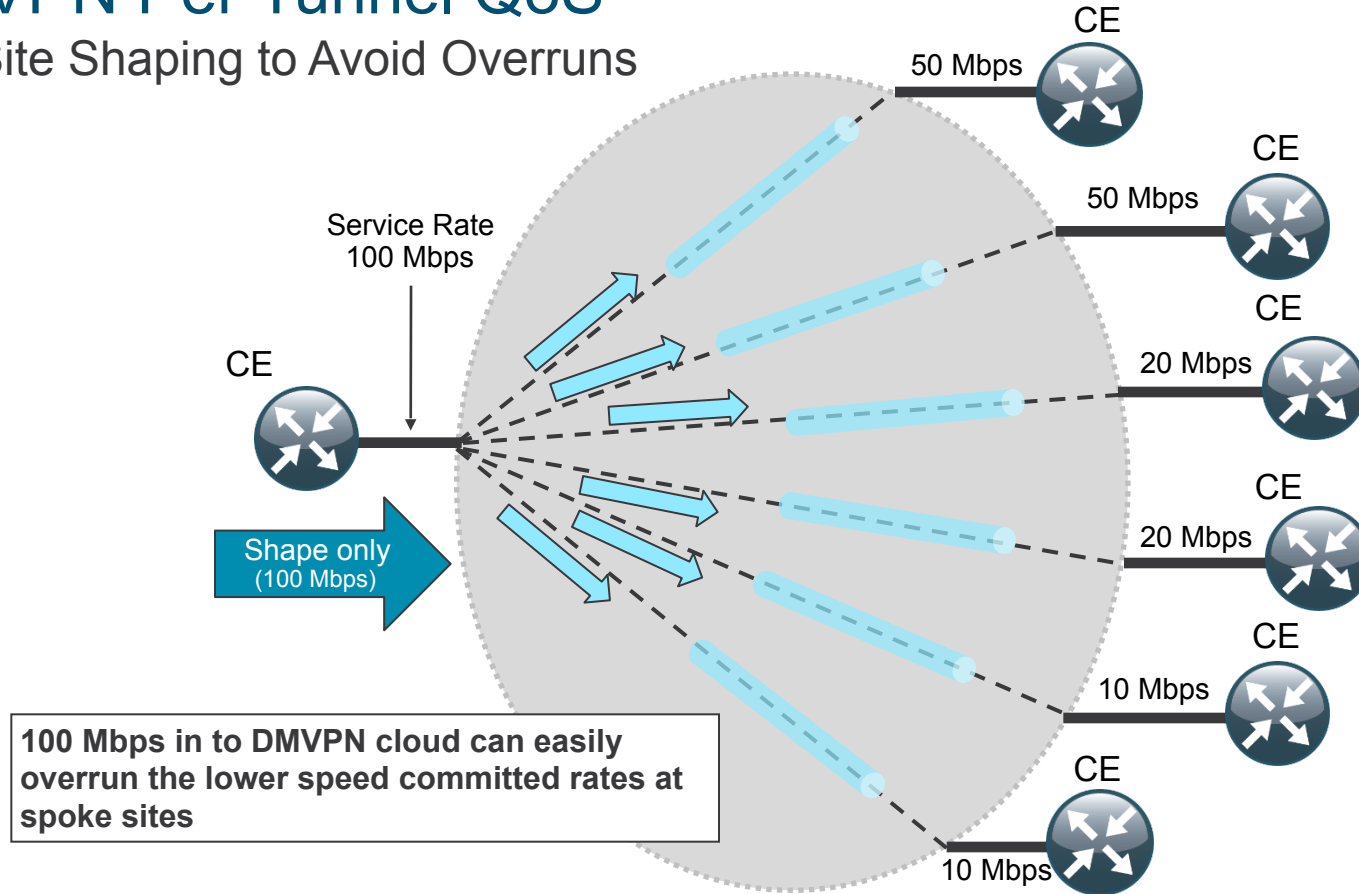
DMVPN Per Tunnel QoS

Per-Site Shaping to Avoid Overruns



DMVPN Per Tunnel QoS

Per-Site Shaping to Avoid Overruns



DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping

```
policy-map GROUP-50MBPS-POLICY
class class-default
  shape average 50 Mbps
  bandwidth remaining ratio 50
  service-policy IWAN-EDGE-QUEUING
```

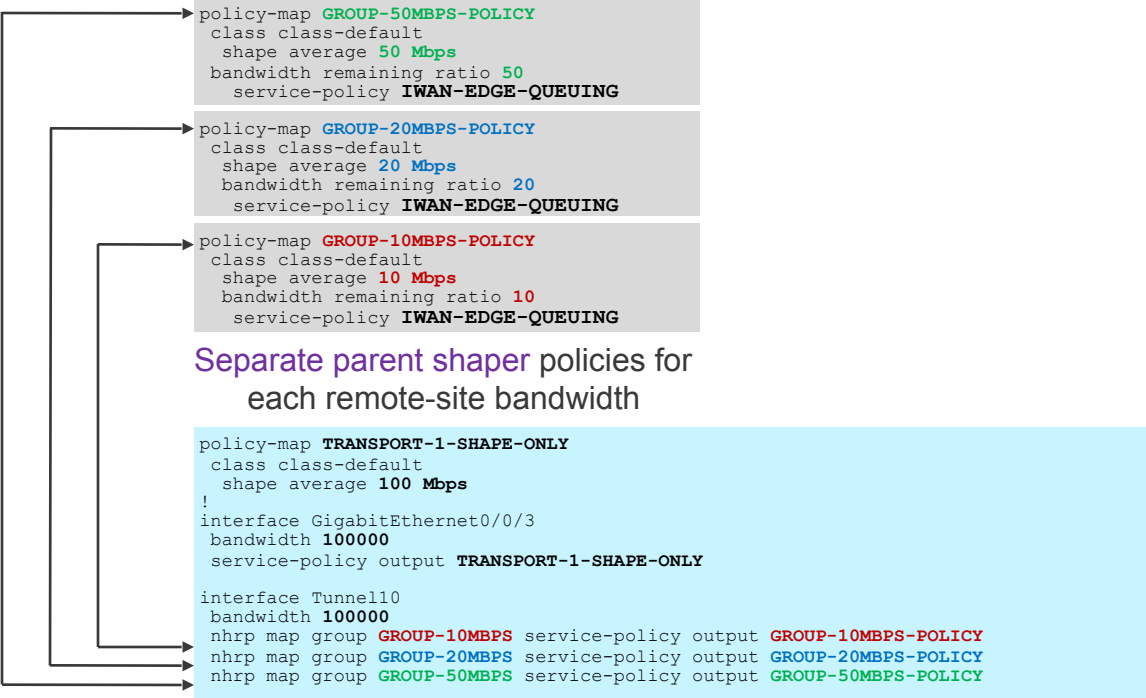
```
policy-map GROUP-20MBPS-POLICY
class class-default
  shape average 20 Mbps
  bandwidth remaining ratio 20
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy IWAN-EDGE-QUEUING
```

Separate parent shaper policies for
each remote-site bandwidth

DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping



```
policy-map GROUP-50MBPS-POLICY
class class-default
  shape average 50 Mbps
  bandwidth remaining ratio 50
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-20MBPS-POLICY
class class-default
  shape average 20 Mbps
  bandwidth remaining ratio 20
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy IWAN-EDGE-QUEUING
```

Separate parent shaper policies for each remote-site bandwidth

```
policy-map TRANSPORT-1-SHAPE-ONLY
class class-default
  shape average 100 Mbps
!
interface GigabitEthernet0/0/3
  bandwidth 100000
  service-policy output TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
  bandwidth 100000
  nhrp map group GROUP-10MBPS service-policy output GROUP-10MBPS-POLICY
  nhrp map group GROUP-20MBPS service-policy output GROUP-20MBPS-POLICY
  nhrp map group GROUP-50MBPS service-policy output GROUP-50MBPS-POLICY
```

List all available policies as **map groups** on hub tunnel interface

DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping

```
policy-map GROUP-50MBPS-POLICY
class class-default
  shape average 50 Mbps
  bandwidth remaining ratio 50
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-20MBPS-POLICY
class class-default
  shape average 20 Mbps
  bandwidth remaining ratio 20
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy IWAN-EDGE-QUEUING
```

Separate parent shaper policies for each remote-site bandwidth

```
policy-map TRANSPORT-1-SHAPE-ONLY
class class-default
  shape average 100 Mbps
!
interface GigabitEthernet0/0/3
  bandwidth 100000
  service-policy output TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
  bandwidth 100000
  nhrp map group GROUP-10MBPS service-policy output GROUP-10MBPS-POLICY
  nhrp map group GROUP-20MBPS service-policy output GROUP-20MBPS-POLICY
  nhrp map group GROUP-50MBPS service-policy output GROUP-50MBPS-POLICY
```

List all available policies as **map groups** on hub tunnel interface

Add a **class-default shape-only** policy on the hub physical interface for the service rate

DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping

```
policy-map GROUP-50MBPS-POLICY
class class-default
  shape average 50 Mbps
  bandwidth remaining ratio 50
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-20MBPS-POLICY
class class-default
  shape average 20 Mbps
  bandwidth remaining ratio 20
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy IWAN-EDGE-QUEUING
```

Bandwidth remaining
ratio provides
proportional sharing
between tunnels

Separate parent shaper policies for
each remote-site bandwidth

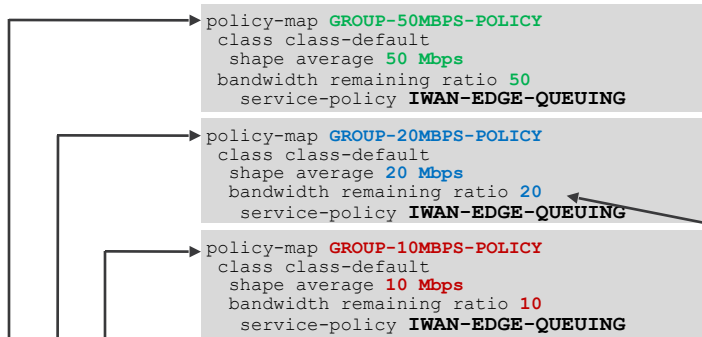
```
policy-map TRANSPORT-1-SHAPE-ONLY
class class-default
  shape average 100 Mbps
!
interface GigabitEthernet0/0/3
  bandwidth 100000
  service-policy output TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
  bandwidth 100000
  nhrp map group GROUP-10MBPS service-policy output GROUP-10MBPS-POLICY
  nhrp map group GROUP-20MBPS service-policy output GROUP-20MBPS-POLICY
  nhrp map group GROUP-50MBPS service-policy output GROUP-50MBPS-POLICY
```

List all available policies as **map groups** on hub tunnel interface
Add a **class-default shape-only** policy on the hub physical interface
for the service rate

DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping



Separate parent shaper policies for each remote-site bandwidth

```
policy-map TRANSPORT-1-SHAPE-ONLY
class class-default
  shape average 100 Mbps
!
interface GigabitEthernet0/0/3
  bandwidth 100000
  service-policy output TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
  bandwidth 100000
  nhrp map group GROUP-10MBPS service-policy output GROUP-10MBPS-POLICY
  nhrp map group GROUP-20MBPS service-policy output GROUP-20MBPS-POLICY
  nhrp map group GROUP-50MBPS service-policy output GROUP-50MBPS-POLICY
```

Signal from the spoke to the hub to use the correct policy for each remote site

Bandwidth remaining ratio provides proportional sharing between tunnels

10 Mbps spoke

20 Mbps spoke

50 Mbps spoke

Remote Site Tunnel Configurations

```
interface GigabitEthernet0/0
  bandwidth 100000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

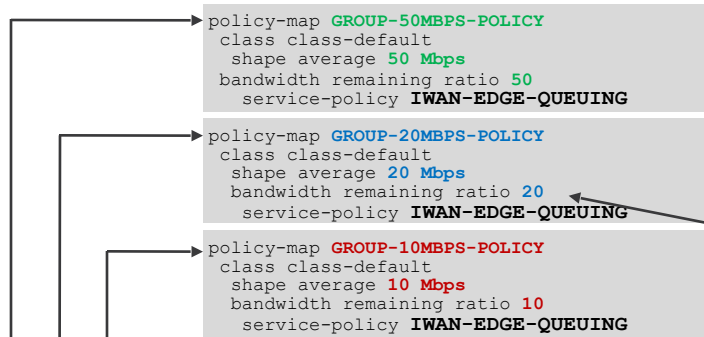
```
interface GigabitEthernet0/0
  bandwidth 20000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 20000
  nhrp group GROUP-20MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

```
interface GigabitEthernet0/0
  bandwidth 50000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 50000
  nhrp group GROUP-50MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

- List all available policies as **map groups** on hub tunnel interface
- Add a **class-default shape-only** policy on the hub physical interface for the service rate

DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping



Separate parent shaper policies for each remote-site bandwidth

```
policy-map TRANSPORT-1-SHAPE-ONLY
class class-default
  shape average 100 Mbps
!
interface GigabitEthernet0/0/3
  bandwidth 100000
  service-policy output TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
  bandwidth 100000
  nhrp map group GROUP-10MBPS service-policy output GROUP-10MBPS-POLICY
  nhrp map group GROUP-20MBPS service-policy output GROUP-20MBPS-POLICY
  nhrp map group GROUP-50MBPS service-policy output GROUP-50MBPS-POLICY
```

Signal from the spoke to the hub to use the correct policy for each remote site

Bandwidth remaining ratio provides proportional sharing between tunnels

10 Mbps spoke

20 Mbps spoke

50 Mbps spoke

Remote Site Tunnel Configurations

```
interface GigabitEthernet0/0
  bandwidth 100000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

```
interface GigabitEthernet0/0
  bandwidth 200000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 20000
  nhrp group GROUP-20MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

```
interface GigabitEthernet0/0
  bandwidth 500000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 50000
  nhrp group GROUP-50MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

- List all available policies as **map groups** on hub tunnel interface
- Add a **class-default shape-only** policy on the hub physical interface for the service rate

DMVPN Hub Per Tunnel QoS

Implementing Per-Site Traffic Shaping

```
policy-map GROUP-50MBPS-POLICY
class class-default
  shape average 50 Mbps
  bandwidth remaining ratio 50
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-20MBPS-POLICY
class class-default
  shape average 20 Mbps
  bandwidth remaining ratio 20
  service-policy IWAN-EDGE-QUEUING
```

```
policy-map GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy IWAN-EDGE-QUEUING
```

Separate parent shaper policies for each remote-site bandwidth

```
policy-map TRANSPORT-1-SHAPE-ONLY
class class-default
  shape average 100 Mbps
!
interface GigabitEthernet0/0/3
  bandwidth 100000
  service-policy output TRANSPORT-1-SHAPE-ONLY

interface Tunnel10
  bandwidth 100000
  nhrp map group GROUP-10MBPS service-policy output GROUP-10MBPS-POLICY
  nhrp map group GROUP-20MBPS service-policy output GROUP-20MBPS-POLICY
  nhrp map group GROUP-50MBPS service-policy output GROUP-50MBPS-POLICY
```

Signal from the spoke to the hub to use the correct policy for each remote site

Bandwidth remaining ratio provides proportional sharing between tunnels

10 Mbps spoke

20 Mbps spoke

50 Mbps spoke

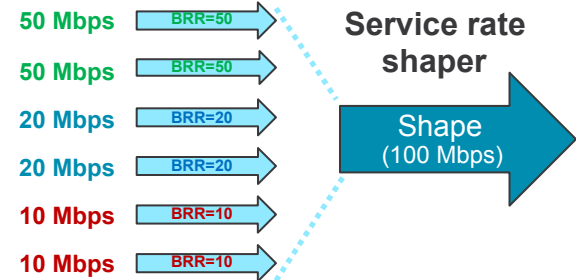
Remote Site Tunnel Configurations

```
interface GigabitEthernet0/0
  bandwidth 100000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

```
interface GigabitEthernet0/0
  bandwidth 20000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 20000
  nhrp group GROUP-20MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

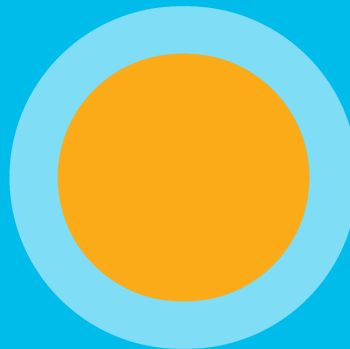
```
interface GigabitEthernet0/0
  bandwidth 50000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 50000
  nhrp group GROUP-50MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

Per-Tunnel shapers



List all available policies as **map groups** on hub tunnel interface
Add a **class-default shape-only** policy on the hub physical interface for the service rate

Enterprise to Service-Provider QoS Mapping



Enterprise to SP Mapping

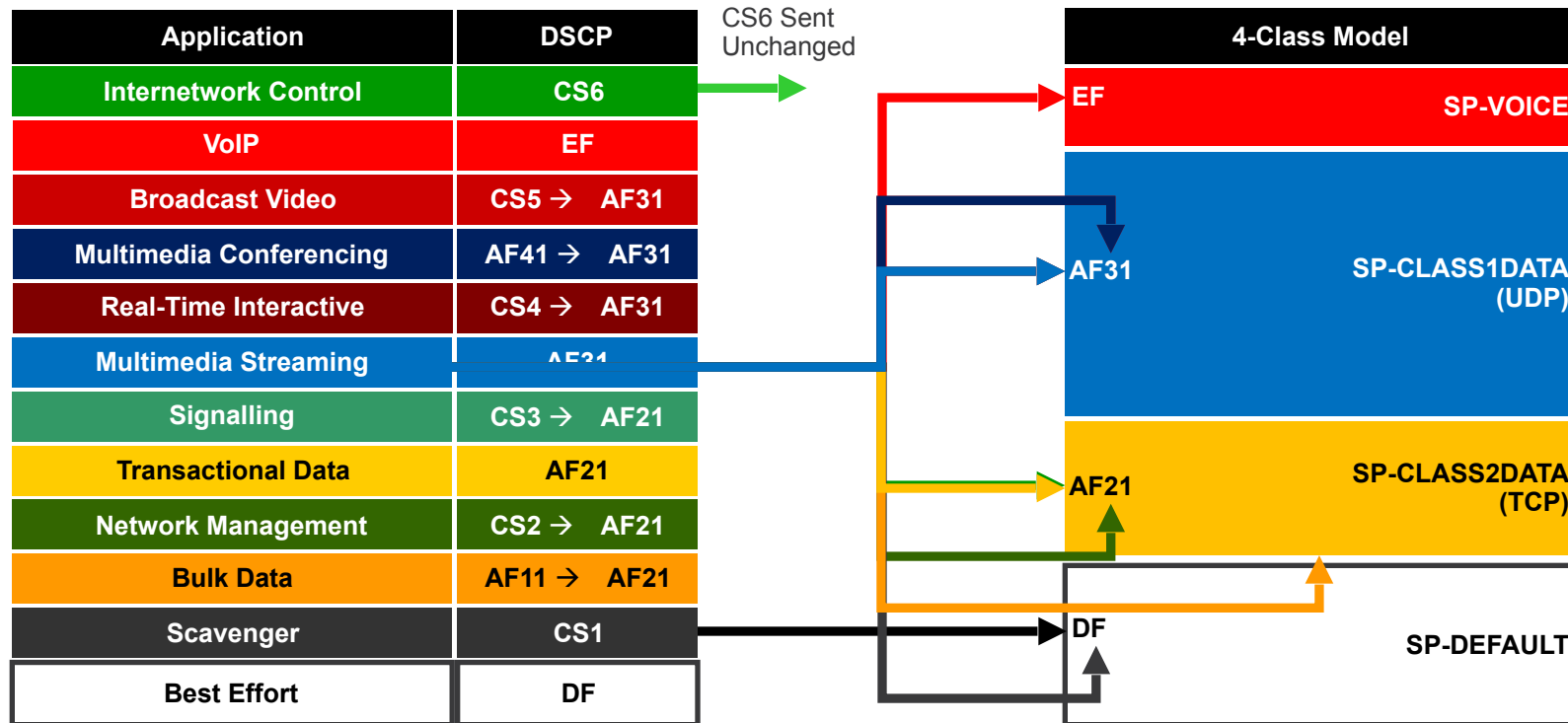
Example: 4-Class SP Model

Application	DSCP
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5 → AF31
Multimedia Conferencing	AF41 → AF31
Real-Time Interactive	CS4 → AF31
Multimedia Streaming	AF31
Signalling	CS3 → AF21
Transactional Data	AF21
Network Management	CS2 → AF21
Bulk Data	AF11 → AF21
Scavenger	CS1
Best Effort	DF

4-Class Model	
EF	SP-VOICE
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
DF	SP-DEFAULT

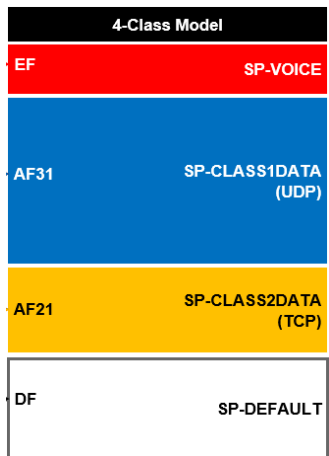
Enterprise to SP Mapping

Example: 4-Class SP Model



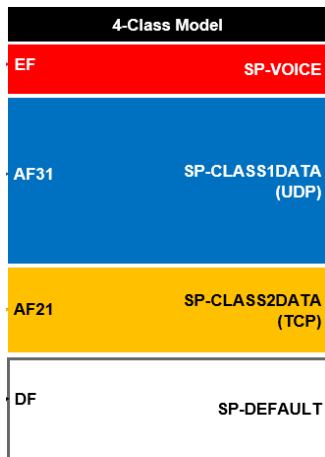
4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



4-Class SP QoS Model Configuration

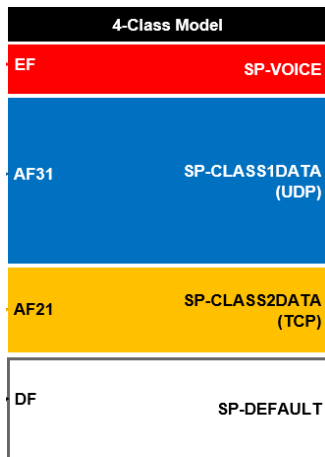
Tunnel Interface
IWAN Hub BR



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

4-Class SP QoS Model Configuration

Tunnel Interface *IWAN Hub BR*



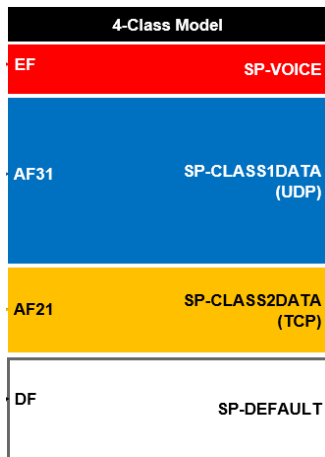
```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

Hub Router:

```
policy-map GROUP-10MBPS-POLICY
  class class-default
    shape average 10 Mbps
    bandwidth remaining ratio 10
    service-policy IWAN-EDGE-QUEUING
```

4-Class SP QoS Model Configuration

Tunnel Interface *IWAN Hub BR*



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

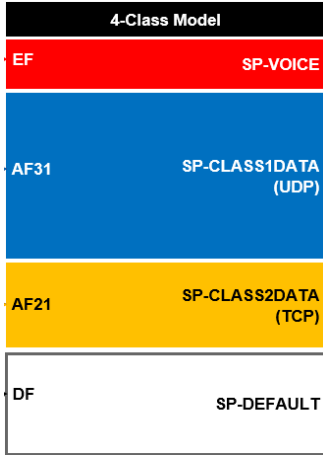
Hub Router:

```
policy-map GROUP-10MBPS-POLICY
  class class-default
    shape average 10 Mbps
    bandwidth remaining ratio 10
    service-policy IWAN-EDGE-QUEUING
```

```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group GROUP-10MBPS service-policy
  output GROUP-10MBPS-POLICY
```

4-Class SP QoS Model Configuration

Tunnel Interface *IWAN Hub BR*



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

Hub Router:

```
policy-map GROUP-10MBPS-POLICY
  class class-default
    shape average 10 Mbps
    bandwidth remaining ratio 10
    service-policy IWAN-EDGE-QUEUING
```

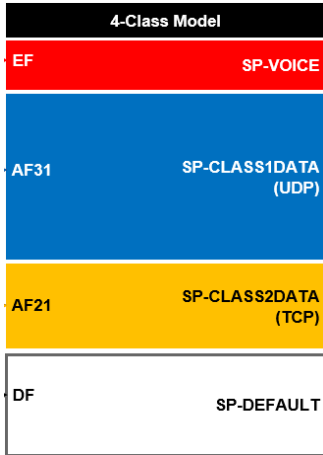
```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group GROUP-10MBPS service-policy
  output GROUP-10MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```


4-Class SP QoS Model Configuration

Tunnel Interface *IWAN Hub BR*



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

Hub Router:

```
policy-map GROUP-10MBPS-POLICY
  class class-default
    shape average 10 Mbps
    bandwidth remaining ratio 10
    service-policy IWAN-EDGE-QUEUING
```

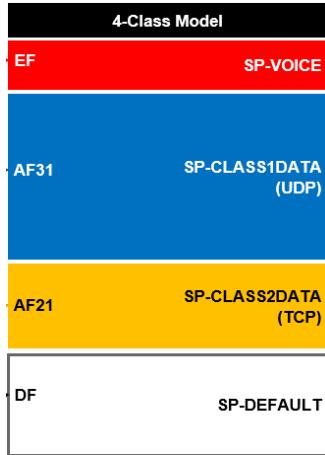
```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group GROUP-10MBPS service-policy
  output GROUP-10MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Tunnel Interface *IWAN Hub BR*



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

Hub Router:

```
policy-map GROUP-10MBPS-POLICY
  class class-default
    shape average 10 Mbps
    bandwidth remaining ratio 10
    service-policy IWAN-EDGE-QUEUING
```

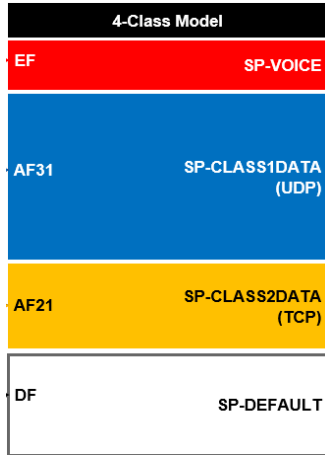
```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group GROUP-10MBPS service-policy
  output GROUP-10MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp tunnel default
```

Hub Router:

```
policy-map GROUP-10MBPS-POLICY
  class class-default
    shape average 10 Mbps
    bandwidth remaining ratio 10
    service-policy IWAN-EDGE-QUEUING
```

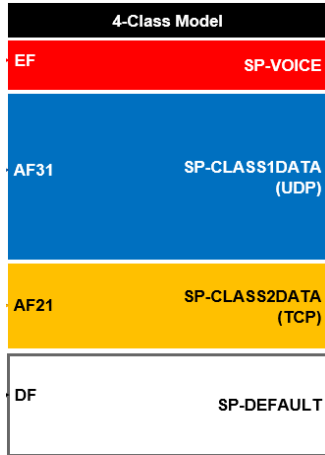
```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group GROUP-10MBPS service-policy
  output GROUP-10MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Tunnel Interface *IWAN Hub BR*



```
policy-map IWAN-EDGE-QUEUING
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
set dscp tunnel af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
set dscp tunnel af31
class NET-CTRL-MGMT
bandwidth remaining percent 5
set dscp tunnel cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dscp tunnel af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
set dscp tunnel af21
class SCAVENGER
bandwidth remaining percent 1
set dscp tunnel default
class VOICE
priority level 1
police cir percent 10
set dscp tunnel ef
class class-default
bandwidth remaining percent 25
random-detect
set dscp tunnel default
```

Hub Router:

```
policy-map GROUP-10MBPS-POLICY
class class-default
shape average 10 Mbps
bandwidth remaining ratio 10
service-policy IWAN-EDGE-QUEUING
```

```
interface Tunnel10
bandwidth <service-rate>
nhrp map group GROUP-10MBPS service-policy
output GROUP-10MBPS-POLICY
```

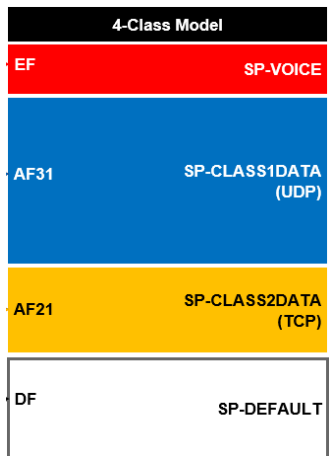
Branch Router:

```
interface GigabitEthernet0/0
bandwidth 10000
service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
bandwidth 10000
nhrp group GROUP-10MBPS
tunnel source GigabitEthernet0/0
tunnel vrf IWAN-TRANSPORT-1
```

4-Class SP QoS Model Configuration

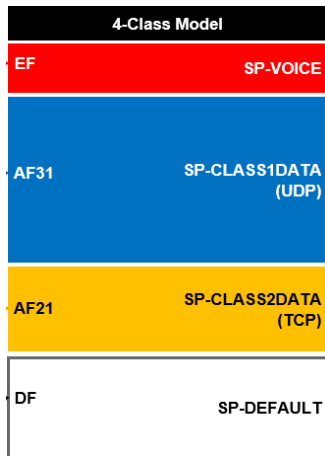
Physical Interface

IWAN Branch



4-Class SP QoS Model Configuration

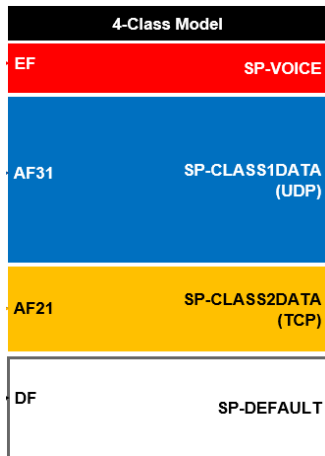
Physical Interface *IWAN Branch*



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp default
```

4-Class SP QoS Model Configuration

Physical Interface *IWAN Branch*



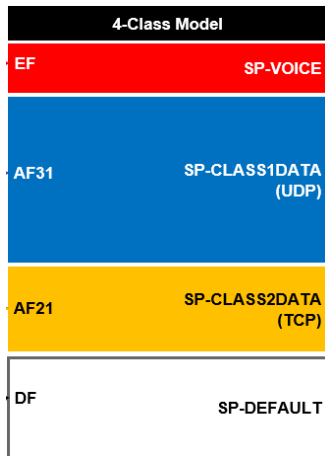
```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp default
```

Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN-EDGE-QUEUING
```

4-Class SP QoS Model Configuration

Physical Interface *IWAN Branch*



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp default
```

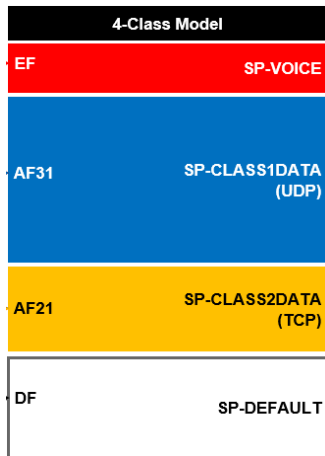
Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN-EDGE-QUEUING
```

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```


4-Class SP QoS Model Configuration

Physical Interface *IWAN Branch*



```
policy-map IWAN-EDGE-QUEUING
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    set dscp default
```

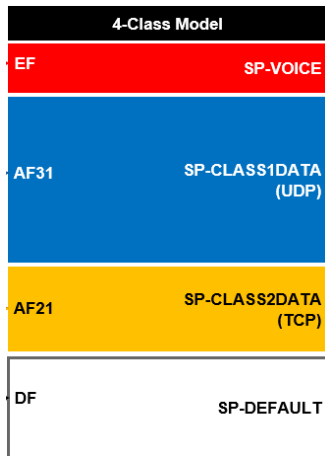
Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN-EDGE-QUEUING
```

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Physical Interface *IWAN Branch*



```
policy-map IWAN-EDGE-QUEUING
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
set dscp af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
set dscp af31
class NET-CTRL-MGMT
bandwidth remaining percent 5
set dscp cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dscp af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
set dscp af21
class SCAVENGER
bandwidth remaining percent 1
set dscp default
class VOICE
priority level 1
police cir percent 10
set dscp ef
class class-default
bandwidth remaining percent 25
random-detect
set dscp default
```

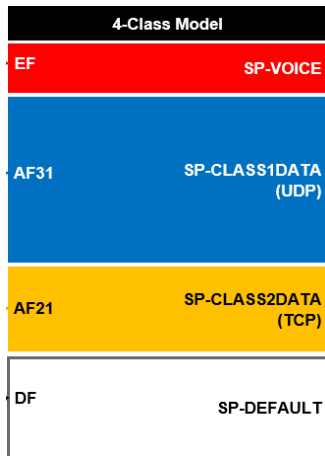
Branch Router:

```
policy-map POLICY-TRANSPORT-1
class class-default
shape average 10 Mbps
service-policy WAN-EDGE-QUEUING
```

```
interface GigabitEthernet0/0
bandwidth 10000
service-policy output POLICY-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Physical Interface *IWAN Branch*



```
policy-map IWAN-EDGE-QUEUING
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
set dscp af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
set dscp af31
class NET-CTRL-MGMT
bandwidth remaining percent 5
set dscp cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dscp af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
set dscp af21
class SCAVENGER
bandwidth remaining percent 1
set dscp default
class VOICE
priority level 1
police cir percent 10
set dscp ef
class class-default
bandwidth remaining percent 25
random-detect
set dscp default
```

Branch Router:

```
policy-map POLICY-TRANSPORT-1
class class-default
shape average 10 Mbps
service-policy WAN-EDGE-QUEUING
```

```
interface GigabitEthernet0/0
bandwidth 10000
service-policy output POLICY-TRANSPORT-1
```

WAN / IWAN QoS Design

Key Takeaways

IWAN Considerations Design Issues

Aggregate Priority Load
Latency for Low Speed
IPSec Anti-Replay

Ingress LAN Marking NBAR2 QoS Attributes

Traffic-Class
Business-Relevance

Egress WAN Queuing QoS and App Control

WAN Queuing
Sub-Line Rate Interfaces
DMVPN Per Tunnel QoS
Enterprise to SP Mapping

IWAN CVD:

<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Sep2017/CVD-IWANDeployment-SEP17.pdf>

IWAN QoS Design: At-A-Glance



Intelligent WAN QoS Design

At-A-Glance

Deploying Cisco IWAN QoS

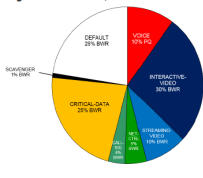
Quality of Service (QoS) has already proven itself as the enabling technology for the convergence of voice, video, and data networks. As business needs evolve, so do demands on QoS technologies. The need to protect voice, video, and critical data with QoS mechanisms is extremely important on the WAN because access speeds are much lower than the LAN networks that feed them.

When configuring WAN-edge QoS, you are defining how traffic egresses your network. It is critical that the classification, marking, and bandwidth allocations align to the service provider, offering to ensure consistent QoS treatment end to end.

Figure 1 shows a typical 8-class queuing model for a Cisco Intelligent WAN (IWAN) deployment. Voice traffic is put into a strict priority queue and the rest of the traffic is put into class-based weighted fair queues. The bandwidth/remaining percentages must equal 100%.

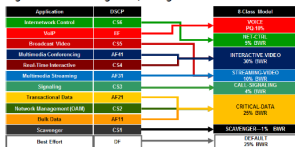
The values used below are a good starting point, but the final numbers should be based on an analysis of your traffic patterns over a period of time.

Figure 1 8-class QoS Model



The following table shows how to combine the twelve RFC 4594 traffic classes into an 8-class model for egress queuing. Combine the 12-class into a smaller number of queues is recommended for IWAN when bandwidth service rates are less than 100 Mbps.

Figure 2 8-class Egress Queuing Model

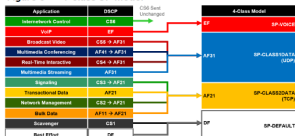


The 12-class view should always be preserved across the Enterprise even though we treat it differently at the egress of the router and send it to different channels in the service provider network.

The twelve classes remain intact on the inner header and the outer tunnel header is remarked as the traffic leaves the tunnel interface. The remarked outer header is discarded after arriving at the tunnel interface on the receiving router, thus leaving the inner header marking unchanged.

The following table shows how to combine the twelve classes into a typical 4-class SP model.

Figure 3 4-class SP Model

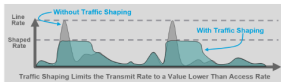


When the access rate of an interface is different from the service rate, traffic shapers are used to limit the transmit rate. A shaper will guarantee that traffic will not exceed the contracted rate. A nested queuing policy will force queuing to engage on the contracted sub-line rate to prioritize packets prior to shaping.

Policers typically drop traffic, but traffic shapers delay excess traffic, smoothing bursts and preventing unnecessary drops.

Shapers are very common with Ethernet WAN as well as Non-Broadcast Multiple-Access (NBMA) network topologies such as Frame-Relay and ATM.

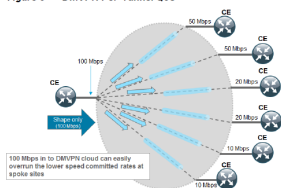
Figure 4 Traffic Shaping



The Per-Tunnel QoS for DMVPN feature allows the configuration of a QoS policy on a DMVPN hub on a per-tunnel basis. The QoS policy on a tunnel instance allows you to shape the tunnel traffic to individual spokes (parent policy) and to differentiate between traffic classes within the tunnel for appropriate treatment (child policy).

Traffic is regulated from the central site (hub) routers to the remote-site routers on a per-tunnel (spoke) basis. The hub site is unable to send more traffic than a single remote-site can handle, and this ensures that high bandwidth hub sites do not overrun lower bandwidth remote-sites.

Figure 5 DMVPN Per-Tunnel QoS



Intelligent WAN QoS Design

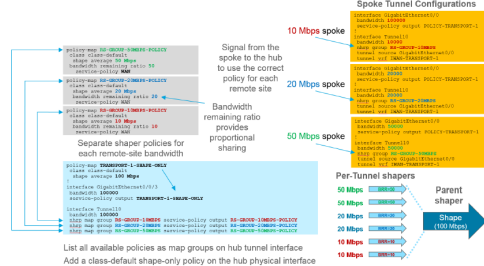
Implementing 8-class Egress Queuing and 4-class SP Mapping

- On all routers, create the 8-class QoS queuing model using class-map with match dspc to combine the twelve classes.
- On the hub border routers, create the 4-class SP mapping using set dspc tunnel.
- On the remote site routers, create the 4-class SP mapping using set dspc.

Class-map for 8-class QoS Model

```
class-map match-any VOICE
match dspc ef
class-map match-any INTERACTIVE-VIDEO
match dspc cs4 af41 af42 af43
class-map match-any STREAMING-VIDEO
match dspc cs5 af31 af32 af33
class-map match-any NET-CTRL
match dspc cs6
class-map match-any CALL-SIGNALING
match dspc cs3
class-map match-any CRITICAL-DATA
match dspc cs2 af11 af12 af13 af21 af22 af23
class-map match-any SCAVENGER
match dspc cs1
```

Implementing Per-Tunnel Traffic Shaping



Hub Border Router: Policy-map for 4-class service provider offering

```
policy-map WAN
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dspc-based
set dspc tunnel af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dspc-based
set dspc tunnel af31
class NET-CTRL
bandwidth remaining percent 5
set dspc tunnel cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dspc tunnel af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dspc-based
set dspc tunnel af21
class SCAVENGER
bandwidth remaining percent 1
set dspc tunnel default
class VOICE
priority level 1
police cir percent 10
set dspc tunnel of
class class-default
bandwidth remaining percent 25
random-detect
set dspc tunnel default
```

Remote Site Router: Policy-map for 4-class service provider offering

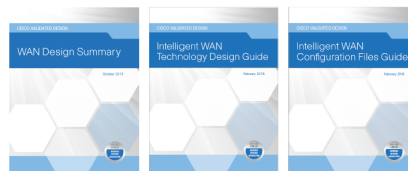
```
policy-map WAN
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dspc-based
set dspc af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dspc-based
set dspc af31
class NET-CTRL
bandwidth remaining percent 5
set dspc cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dspc af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dspc-based
set dspc af21
class SCAVENGER
bandwidth remaining percent 1
set dspc default
class VOICE
priority level 1
police cir percent 10
set dspc of
class class-default
bandwidth remaining percent 25
random-detect
set dspc tunnel default
```

- On the hub border router, create the child shaper policies for each remote site bandwidth type using the policy-map for the service provider.
- List the available policies as nhp map groups on the hub tunnel interfaces.
- Create a "shape only" parent policy and apply it on the hub outbound physical interface.
- On the remote site router, signal from the spoke to the hub using the nhp group command specifying the correct bandwidth policy. This creates a per-tunnel shaper for each remote site on the hub border router.

You can find more details about configuring QoS for IWAN in the IWAN Technical Design Guide. The full routers configurations used in the CVD Lab can be found in the IWAN Configurations Files Guide.

Cisco Validated Design (CVD)

Branch WAN: <http://www.cisco.com/go/cvd/wan>



Copyright © 2016 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

<https://cisco.box.com/v/QoS-AAGs>

Agenda

- Introduction to Strategic QoS Design
- WAN / IWAN QoS Design
- **Campus QoS Design**
- WLAN QoS Design
- Automating and Assuring QoS
- Summary and References
- Appendices

Campus QoS Design

The Case for Campus QoS

The Case for Campus QoS

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

Why Is Video So Sensitive to Packet Loss?



1080p60

1080 x 1920 lines =

2,073,600 pixels per frame

x 24 bits of colour per pixel

x 60 frames per second

= 2,985,984,000 bps

or 3 Gbps Uncompressed!

Cisco (H.264/H.265) codecs transmit 3-5 Mbps per 1080p60 video stream
which represents over **99.8%** compression (~ 1000:1)

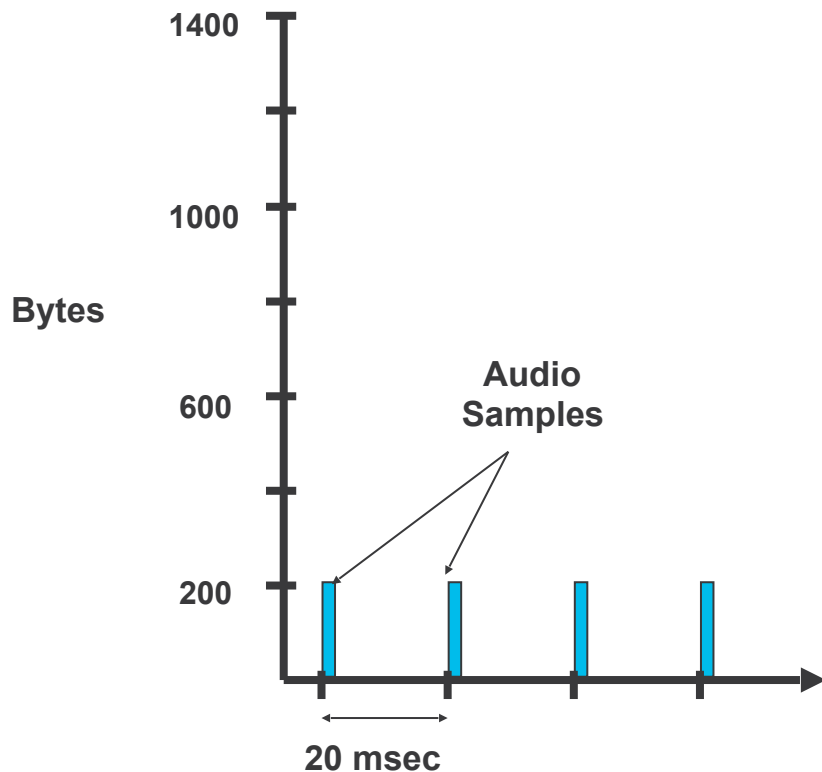
Packet loss is proportionally magnified by compression ratios

Users can notice a single packet lost in 10,000—

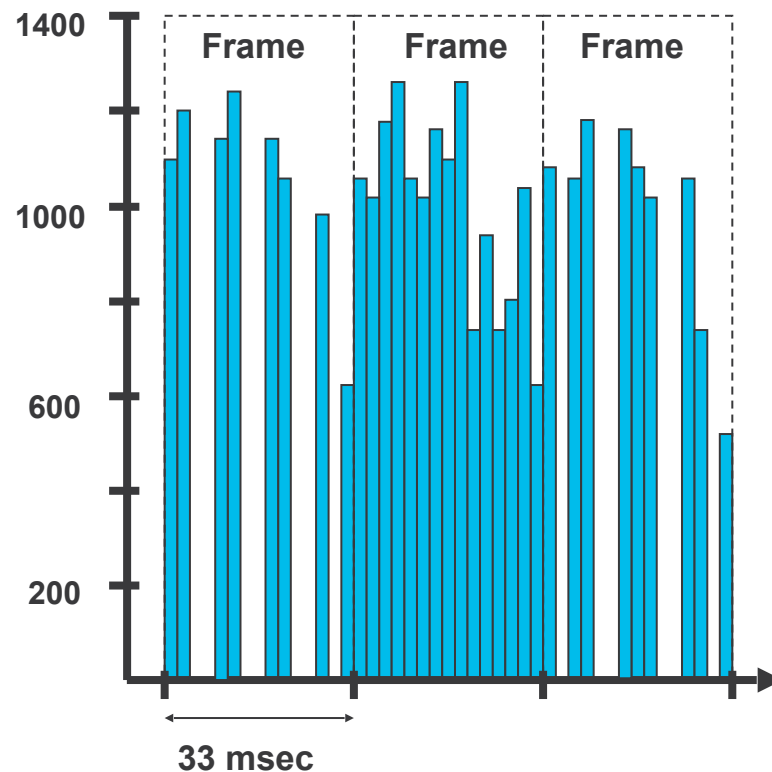
Making HD Video **One Hundred Times More Sensitive to Packet Loss than VoIP!**

VoIP vs. HD Video—At the Packet Level

Voice Packets

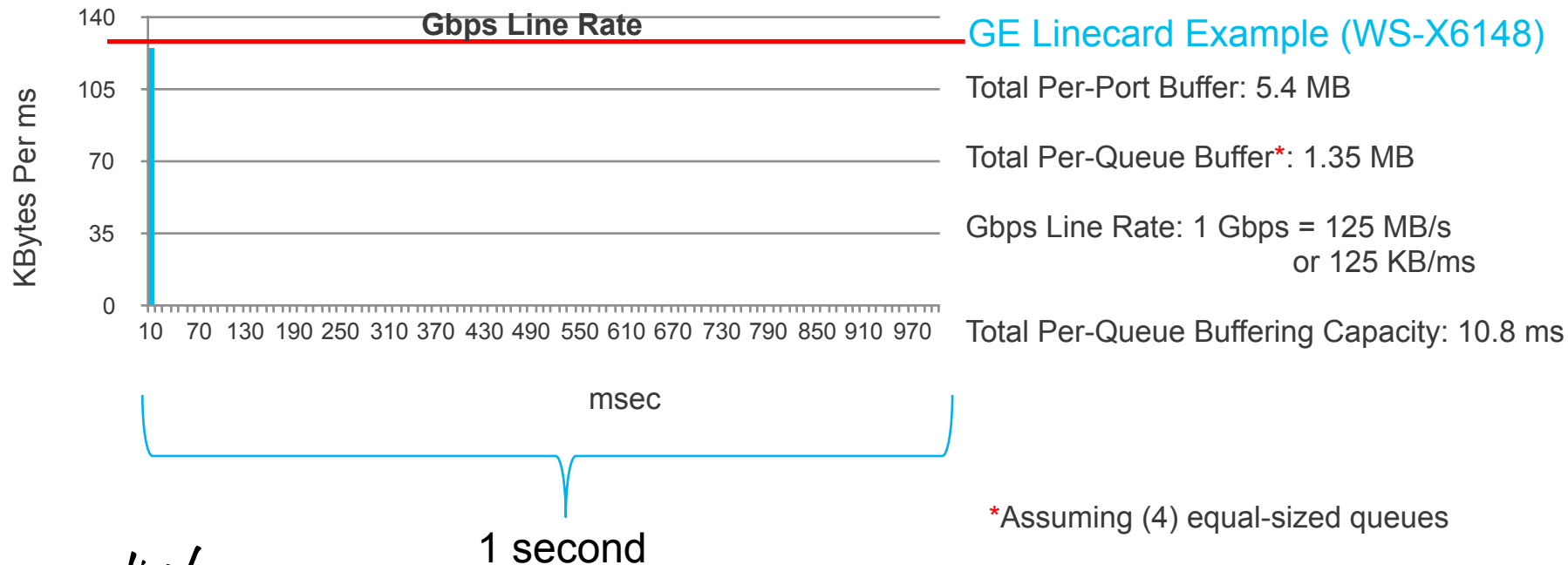


Video Packets



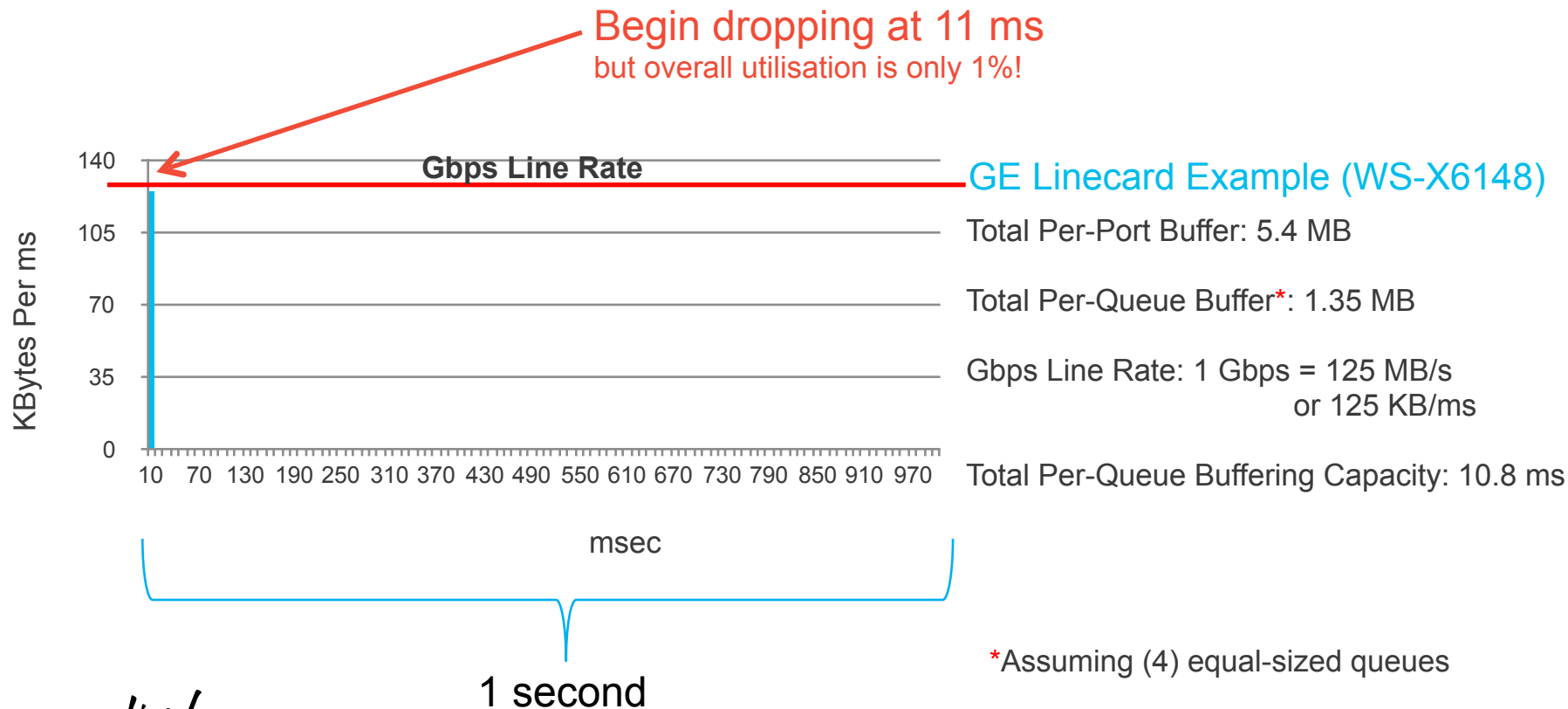
Campus QoS Design Considerations

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



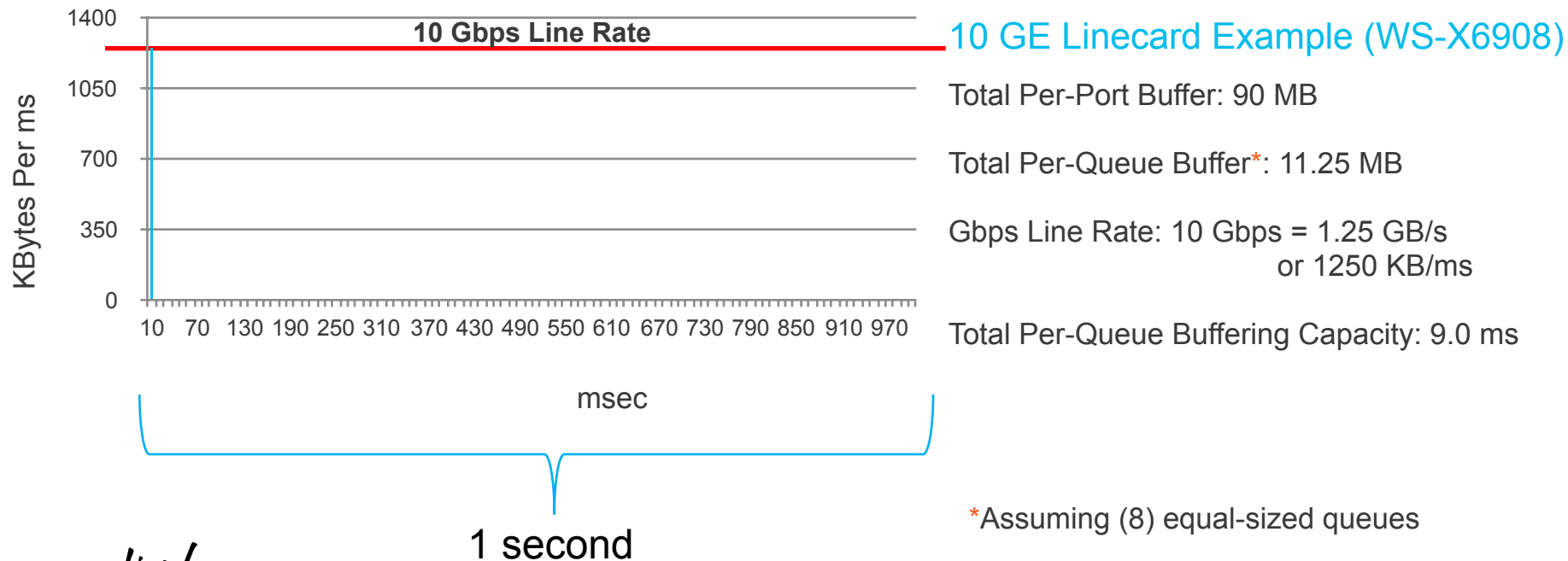
Campus QoS Design Considerations

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



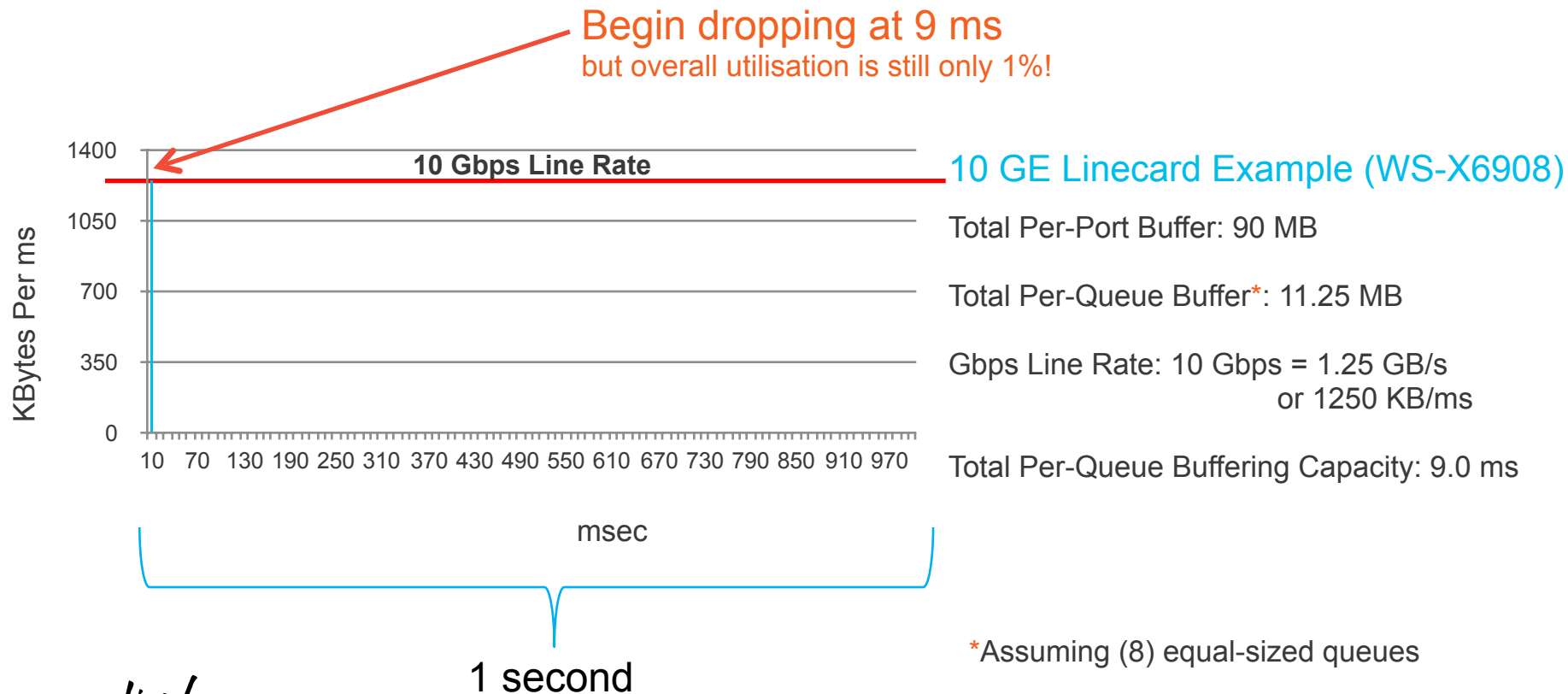
Campus QoS Design Considerations

How Long Can Queue-Buffers Accommodate Line-Rate Bursts

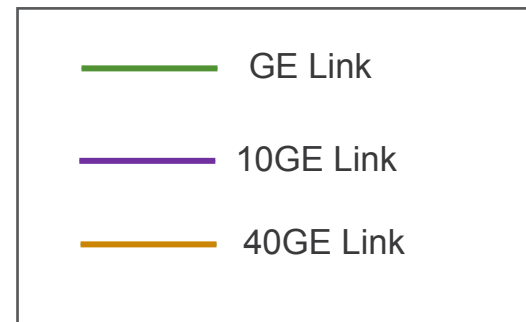


Campus QoS Design Considerations

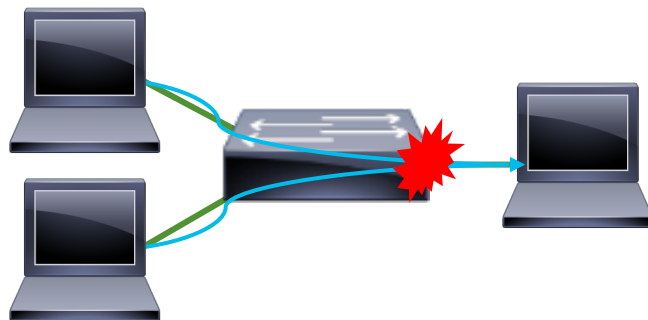
How Long Can Queue-Buffers Accommodate Line-Rate Bursts



Congestion at the Access Layer of the Campus

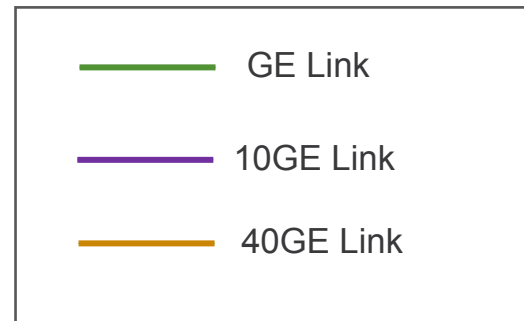


Congestion at the Access Layer of the Campus

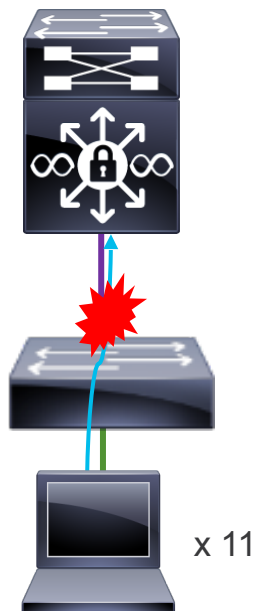
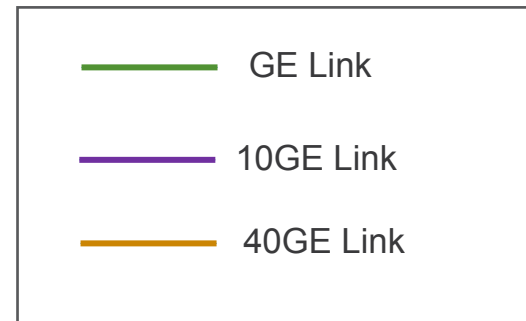


- GE Link
- 10GE Link
- 40GE Link

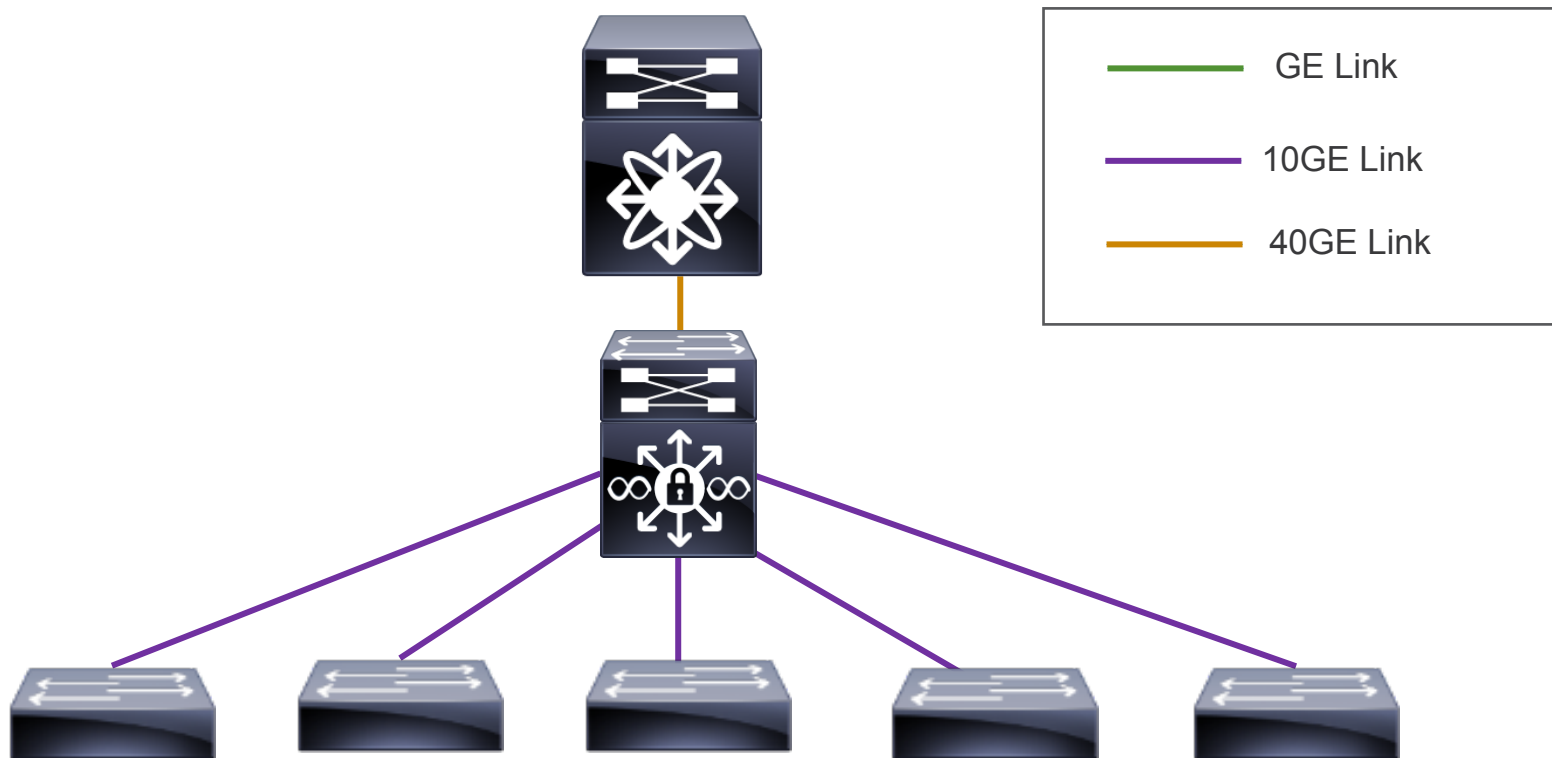
Congestion at the Access Layer of the Campus



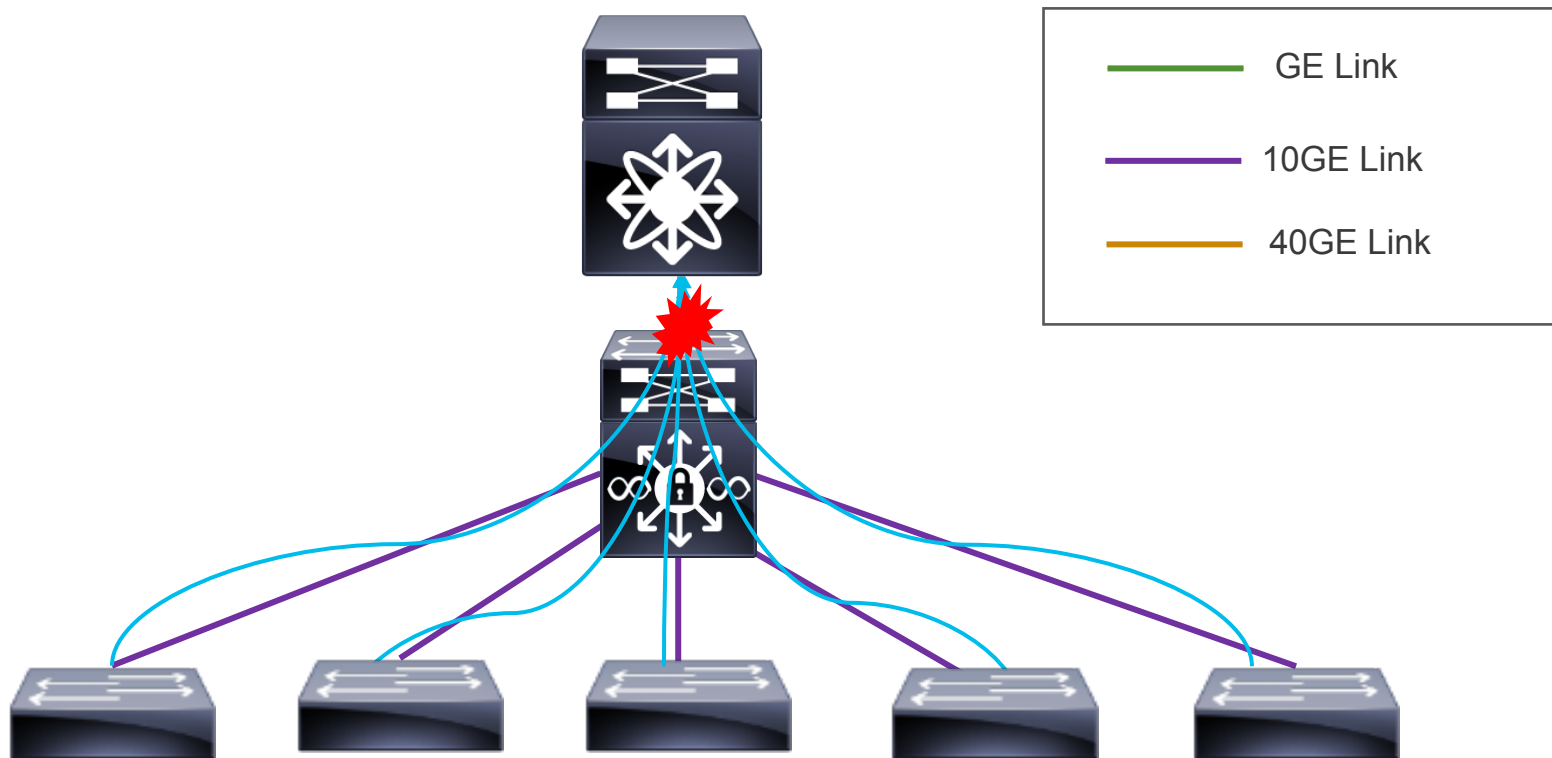
Congestion at the Access Layer of the Campus



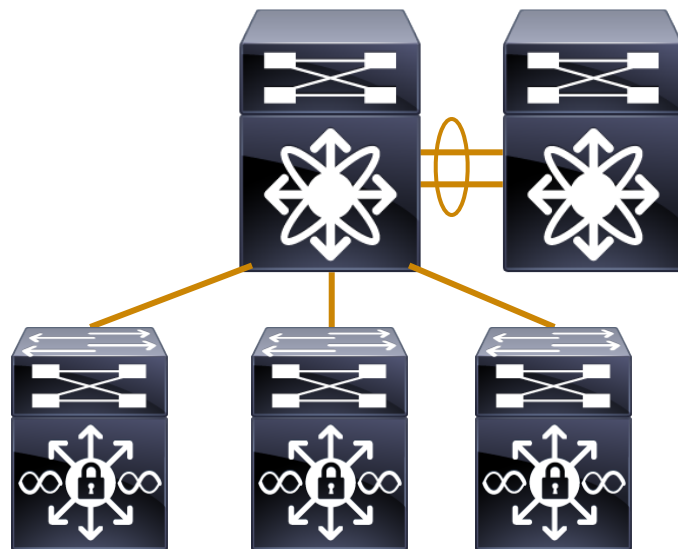
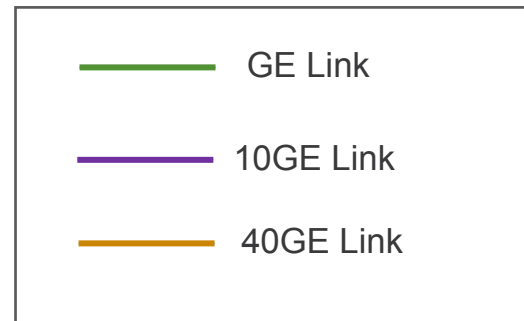
Congestion at the Distribution Layer of the Campus



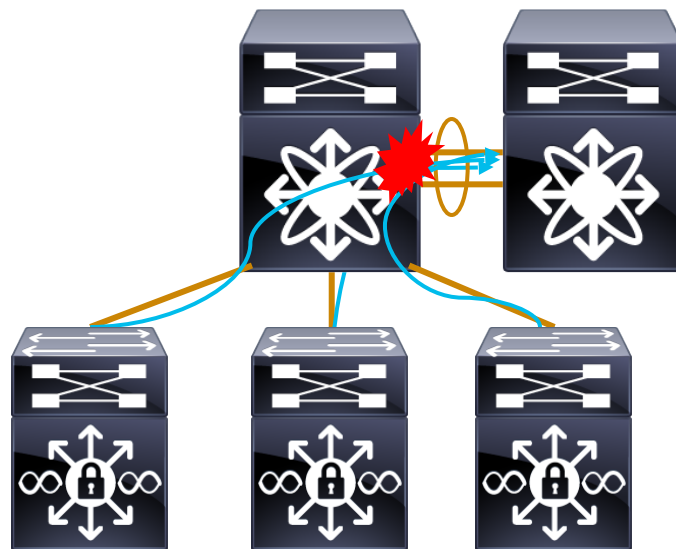
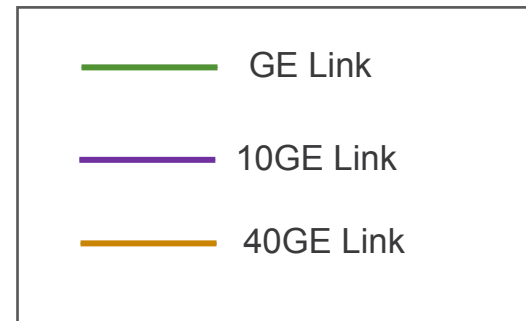
Congestion at the Distribution Layer of the Campus



Congestion at the Core Layer of the Campus



Congestion at the Core Layer of the Campus



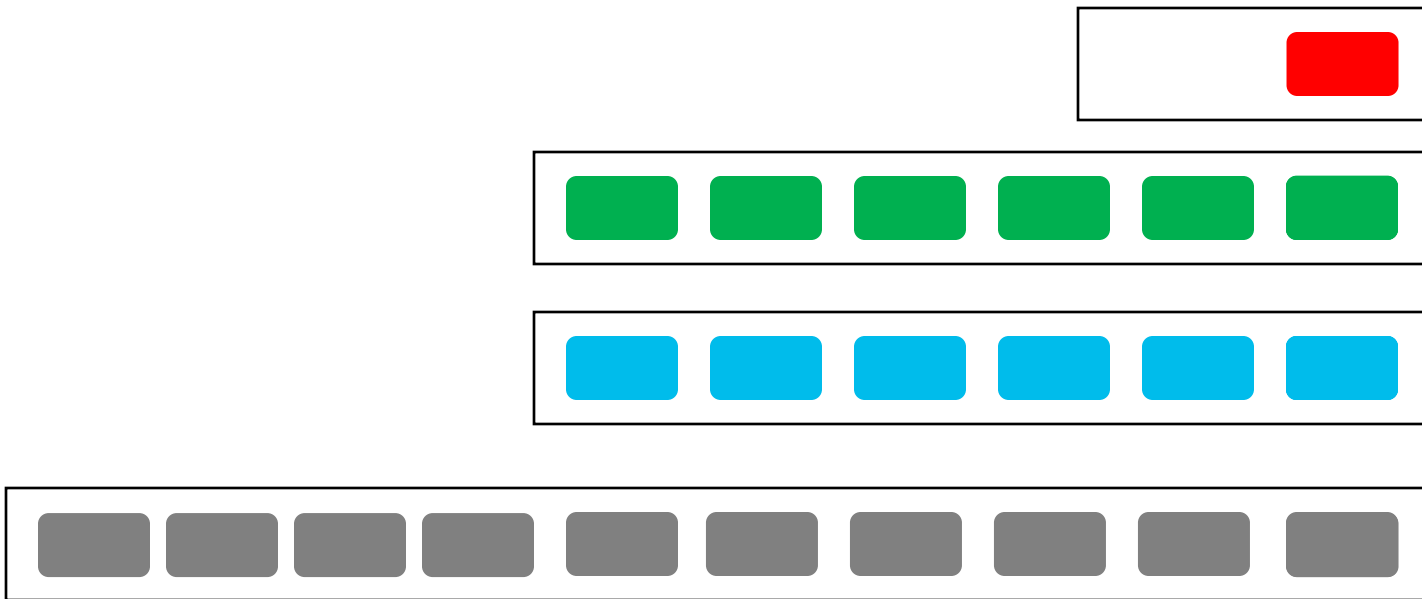
Know Your Tools

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



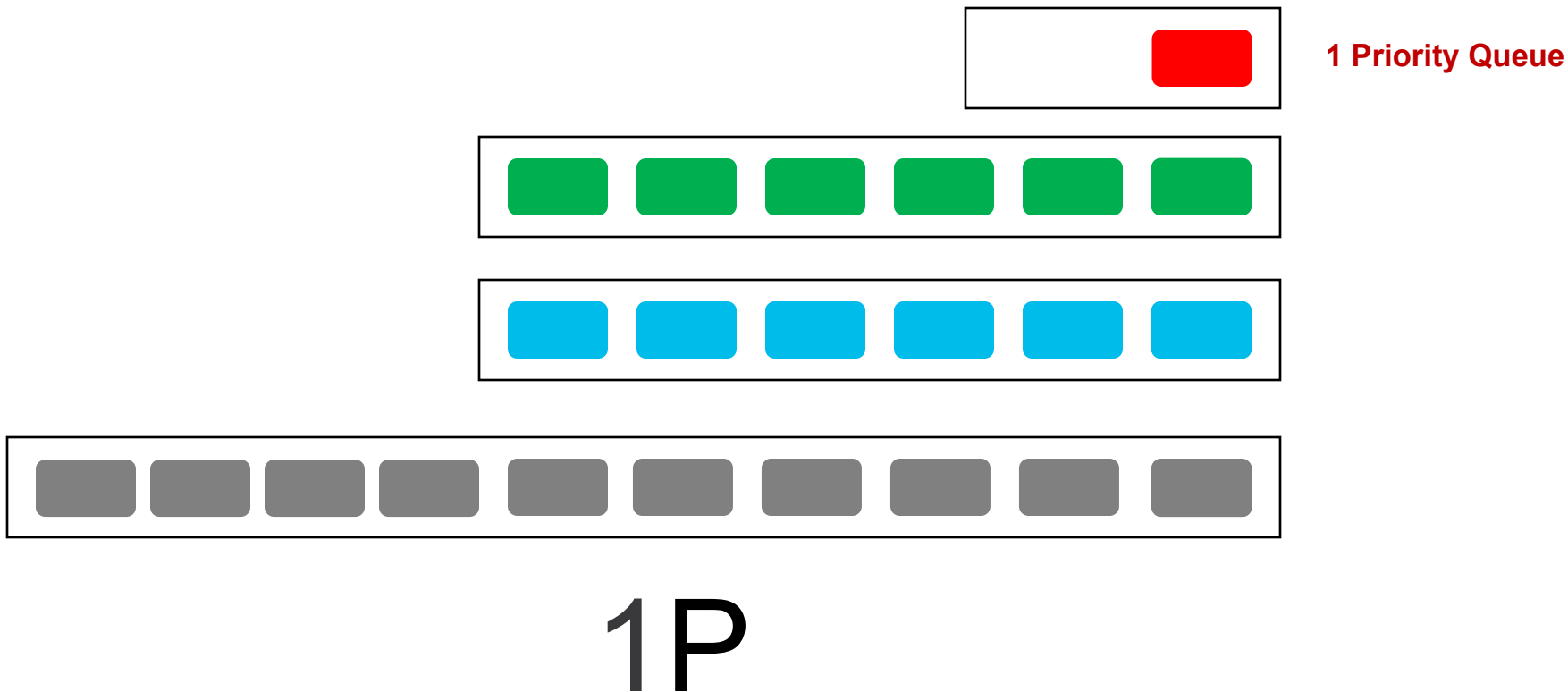
Catalyst Hardware Queuing

1P3Q1T Example



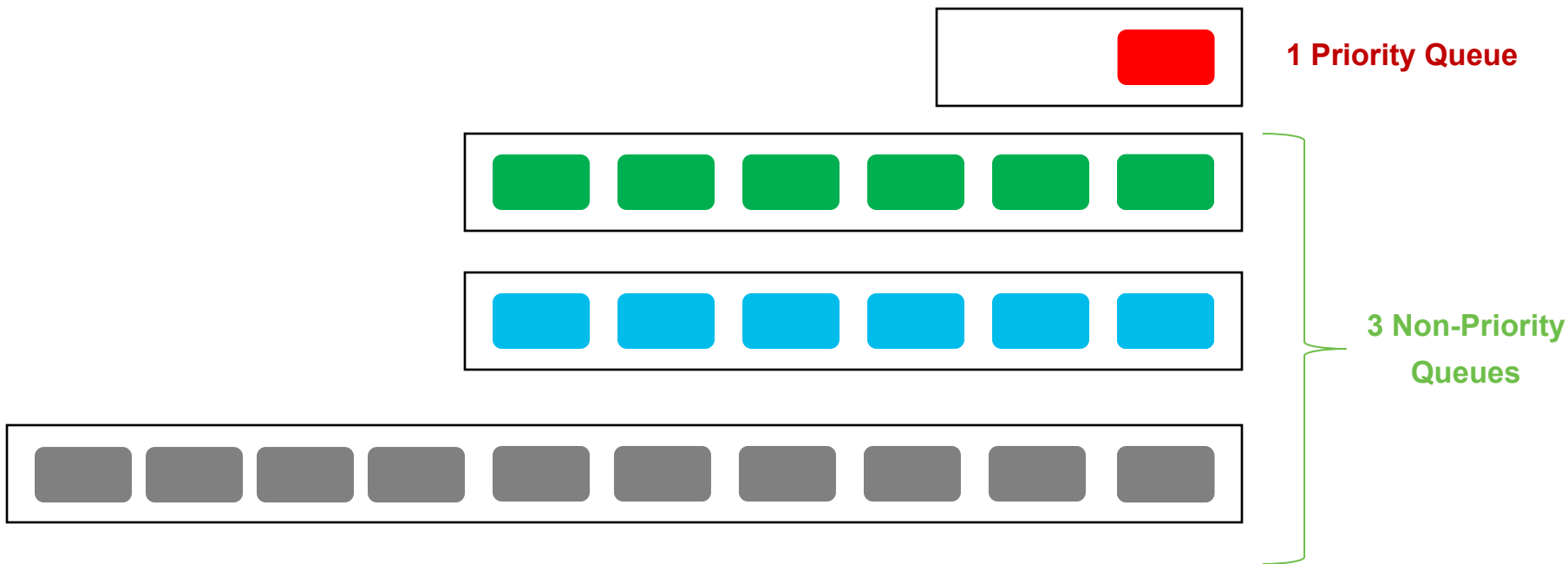
Catalyst Hardware Queuing

1P3Q1T Example



Catalyst Hardware Queuing

1P3Q1T Example

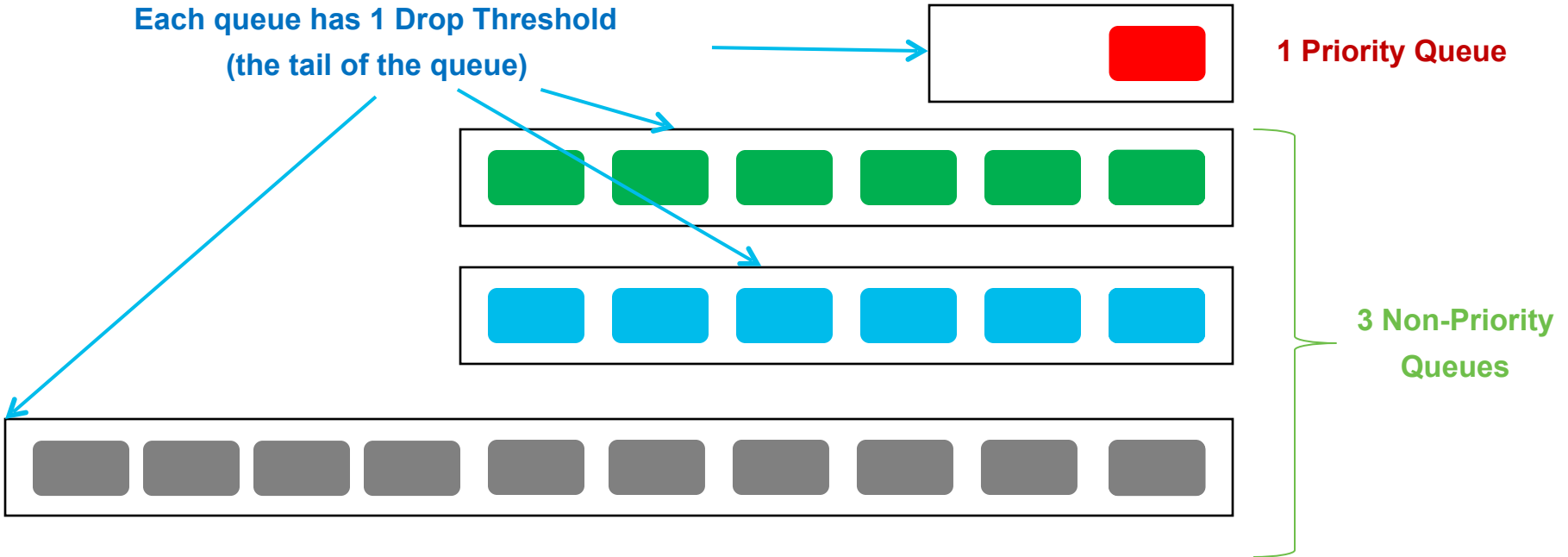


1P3Q

Catalyst Hardware Queuing

1P3Q1T Example

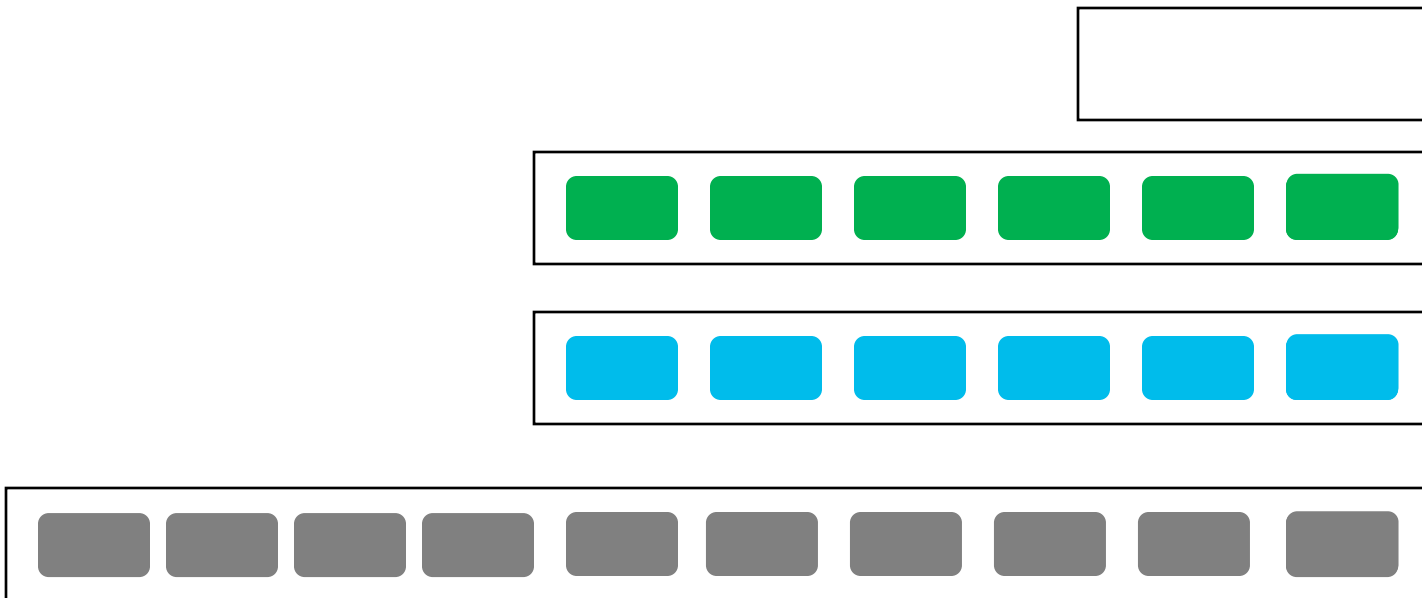
Each queue has 1 Drop Threshold
(the tail of the queue)



1P3Q 1T

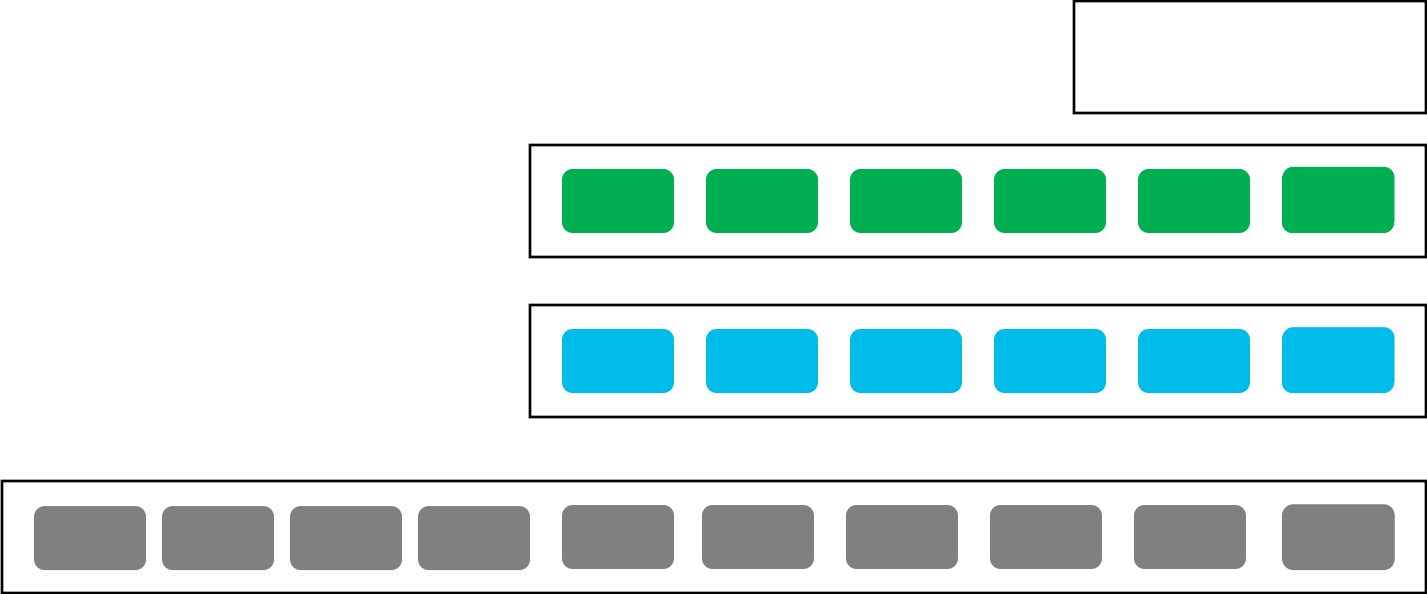
Catalyst Hardware Queuing

1P3Q1T Example



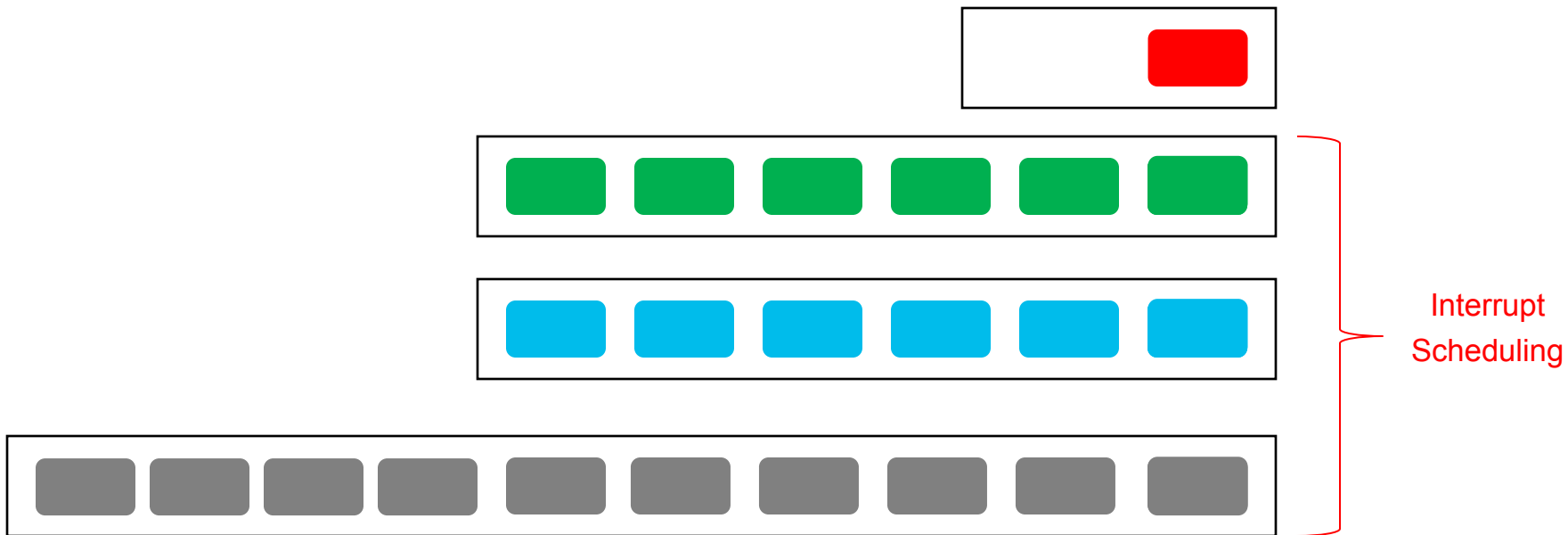
Catalyst Hardware Queuing

1P3Q1T Example



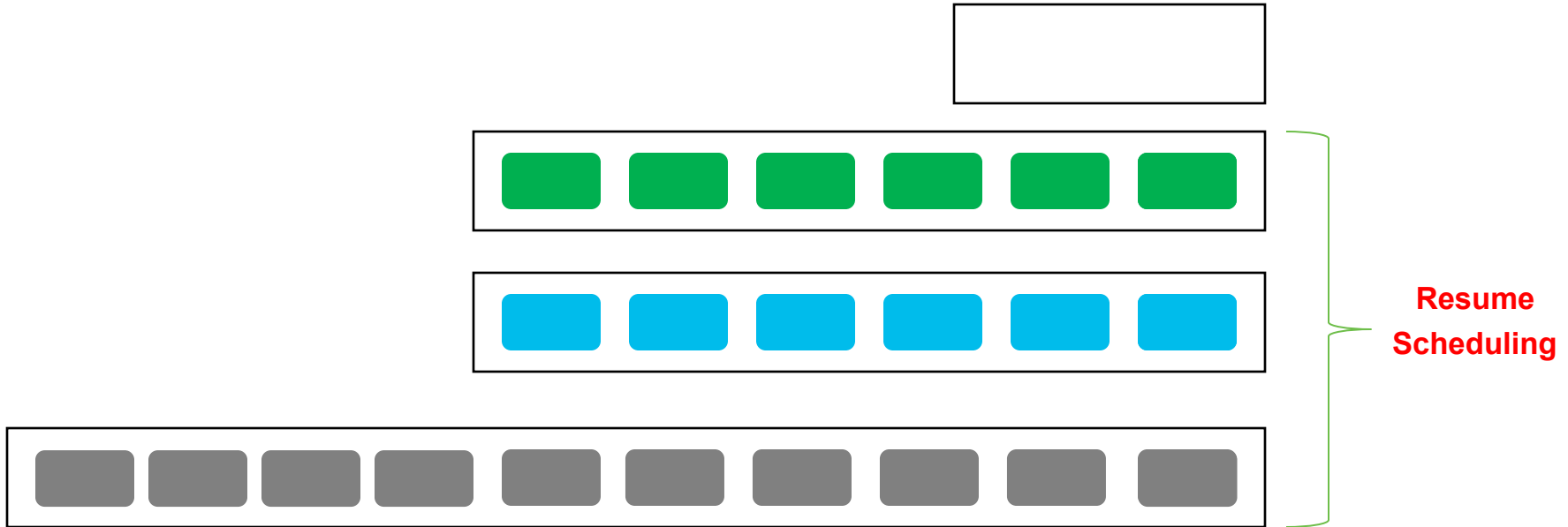
Catalyst Hardware Queuing

1P3Q1T Example



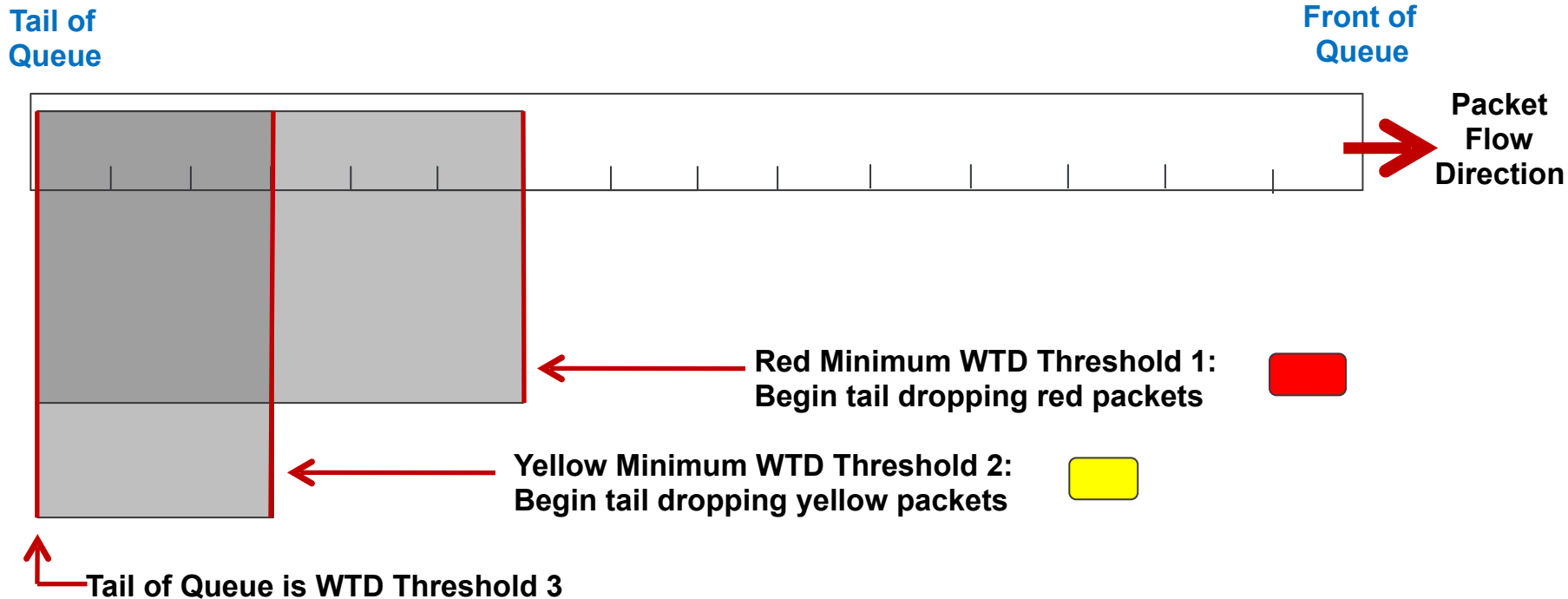
Catalyst Hardware Queuing

1P3Q1T Example



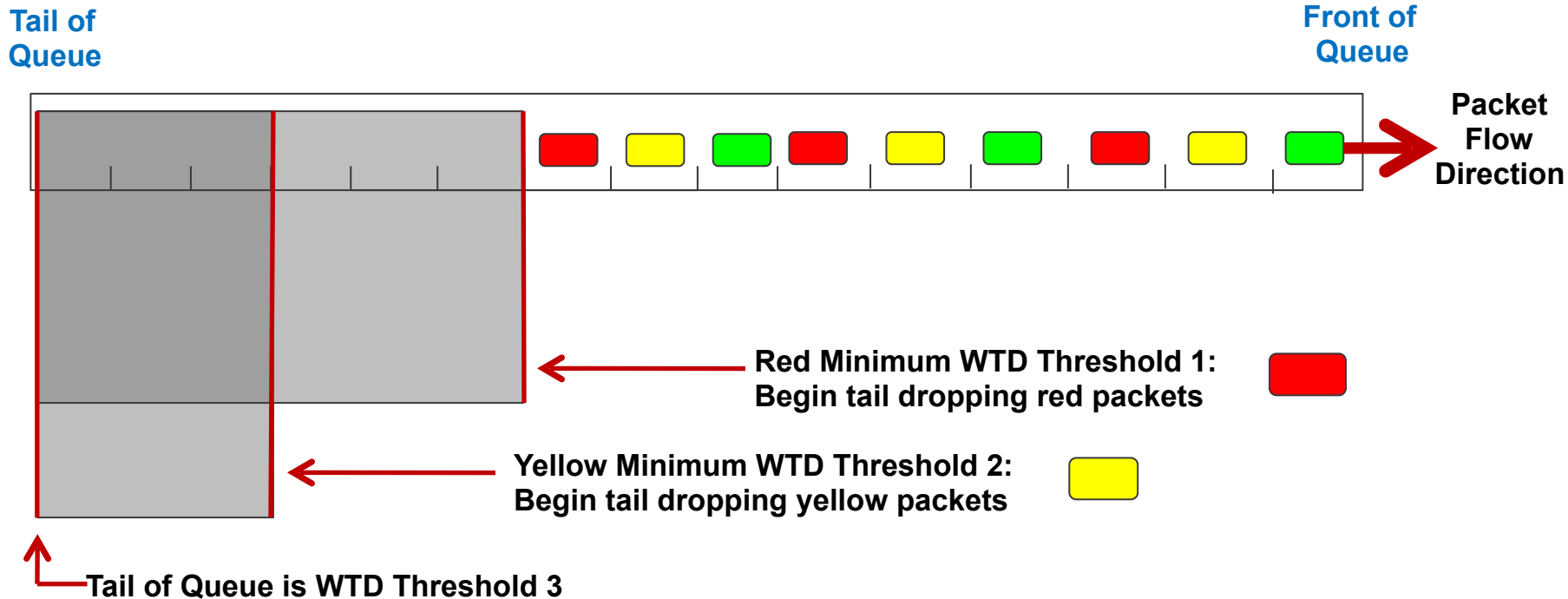
Weighted Tail Drop (WTD) Operation

3T WTD Example



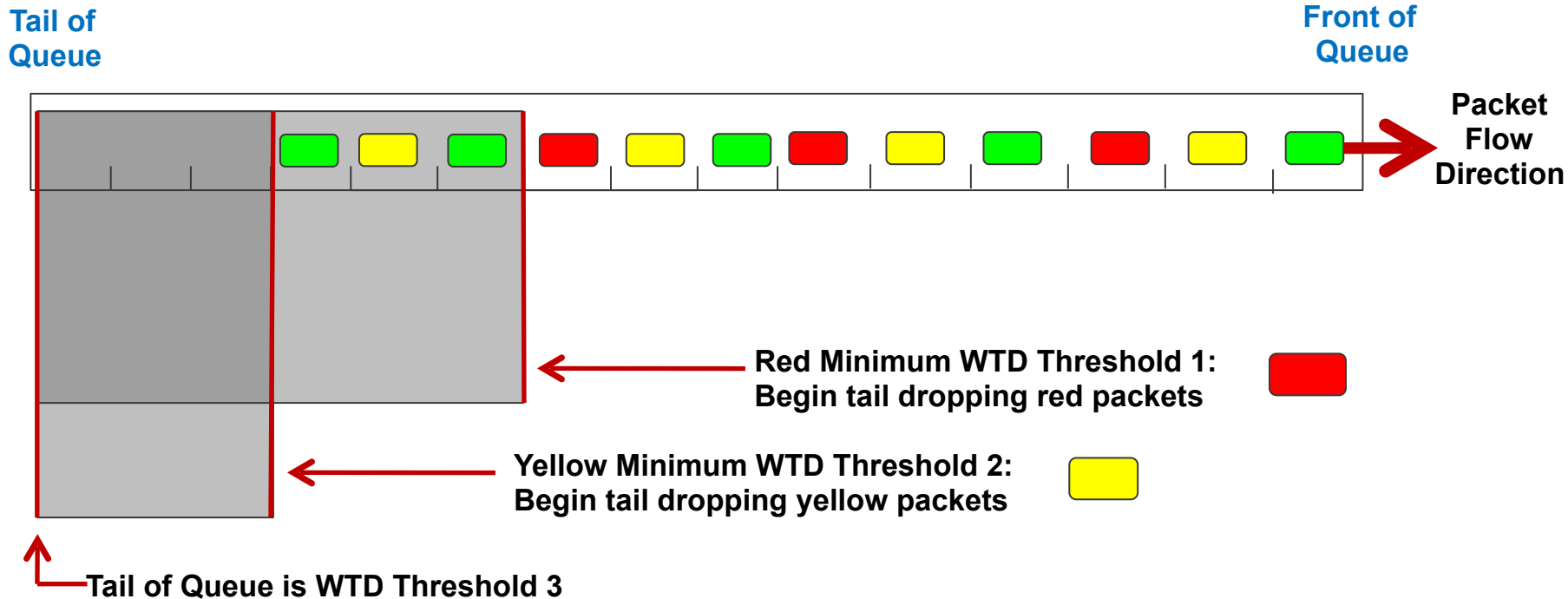
Weighted Tail Drop (WTD) Operation

3T WTD Example



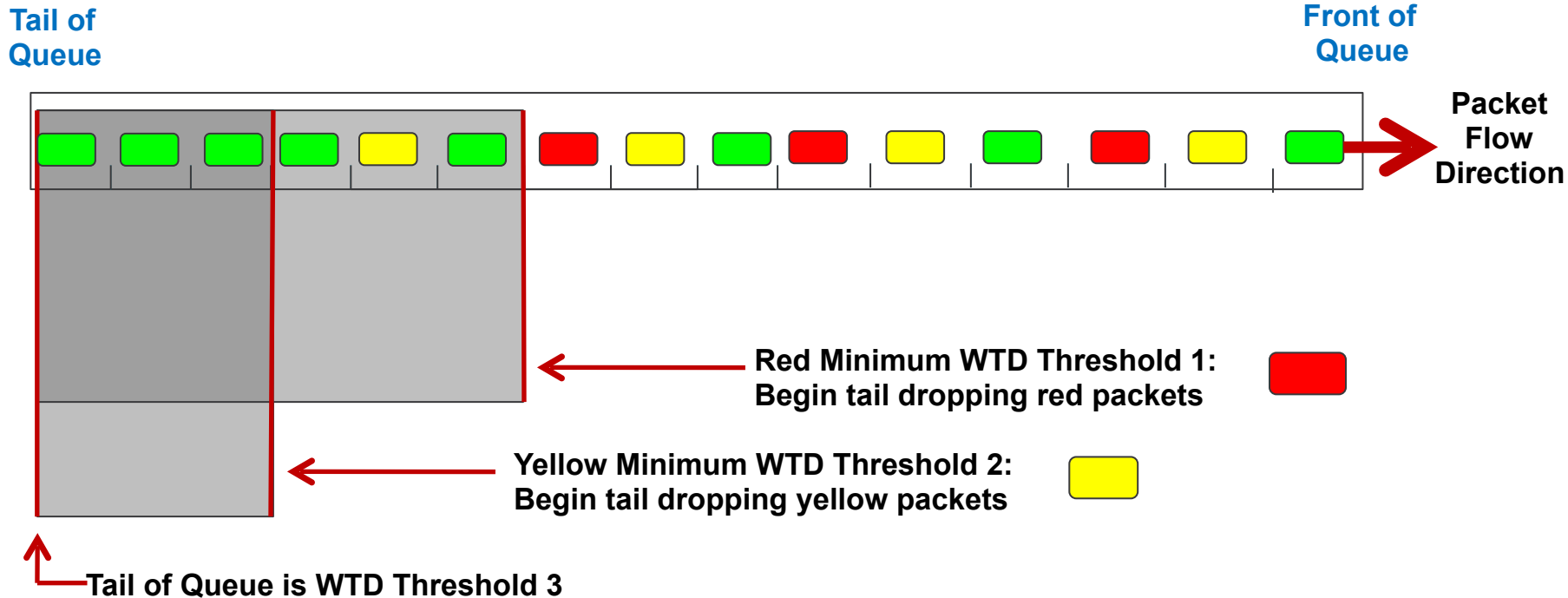
Weighted Tail Drop (WTD) Operation

3T WTD Example



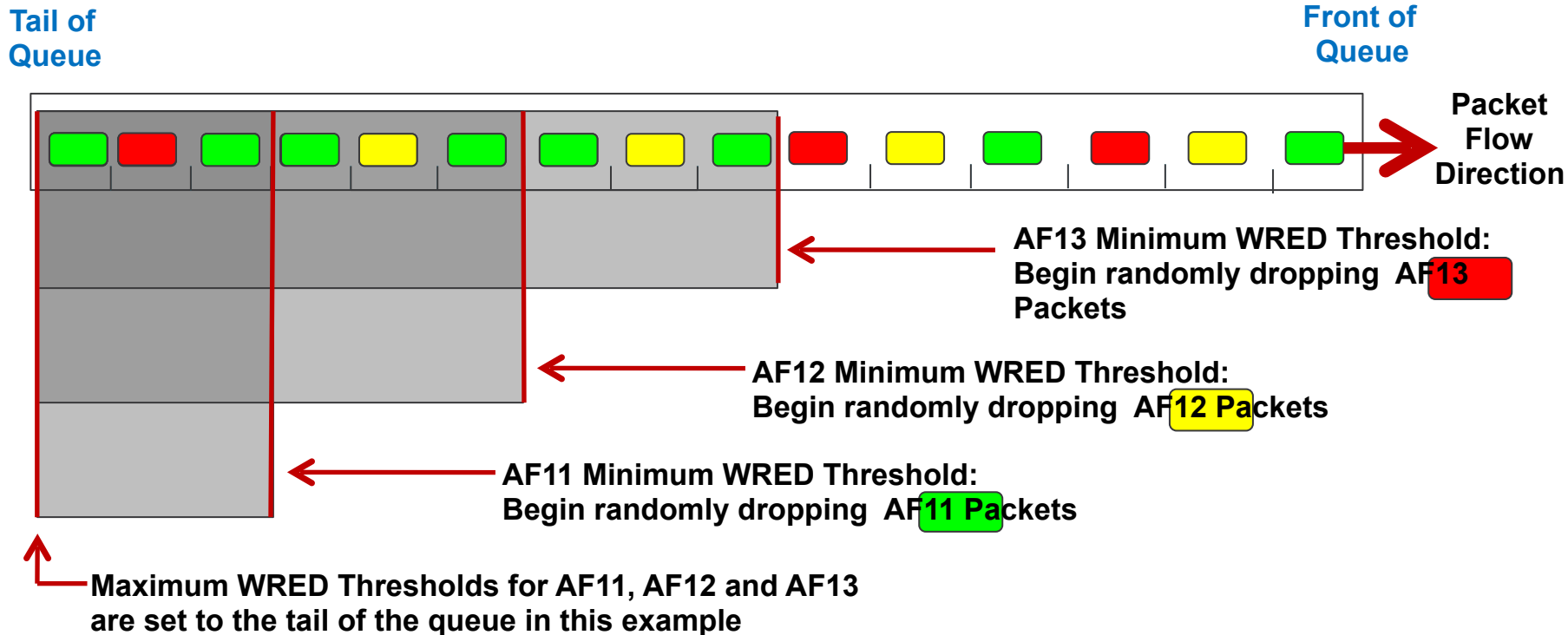
Weighted Tail Drop (WTD) Operation

3T WTD Example



Weighted Random Early Detect (WRED) Operation

4T WTD Example



Software and Syntax Variations

Software and Syntax Variations

- Catalyst 2960-X / 3560 / 3750 are the last platforms to use Multilayer Switch QoS (MLS QoS)
 - **QoS is disabled by default** and must be globally enabled with **mls qos** command
 - Once enabled, all ports are set to an **untrusted** port-state
- Catalyst 3650/3850 and 4500 use IOS Modular QoS Command Line Interface (MQC)
 - QoS is enabled by default
 - All ports are trusted at layer 2 and layer 3 by default
- Catalyst 6500/6800 use Cisco Common Classification Policy Language (C3PL) QoS
 - QoS is enabled by default (Sup2T) – Disabled by default (Sup720)
 - All ports are trusted at layer 2 and layer 3 by default
 - C3PL presents queuing policies similar to MQC, but as a defined “type” of policy

Software and Syntax Variations

- Catalyst 2960-X / 3560 / 3750 are the last platforms to use Multilayer Switch QoS (MLS QoS)
 - **QoS is disabled by default** and must be globally enabled with **mls qos** command
 - Once enabled, all ports are set to an **untrusted** port-state
- Catalyst 3650/3850 and 4500 use IOS Modular QoS Command Line Interface (MQC)
 - QoS is enabled by default
 - All ports are trusted at layer 2 and layer 3 by default
- Catalyst 6500/6800 use Cisco Common Classification Policy Language (C3PL) QoS
 - QoS is enabled by default (Sup2T) – Disabled by default (Sup720)
 - All ports are trusted at layer 2 and layer 3 by default
 - C3PL presents queuing policies similar to MQC, but as a defined “type” of policy
- Nexus 7000/7700 use NX-OS QoS
 - QoS is enabled by default
 - All ports are trusted at layer 2 and layer 3 by default
 - NX-OS presents queuing policies similar to MQC, but as a defined “type” and with default class-map names

Trust Boundaries

The trust boundary is the edge where Layer 2 (CoS / UP) and/or Layer 3 (DSCP) markings are accepted or rejected

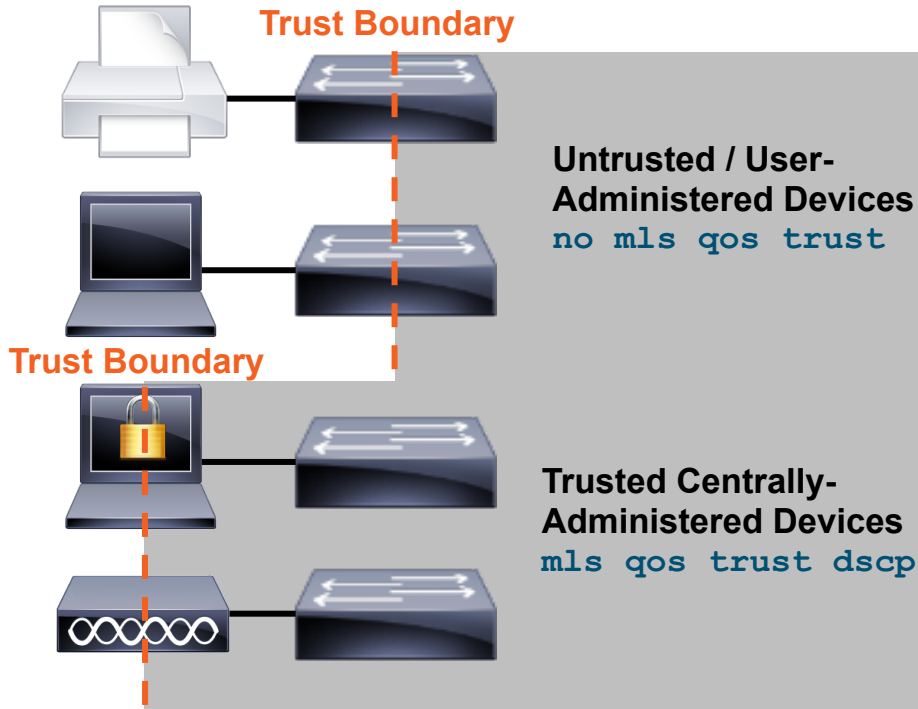
Trust Boundaries

The trust boundary is the edge where Layer 2 (CoS / UP) and/or Layer 3 (DSCP) markings are accepted or rejected



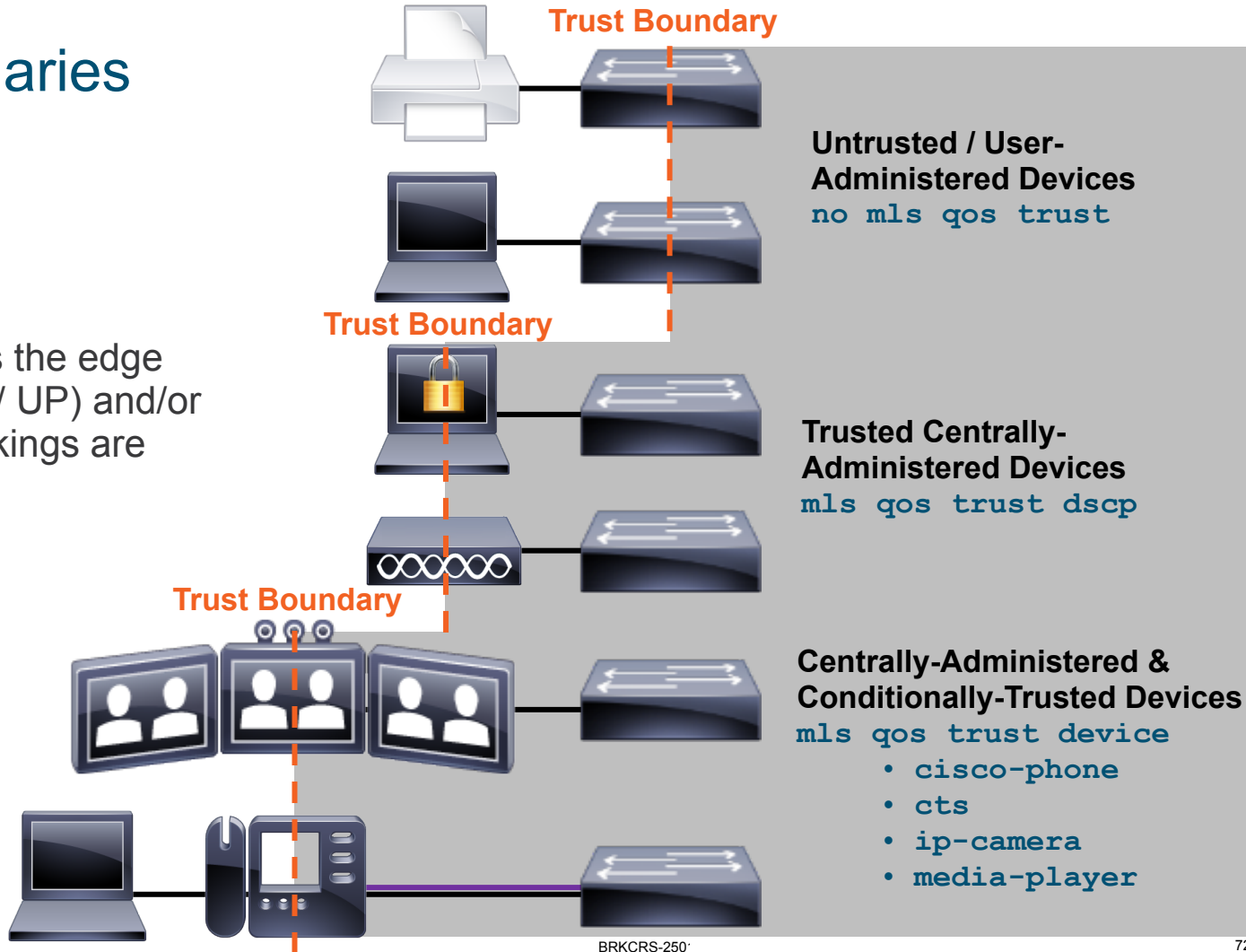
Trust Boundaries

The trust boundary is the edge where Layer 2 (CoS / UP) and/or Layer 3 (DSCP) markings are accepted or rejected

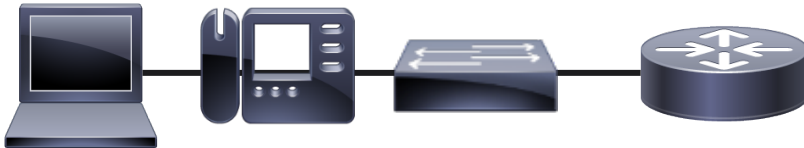


Trust Boundaries

The trust boundary is the edge where Layer 2 (CoS / UP) and/or Layer 3 (DSCP) markings are accepted or rejected



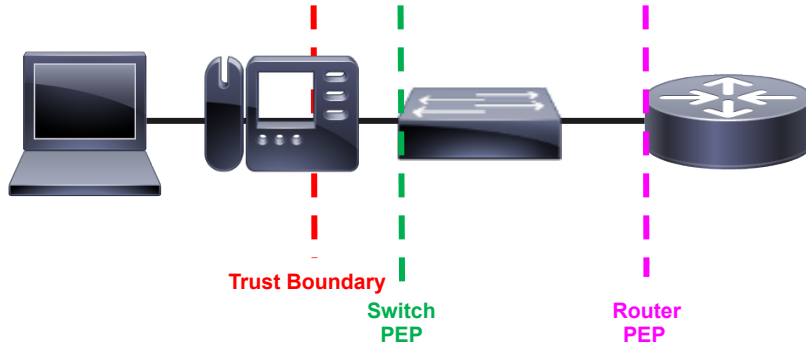
Policy Enforcement Points (PEPs)



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

Policy Enforcement Points (PEPs)

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



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

EtherChannel QoS

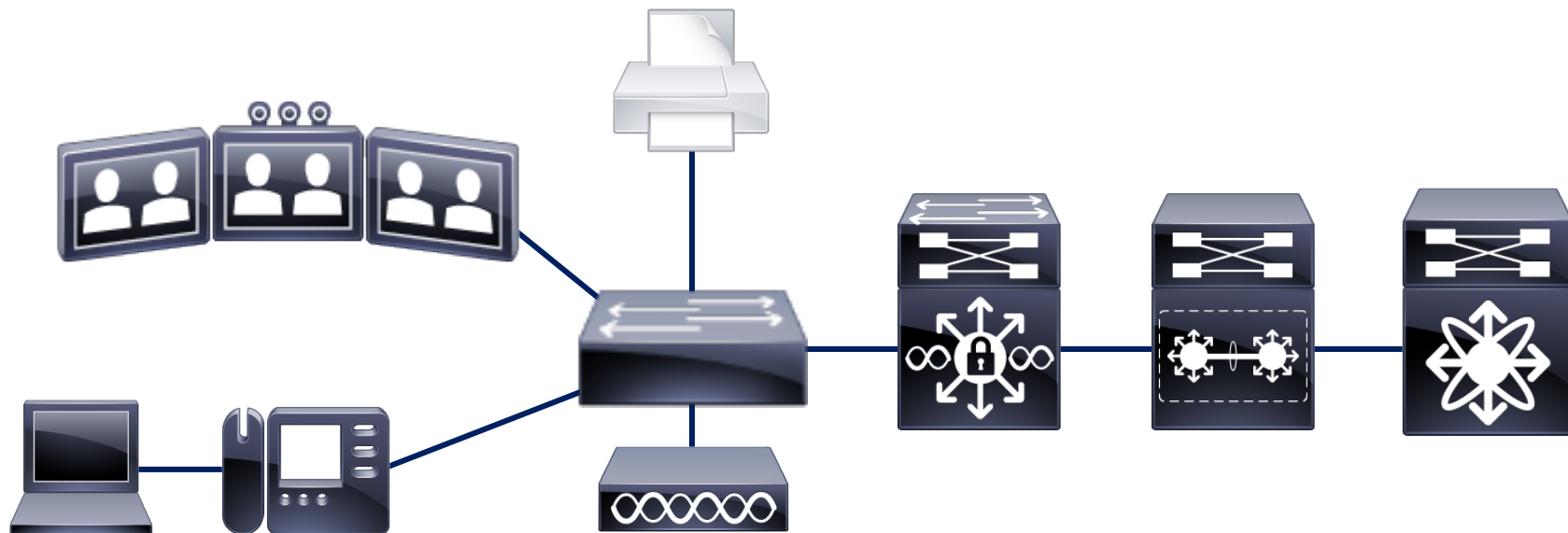
- EtherChannels are comprised of logical (port-channel) interfaces and physical (port-member) interfaces

Platform	QoS Policies Applied to the (Logical) Port-Channel Interface	QoS Policies Applied to the (Physical) Port-Member Interfaces
Catalyst 2960-X		<ul style="list-style-type: none">• Classification & Marking (Ingress) and Queuing (Egress)
Catalyst 3650/3850		<ul style="list-style-type: none">• Classification & Marking (Ingress) and Queuing (Egress)
Catalyst 4500	<ul style="list-style-type: none">• Classification & Marking (Ingress)	<ul style="list-style-type: none">• Queuing (Egress)
Catalyst 6500	<ul style="list-style-type: none">• Classification & Marking (Ingress)	<ul style="list-style-type: none">• Queuing (Ingress & Egress)
Cisco Nexus 7000/7700	<ul style="list-style-type: none">• Classification & Marking (Ingress) and Queuing (Ingress & Egress)	

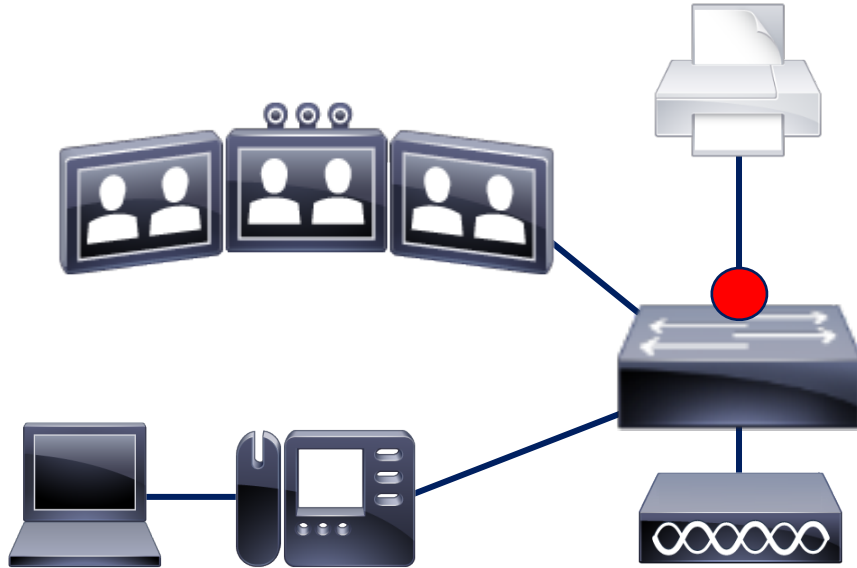
Campus QoS Design Best Practices

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

Campus Port QoS Roles



Campus Port QoS Roles

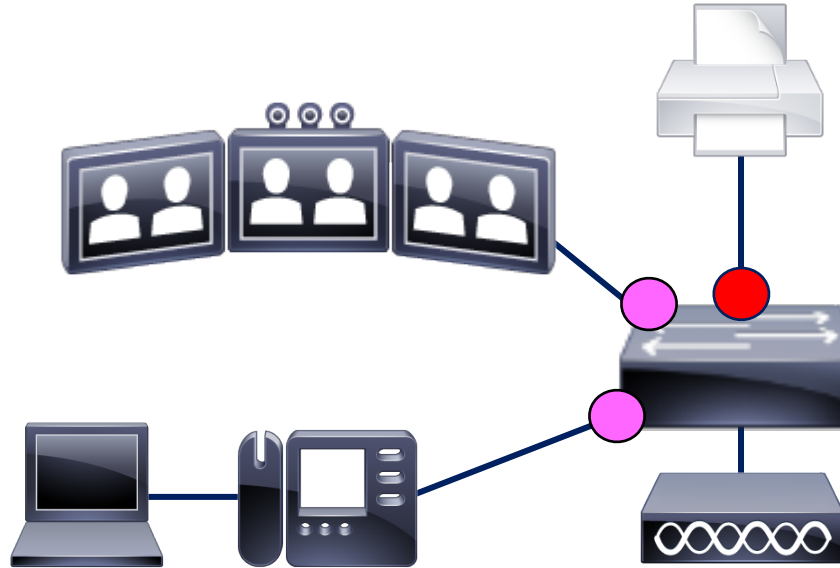


Untrusted Endpoint:

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



Campus Port QoS Roles



Untrusted Endpoint:

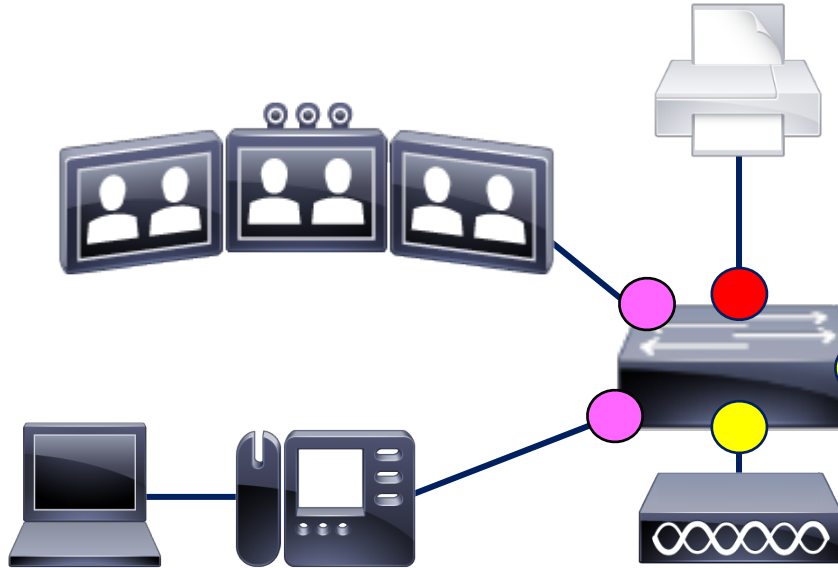
- Port Set to Untrusted State (or Explicit Policy to Mark to DSCP 0)
- [Optional Ingress Marking and/or Policing]
- [Ingress and] Egress Queuing



Conditionally-Trusted Endpoint

- Conditional-Trust with Trust-CoS or DSCP
- [Optional Ingress Marking and/or Policing]
- [Ingress and] Egress Queuing

Campus Port QoS Roles



Conditionally-Trusted Endpoint

- Conditional-Trust with Trust-CoS or DSCP
- [Optional Ingress Marking and/or Policing]
- [Ingress and] Egress Queuing



Untrusted Endpoint:

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



Trusted Port

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

Campus QoS Design—At-A-Glance



Campus QoS Design

At-A-Glance

The Case for QoS in Campus Networks

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

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

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

Campus QoS Design Considerations

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

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

Global Default QoS Setting

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

Trust States

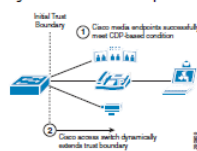
A switch port that is set to trust will accept and preserve either Layer 2 or Layer 3 packet markings. There are four static trust states with which a switch port may be configured:

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

Conditional Trust

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

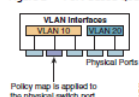
Figure 1 Conditional Trust Operation



Per-Port QoS

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

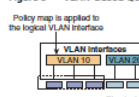
Figure 2 Port-Based QoS



Per-VLAN QoS

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

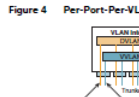
Figure 3 VLAN-Based QoS



Per-Port/Per-VLAN QoS

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

Figure 4 Per-Port/Per-VLAN-based QoS



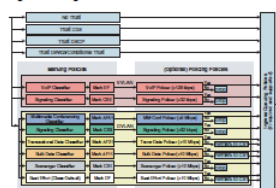
Ingress QoS Models

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

Campus QoS Design

At-A-Glance

Figure 5 Ingress QoS Models



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

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

Combinations of these may be used at the same time.

Egress QoS Models

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

- **IP** represents a strict priority queue
- **iQ** represents a number of non-priority queues
- **yT** represents a number of drop-thresholds per non-priority queue

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

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

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

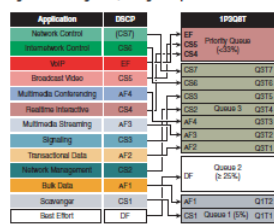
- Realtime queue should not exceed 33% BW
- Default queue should be at least 25% BW
- Bulk/scavenger queue should not exceed 5% BW

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

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

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

Figure 6 An Egress Queuing Example Model



EtherChannel QoS

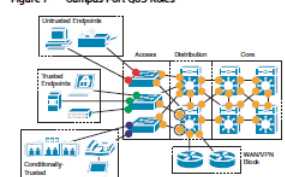
On some platforms ingress QoS policies (such as DSCP) are applied on the logical Port-Channel interface; however, on all platforms egress QoS policies (such as

queuing policies) are always applied to the physical port-member interfaces.

QoS Roles in a Campus

Access edge switch ports have the most variation in QoS policy roles and these will vary depending on the type of endpoint to which these are connecting. For all switch-to-switch links the only QoS policies that are required are DSCP-trust (on ingress) and queuing (on egress). QoS roles in a campus network are shown in Figure 7.

Figure 7 Campus Port QoS Roles



- **Untrusted Endpoint Port QoS:**
 - Trust DSCP
 - IPiQyT or IP1Q1T Queuing
- **Trusted Endpoint Port QoS:**
 - Trust DSCP
 - DSCP-to-CoS Mapping
 - IPiQyT Queuing
- **Conditionally-Trusted Endpoint Port QoS:**
 - Conditional Trust with Trust DSCP
 - DSCP-to-CoS Mapping
 - IPiQyT Queuing

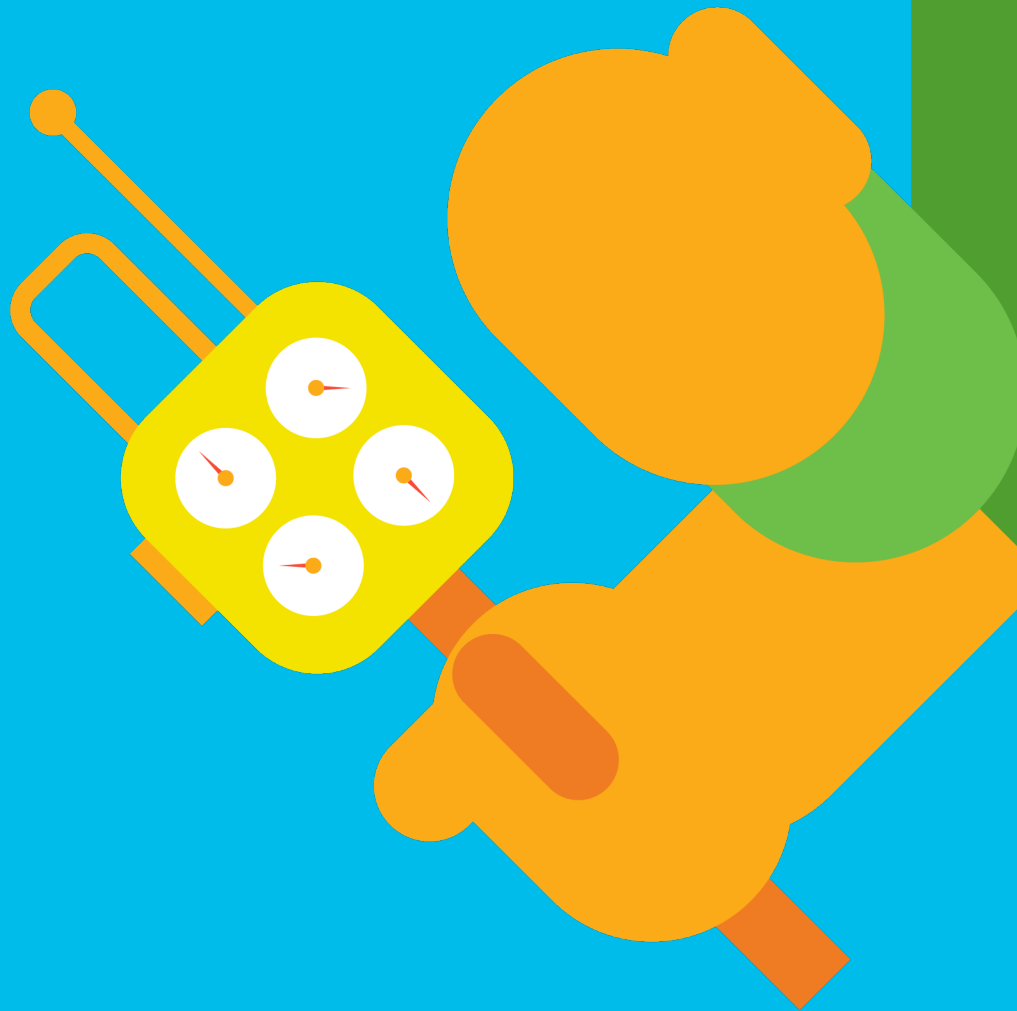
AutoQoS

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

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

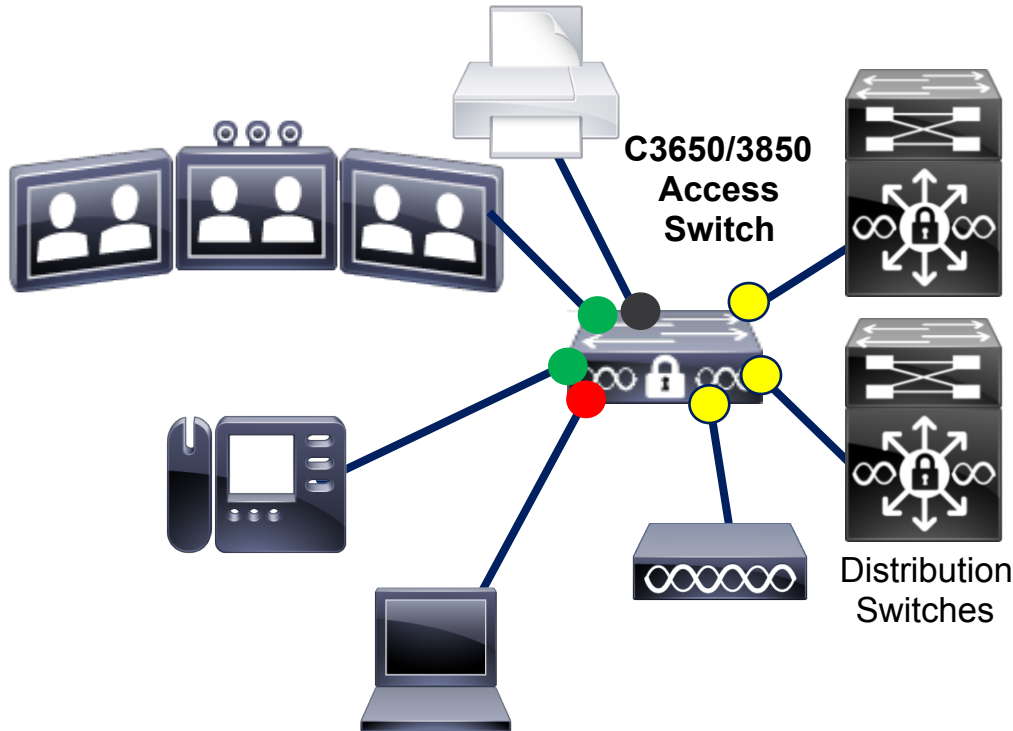
For more details, see Campus QoS Design 4.0: http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS/QRD_40/QoS_Campus_40.html And the Cisco Press book: *End-to-End QoS Network Design* (Second Edition) Chapter 13

Catalyst 3650/3850 (and 9300/9400/9500) QoS Design



Catalyst 3650/3850/9300

QoS Roles in the Campus Access



No Trust +
Egress Queuing

Trust DSCP +
Egress Queuing

Conditional Trust +
Egress Queuing

Classification/Marking +
[Optional Policing] +
Egress Queuing

Catalyst 3650/3850

QoS Design Steps

1. Configure Ingress QoS Model(s):

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

2. Configure Egress Queuing

- ❑ Wired Queuing Models (2P6Q3T)

***Note:** Catalyst 3650/3850 uses IOS MQC, which trusts by default; therefore no explicit policy is required for DSCP trust

Catalyst 3650/3850

Conditional Trust Models

Catalyst 3650/3850

Conditional Trust Models

Conditional-Trust Models:

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

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

Catalyst 3650/3850

Conditional Trust Models

Only match-any is supported (i.e. match-all is not supported)

Conditional-Trust Models:

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

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

Conditional-Trust (Cisco IP Phone) Example:

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

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

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

Catalyst 3650/3850

Conditional Trust Models

Only match-any is supported (i.e. match-all is not supported)

Conditional-Trust Models:

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

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

Conditional-Trust (Cisco IP Phone) Example:

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

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

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

```
interface GigabitEthernet 1/0/1
  trust device cisco-phone
  service-policy input CISCO-IPPHONE
```

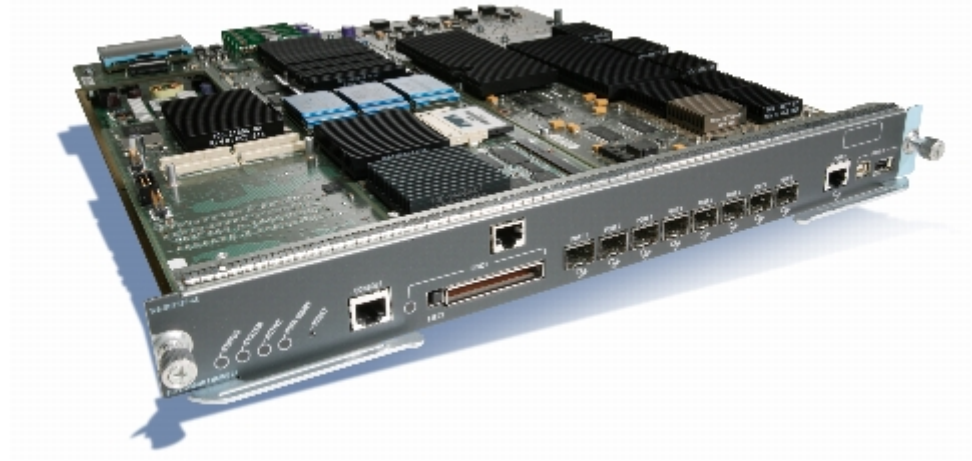
Catalyst 3650/3850

Classification Options

- ACL-based classification: **match access-group *ACL_NAME***
 - Syntax is identical to Catalyst 2K ACL-based classification & marking examples
- NBAR2 classification (as of IOS XE 16.3): **match protocol *APPLICATION***

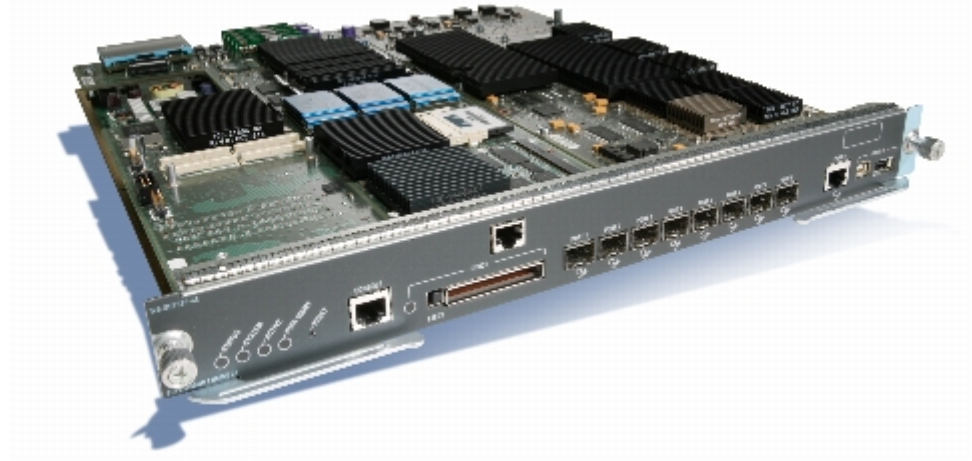
NBAR in Hardware—Yesterday

- Cisco Catalyst 6500 Sup32 Programmable Intelligent Services Accelerator (PISA)—Jan 2007



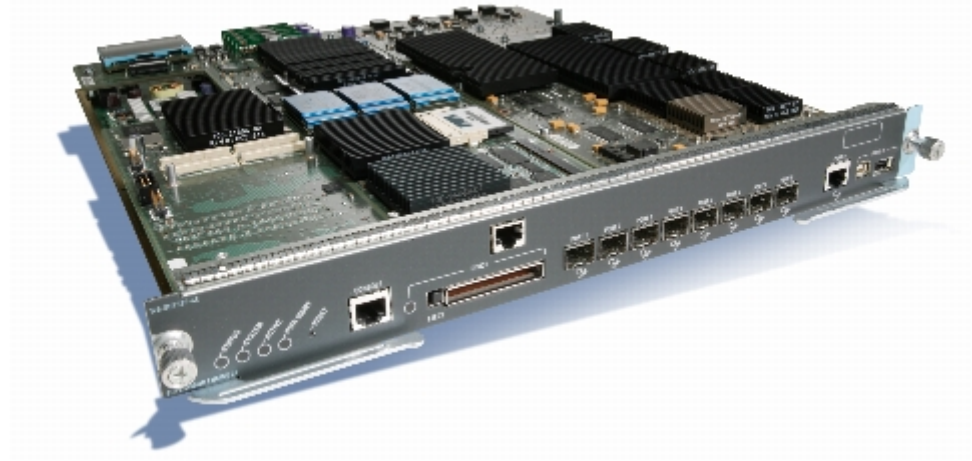
NBAR in Hardware—Yesterday

- Cisco Catalyst 6500 Sup32 Programmable Intelligent Services Accelerator (PISA)—Jan 2007
- Supported 90+ protocols



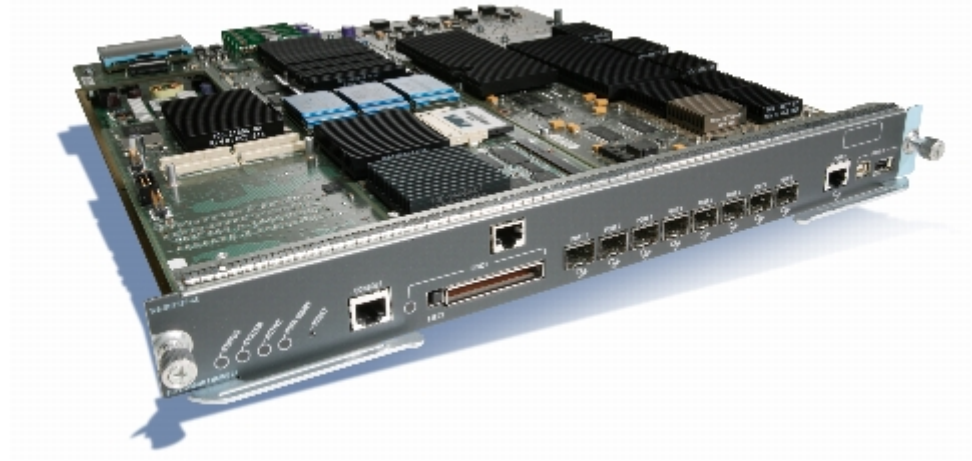
NBAR in Hardware—Yesterday

- Cisco Catalyst 6500 Sup32 Programmable Intelligent Services Accelerator (PISA)—Jan 2007
- Supported 90+ protocols
- Maximum Throughput: 2 Gbps



NBAR in Hardware—Yesterday

- Cisco Catalyst 6500 Sup32 Programmable Intelligent Services Accelerator (PISA)—Jan 2007
- Supported 90+ protocols
- Maximum Throughput: 2 Gbps
- MSRP ~\$30K



NBAR2 in Hardware—Today

- UADP-based platforms:
 - Catalyst 3650
 - Catalyst 3850
 - Catalyst 9000-series (UADP 2.0)



NBAR2 in Hardware—Today

- UADP-based platforms:
 - Catalyst 3650
 - Catalyst 3850
 - Catalyst 9000-series (UADP 2.0)
- Supports 1400+ protocols

1400% increase



NBAR2 in Hardware—Today

- UADP-based platforms:
 - Catalyst 3650
 - Catalyst 3850
 - Catalyst 9000-series (UADP 2.0)
- Supports 1400+ protocols **1400% increase**
- Maximum Throughput (Catalyst 3850 / 3650):
 - ~500 connections per second
 - Up to 5,000 bi-directional flows (24 access ports)
 - Up to 10,000 bi-directional flows (48 access ports)



NBAR2 in Hardware—Today

- UADP-based platforms:
 - Catalyst 3650
 - Catalyst 3850
 - Catalyst 9000-series (UADP 2.0)
- Supports 1400+ protocols **1400% increase**
- Maximum Throughput (Catalyst 3850 / 3650):
 - ~500 connections per second
 - Up to 5,000 bi-directional flows (24 access ports)
 - Up to 10,000 bi-directional flows (48 access ports)
- MSRP (beginning at) ~\$3K **90% decrease**



Configuring NBAR2 QoS Policies

```
class-map match-any VOICE
  match protocol cisco-phone
  match protocol cisco-jabber-audio
  match protocol ms-lync-audio
  match protocol citrix-audio
class-map match-any BROADCAST-VIDEO
  match protocol cisco-ip-camera
class-map match-any REAL-TIME-INTERACTIVE
  match protocol telepresence-media
class-map match-any CALL-SIGNALING
  match protocol skinny
  match protocol telepresence-control
class-map match-any TRANSACTIONAL-DATA
  match protocol citrix
  match protocol sap
class-map match-any BULK-DATA
  match protocol attribute category email
  match protocol attribute category file-sharing
  match protocol attribute sub-category backup-systems
class-map match-any SCAVENGER
  match protocol attribute category gaming
  match protocol attribute application-group skype-group
```

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

match protocol enables NBAR2 classification
Note: Up to 16 **match protocol** statements are supported per class-map

Configuring NBAR2 QoS Policies

```
class-map match-any VOICE
  match protocol cisco-phone
  match protocol cisco-jabber-audio
  match protocol ms-lync-audio
  match protocol citrix-audio
class-map match-any BROADCAST-VIDEO
  match protocol cisco-ip-camera
class-map match-any REAL-TIME-INTERACTIVE
  match protocol telepresence-media
class-map match-any CALL-SIGNALING
  match protocol skinny
  match protocol telepresence-control
class-map match-any TRANSACTIONAL-DATA
  match protocol citrix
  match protocol sap
class-map match-any BULK-DATA
  match protocol attribute category email
  match protocol attribute category file-sharing
  match protocol attribute sub-category backup-systems
class-map match-any SCAVENGER
  match protocol attribute category gaming
  match protocol attribute application-group skype-group
```

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

Note: Multiple application protocols can be identified using attributes, including:

- category
- sub-category
- application-group

More to come!

Catalyst 3650/3850/9300/9400/8500 NBAR2 QoS Attributes Support

IOS XE 16.8—March 2018

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

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


Catalyst 3650/3850

Marking & Policing Policy Example

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

Catalyst 3650/3850

Marking & Policing Policy Example

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

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

Catalyst 3650/3850

Marking & Policing Policy Example

```
policy-map MARKING&POLICING
class VVLAN-VOIP
  set dscp ef
  police 128k
    conform-action transmit
    exceed-action drop
class VVLAN-SIGNALING
  set dscp cs3
  police 32k
    conform-action transmit
    exceed-action drop
class MULTIMEDIA-CONFERENCING
  set dscp af41
  police 5m
    conform-action transmit
    exceed-action drop
class SIGNALING
  set dscp cs3
  police 32k
    conform-action transmit
    exceed-action drop
```

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

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

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

Catalyst 3650/3850

Marking & Policing Policy Example

```
policy-map MARKING&POLICING
  class VVLAN-VOIP
    set dscp ef
    police 128k
      conform-action transmit
      exceed-action drop
  class VVLAN-SIGNALING
    set dscp cs3
    police 32k
      conform-action transmit
      exceed-action drop
  class MULTIMEDIA-CONFERENCING
    set dscp af41
    police 5m
      conform-action transmit
      exceed-action drop
  class SIGNALING
    set dscp cs3
    police 32k
      conform-action transmit
      exceed-action drop
```

...[continued]

```
class TRANSACTIONAL-DATA
  set dscp af21
  police 10m
    conform-action transmit
    exceed-action TABLE-MAP
class BULK-DATA
  set dscp af11
  police 10m
    conform-action transmit
    exceed-action TABLE-MAP
class SCAVENGER
  set dscp cs1
  police 10m
    conform-action transmit
    exceed-action drop
class class-default
  set dscp default
  police 10m
    conform-action transmit
    exceed-action TABLE-MAP
```

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

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

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

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

Catalyst 3650/3850

Marking & Policing Policy Example

```
policy-map MARKING&POLICING
class VVLAN-VOIP
  set dscp ef
  police 128k
    conform-action transmit
    exceed-action drop
class VVLAN-SIGNALING
  set dscp cs3
  police 32k
    conform-action transmit
    exceed-action drop
class MULTIMEDIA-CONFERENCING
  set dscp af41
  police 5m
    conform-action transmit
    exceed-action drop
class SIGNALING
  set dscp cs3
  police 32k
    conform-action transmit
    exceed-action drop
```

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

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

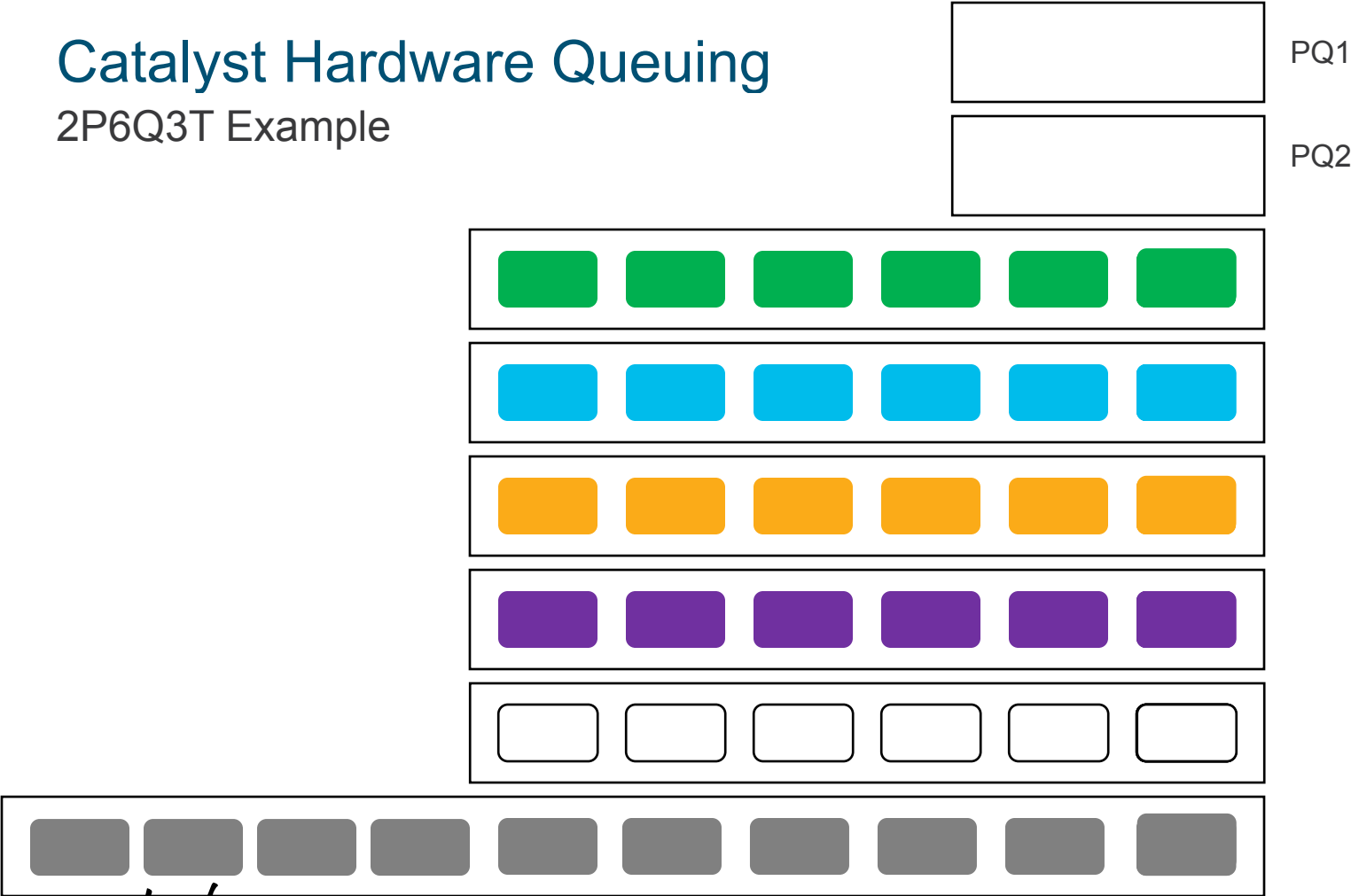
Policing to remark traffic is done by referencing the previously-configured **table-map**

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

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

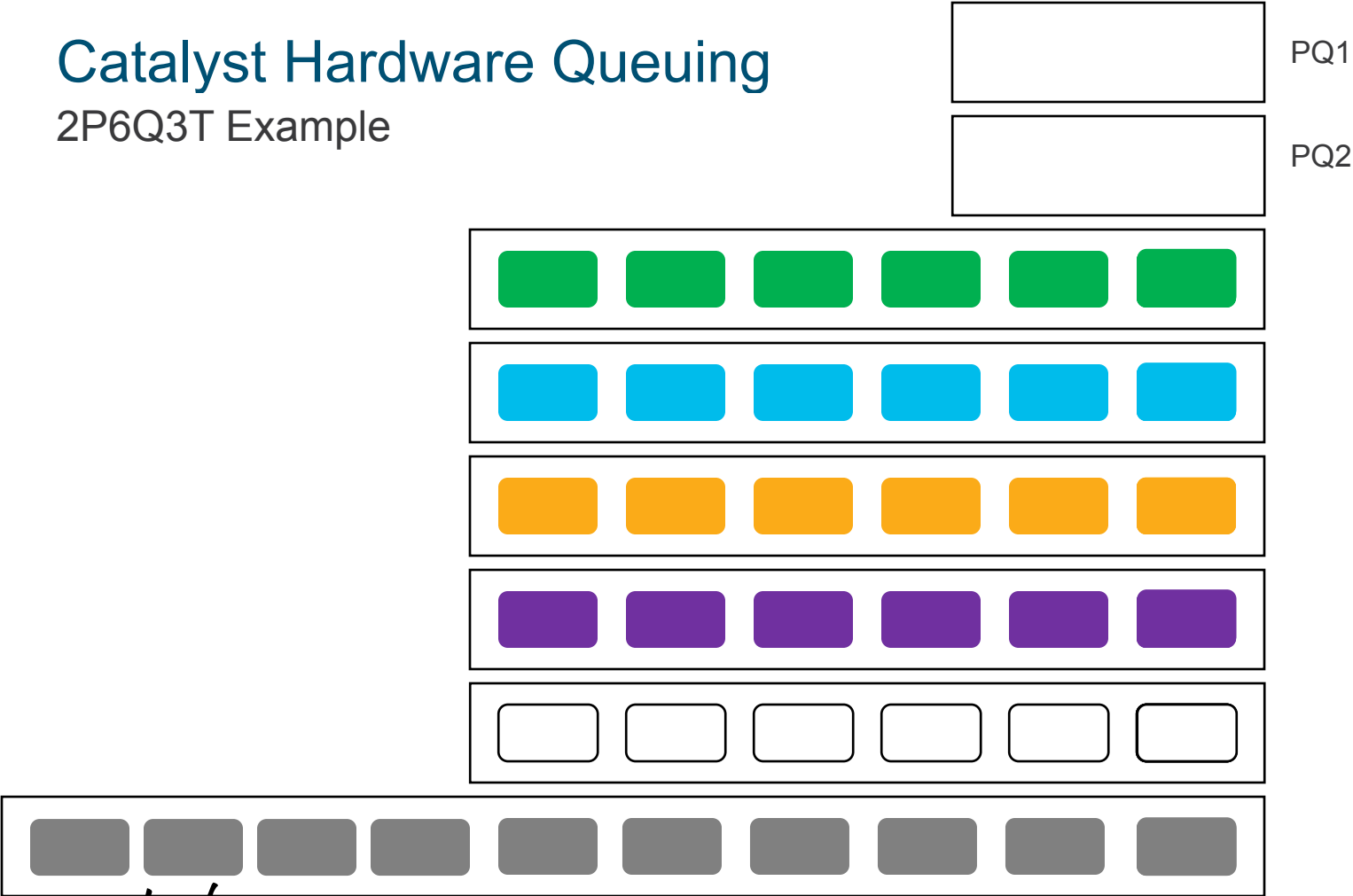
Catalyst Hardware Queuing

2P6Q3T Example



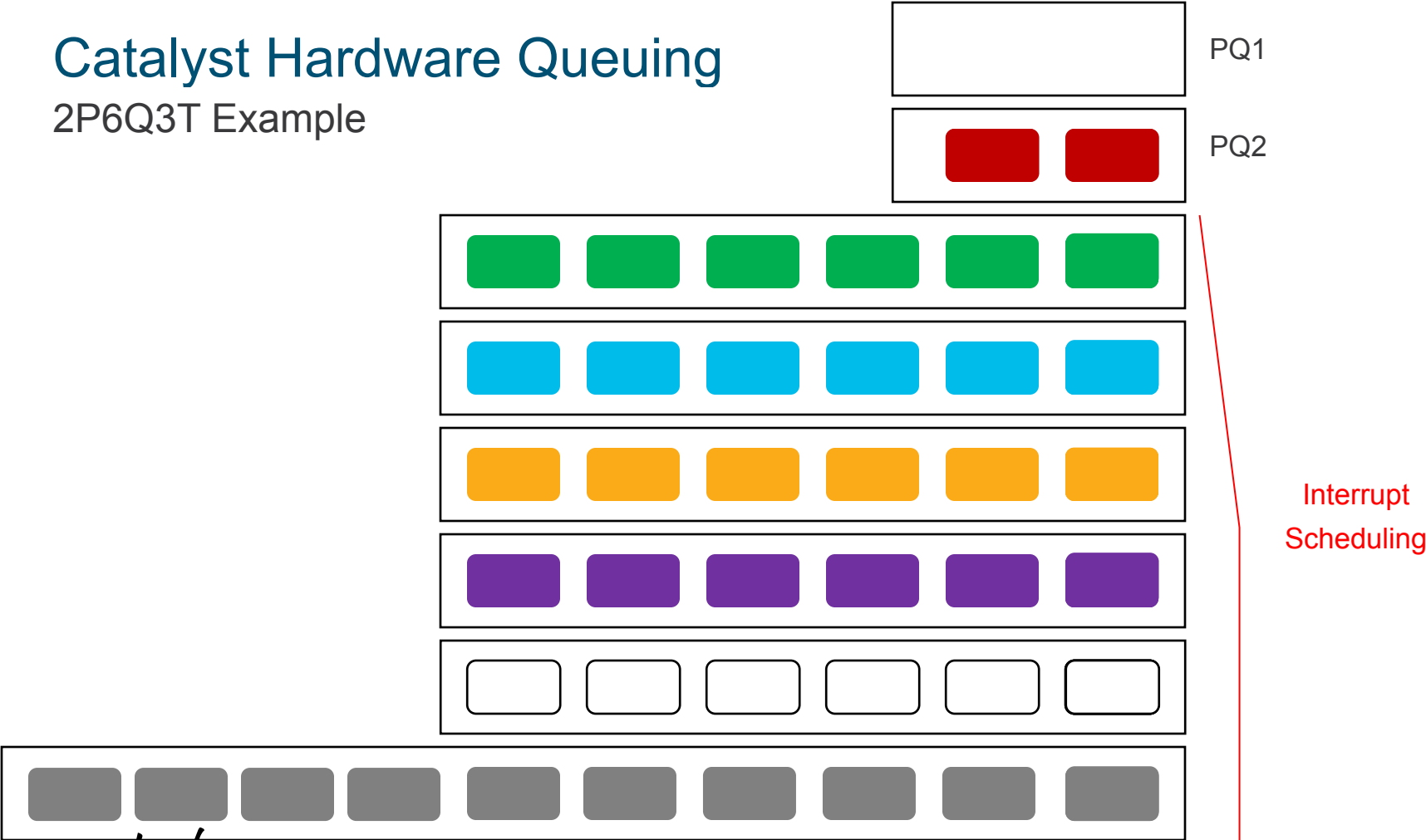
Catalyst Hardware Queuing

2P6Q3T Example



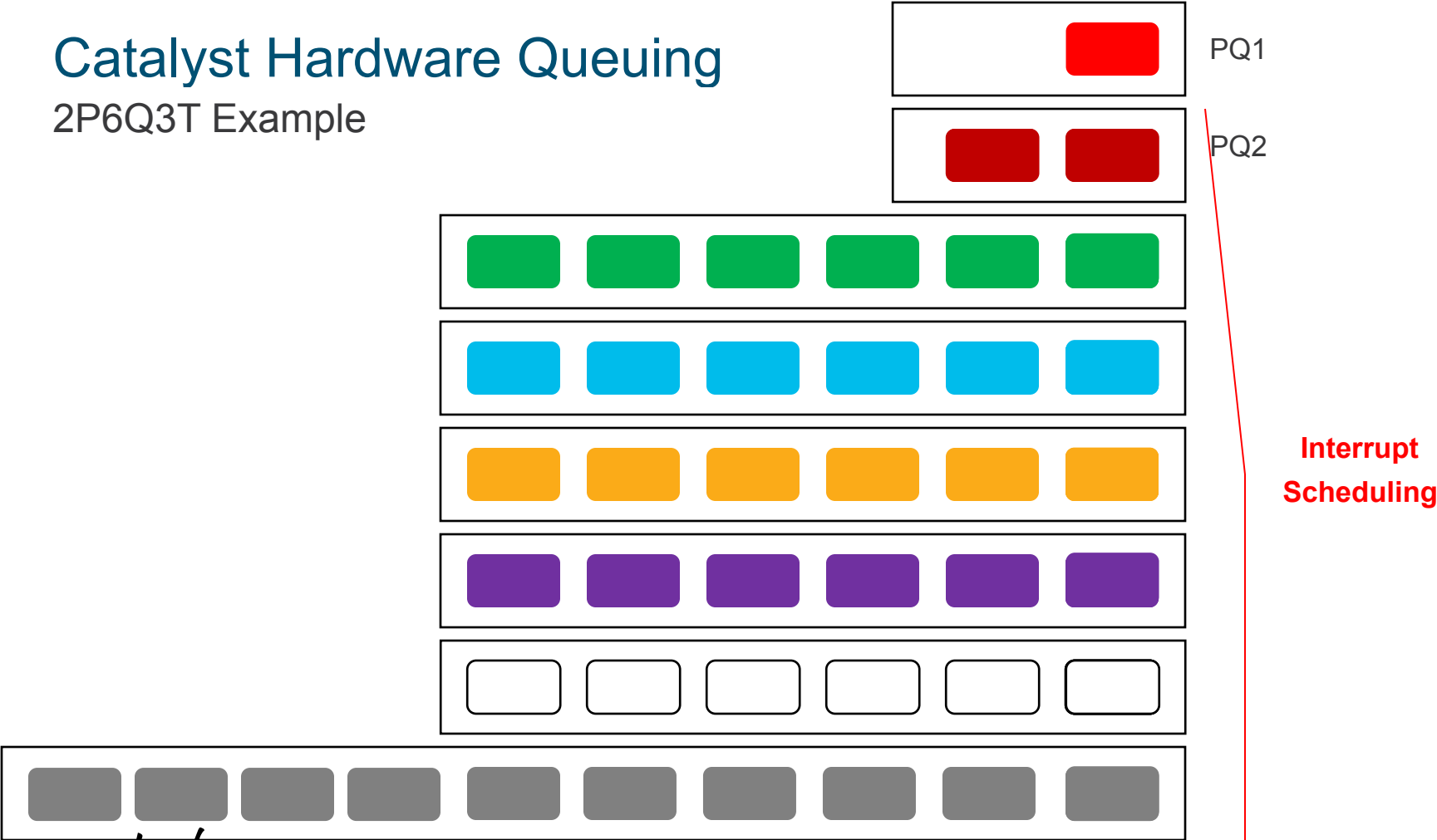
Catalyst Hardware Queuing

2P6Q3T Example



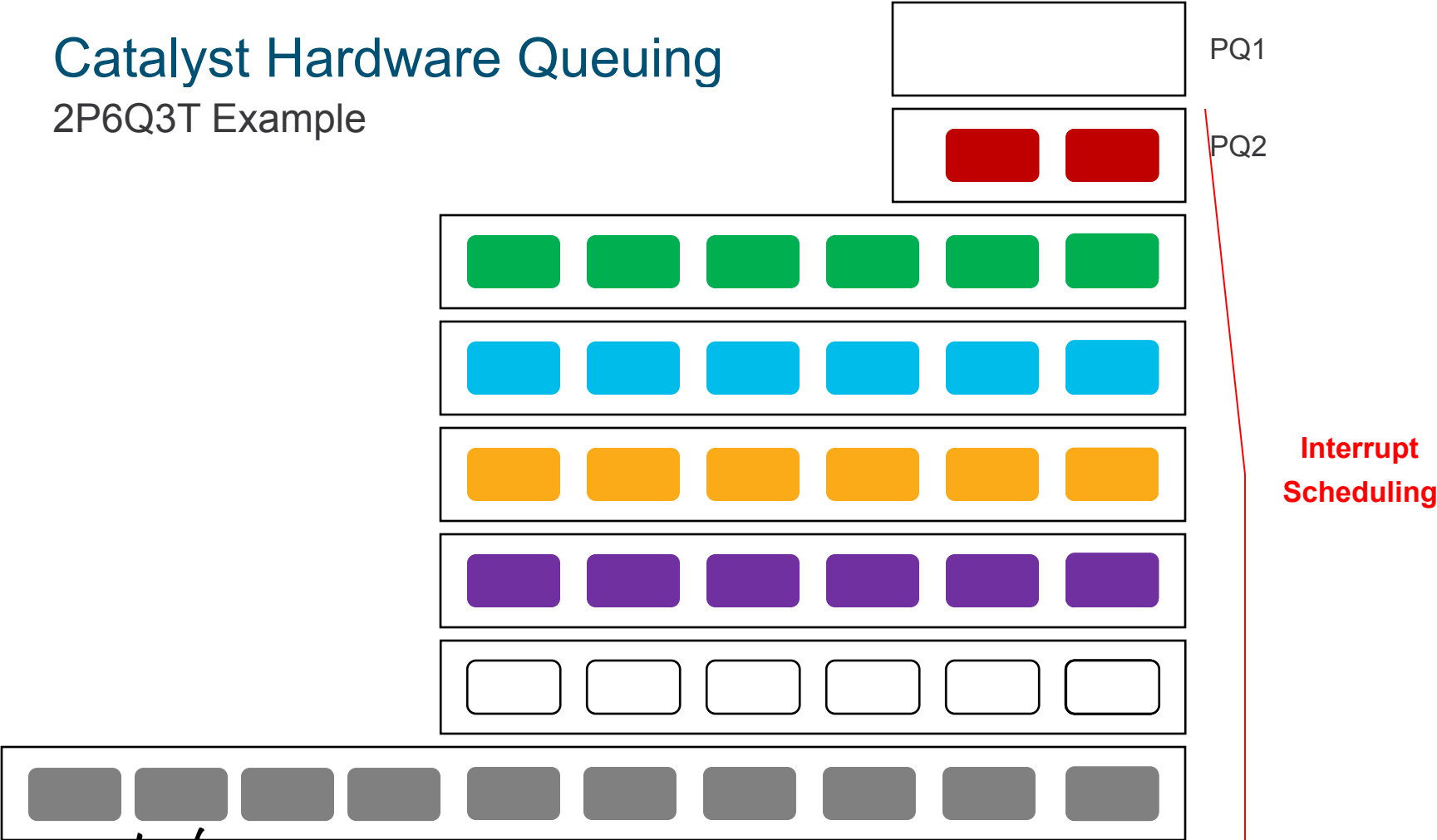
Catalyst Hardware Queuing

2P6Q3T Example



Catalyst Hardware Queuing

2P6Q3T Example



Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model

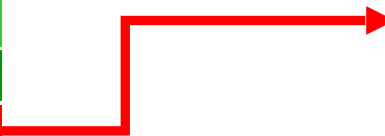
Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signalling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

2P6Q3T	
EF	PQ Level 1 (10%)
CS4 & CS5 AF4	PQ Level 2 (33%)
CS7 & CS6 CS3 & CS2	Q6 (BWR 12%)
AF3	Q4 (BWR 18% + DSCP-Based WTD)
AF2	Q3 (BWR 18% + DSCP-Based WTD)
AF1	Q2 (BWR 7% + DSCP-Based WTD)
CS1	Q2 (BWR 1%)
DF	Q1 (BWR 44%)

Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model

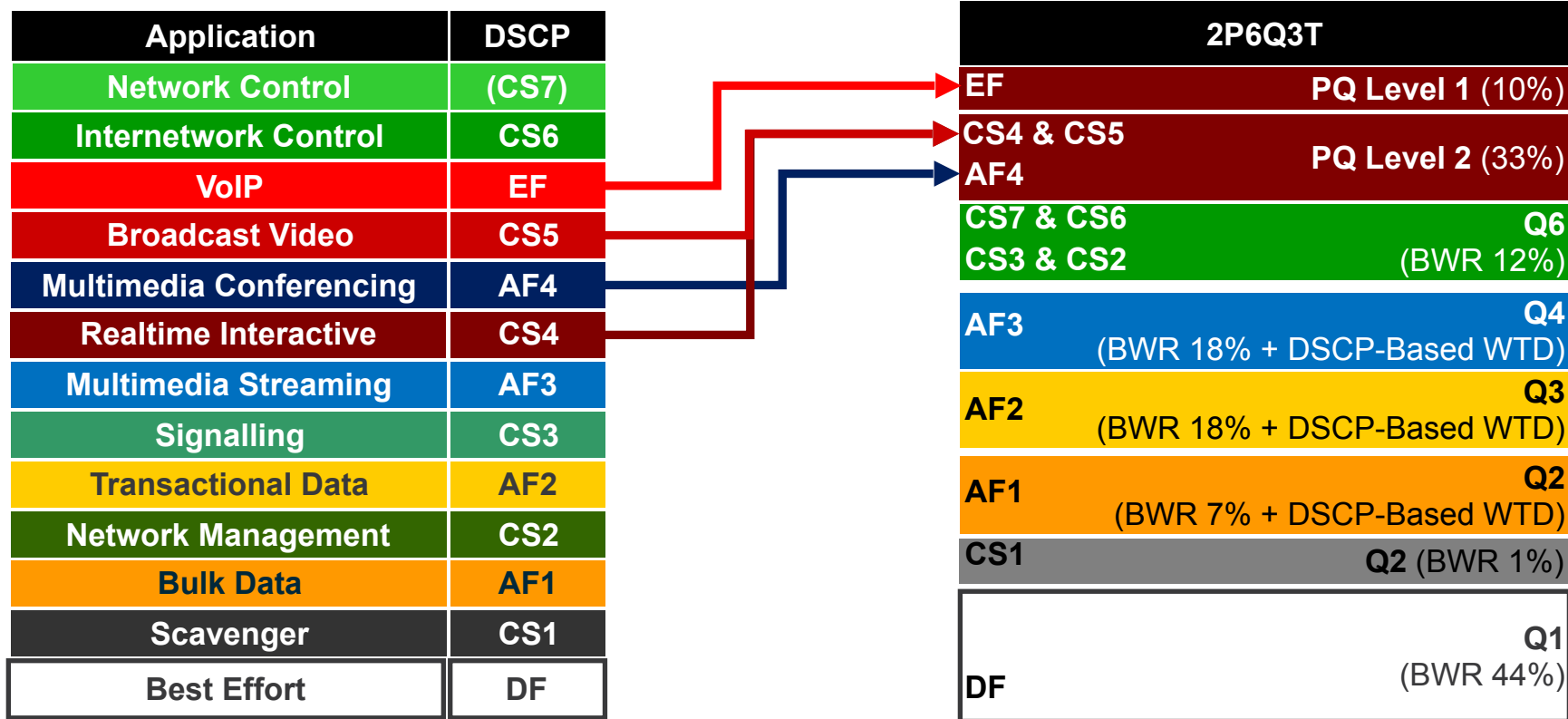
Application	DSCP
Network Control	(CS7)
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signalling	CS3
Transactional Data	AF2
Network Management	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF



2P6Q3T	
EF	PQ Level 1 (10%)
CS4 & CS5 AF4	PQ Level 2 (33%)
CS7 & CS6 CS3 & CS2	Q6 (BWR 12%)
AF3	Q4 (BWR 18% + DSCP-Based WTD)
AF2	Q3 (BWR 18% + DSCP-Based WTD)
AF1	Q2 (BWR 7% + DSCP-Based WTD)
CS1	Q2 (BWR 1%)
DF	Q1 (BWR 44%)

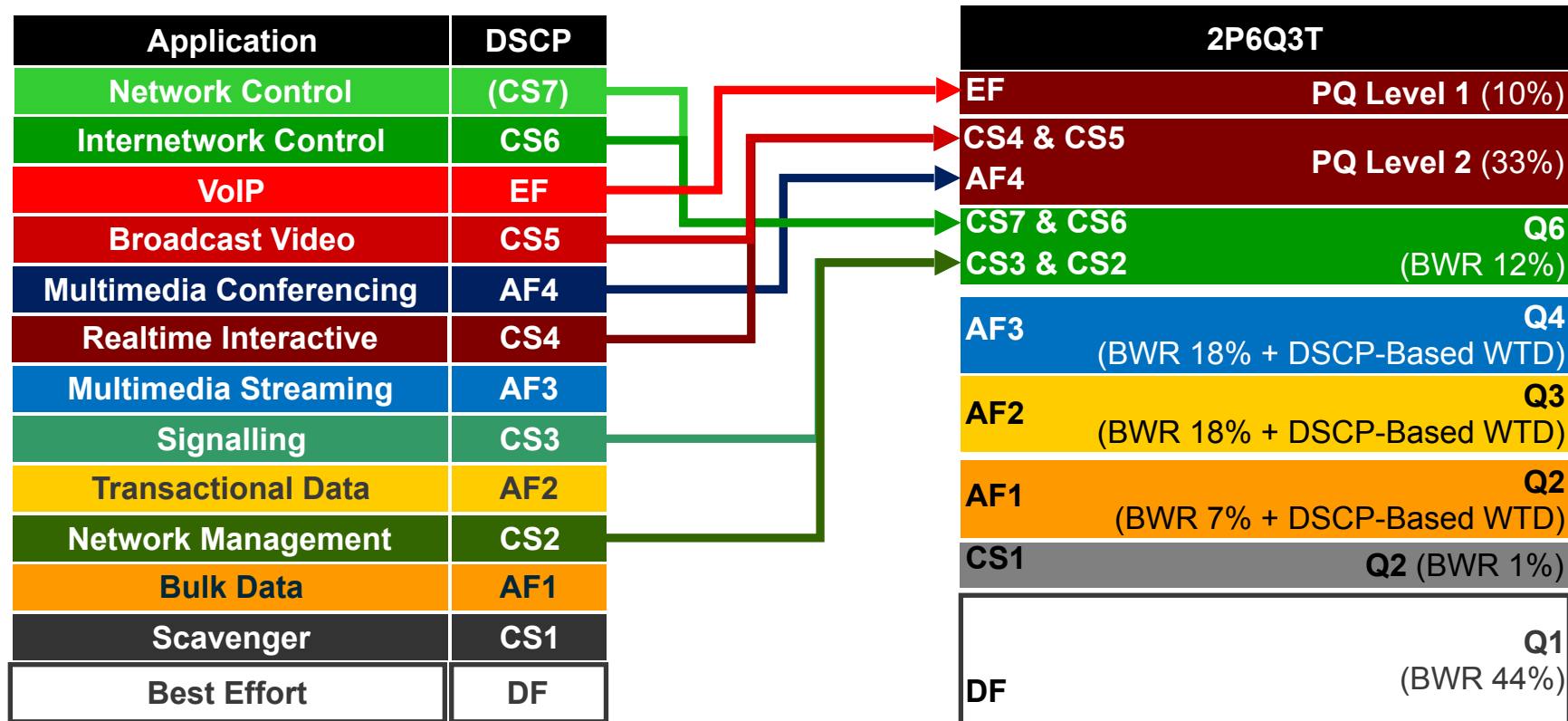
Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



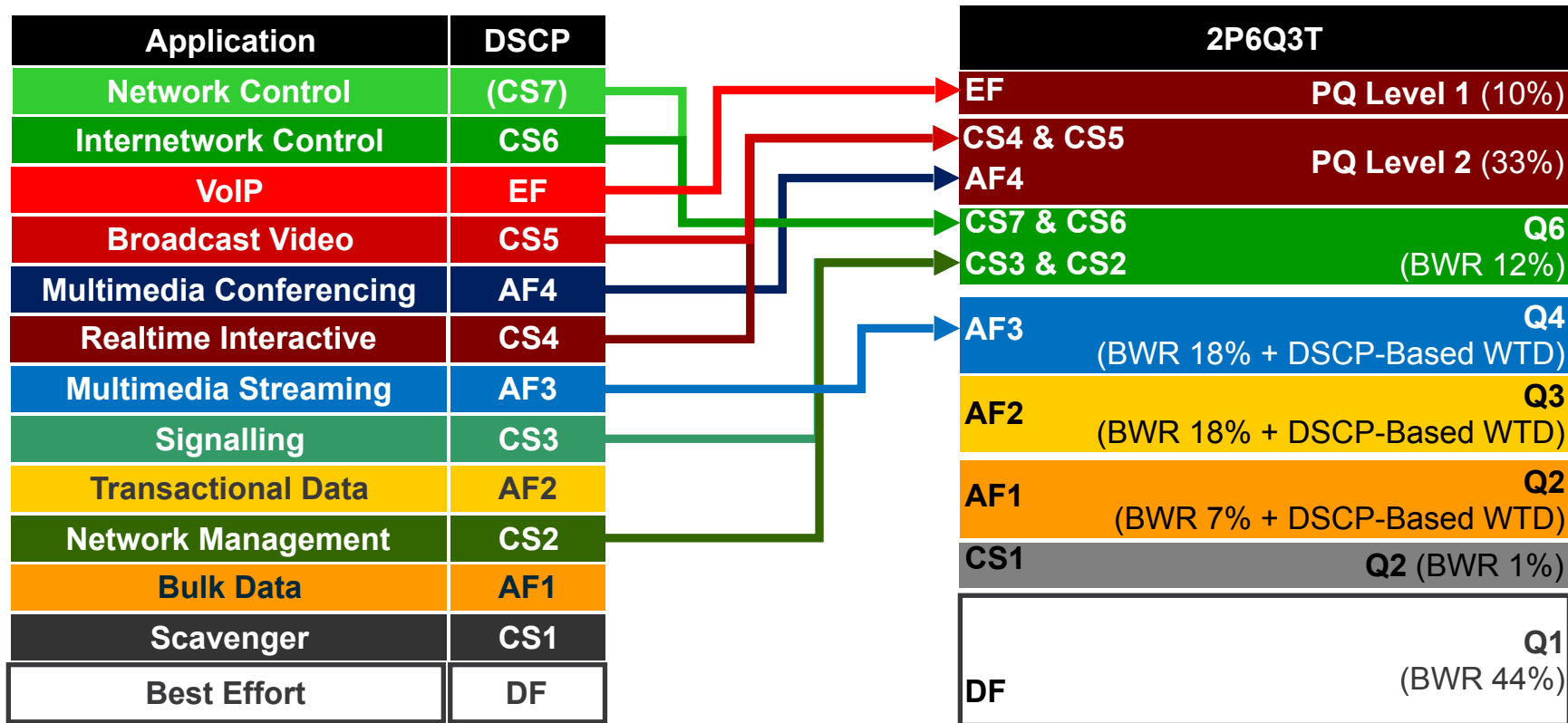
Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



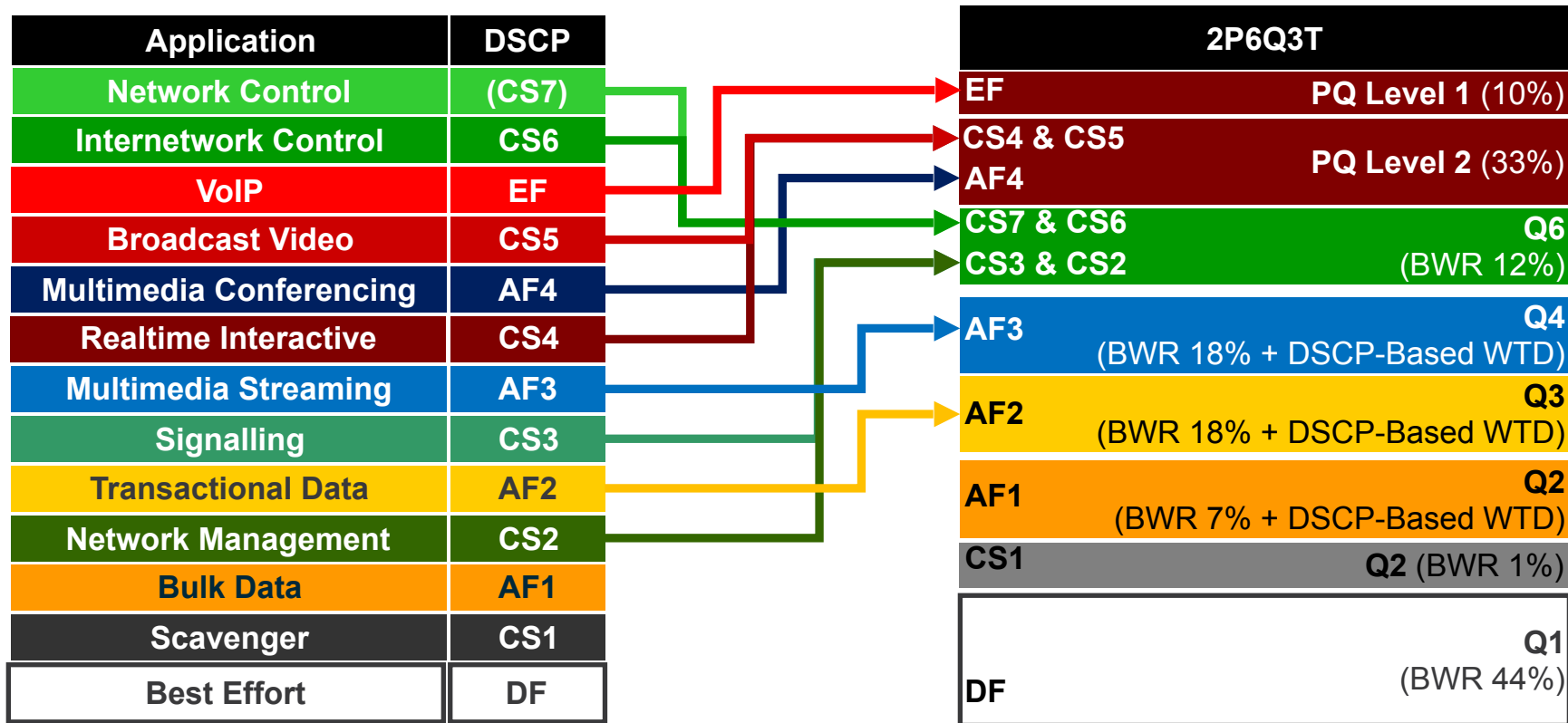
Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



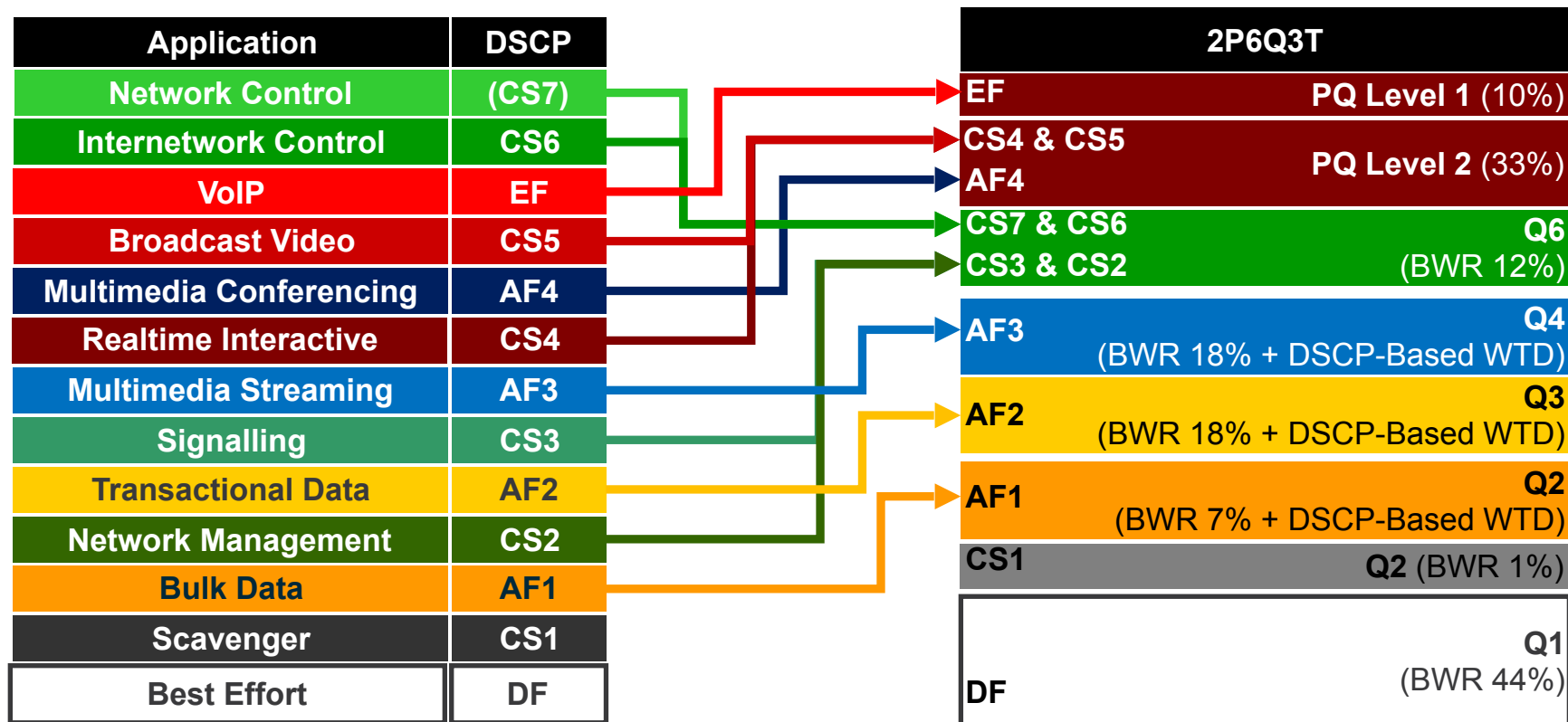
Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



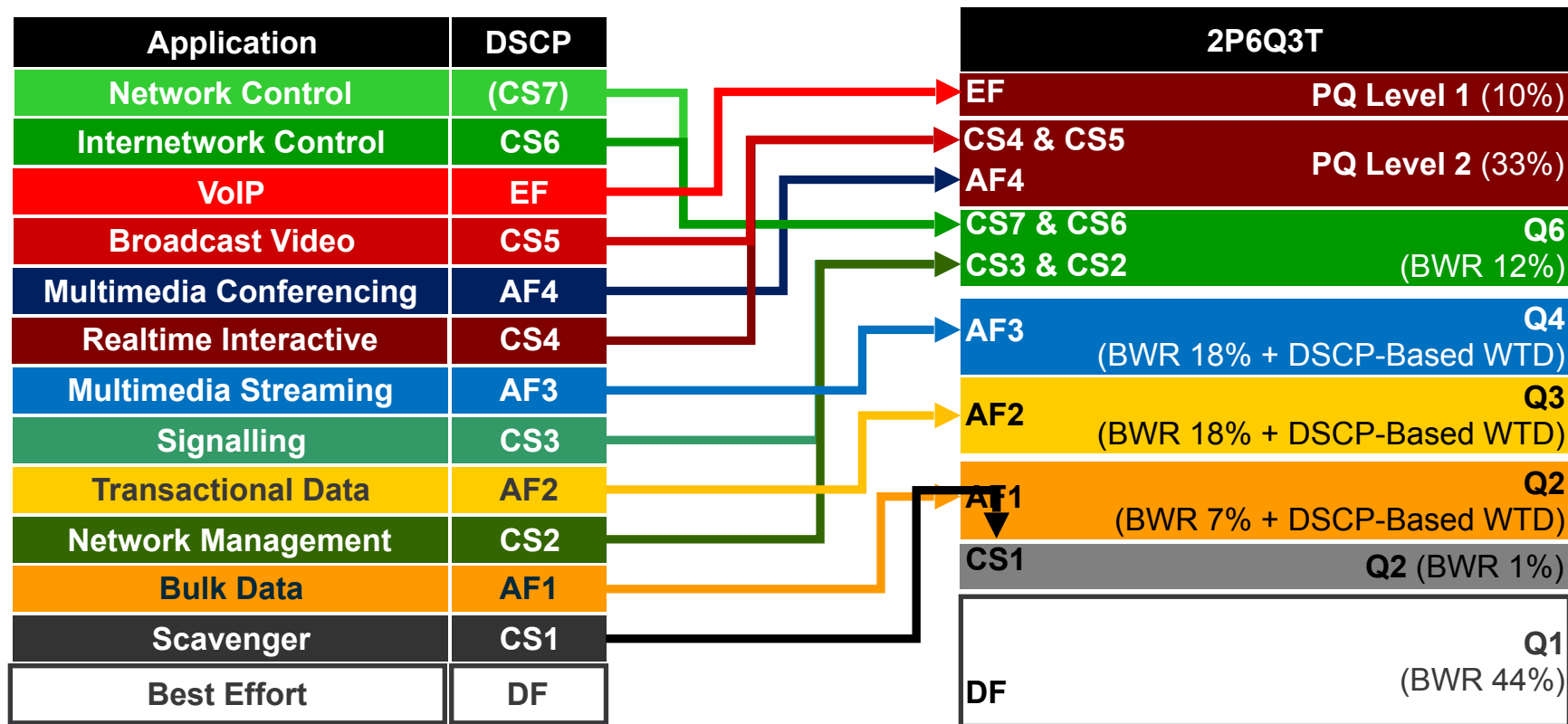
Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



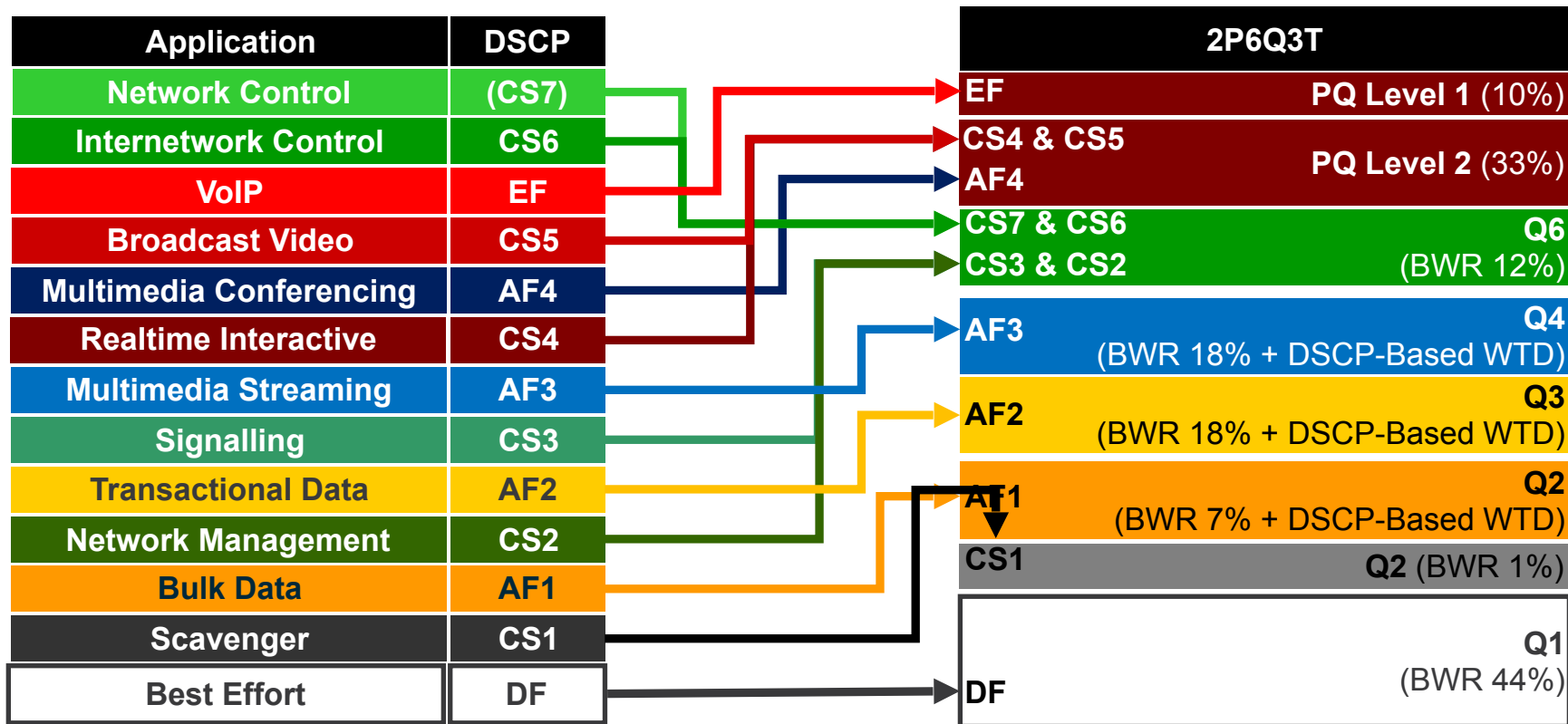
Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



Catalyst 3650/3850

2P6Q3T+WTD Wired Port Egress Queuing Config – Part 1 of 2

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

Catalyst 3650/3850

2P6Q3T+WTD Wired Port Egress Queuing Config – Part 2 of 2

```
policy-map 2P6Q3T
  class VOICE-PQ1
    priority level 1 percent 10
    queue-buffers ratio 5
  class VIDEO-PQ2
    priority level 2 percent 33
    queue-buffers ratio 5
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 12
    queue-buffers ratio 5
  class MULTIMEDIA-STREAMING-QUEUE
    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
```

...

[continued]

```
class TRANSACTIONAL-DATA-QUEUE
  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 BULK-DATA-QUEUE
  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 SCAVENGER-QUEUE
  bandwidth remaining percent 1
  queue-buffers ratio 5
class class-default
  bandwidth remaining percent 44
  queue-buffers ratio 40
```

Catalyst 3650/3850

2P6Q3T+WTD Wired Port Egress Queuing Config – Part 2 of 2

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

```
policy-map 2P6Q3T
class VOICE-PQ1
  priority level 1 percent 10
  queue-buffers ratio 5
class VIDEO-PQ2
  priority level 2 percent 33
  queue-buffers ratio 5
class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 12
  queue-buffers ratio 5
class MULTIMEDIA-STREAMING-QUEUE
  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
...
```

Two-levels of priority queuing are supported

[continued]

```
class TRANSACTIONAL-DATA-QUEUE
  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 BULK-DATA-QUEUE
  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 SCAVENGER-QUEUE
  bandwidth remaining percent 1
  queue-buffers ratio 5
class class-default
  bandwidth remaining percent 44
  queue-buffers ratio 40
```

Allocates buffers to queues

Tunes WTD to align to an AF PHB

Catalyst 3650/3850

2P6Q3T+WTD Wired Port Egress Queuing Config – Part 2 of 2

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

```
policy-map 2P6Q3T
class VOICE-PQ1
  priority level 1 percent 10
  queue-buffers ratio 5
class VIDEO-PQ2
  priority level 2 percent 33
  queue-buffers ratio 5
class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 12
  queue-buffers ratio 5
class MULTIMEDIA-STREAMING-QUEUE
  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
...
```

Two-levels of priority queuing are supported

[continued]

```
class TRANSACTIONAL-DATA-QUEUE
  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 BULK-DATA-QUEUE
  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 SCAVENGER-QUEUE
  bandwidth remaining percent 1
  queue-buffers ratio 5
class class-default
  bandwidth remaining percent 44
  queue-buffers ratio 40
```

Allocates buffers to queues

Tunes WTD to align to an AF PHB

```
interface range GigabitEthernet 1/0/1-48
  service-policy output 2P6Q3T
```

Catalyst 3650/3850

Hierarchical QoS Policies—Queuing within Shaped Rate Example

```
policy-map 50MBPS-SHAPER  
  class class-default  
    shape average 50000000  
    service-policy 2P6Q3T
```

Defines the sub-line rate (CIR)

```
interface GigabitEthernet 1/0/1  
  service-policy output 50MBPS-SHAPER
```

Provides back-pressure to the system to engage the (previously-defined) queuing policy, so that packets are properly prioritised within the sub-line rate

Only the Hierarchical Shaping policy is attached to the interface(s)

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



Cisco Catalyst 3650/3850 QoS Design

At-A-Glance

Role in Campus Network

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

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



QoS Design Steps

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

1. Configure Ingress QoS Model(s):
 - Trust DSCP Model
 - Conditional Trust Model (wired ports only)
 - Service Policy Models
2. Configure Egress Queuing
 - Wired Queuing Models: 1PQ3T or 2P6Q3T
 - Wireless Queuing Model: 2P2Q+AFD

Step 1: Configure Ingress QoS Model(s)

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

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

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

Trust DSCP Model

Wired ports on the Catalyst 3650/3850 default to a trusted state (shown as orange circles in Figure 1). Prior to IOS XE 3.3 SE wireless ports defaulted to an untrusted state. However, wireless ports could also be configured to be trusted by the global configuration command: `no qos wireless-default-untrust`.

Conditional Trust Model

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

This model is suitable for switch ports connecting to:

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

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

Service Policy Models

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

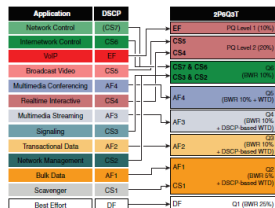
- **class-maps** which identify the flows using packet markings or by access-lists or other criteria. As of IOS XE 16.3 NBAR2 classification on wired ports is also supported.
- **policy-maps** which specify policy actions to be taken on a class-by-class basis
- **service-policy** statements which apply a specific policy-map to an interface(s) and specify direction

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

Step 2a: Configure Egress Queuing for Wired Ports

Wired ports can be configured with a 1PQ3T or 2P6Q3T egress queuing model. The only difference between the models is the number of priority queues configured with the **priority level 1** or **priority level 2** policy-map action commands.

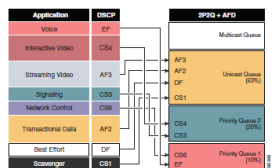
Figure 2 Catalyst 3650/3850 2P6Q3T (Wired Port) Egress Queuing Model



Step 2b: Configure Egress Queuing for Wireless Ports

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

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



Campus Cisco Catalyst 3650/3850 QoS Design

At-A-Glance

IOS XE 16.3 AVC / NBAR2 Policy Example

An example design for a Catalyst 3650/3850 series switch in the role of a converged access switch in a campus network are presented below.

Step 1: Configure Ingress QoS Model :

Trust DSCP Model:
Wired Ports : default
Wireless Ports : default since IOS XE 3.3 SE

Conditional Trust Model:

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

Service Policy Models(Wired):

```
class-map match-any VOICE
match protocol cisco-phone
match protocol cisco-jabber-audio
match protocol ms-lync-audio
match protocol citrix-audio
class-map match-any BROADCAST-VIDEO
match protocol cisco-ip-camera
class-map match-any REAL-TIME-INTERACTIVE
match protocol telepresence-media
class-map match-any CALL-SIGNALING
match protocol skinny
match protocol telepresence-control
class-map match-any TRANSACTIONAL-DATA
match protocol citrix
match protocol map
class-map match-any BULK-DATA
match protocol attribute category email
match protocol attribute category file-sharing
match protocol attribute sub-category backup-systems
class-map match-any SCAVENGER
match protocol attribute category gaming
match protocol attribute application-group skype-group
```

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

Wired Port Application:
interface GigabitEthernet 1/0/1
service-policy input NBAR-MARKING

Per-Wireless-Client Application:
wlan wlan-1
service-policy client input NBAR-MARKING

Step 2a: Configure 1PQ3T or 2P6Q3T Egress Queuing on Wired Ports (2P6Q3T Example is shown) :

```
policy-map 2P6Q3T
class VOICE-POL
priority level 1
police rate percent 10
conform-action transmit
exceed-action drop
class VIDEO-PQ2
priority level 2
police rate percent 20
class CONTROL-MGMT-QUEUE
bandwidth remaining percent 10
queue-buffers ratio 10
class MULTIMEDIA-CONFERENCING-QUEUE
bandwidth remaining percent 10
queue-buffers ratio 10
queue-limit dscp af43 percent 80
queue-limit dscp af42 percent 80
queue-limit dscp af41 percent 100
```

```
class MULTIMEDIA-STREAMING-QUEUE
bandwidth remaining percent 10
queue-buffers ratio 10
queue-limit dscp af33 percent 80
queue-limit dscp af32 percent 90
queue-limit dscp af31 percent 100
class TRANSACTIONAL-DATA-QUEUE
bandwidth remaining percent 10
queue-buffers ratio 10
queue-limit dscp af23 percent 80
queue-limit dscp af22 percent 90
queue-limit dscp af21 percent 100
class SCAVENGER-BULK-DATA-QUEUE
bandwidth remaining percent 5
queue-buffers ratio 10
queue-limit dscp values af13 csl percent 80
queue-limit dscp values af12 percent 100
class class-default
bandwidth remaining percent 25
queue-buffers ratio 25
```

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

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

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

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

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

Copyright © 2018 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

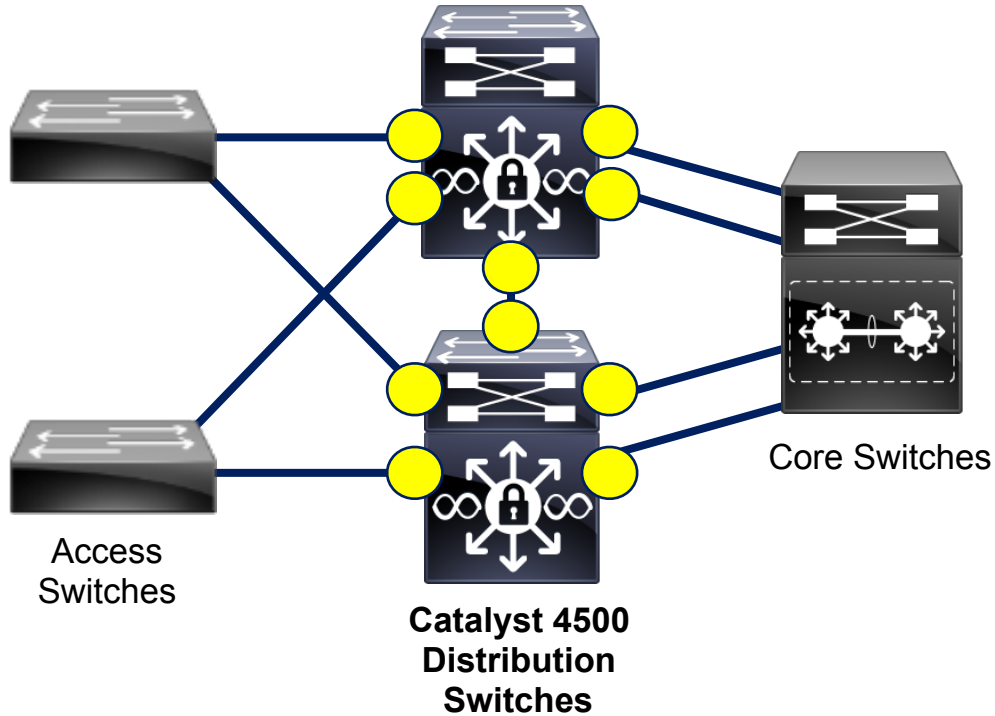
<https://cisco.box.com/v/QoS-AAGs>

Cisco live!

Catalyst 4500 QoS Design

Catalyst 4500

QoS Roles in the Campus Distribution



Catalyst 4500

QoS Design Steps

1. Configure Ingress QoS Model(s):

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

2. Configure Egress Queuing

***Note:** Catalyst 4500 uses IOS MQC, which trusts by default; therefore no explicit policy is required for DSCP trust

Catalyst 4500

Conditional Trust Example

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

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

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

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

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

Catalyst 4500

Part 1 of 2 – Marking & Policing Policy Example

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

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

Catalyst 4500

Part 2 of 2 – Marking & Policing Policy Example

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

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

Catalyst 4500

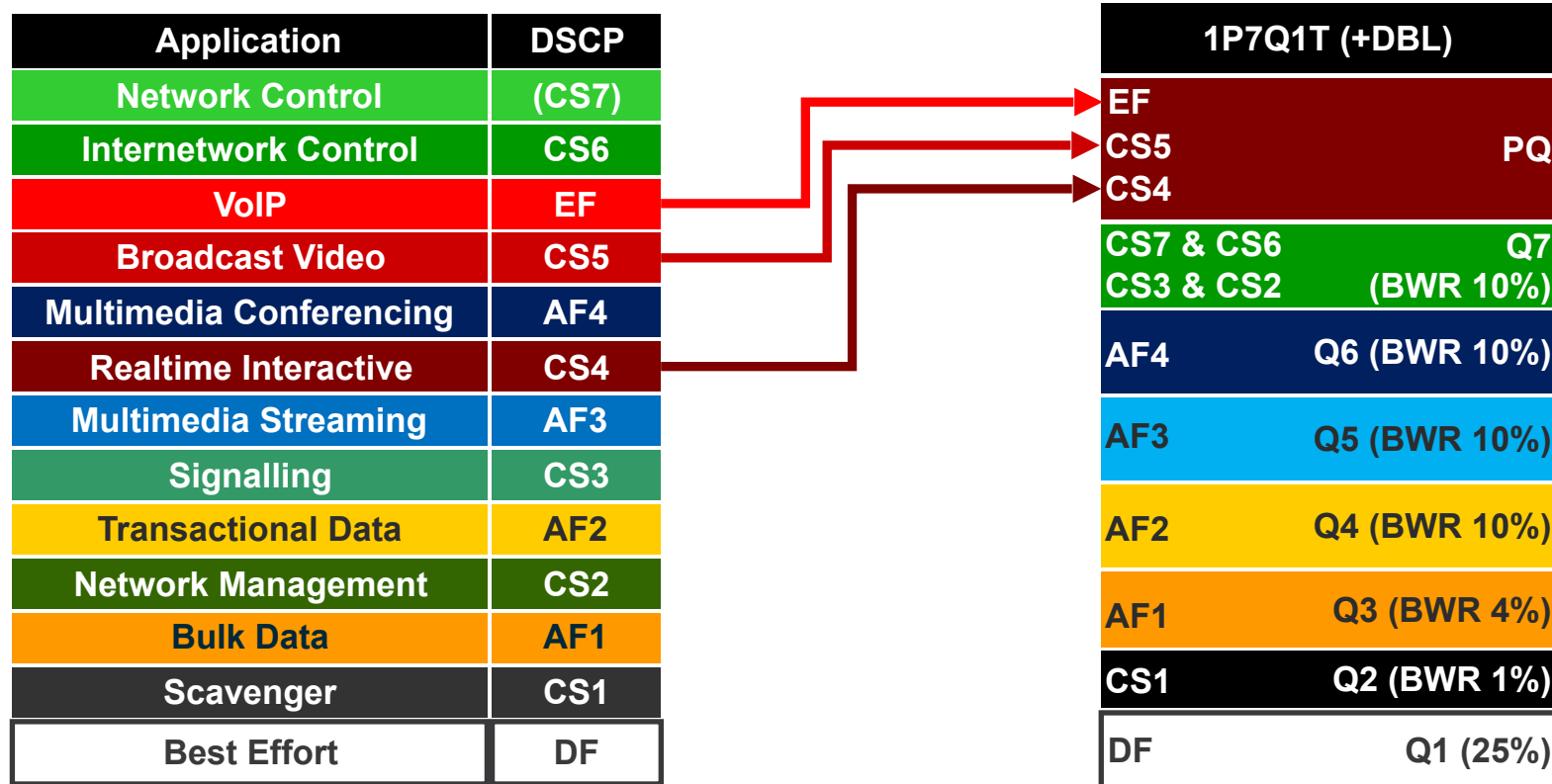
1P7Q1T+Dynamic Buffer Limiting (DBL) Egress Queuing Model

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

1P7Q1T (+DBL)	
EF CS5 CS4	PQ
CS7 & CS6 CS3 & CS2	Q7 (BWR 10%)
AF4	Q6 (BWR 10%)
AF3	Q5 (BWR 10%)
AF2	Q4 (BWR 10%)
AF1	Q3 (BWR 4%)
CS1	Q2 (BWR 1%)
DF	Q1 (25%)

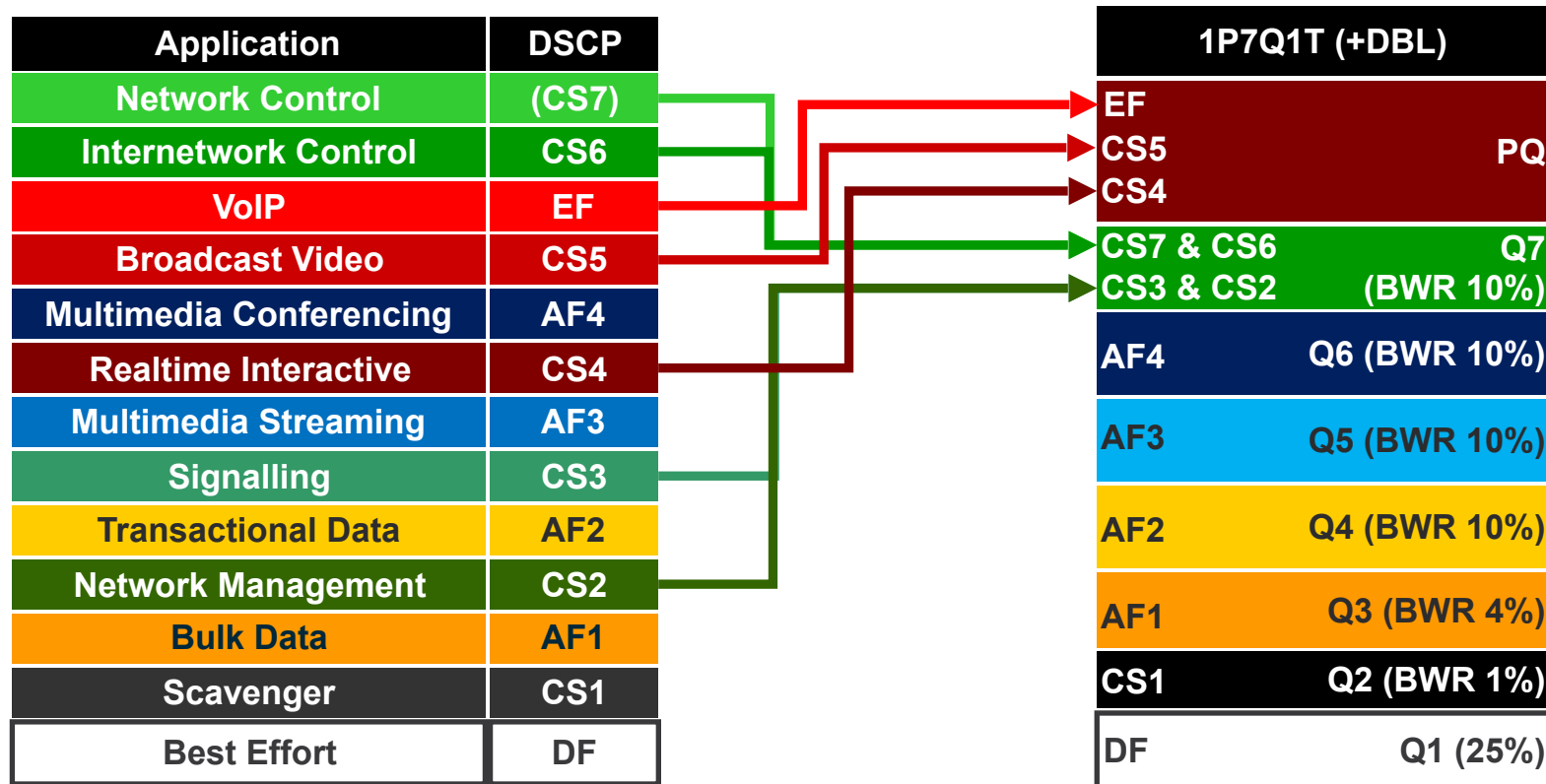
Catalyst 4500

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



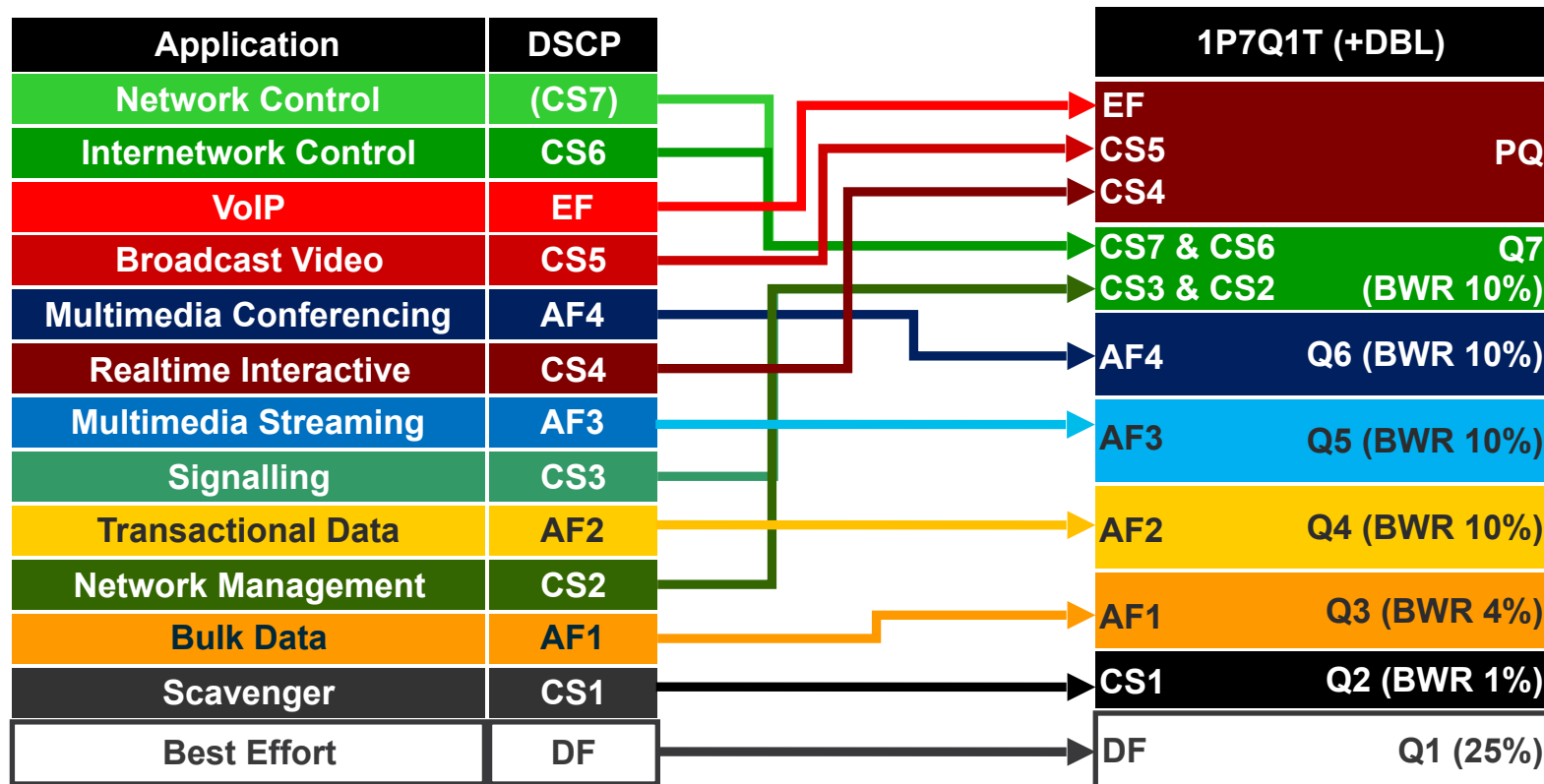
Catalyst 4500

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



Catalyst 4500

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



Catalyst 4500

1P7Q1T+DBL Egress Queuing Config

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

```
policy-map 1P7Q1T
  class PRIORITY-QUEUE
    priority
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 10
  class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    dbl
  class BULK-DATA-QUEUE
    bandwidth remaining percent 4
    dbl
  class SCAVENGER-QUEUE
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 25
    dbl
```

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

Catalyst 4500

1P7Q1T+DBL Egress Queuing Config

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

Enables the PQ

DBL can be enabled on a per-class basis,
but should not be enabled on the PQ or Control traffic queues

Enabling DBL on UDP-based queues and/or Scavenger queue
is optional

```
policy-map 1P7Q1T
  class PRIORITY-QUEUE
    priority
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 10
  class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 10
  class TRANSACTIONAL-DATA-QUEUE
    bandwidth remaining percent 10
    dbl
  class BULK-DATA-QUEUE
    bandwidth remaining percent 4
    dbl
  class SCAVENGER-QUEUE
    bandwidth remaining percent 1
  class class-default
    bandwidth remaining percent 25
    dbl
```

If PQ is enabled then
bandwidth remaining
must be used

service-policy output 1P7Q1T

Catalyst 4500 Campus QoS Design At-A-Glance



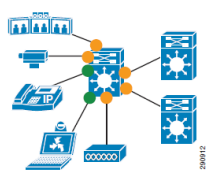
Cisco Catalyst 4500 (Supervisor 6-E / 7-E / 8-E) QoS Design

At-A-Glance

Role in Campus Network

The Cisco Catalyst 4500 series switches with Supervisor 6-E/7-E/8-E are well-suited to the role of access- or distribution-layer switches in campus networks. As such, these switches may connect directly to a variety of endpoints, as well as to distribution-layer and/or core-layer switches, as shown in Figure 1.

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



QoS Design Steps

There are only two main steps to configure QoS on a Cisco Catalyst 4500 series switch with Supervisor 6-E/7-E/8-E:

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

Step 1: Configure Ingress QoS Model(s)

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

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

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

Trust DSCP Model

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

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

Conditional Trust Model

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

This model is suitable for switch ports connecting to:

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

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

Service Policy Models

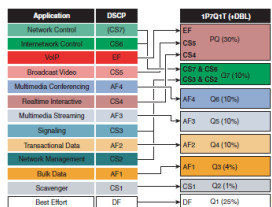
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC policies to implement classification, marking, and/or policing policies. These policies are constructed with:

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

Step 2: Configure Egress Queuing

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

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



EtherChannel QoS

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

Cisco Validated Design (CVD)

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

Step 1: Configure Ingress QoS Model:

Trust DSCP Model:

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

Conditional Trust Model:

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

policy-map CISCO-IPPHONE

```
class VOICE
set dscp ef
class SIGNALING
set dscp cs3
class class-default
set dscp default
```

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

Service Policy Models:

[class-maps omitted for brevity]

policy-map MARKING-POLICY

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

service-policy input MARKING-POLICY

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

Step 2: Egress Queuing Configuration

class-map match-any PRIORITY-QUEUE

```
match dscp ef
match dscp cs5
match dscp cs4
class-map match-any CONTROL-MGMT-QUEUE
match dscp cs7
match dscp cs6
match dscp cs3
match dscp cs2
```

class-map match-all MULTIMEDIA-CONFERENCING-QUEUE

```
match dscp af41 af42 af43
```

class-map match-all MULTIMEDIA-STREAMING-QUEUE

```
match dscp af31 af32 af33
```

class-map match-all TRANSACTIONAL-DATA-QUEUE

```
match dscp af21 af22 af23
```

class-map match-all BULK-DATA-QUEUE

```
match dscp af11 af12 af13
```

class-map match-all SCAVENGER-QUEUE

```
match dscp cs1
```

policy-map EGRESS-QUEUING

```
class PRIORITY-QUEUE
```

```
priority
```

```
class CONTROL-MGMT-QUEUE
```

```
bandwidth remaining percent 10
```

```
class MULTIMEDIA-CONFERENCING-QUEUE
```

```
bandwidth remaining percent 10
```

```
class MULTIMEDIA-STREAMING-QUEUE
```

```
bandwidth remaining percent 10
```

```
class TRANSACTIONAL-DATA-QUEUE
```

```
bandwidth remaining percent 10
```

```
class BULK-DATA-QUEUE
```

```
bandwidth remaining percent 4
```

```
class SCAVENGER-QUEUE
```

```
bandwidth remaining percent 1
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

```
class class-default
```

```
bandwidth remaining percent 25
```

- Assigns VoIP (EF) Broadcast Video (CS5) and Realtime Interactive (CS4) to the PRIORITY-QUEUE
- Assigns Network Control (CS7), Internetwork Control (CS6), Signaling (CS3) and Management (CS2) to the CONTROL-MGMT-QUEUE
- Assigns AF4 to the MULTIMEDIA-CONFERENCING-QUEUE
- Assigns AF3 to the MULTIMEDIA-STREAMING-QUEUE
- Assigns AF2 to the TRANSACTIONAL-DATA-QUEUE
- Assigns AF1 to the BULK-DATA-QUEUE
- Assigns CS1 to the SCAVENGER-QUEUE
- PRIORITY-QUEUE gets strict priority servicing (All other queues get percentages of bandwidth remaining after the PQ has been fully serviced)
- CONTROL-MGMT-QUEUE gets 10% of remaining bandwidth
- MM-CONF-QUEUE gets 10% of remaining bandwidth
- MM-STREAMING-QUEUE gets 10% of remaining bandwidth
- TRANS-DATA-QUEUE gets 10% of remaining bandwidth and Dynamic Buffer Limiting
- BULK-DATA-QUEUE gets 4% of remaining bandwidth and Dynamic Buffer Limiting
- SCAVENGER-QUEUE is limited to 1% of remaining bandwidth
- Default (Best-Effort) queue 25% of remaining bandwidth and Dynamic Buffer Limiting
- Applies EGRESS-QUEUING policy to interface



End-to-End QoS Network Design
Quality of Service for Network Design
Cisco Press

For more details, see Campus QoS Design 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN/MAN/QoS_SRND_40/QoS_Campus_40.html
And the Cisco Press Book: End-to-End QoS Network Design (Second Edition)-Chapter 15

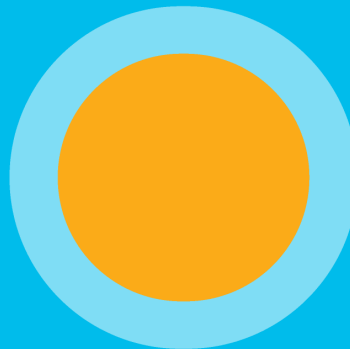
Copyright © 2013 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

<https://cisco.box.com/v/QoS-AAGs>

Cisco live!

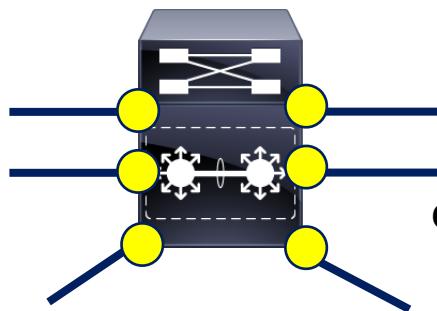
Catalyst 6500/6800

QoS Design



Cisco Catalyst 6500/6800

QoS Roles in the Campus Core



**Catalyst 6500/6800
Core Switches**

- Trust DSCP
 - + Ingress Queuing
 - + Egress Queuing

Cisco Catalyst 6500/6800

QoS Design Steps

1. Configure Ingress Queuing-
2. Configure Egress Queuing

Catalyst 6500 IOS C3PL trusts by default;
therefore no explicit policy is required for DSCP trust

Cisco Catalyst 6500/6800

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

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

2P6Q4T	
EF	Voice-PQ1 (Priority Level 1)
CS5 CS4	Video-PQ2 (Priority Level 2)
CS6 & CS7 CS2 & CS3	Control/Mgmt Queue (5% BWR)
AF4	Multimedia-Conferencing Queue (20% BWR + DSCP-WRED)
AF3	Multimedia-Streaming Queue (20% BWR + DSCP-WRED)
AF2	Transactional Data Queue (10% BWR + DSCP-WRED)
AF1 CS1	Bulk Data Queue (5% BWR + DSCP-WRED)
DF	Default Queue (WRED)

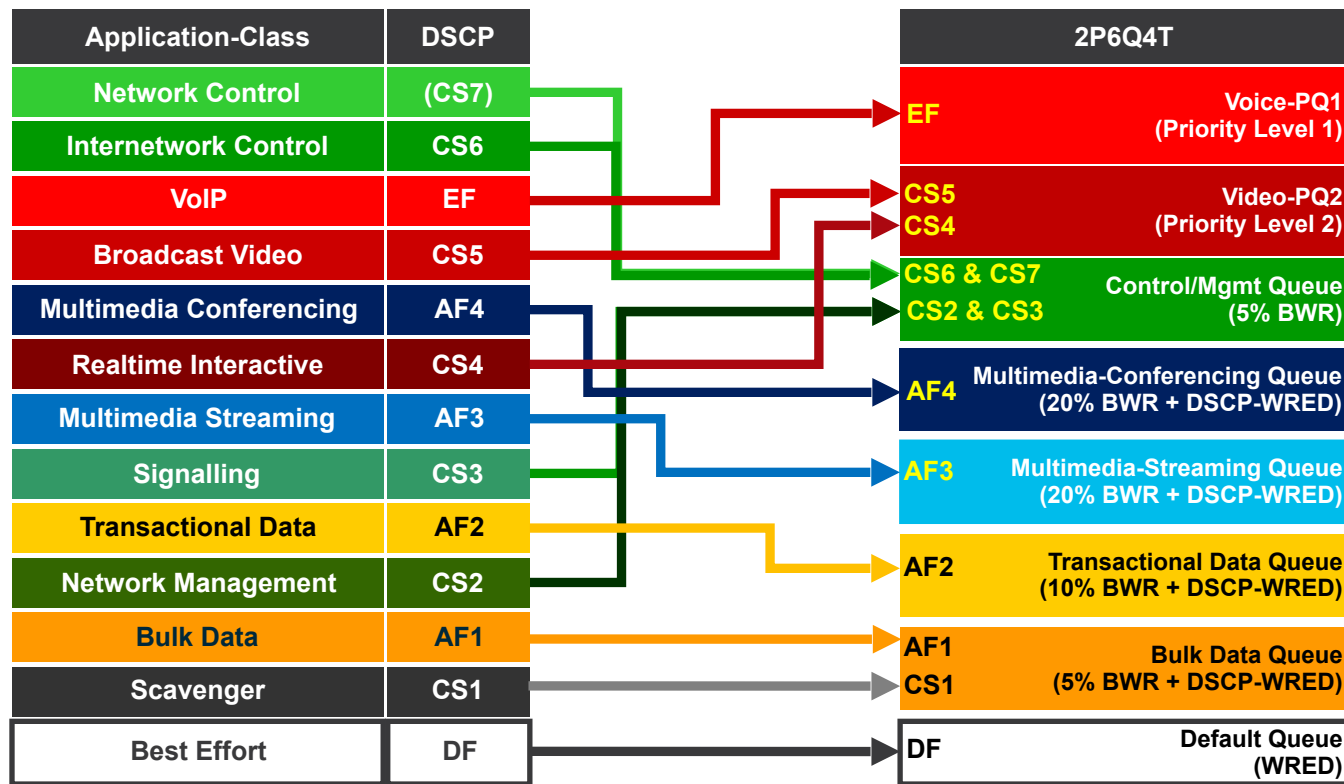
Ingress and Egress queuing models varies by line card/module.

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

Cisco Catalyst 6500/6800

All Catalyst 6500-Sup2T Queuing Models are detailed in the Appendix

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



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

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

Cisco Catalyst 6500/6800—2P6Q4T Model

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

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

Note: A C3PL interface may support up to 4 QoS policies:

- service-policy type qos input
- service-policy type qos output
- service-policy type lan-queuing input
- service-policy type lan-queuing output

Cisco Catalyst 6500/6800—2P6Q4T Model

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

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

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

Note: A C3PL interface may support up to 4 QoS policies:

- service-policy type qos input
- service-policy type qos output
- service-policy type lan-queuing input
- service-policy type lan-queuing output

Cisco Catalyst 6500/6800—2P6Q4T Model

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

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

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

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

Note: A C3PL interface may support up to 4 QoS policies:

- service-policy type qos input
- service-policy type qos output
- service-policy type lan-queuing input
- service-policy type lan-queuing output

Cisco Catalyst 6500/6800—2P6Q4T Model

Part 2 of 3—2P6Q4T Queuing Policy-Map

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

```
policy-map type lan-queuing 2P6Q4T
  class VOICE-PQ1
    priority level 1
  class VIDEO-PQ2
    priority level 2
  class CONTROL-MGMT-QUEUE
    bandwidth remaining percent 5
  class MULTIMEDIA-CONFERENCING-QUEUE
    bandwidth remaining percent 20
    random-detect dscp af41 percent 80 100
    random-detect dscp af42 percent 70 100
    random-detect dscp af43 percent 60 100
  class MULTIMEDIA-STREAMING-QUEUE
    bandwidth remaining percent 20
    random-detect dscp af31 percent 80 100
    random-detect dscp af32 percent 70 100
    random-detect dscp af33 percent 60 100
  ...
```

Enables egress Priority Queue 1 (highest level of service)

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

bandwidth remaining is required
(as PQ is enabled)

Tunes WRED to better align to
the AF PHB

Cisco Catalyst 6500/6800—2P6Q4T Model

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

[continued]

```
class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect dscp af21 percent 80 100
  random-detect dscp af22 percent 70 100
  random-detect dscp af23 percent 60 100
class BULK-DATA-QUEUE
  bandwidth remaining percent 5
  random-detect dscp-based
  random-detect dscp af11 percent 80 100
  random-detect dscp af12 percent 70 100
  random-detect dscp cs1 percent 50 100
class class-default
  random-detect dscp-based
  random-detect dscp default percent 80 100
```

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

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

Cisco Catalyst 6500 QoS Design At-A-Glance



Cisco Catalyst 6500 (Supervisor 2T) QoS Design

At-A-Glance

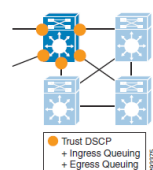
Campus Cisco Catalyst 6500 Supervisor 2T QoS Design

At-A-Glance

Role in Campus Network

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

Figure 1 Cisco Catalyst 6500 Supervisor 2T Switches in a Campus Network



QoS Design Steps

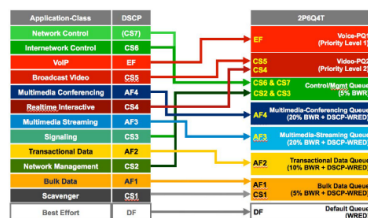
There are two main steps to configure QoS on Cisco Catalyst 6500 series switches with Supervisor 2T:

1. Configure Ingress Queuing
2. Configure Egress Queuing

Steps 1 & 2: Configure Ingress & Egress Queuing:

The 2P6Q4T queuing model for both ingress and egress queuing for the Cisco Catalyst 6500 with Supervisor 2T is shown in Figure 2.

Figure 2 Catalyst 6500 Sup2T (2P6Q4T) Ingress and Egress Queuing Model



EtherChannel QoS

Ingress classification and marking QoS policies on the Cisco Catalyst 6500 are configured on the logical Port-Channel interface (typically these are simply to enable DSCP trust, which is enabled by default on the Sup2T). Ingress and egress queuing QoS policies are configured on the physical port-member interfaces.

Cisco Validated Design (CVD)

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

```
Step 1: Configure (Common) Class-Maps to be used for both Ingress & Egress Queuing Policies
class-map type lan-queuing VOICE-PQ1
match dscp ef
class-map type lan-queuing VIDEO-PQ2
match dscp cs4 cs5
class-map type lan-queuing CONTROL-MGMT-QUEUE
match dscp cs2 cs3 cs6 cs7
class-map type lan-queuing MULTIMEDIA-CONFERENCING-QUEUE
match dscp af41 af42 af43
class-map type lan-queuing MULTIMEDIA-STREAMING-QUEUE
match dscp af31 af32 af33
class-map type lan-queuing TRANSACTIONAL-DATA-QUEUE
match dscp af21 af22 af23
class-map type lan-queuing SCAVENGER-BULK-DATA-QUEUE
match dscp cs1 af11 af12 af13
```

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

```
policy-map type lan-queuing 2P6Q4T
class VOICE-PQ1
priority level 1
class VIDEO-PQ2
priority level 2
class CONTROL-MGMT-QUEUE
bandwidth remaining percent 5
class MULTIMEDIA-CONFERENCING-QUEUE
bandwidth remaining percent 20
random-detect dscp af41 percent 80 100
random-detect dscp af42 percent 70 100
random-detect dscp af43 percent 60 100
class MULTIMEDIA-STREAMING-QUEUE
bandwidth remaining percent 20
random-detect dscp af31 percent 80 100
random-detect dscp af32 percent 70 100
random-detect dscp af33 percent 60 100
class TRANSACTIONAL-DATA-QUEUE
bandwidth remaining percent 10
random-detect dscp-based
random-detect dscp af21 percent 80 100
random-detect dscp af22 percent 70 100
random-detect dscp af23 percent 60 100
class BULK-DATA-QUEUE
bandwidth remaining percent 5
random-detect dscp-based
random-detect dscp af11 percent 80 100
random-detect dscp af12 percent 70 100
random-detect dscp cs1 percent 50 100
class class-default
random-detect dscp-based
random-detect dscp default percent 80 100
```

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

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

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

For more details, see Campus QoS Design 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoS_Campus_40.html

<https://cisco.box.com/v/QoS-AAGs>



Campus QoS Design

Key Takeaways

- Start by defining your QoS Strategy
- Campus QoS is needed primarily to control packet drops
- Know your QoS toolset, as this varies platform-to-platform
- Cisco provides many At-A-Glance guides to get you up and running quickly
- Cisco also provides Cisco Validated Design guides for more detail

Agenda

- Introduction to Strategic QoS Design
- WAN / IWAN QoS Design
- Campus QoS Design
- **WLAN QoS Design**
- Automating and Assuring QoS
- Summary and References
- Appendices

WLAN QoS Design

The Case for Wireless QoS

The Case for Wireless QoS

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

enterp



The Case for Wireless QoS

- QoS is like a chain
 - It's only as strong as its weakest link
- the WLAN is one of the weakest links in QoS designs for three primary reasons:
 - 1) Typical downshift in speed (and throughput)
 - 2) Shift from full-duplex to half-duplex media
 - 3) Shift from a dedicated media to a shared media



The Case for Wireless QoS

- QoS is like a chain
 - It's only as strong as its weakest link
- the WLAN is one of the weakest links in QoS designs for three primary reasons:
 - 1) Typical downshift in speed (and throughput)
 - 2) Shift from full-duplex to half-duplex media
 - 3) Shift from a dedicated media to a shared media
- WLAN QoS policies control **both** jitter and packet loss



enterp



Wireless QoS-Specific Limitations

Wireless QoS-Specific Limitations

- No priority servicing



Wireless QoS-Specific Limitations

- No priority servicing
- No bandwidth guarantees



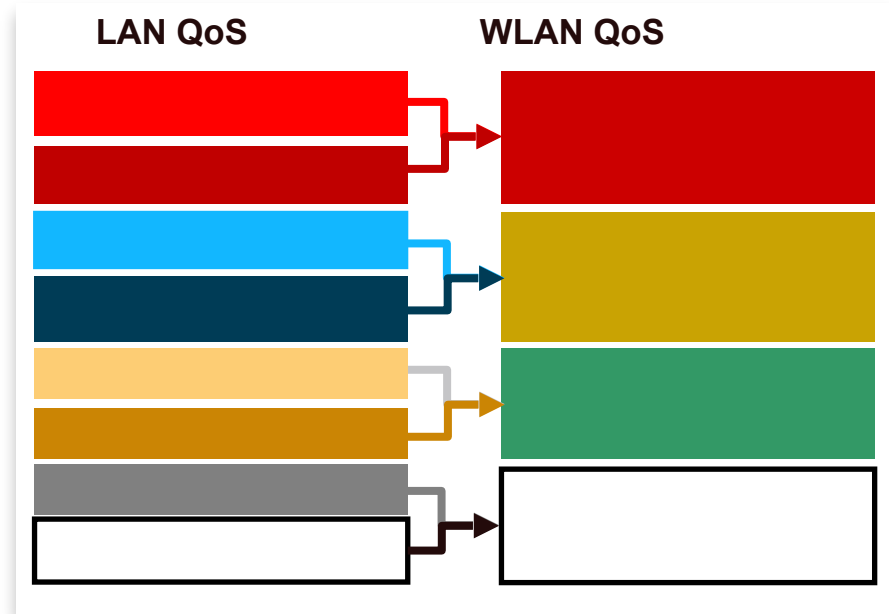
Wireless QoS-Specific Limitations

- No priority servicing
- No bandwidth guarantees
- Non-deterministic media access



Wireless QoS-Specific Limitations

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



WLAN QoS Improvements Quantified

Application	Original Metric	Improved Metric	Percentage Improvement
Voice	15 ms max jitter	5 ms max jitter	300%
	3.92 MOS (Cellular Quality)	4.2 MOS (Toll Quality)	
Video	9 fps	14 fps	55%
	Visual MOS: Good	Visual MOS: Excellent	
Transactional Data	14 ms latency	2 ms latency	700%

http://www.cisco.com/en/US/prod/collateral/wireless/cisco_avc_application_improvement.pdf

Know Your Tools

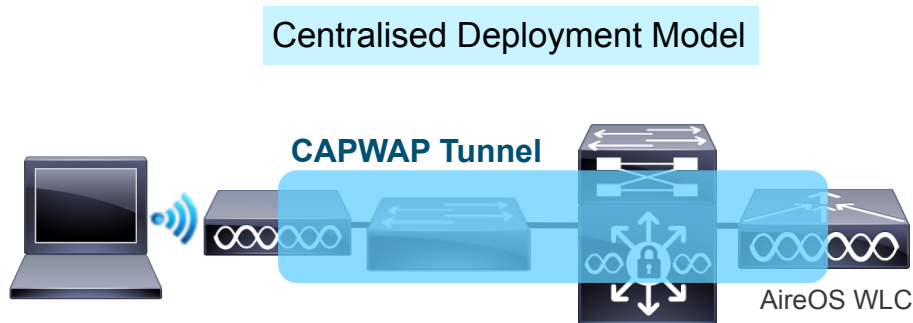
- Trust Boundaries and PEPs
- Wi-Fi OTA Access and Queuing
- Maintaining Access (EDCA)
- Bandwidth Control
- AVC
- Marking and Mapping



Cisco AireOS WLC

QoS Roles in the Wireless LAN

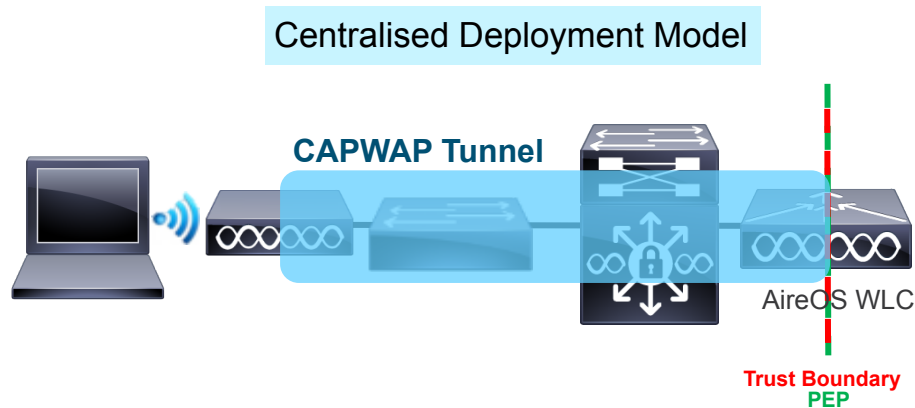
- AireOS WLCs are deployed in a Centralised Deployment Model, where:
 - Trust Boundary is at the WLC
 - PEP is at the WLC



Cisco AireOS WLC

QoS Roles in the Wireless LAN

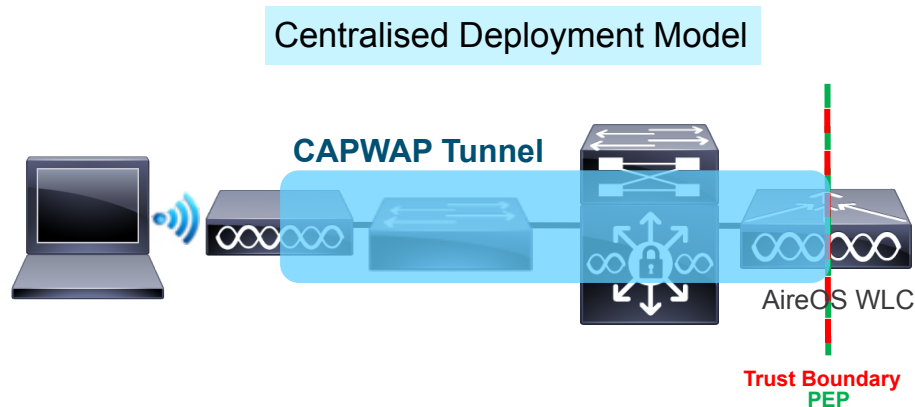
- AireOS WLCs are deployed in a Centralised Deployment Model, where:
 - Trust Boundary is at the WLC
 - PEP is at the WLC



Cisco AireOS WLC

QoS Roles in the Wireless LAN **(Introduced in AireOS 8.1MR)**

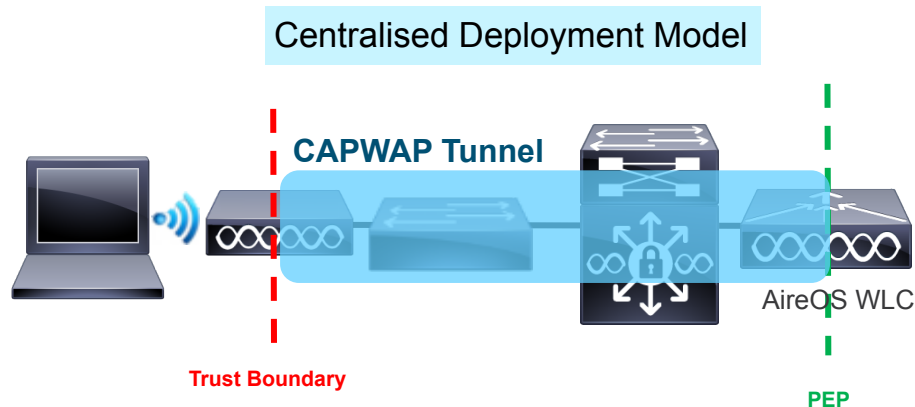
- Customisable DSCP $\leftrightarrow$ UP Mappings will modify QoS Roles:
 - Trust Boundary moves to the AP
 - PEP remains at the WLC



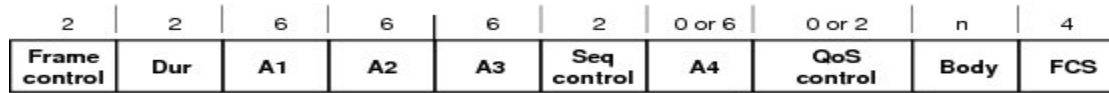
Cisco AireOS WLC

QoS Roles in the Wireless LAN **(Introduced in AireOS 8.1MR)**

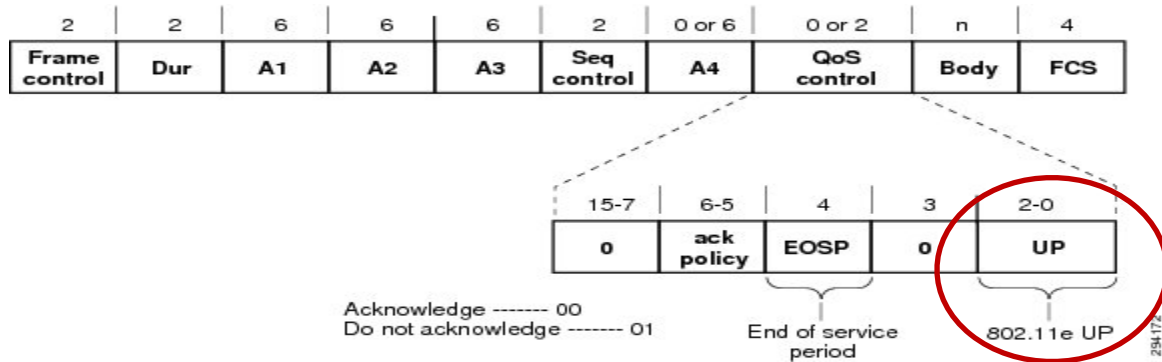
- Customisable DSCP $\leftrightarrow$ UP Mappings will modify QoS Roles:
 - Trust Boundary moves to the AP
 - PEP remains at the WLC



IEEE 802.11 User Priority (UP)



IEEE 802.11 User Priority (UP)



3 Bit Field allows for UP values 0-7

IEEE 802.11 UP Values and Access Categories

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

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



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

- due to the nature of wireless as a shared media, a Congestion Avoidance algorithm (CSMA/CA) must be utilised



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

- due to the nature of wireless as a shared media, a Congestion Avoidance algorithm (CSMA/CA) must be utilised
- wireless senders have to wait a **fixed amount of time** (the AIFS)

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



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

- due to the nature of wireless as a shared media, a Congestion Avoidance algorithm (CSMA/CA) must be utilised
- wireless senders have to wait a **fixed amount of time** (the AIFS)
- wireless senders also have to wait a **random amount of time** (the Contention Window)

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

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

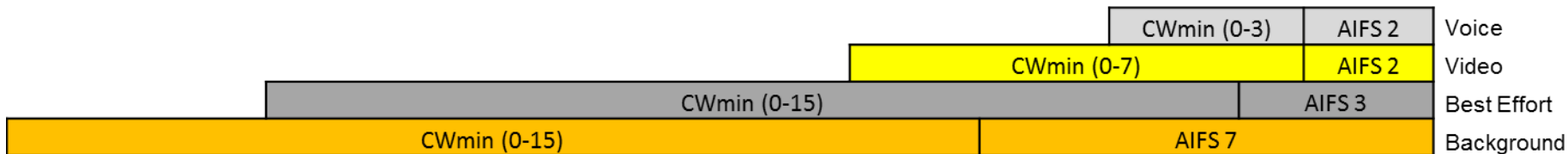


IEEE 802.11 Arbitration Inter-Frame Spacing (AIFS) and Contention Windows (CW)

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

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

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



EDCF Operation

EDCF Operation

Round 1

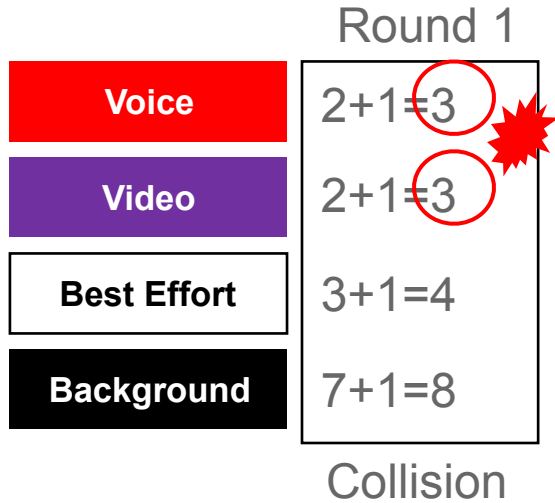
Voice

Video

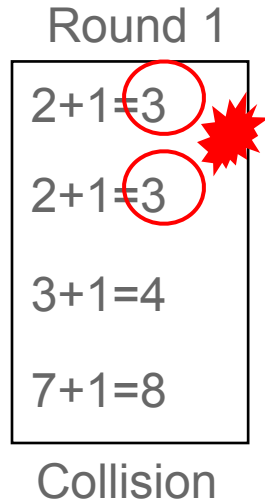
Best Effort

Background

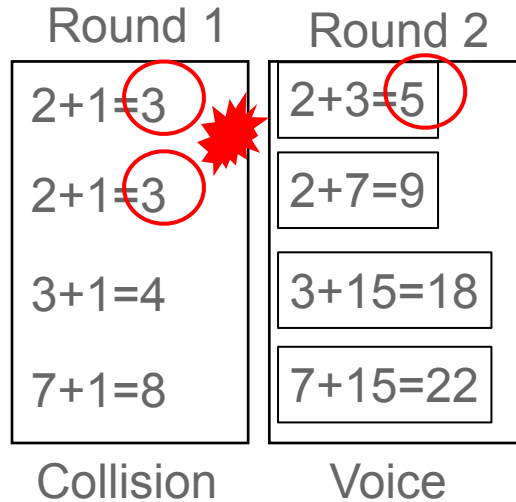
EDCF Operation



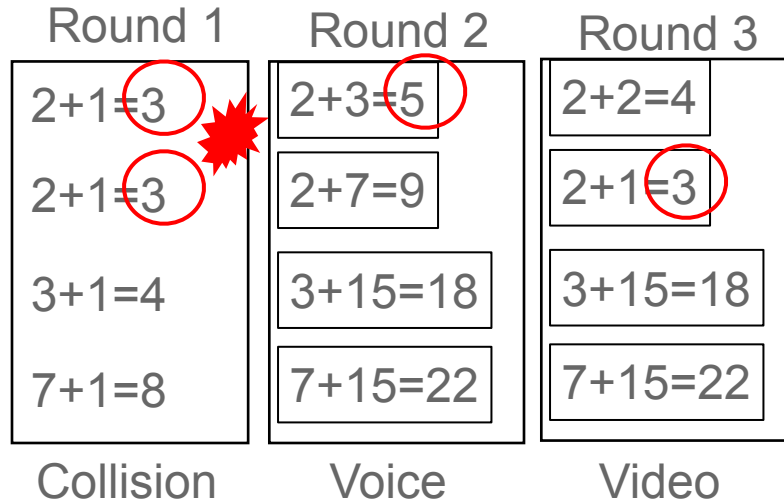
EDCF Operation



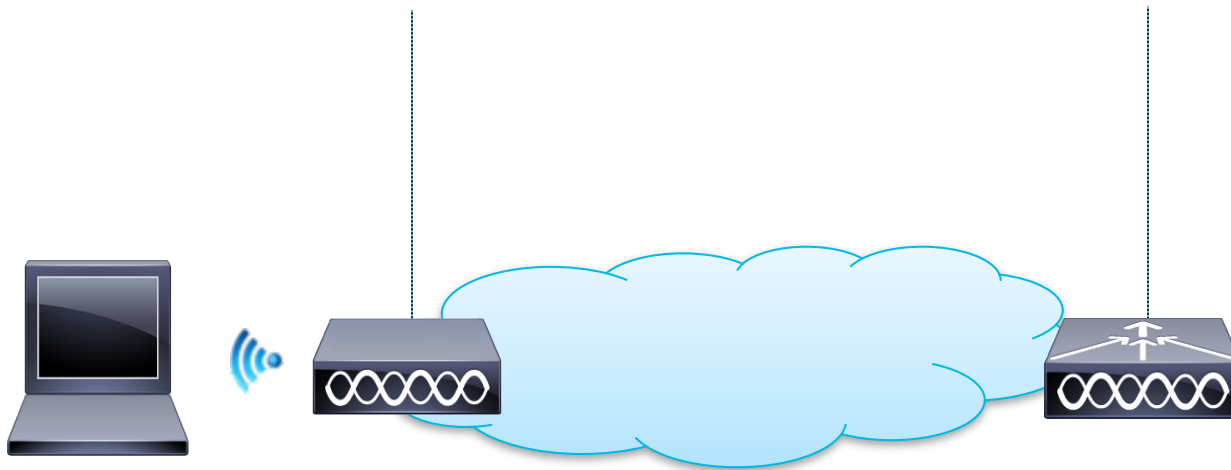
EDCF Operation



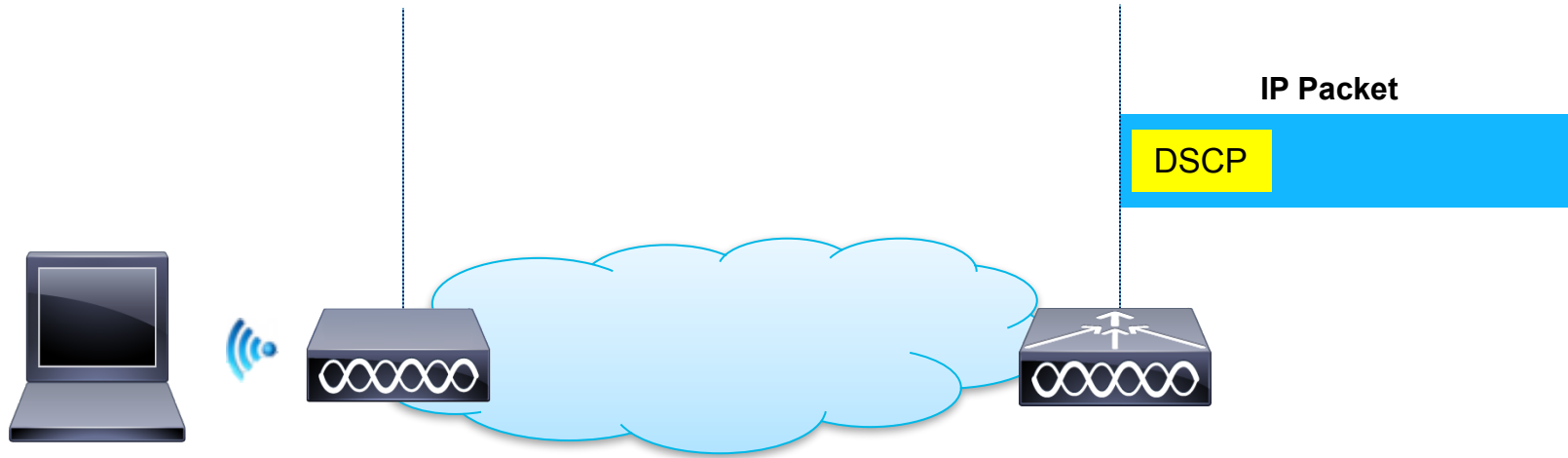
EDCF Operation



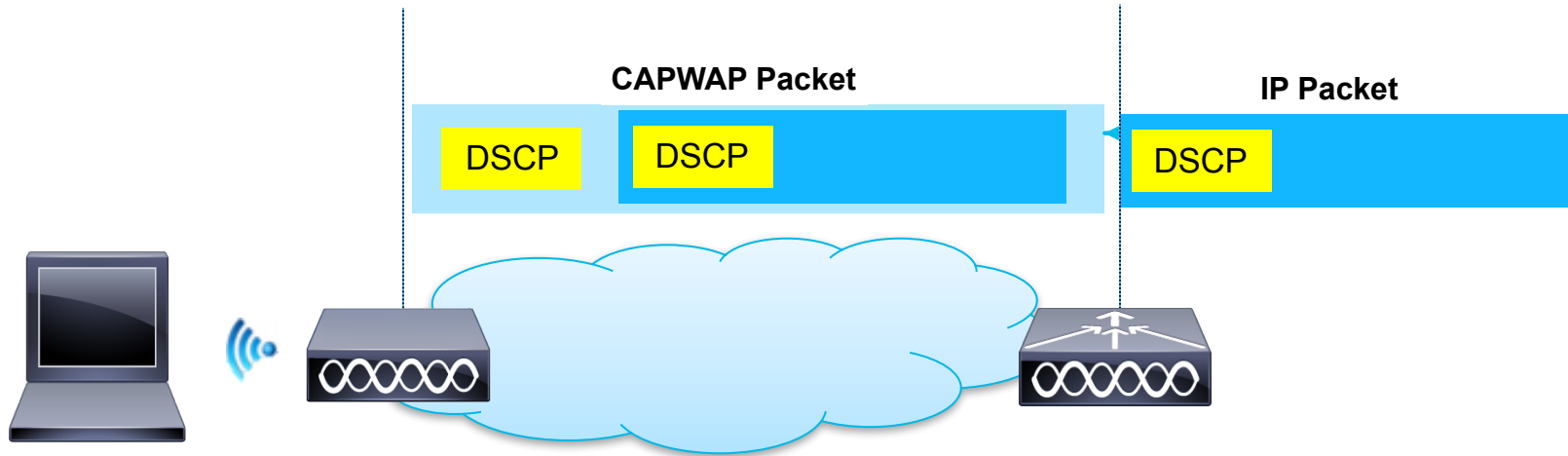
Downstream DSCP-to-UP Default Mapping



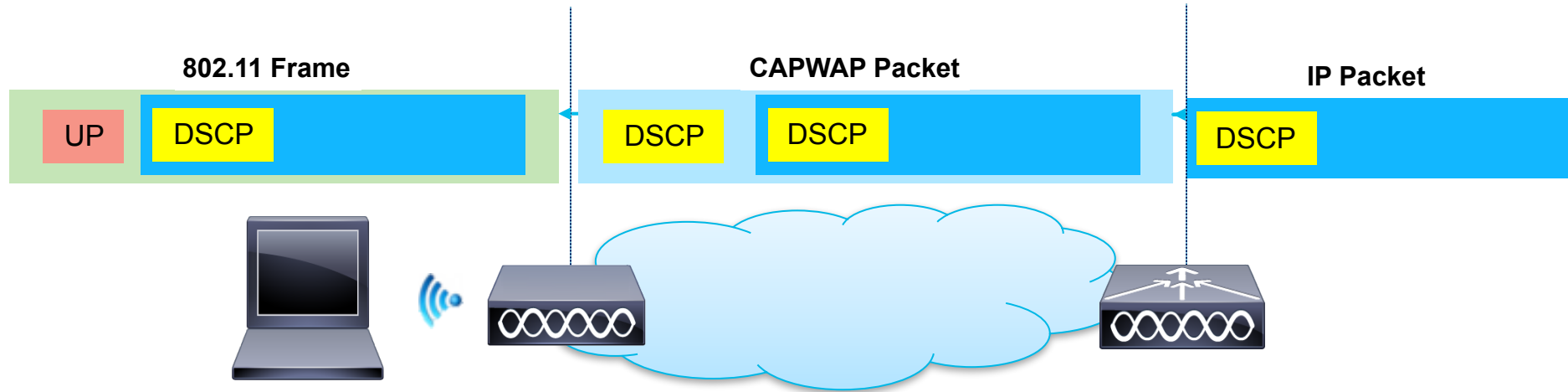
Downstream DSCP-to-UP Default Mapping



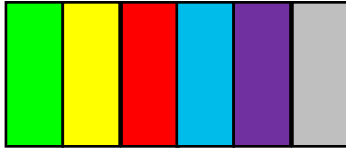
Downstream DSCP-to-UP Default Mapping



Downstream DSCP-to-UP Default Mapping



Downstream DSCP-to-UP Default Mapping

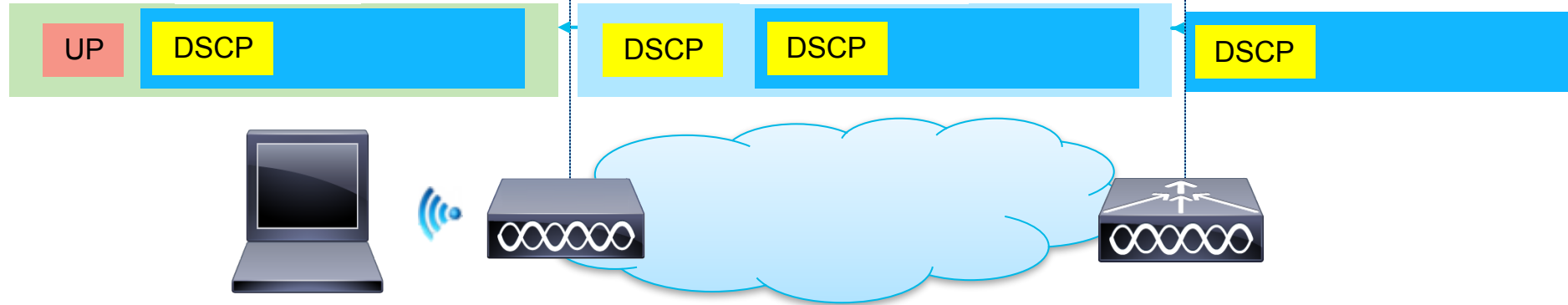


6-Bit DSCP

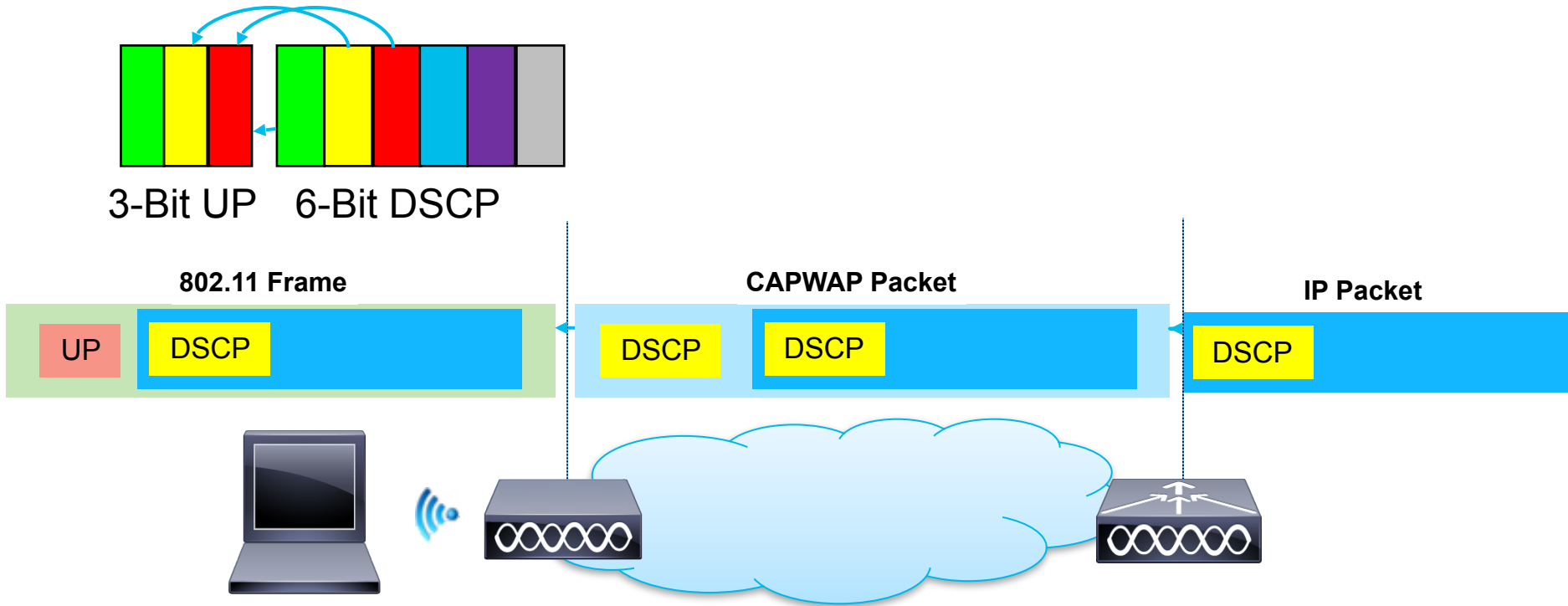
802.11 Frame

CAPWAP Packet

IP Packet



Downstream DSCP-to-UP Default Mapping



Default DSCP-to-UP Mapping Table

DSCP	802.11 UP	WLC QoS Profile
56-63	7	Platinum (Voice)
48-55	6	
40-47	5	Gold (Video)
32-39	4	
24-31	3	Silver (Best Effort)
0-7	0	
16-23	2	Bronze (Background)
8-15	1	

Default DSCP-to-UP Mapping Table

IETF PHB for VoIP: EF

DSCP	802.11 UP	WLC QoS Profile
56-63	7	Platinum (Voice)
48-55	6	
40-47 46	5	Gold (Video)
32-39	4	
24-31	3	Silver (Best Effort)
0-7	0	
16-23	2	Bronze (Background)
8-15	1	

Per RFC 4594 & 3246

Default DSCP-to-UP Mapping Table

DSCP	802.11 UP	WLC QoS Profile
56-63	7	Platinum (Voice)
48-55	6	
40-47 46	5	Gold (Video)
32-39	4	Silver (Best Effort)
24-31	3	
0-7	0	
16-23	2	Bronze (Background)
8-15	1	

IETF PHB for VoIP: EF

Per RFC 4594 & 3246

Default DSCP-to-UP Mapping Table

DSCP	802.11 UP	WLC QoS Profile
56-63	7	Platinum (Voice)
48-55	6	
40-47 46	5	Gold (Video)
32-39	4	
24-31	3	Silver (Best Effort)
0-7	0	
16-23	2	Bronze (Background)
8-15	1	

IETF PHB for VoIP: EF

Per RFC 4594 & 3246

Default DSCP-to-UP Mapping Table

DSCP	802.11 UP	WLC QoS Profile
56-63	7	Platinum (Voice)
48-55	6	
40-47 46	5	Gold (Video)
32-39	4	
24-31	3	Silver (Best Effort)
0-7	0	
16-23	2	Bronze (Background)
8-15	1	

IETF PHB for VoIP: EF

Per RFC 4594 & 3246

Downstream DSCP-to-UP Mapping Model

Ratified Cisco Consensus Model (June 2015)

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

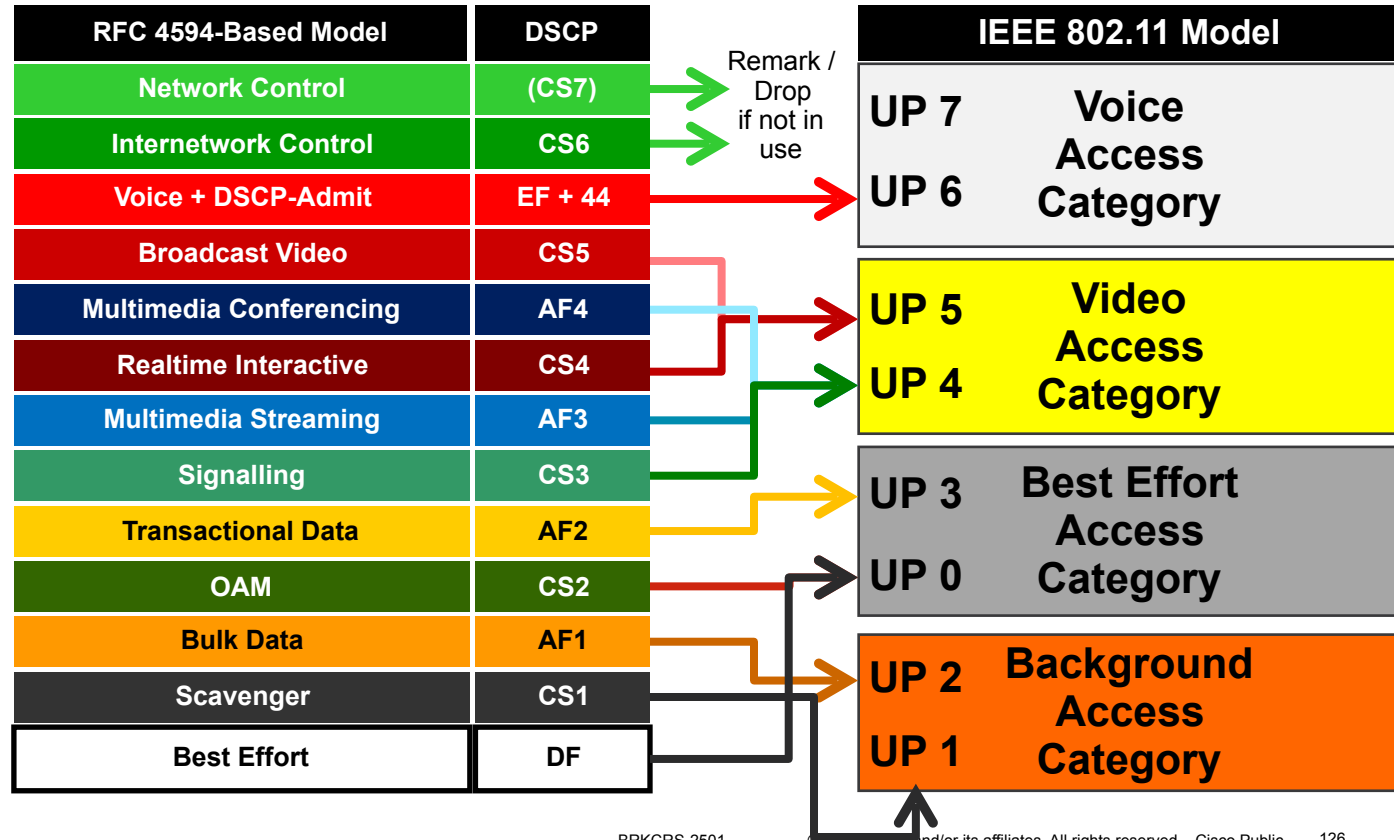
RFC 4594-Based Model	DSCP
Network Control	(CS7)
Internetwork Control	CS6
Voice + DSCP-Admit	EF + 44
Broadcast Video	CS5
Multimedia Conferencing	AF4
Realtime Interactive	CS4
Multimedia Streaming	AF3
Signalling	CS3
Transactional Data	AF2
OAM	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

IEEE 802.11 Model	
UP 7	Voice
UP 6	Access Category
UP 5	Video
UP 4	Access Category
UP 3	Best Effort
UP 0	Access Category
UP 2	Background
UP 1	Access Category

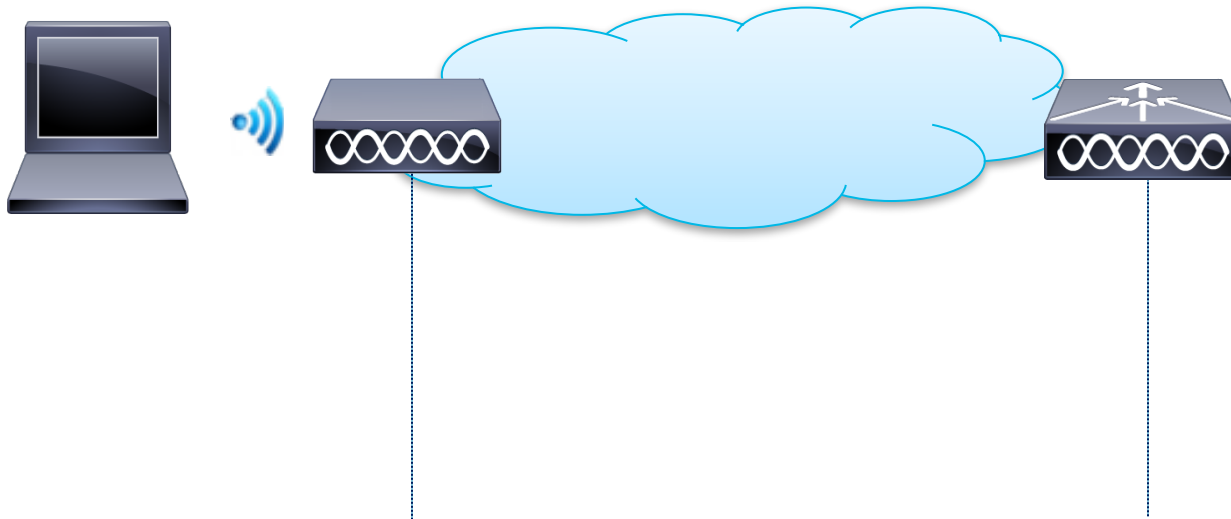
Downstream DSCP-to-UP Mapping Model

Ratified Cisco Consensus Model (June 2015)

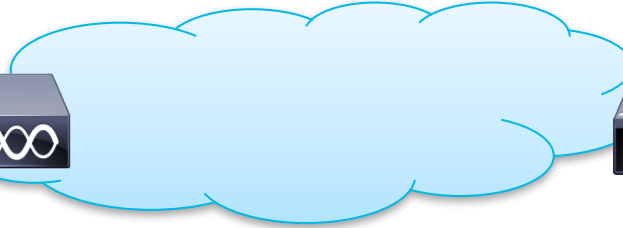
- Plugs potential security vulnerabilities
- Provides distinction between elastic and inelastic video classes
- Aligns RFC 4594 recommendations into the IEEE 802.11 model
- Requires several custom DSCP-to-UP mappings



Upstream UP-to-DSCP Default Mapping



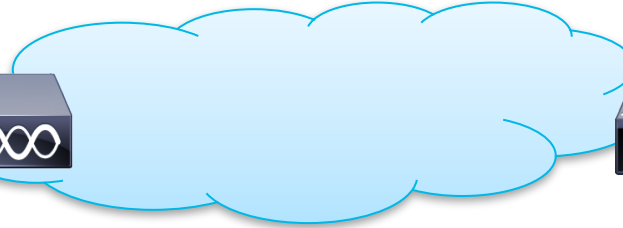
Upstream UP-to-DSCP Default Mapping



802.11 Frame

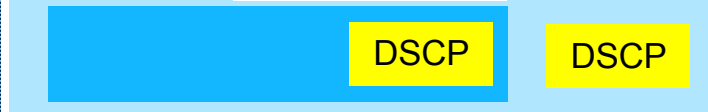


Upstream UP-to-DSCP Default Mapping

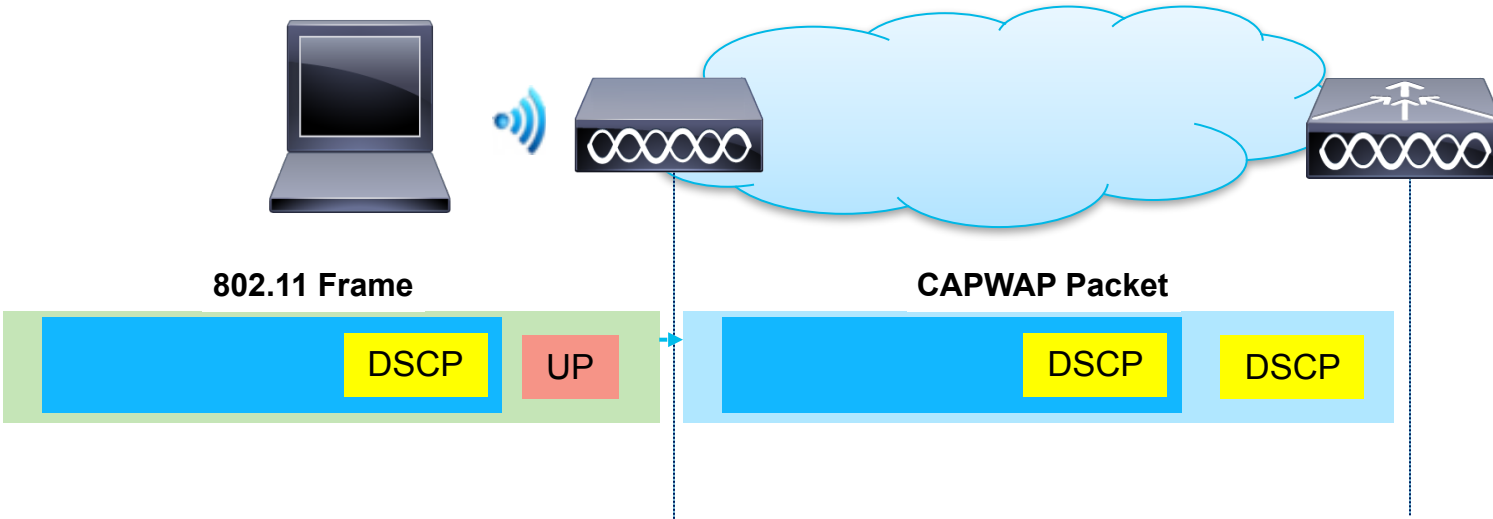


802.11 Frame

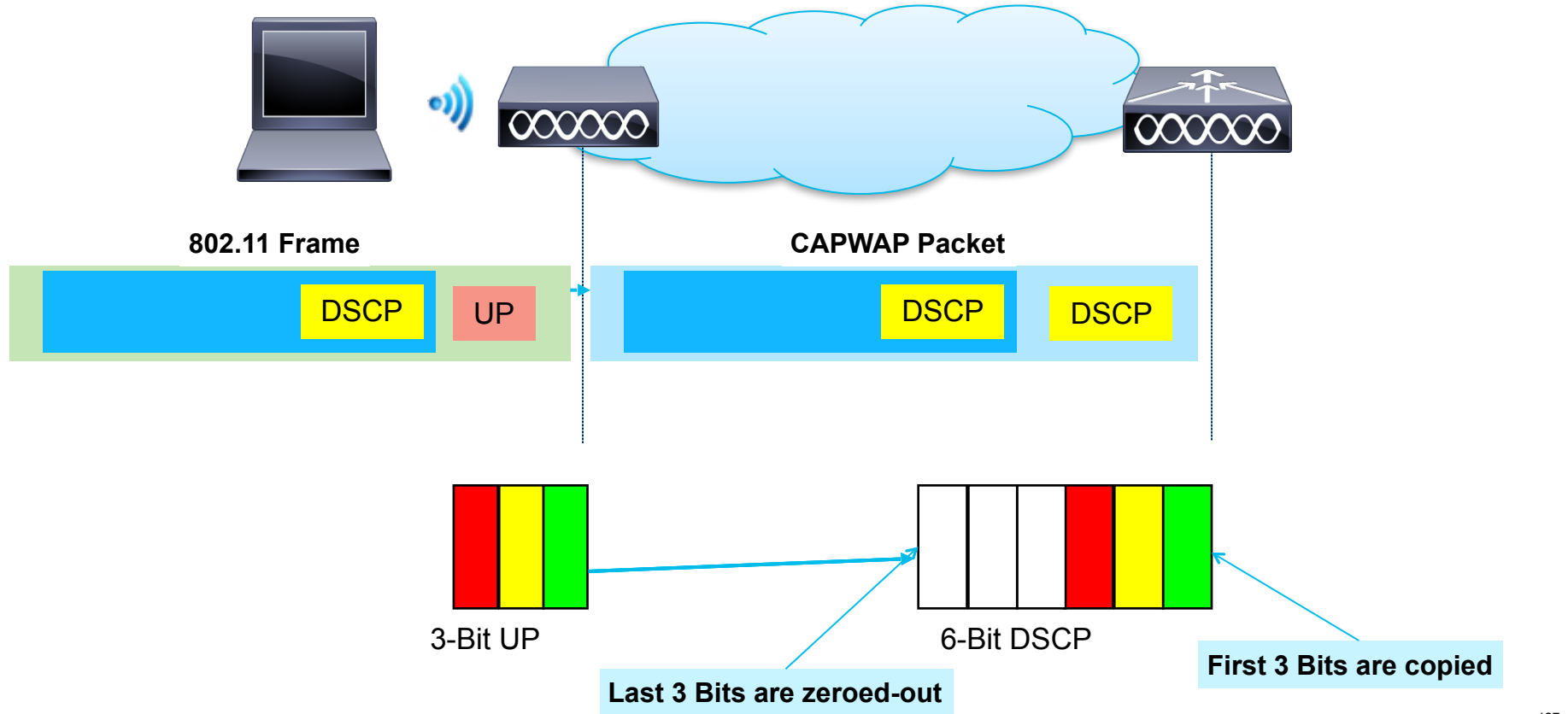
CAPWAP Packet



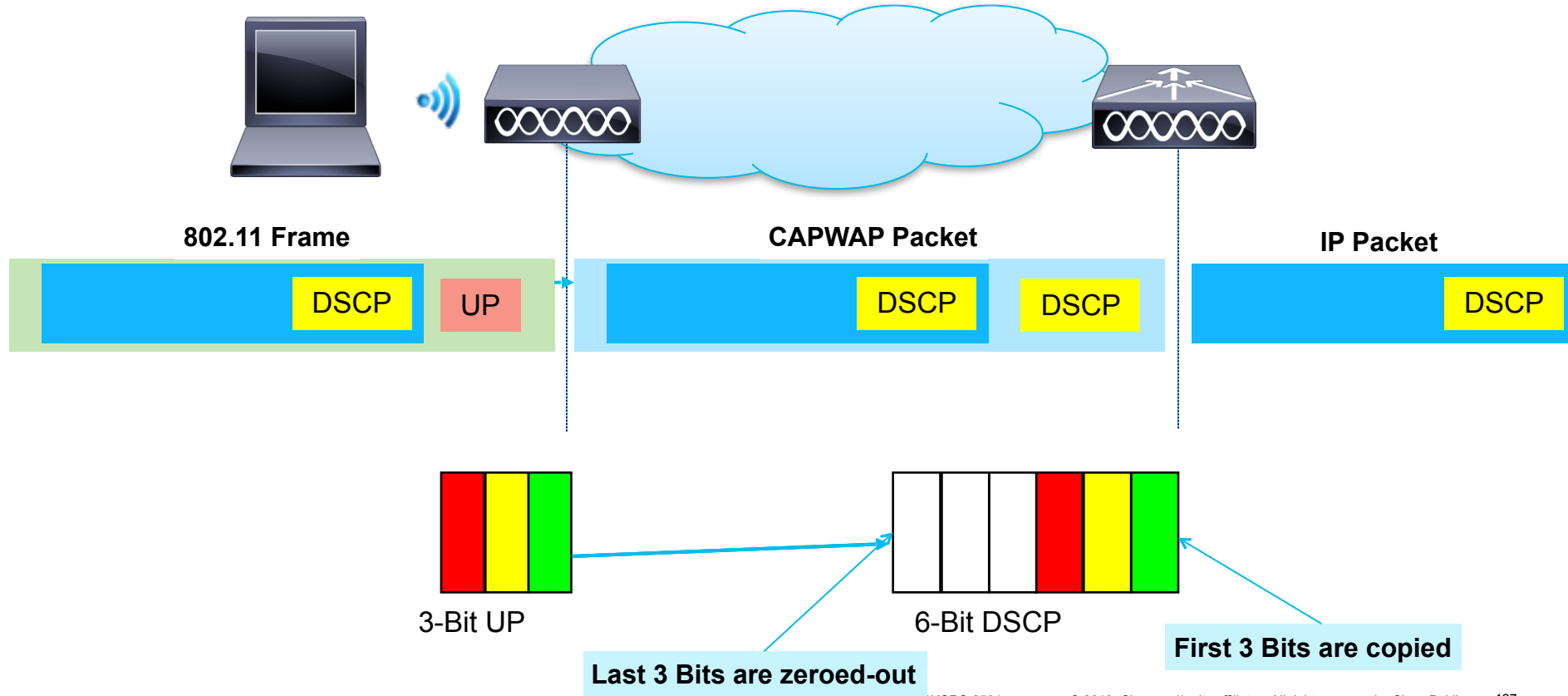
Upstream UP-to-DSCP Default Mapping



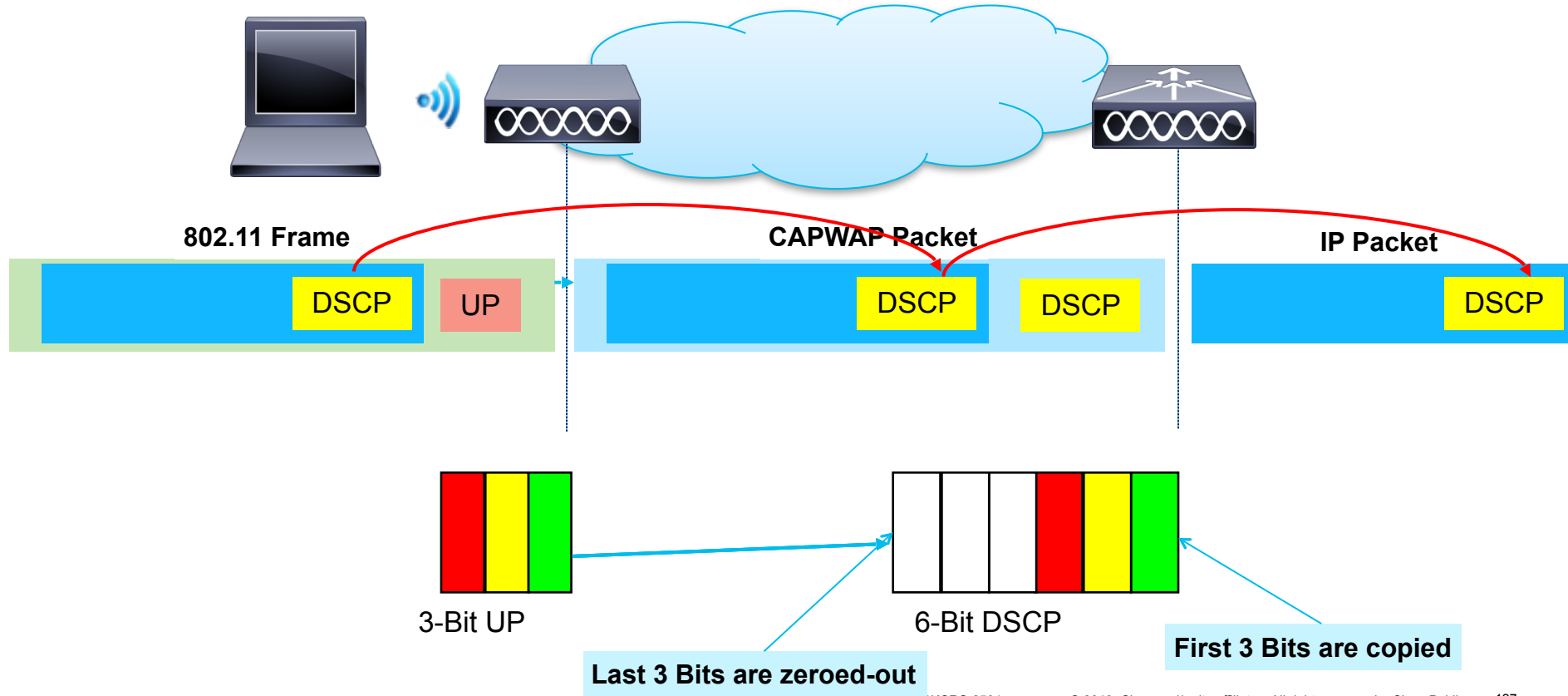
Upstream UP-to-DSCP Default Mapping



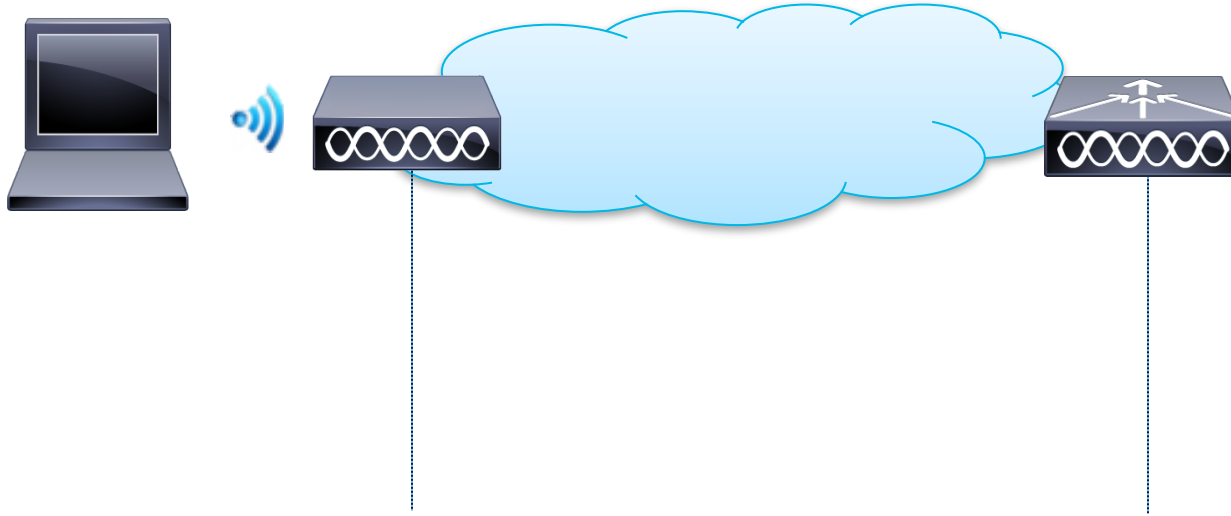
Upstream UP-to-DSCP Default Mapping



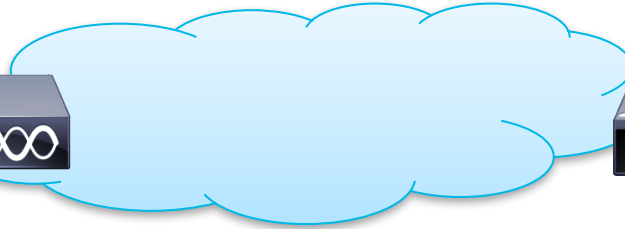
Upstream UP-to-DSCP Default Mapping



Upstream DSCP Trust Model



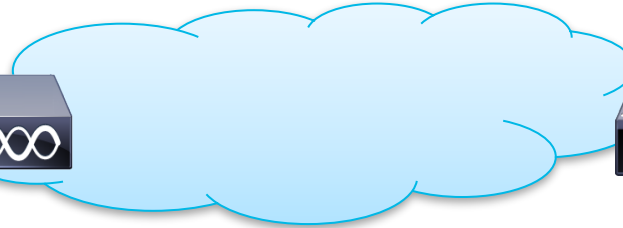
Upstream DSCP Trust Model



802.11 Frame

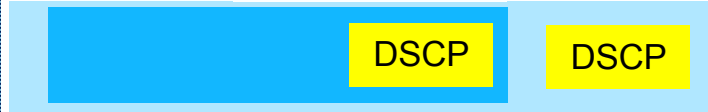


Upstream DSCP Trust Model

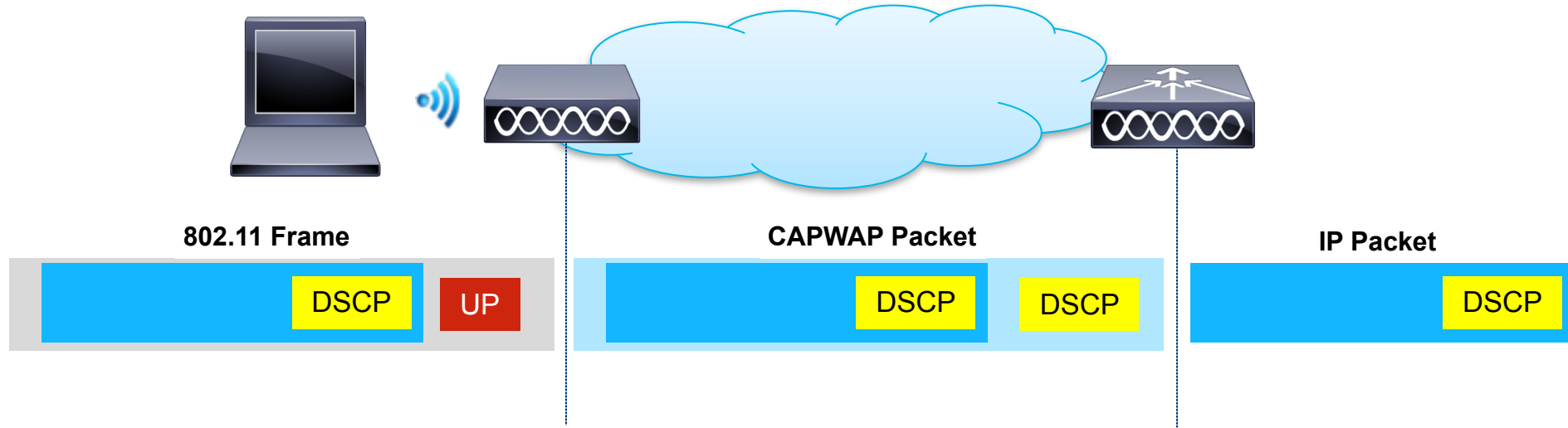


802.11 Frame

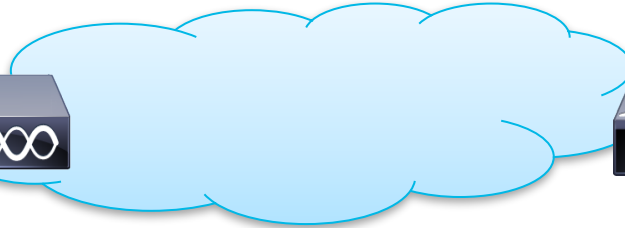
CAPWAP Packet



Upstream DSCP Trust Model



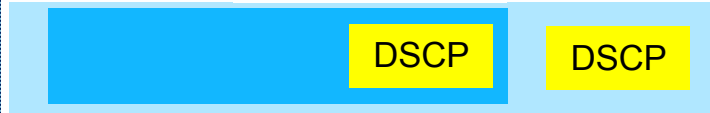
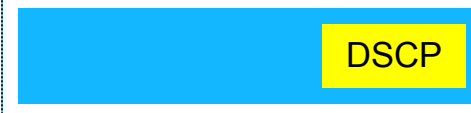
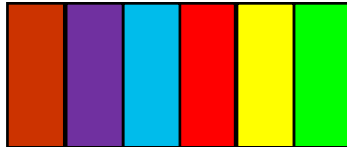
Upstream DSCP Trust Model



802.11 Frame

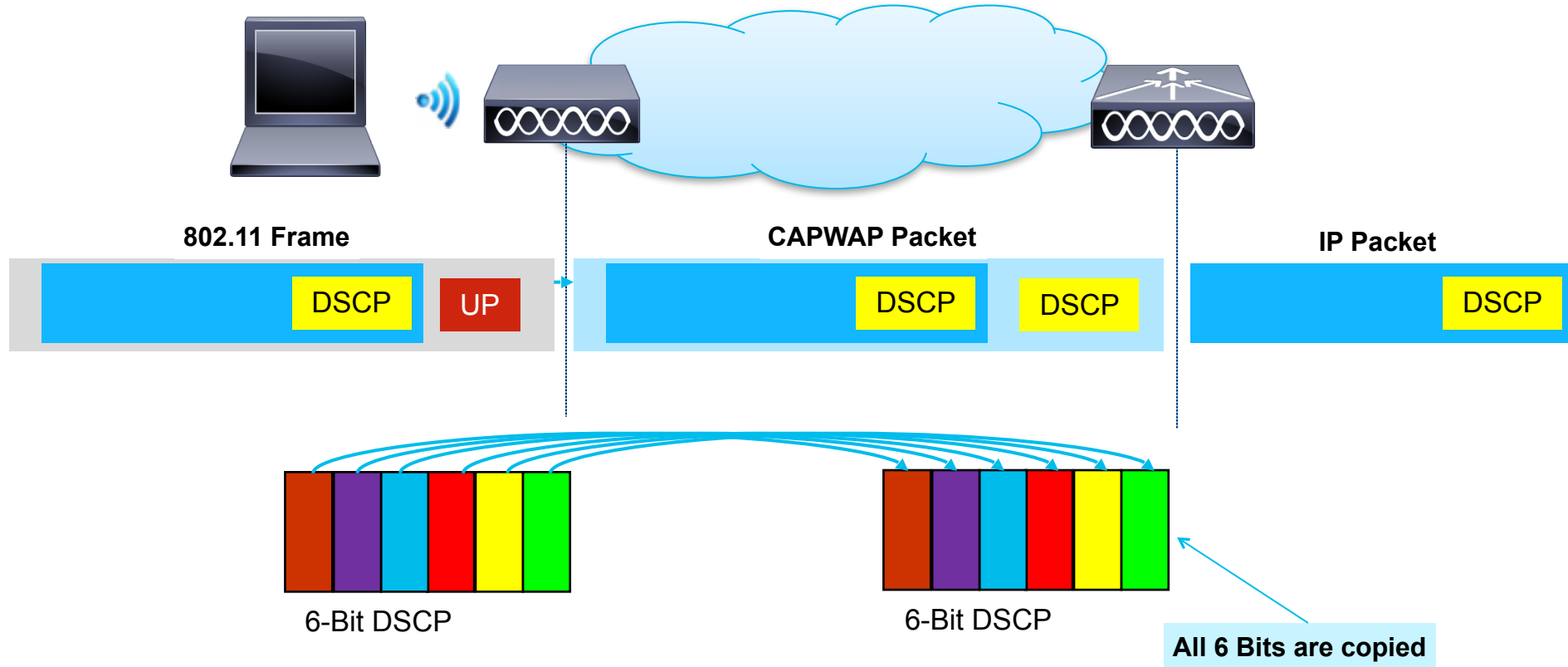
CAPWAP Packet

IP Packet

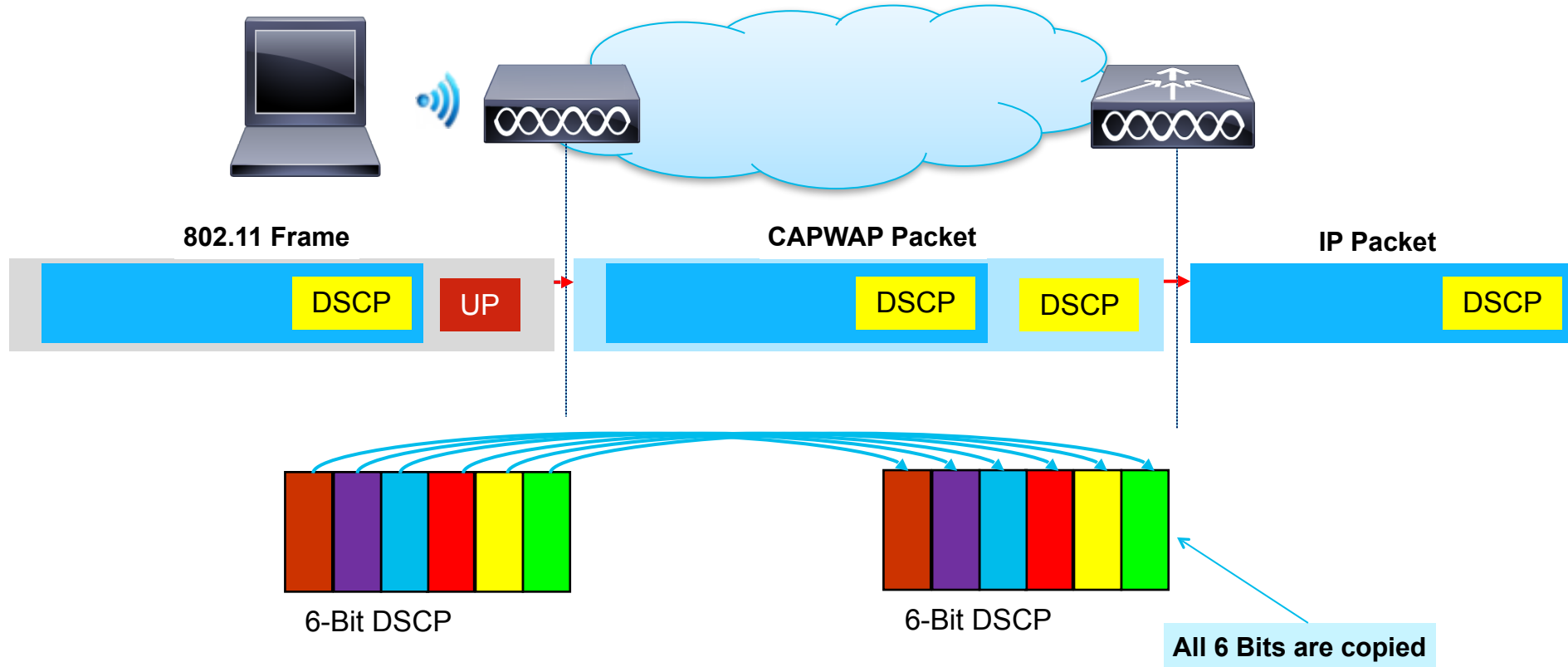


6-Bit DSCP

Upstream DSCP Trust Model



Upstream DSCP Trust Model



IETF Draft on DSCP↔UP Mapping

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

<https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-00>

Diffserv to IEEE 802.11 Mapping draft-ietf-tsvwg-ieee-802-11-11

Abstract

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

Status of This Memo

Expected to be an RFC by CL Melbourne
Update Accordingly

conformance with the

the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 21, 2018.

Copyright Notice

Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

Cisco WLAN QoS Design At-A-Glance



WLAN QoS Design

The Case for QoS in the Wireless LAN

Wireless access points are the second most-likely places in the enterprise network to experience congestion (after LAN-to-WAN links). This is because wireless media:

- generally presents a downshift in speed/throughput
- is a half-duplex media
- is a shared media

Furthermore, the nature of wireless media presents additional challenges from a QoS provisioning perspective, including:

- No support for strict priority queuing
- No support for guaranteed bandwidth allocations
- Non-deterministic media access
- A maximum of four levels of service

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

WLAN QoS Design Best Practices

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

WLAN QoS Design Considerations

There are several considerations unique to WLANs that must be factored into QoS designs:

- The IEEE 802.11e Enhanced Distributed Coordination Function (EDCF), including:
 - User Priorities
 - Access Categories
 - Arbitration Inter-Frame Spaces (AIFS)
 - Contention Windows (CW)
 - EDCF Operation
 - Transmission Opportunity (TXOP)
 - Transmission Specification (TSPEC)
- UP-to-DSCP and DSCP-to-UP Mapping

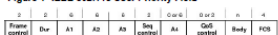
IEEE 802.11e EDCF

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

User Priorities (UP)

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

Figure 1 IEEE 802.11e User Priority Field



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

Access Categories (AC)

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

Figure 2 IEEE 802.11e Access Categories

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

Arbitration Interframe Spaces (AIFS)

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

Figure 3 IEEE 802.11e AIFS by Access Category

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

Contention Windows

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

Figure 4 IEEE 802.11e Contention Windows by AC

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

WLAN QoS Design

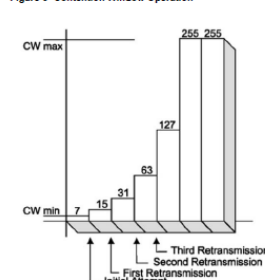
EDCF Operation

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

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

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

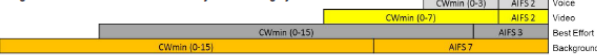
Figure 6 Contention Window Operation



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

Copyright © 2010 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Figure 5 IEEE 802.11e AIFS and CWmin by Access Category



Transmission Opportunity (TXOP)

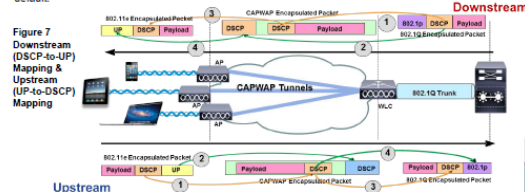
EDCF provides contention-free period access to the wireless medium, called the Transmission Opportunity (TXOP). The TXOP is a set period of time when a wireless station may send as many frames as possible without having to contend with other stations. With TXOP, each station has a set time limit when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

Transmission Specification (TSPEC)

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

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

Upstream and downstream DSCP-to-UP mapping is shown in Figure 7. By default, 8-bit DSCP values are mapped to 3-bit 802.11e UP values by taking the three Most-Significant Bits (MSB) of the DSCP and copying these as UP values. For example, DSCP EF48 (binary 101110) is mapped to CoS or UP 5 (binary 101), by

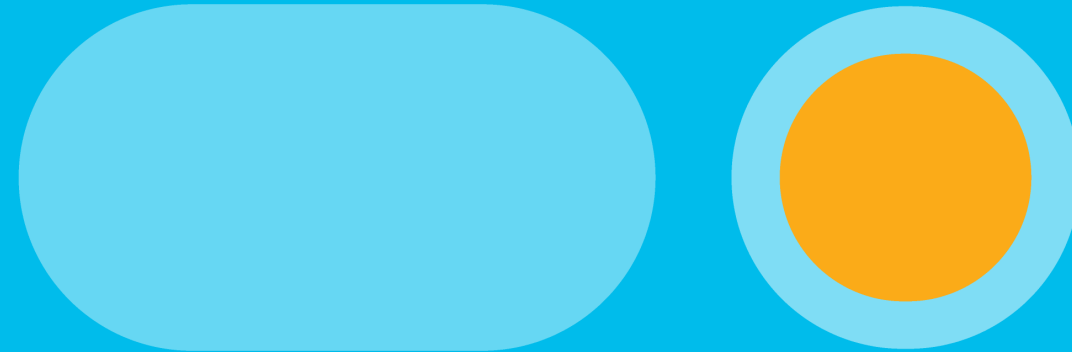


For more details, see the AVC/QoS Design chapter of the BYOD CVD at: http://www.cisco.com/en/US/docs/solutions/Enterprise/Networks/Unified_Enterprise/BYOD_Design_Guide/BYOD_AVC.html And/or the Cisco Press book: End-to-End QoS Network Design (Second Edition)-Chapter 18

<https://cisco.box.com/v/QoS-AAGs>



AireOS QoS Design



AireOS QoS Policy Deployment

List of Steps

AireOS QoS Policy Deployment

List of Steps

- 1) Disable Radios and WLANs
- 2) Tune EDCA and CAC
- 3) Tune QoS Profile
- 4) Create AVC Profile
- 5) Attach QoS and AVC Profiles to WLAN and Enable AVC
- 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust
- 7) Re-enable WLANs and radios

AireOS QoS Policy Deployment

Step 1) Disable Radios and WLANs

```
(Cisco Controller) > config 802.11a disable network
(Cisco Controller) > config 802.11b disable network
! Must disable 802.11a/b networks to make changes to QoS

(Cisco Controller) > config wlan disable all
! Must disable all WLANs to make changes to QoS
```

802.11a Global Parameters Apply

General Data

802.11a Network Status	☒ Enabled	6 Mb
------------------------	---	------

WLANs Entries 1 - 7 of 7

Current Filter: None [\[Change Filter\]](#) [\[Clear Filter\]](#) Disable Selected

☒	WLAN ID	Type	Profile Name
☒	1	WLAN	none
☒	2	WLAN	tt
☒	3	WLAN	PublicWifi
☒	4	WLAN	Mynet
☒	5	WLAN	Mynet2
☒	6	WLAN	WHOPPERWIFI
☒	7	WLAN	guest

AireOS QoS Policy Deployment

Step 2) Tune EDCA and CAC

General

EDCA Profile Fastlane ▼
Enable Low ☐
Latency MAC ☐

Voice Video Media

Call Admission Control (CAC)

Admission Control (ACM) ☒ Enabled
CAC Method ☒ Load Based
Max RF Bandwidth (5-85)(%)
Reserved Roaming Bandwidth (0-25)(%)
Expedited bandwidth ☒

```
(Cisco Controller) > config 802.11a Qos Mode 7
(Cisco Controller) > config 802.11b Qos Mode 7
! Apply Fastlane EDCA profile (best of current EDCA profiles) for 802.11a/b

(Cisco Controller) > config 802.11a cac voice acm enable
(Cisco Controller) > config 802.11b cac voice acm enable
! Enable ACM for 802.11a/b

(Cisco Controller) > config 802.11a cac voice max-bandwidth 50
(Cisco Controller) > config 802.11b cac voice max-bandwidth 50
! Limit voice traffic to 50% of total bandwidth for 802.11a/b

(Cisco Controller) > config 802.11a cac voice roam-bandwidth 6
(Cisco Controller) > config 802.11b cac voice roam-bandwidth 6
! Keep 6% bandwidth for roaming users for 802.11a/b

(Cisco Controller) > config 802.11a exp-bwreq enable
(Cisco Controller) > config 802.11b exp-bwreq enable
! Enable Expedited Bandwidth for 802.11a/b
```

AireOS QoS Policy Deployment

Step 3) Tune Platinum QoS Profile

```
(Cisco Controller) > config qos priority platinum voice besteffort besteffort
! Set QoS Profile to Platinum
! Set default marking to unmarked unicast and multicast traffic to best effort
```

```
(Cisco Controller) > config qos protocol-type platinum none
! Disables 802.1p marking (all wired marking is DSCP-based)
```

```
(Cisco Controller) > config qos burst-realtime-rate platinum per-ssid downstream 0
! Do not restrict profile bandwidth for UDP traffic
```

```
(Cisco Controller) > config qos average-realtime-rate platinum per-ssid downstream 0
! Do not restrict profile bandwidth for TCP traffic
```

Edit QoS Profile

QoS Profile Name

Description

Per-User Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

Per-SSID Bandwidth Contracts (kbps) *

	DownStream	UpStream
Average Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Data Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Average Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>
Burst Real-Time Rate	<input type="text" value="0"/>	<input type="text" value="0"/>

WLAN QoS Parameters

Maximum Priority

Unicast Default Priority

Multicast Default Priority

Wired QoS Protocol

Protocol Type

Application Name	Applic Name
cisco-phone-audio	other
cisco-jabber-audio	voice-i
ms-lync-audio	business

AireOS QoS Policy Deployment

Step 4) Create an AVC Profile—Example (Part 1 of 2)

```
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE create
! Creates the AVC Profile

! This section configures AVC to mark Voice applications/sub-components to EF (DSCP 46)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cisco-phone-audio mark 46
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-audio mark 46
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ms-lync-audio mark 46
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application citrix-audio mark 46

! This section configures AVC to mark Multimedia Conferencing applications to AF41 (DSCP 34)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cisco-phone-video mark 34
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-video mark 34
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ms-lync-video mark 34
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application webex-media mark 34

! This section configures AVC to mark Multimedia Streaming applications to AF31 (DSCP 26)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application citrix mark 26
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application pcoip mark 26
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application vnc mark 26
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application vnc-http mark 26

! This section configures AVC to mark Signaling protocols to CS3 (DSCP 24)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application skinny mark 24
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-control mark 24
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application sip mark 24
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application sip-tls mark 24
```

AireOS QoS Policy Deployment

Step 4) Create an AVC Profile—Example (Part 2 of 2)

```
! This section configures AVC to mark Transactional Data applications to AF21 (DSCP 18)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cisco-jabber-im mark 18
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ms-office-web-apps mark 18
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application salesforce mark 18
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application sap mark 18

! This section configures AVC to mark OAM applications to CS2 (DSCP 16)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application dhcp mark 16
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application dns mark 16
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ntp mark 16
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application snmp mark 16

! This section configures AVC to mark Bulk Data applications marking to AF11 (DSCP 10)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ftp mark 10
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ftp-data mark 10
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application ftps-data mark 10
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application cifs mark 10

! This section configures AVC to mark Scavenger applications to CS1 (DSCP 8)
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application netflix mark 8
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application youtube mark 8
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application skype mark 8
(Cisco WLC) > config avc profile AVC-STATIC-PROFILE rule add application bittorrent mark 8
```

AireOS QoS Policy Deployment

Step 5) Attach QoS and AVC Profiles to WLAN and Enable AVC

```
(Cisco WLC) > config wlan qos 10 platinum  
! Applies the Platinum QoS profile to the WLAN  
  
(Cisco WLC) > config wlan avc 10 visibility enable  
! Enables AVC Visibility on WLAN 10  
  
(Cisco WLC) > config wlan avc 10 profile AVC-APPS enable  
! This command applies the AVC profile AVC-APPS to WLAN ID 10
```

General	Security	QoS	Policy-Mapping
Quality of Service (QoS) Platinum (voice) ▼			
Application Visibility ☒ Enabled			
AVC Profile EZQoS-WlanId-4 ▼			
Netflow Monitor none ▼			
Fastlane Disable ▼			

AireOS QoS Policy Deployment

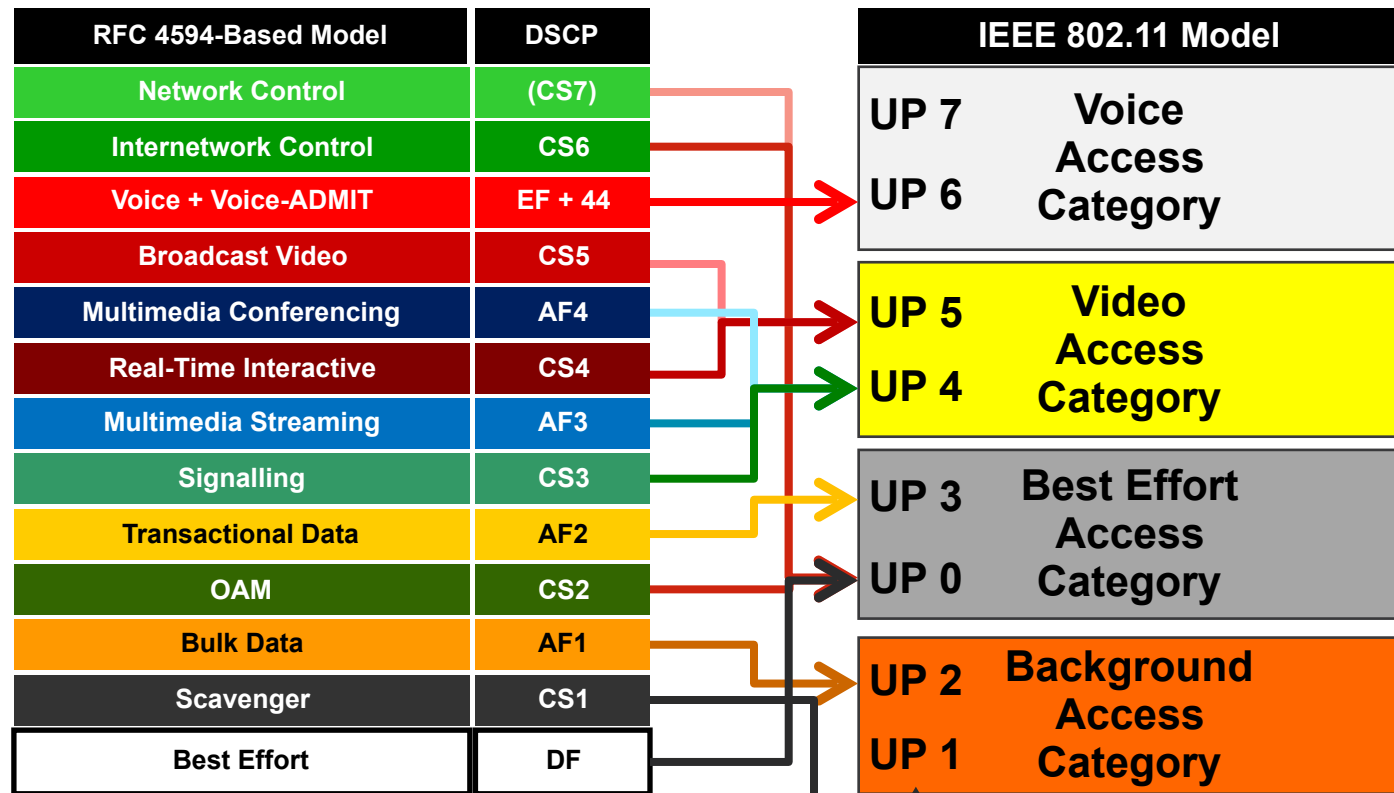
Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust

RFC 4594-Based Model	DSCP
Network Control	(CS7)
Internetwork Control	CS6
Voice + Voice-ADMIT	EF + 44
Broadcast Video	CS5
Multimedia Conferencing	AF4
Real-Time Interactive	CS4
Multimedia Streaming	AF3
Signalling	CS3
Transactional Data	AF2
OAM	CS2
Bulk Data	AF1
Scavenger	CS1
Best Effort	DF

IEEE 802.11 Model	
UP 7	Voice Access Category
UP 6	
UP 5	Video Access Category
UP 4	
UP 3	Best Effort Access Category
UP 0	
UP 2	Background Access Category
UP 1	

AireOS QoS Policy Deployment

Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust



AireOS QoS Policy Deployment

Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust—Configuration (Part 1 of 2)

Step 1: Disable the Current QoS Map

```
(Cisco WLC) > config qos qosmap disable
```

Step 2: Configure the UP-to-DSCP Maps

```
(Cisco WLC) > config qos qosmap up-to-dscp-map 0 0 0 7
(Cisco WLC) > config qos qosmap up-to-dscp-map 1 8 8 15
(Cisco WLC) > config qos qosmap up-to-dscp-map 2 16 16 23
(Cisco WLC) > config qos qosmap up-to-dscp-map 3 24 24 31
(Cisco WLC) > config qos qosmap up-to-dscp-map 4 32 32 39
(Cisco WLC) > config qos qosmap up-to-dscp-map 5 34 40 47
(Cisco WLC) > config qos qosmap up-to-dscp-map 6 46 48 62
(Cisco WLC) > config qos qosmap up-to-dscp-map 7 56 63 63
```

QoS Map Config

Qos Map

Trust DSCP UpStream ☒

UP to DSCP Map

User Priority

DSCP Default

DSCP Start

DSCP End

Add DSCP Exception

DSCP Exception

User Priority

DSCP Exception List

DSCP	UP	
16	0	<input type="button" value="v"/>
8	1	<input type="button" value="v"/>
10	2	<input type="button" value="v"/>
12	2	<input type="button" value="v"/>
14	2	<input type="button" value="v"/>
18	3	<input type="button" value="v"/>
20	3	<input type="button" value="v"/>
22	3	<input type="button" value="v"/>
38	4	<input type="button" value="v"/>
36	4	<input type="button" value="v"/>

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	40	40	47
6	48	48	55

AireOS QoS Policy Deployment

Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust—Configuration (Part 2 of 3)

Step 3: Configure DSCP-to-UP Mapping Exceptions

```
(Cisco Controller) > config qos qosmap dscp-to-up-exception 56 0
(Cisco Controller) > config qos qosmap dscp-to-up-exception 48 0
(Cisco Controller) > config qos qosmap dscp-to-up-exception 46 6
(Cisco Controller) > config qos qosmap dscp-to-up-exception 44 6
(Cisco Controller) > config qos qosmap dscp-to-up-exception 40 5
(Cisco Controller) > config qos qosmap dscp-to-up-exception 38 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 36 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 34 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 32 5
(Cisco Controller) > config qos qosmap dscp-to-up-exception 30 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 28 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 26 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 24 4
(Cisco Controller) > config qos qosmap dscp-to-up-exception 22 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 20 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 18 3
(Cisco Controller) > config qos qosmap dscp-to-up-exception 16 0
(Cisco Controller) > config qos qosmap dscp-to-up-exception 14 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 12 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 10 2
(Cisco Controller) > config qos qosmap dscp-to-up-exception 8 1
```

AireOS QoS Policy Deployment

Step 6) Configure Downstream DSCP-to-UP Mapping and Enable Upstream DSCP-Trust—Configuration (Part 3 of 3)

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

```
(Cisco Controller) > config qos qosmap trust-dscp-upstream enable
```

```
(Cisco Controller) > config qos qosmap enable
```

AireOS Static QoS Policy Deployment

Step 7) Re-Enable Radios and WLANs

```
(Cisco Controller) > config 802.11a enable network  
(Cisco Controller) > config 802.11b enable network  
(Cisco Controller) > config wlan enable all
```

WLAN QoS Design

Key Takeaways

- Start by defining your QoS Strategy
- Design your RF for Voice Efficiency
 - Small cells, lower rates disabled, 15% overlap, AP at client power level
 - See BRKWEN 2000 for more details
- Restructure upstream and downstream marking and trust
- Use Platinum for your WLANs
- Apply efficient EDCA if possible, CAC if needed

Agenda

- Introduction to Strategic QoS Design
- WAN / IWAN QoS Design
- Campus QoS Design
- WLAN QoS Design
- Automating and Assuring QoS
- Summary and References
- Appendices

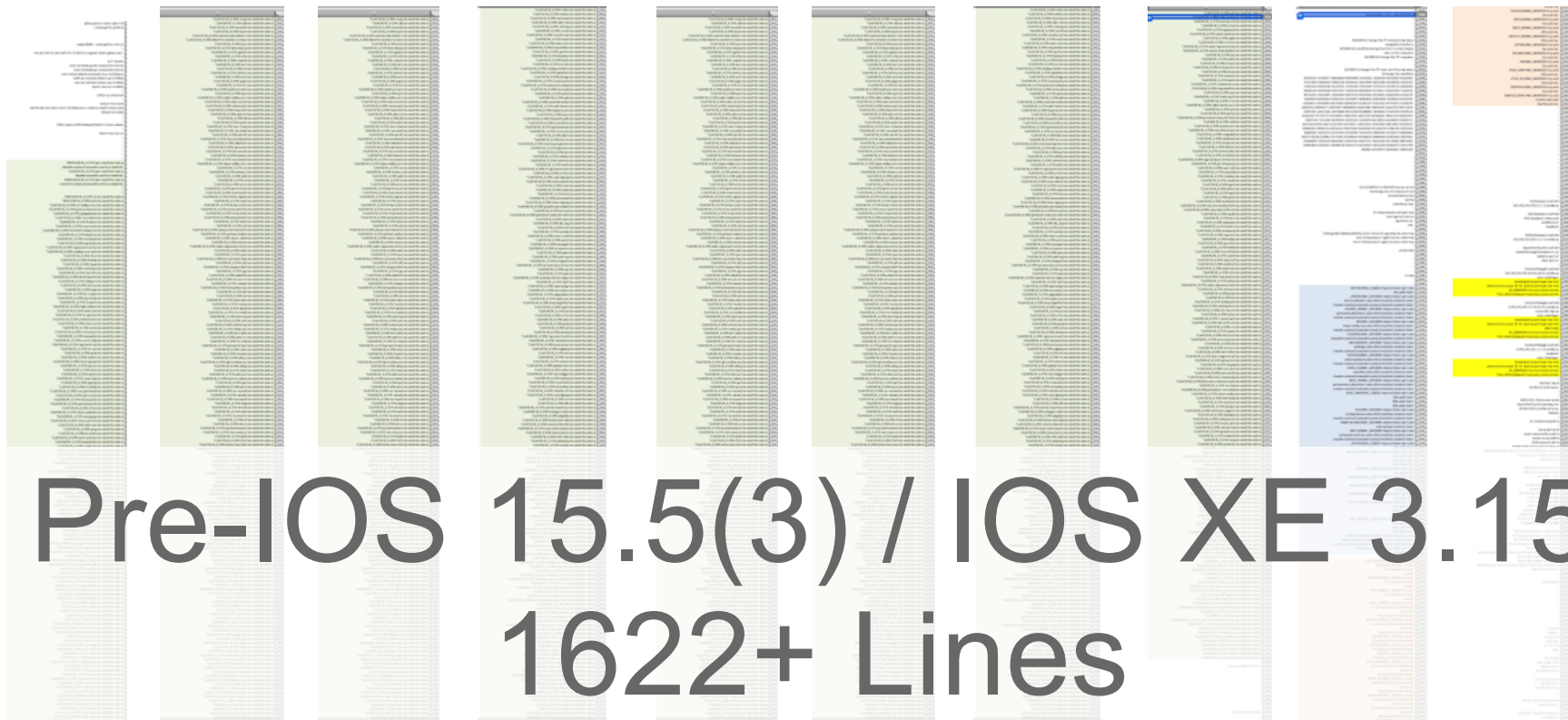
Automating and Assuring QoS

AutoQoS 5.0



How Many Lines of CLI Does it take to Configure QoS for All 1400+ Apps in Our Common Library?

How Many Lines of CLI Does it take to Configure QoS for All 1400+ Apps in Our Common Library?



How Many Lines of CLI Does it take to Configure QoS for All 1400+ Apps in Our Common Library?

How Many Lines of CLI Does it take to Configure QoS for All 1400+ Apps in Our Common Library?

```
class-map match-all VOICE-NBAR
  match protocol attribute traffic-class voip-telephony
  match protocol attribute business-relevance business-relevant
class-map match-all BROADCAST_VIDEO-NBAR
  match protocol attribute traffic-class broadcast-video
  match protocol attribute business-relevance business-relevant
class-map match-all REALTIME_INTERACTIVE-NBAR
  match protocol attribute traffic-class real-time-interactive
  match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
  match protocol attribute traffic-class multimedia-conferencing
  match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA_STREAMING-NBAR
  match protocol attribute traffic-class multimedia-streaming
  match protocol attribute business-relevance business-relevant
class-map match-all SIGNALING-NBAR
  match protocol attribute traffic-class signaling
  match protocol attribute business-relevance business-relevant
class-map match-all NETWORK_CONTROL-NBAR
  match protocol attribute traffic-class network-control
  match protocol attribute business-relevance business-relevant
class-map match-all NETWORK_MANAGEMENT-NBAR
  match protocol attribute traffic-class ops-admin-mgmt
  match protocol attribute business-relevance business-relevant
class-map match-all TRANSACTIONAL_DATA-NBAR
  match protocol attribute traffic-class transactional-data
  match protocol attribute business-relevance business-relevant
class-map match-all BULK_DATA-NBAR
  match protocol attribute traffic-class bulk-data
  match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER-NBAR
  match protocol attribute business-relevance business-relevant
```

```
policy-map LAN_EDGE-IN
class VOICE-NBAR
  set dscp ef
class BROADCAST_VIDEO-NBAR
  set dscp cs5
class REALTIME_INTERACTIVE-NBAR
  set dscp cs4
class MULTIMEDIA_CONFERENCING-NBAR
  set dscp af41
class MULTIMEDIA_STREAMING-NBAR
  set dscp af31
class SIGNALING-NBAR
  set dscp cs3
class NETWORK_CONTROL-NBAR
  set dscp cs6
class NETWORK_MANAGEMENT-NBAR
  set dscp cs2
class TRANSACTIONAL_DATA-NBAR
  set dscp af21
class BULK_DATA-NBAR
  set dscp af11
class SCAVENGER-NBAR
  set dscp cs1
class class-default
  set dscp default
```

```
class-map match-all VOICE-DSCP
  match dscp ef
class-map match-all BROADCAST_VIDEO-DSCP
  match dscp cs5
class-map match-all REALTIME_INTERACTIVE-DSCP
  match dscp cs4
class-map match-all NETWORK_CONTROL-DSCP
  match dscp cs6
class-map match-all SIGNALING-DSCP
  match dscp cs3
class-map match-all NETWORK_MANAGEMENT-DSCP
  match dscp cs2
class-map match-all MULTIMEDIA_CONFERENCING-DSCP
  match dscp af41
class-map match-all MULTIMEDIA_STREAMING-DSCP
  match dscp af31
class-map match-all TRANSACTIONAL_DATA-DSCP
  match dscp af21
class-map match-all BULK_DATA-DSCP
  match dscp af11
class-map match-all SCAVENGER-DSCP
  match dscp cs1
```

```
policy-map WAN_EDGE-OUT
class VOICE-DSCP
  priority percent 10
class BROADCAST_VIDEO-DSCP
  priority percent 10
class REALTIME_INTERACTIVE-DSCP
  priority percent 13
class NETWORK_CONTROL-DSCP
  bandwidth percent 2
class SIGNALING-DSCP
  bandwidth percent 2
class NETWORK_MANAGEMENT-DSCP
  bandwidth percent 3
class MULTIMEDIA_CONFERENCING-DSCP
  bandwidth percent 10
  fair-queue
  random-detect dscp-based
class MULTIMEDIA_STREAMING-DSCP
  bandwidth percent 10
  fair-queue
  random-detect dscp-based
class TRANSACTIONAL_DATA-DSCP
  bandwidth percent 10
  fair-queue
  random-detect dscp-based
class BULK_DATA-DSCP
  bandwidth percent 4
  fair-queue
  random-detect dscp-based
class SCAVENGER-DSCP
  bandwidth percent 1
class class-default
  bandwidth percent 25
  fair-queue
  random-detect dscp-based
```

IOS XE 3.16+ 114 Lines

Where Do We Want To Get To? (with AutoQoS 5.0)

```
class-map match-all VOICE-NBAR
  match protocol attribute traffic-class voip-telephony
  match protocol attribute business-relevance business-relevant
class-map match-all BROADCAST_VIDEO-NBAR
  match protocol attribute traffic-class broadcast-video
  match protocol attribute business-relevance business-relevant
class-map match-all REALTIME_INTERACTIVE-NBAR
  match protocol attribute traffic-class real-time-interactive
  match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
  match protocol attribute traffic-class multimedia-conferencing
  match protocol attribute business-relevance business-relevant
class-map match-all MULTIMEDIA_STREAMING-NBAR
  match protocol attribute traffic-class streaming
  match protocol attribute business-relevance business-relevant
class-map match-all NETWORK_CONTROL-NBAR
  match protocol attribute traffic-class network-control
  match protocol attribute business-relevance business-relevant
class-map match-all NETWORK_MANAGEMENT-NBAR
  match protocol attribute traffic-class ops-admin-mgmt
  match protocol attribute business-relevance business-relevant
class-map match-all TRANSACTIONAL_DATA-NBAR
  match protocol attribute traffic-class transactional-data
  match protocol attribute business-relevance business-relevant
class-map match-all BULK_DATA-NBAR
  match protocol attribute traffic-class bulk-data
  match protocol attribute business-relevance business-relevant
class-map match-all SCAVENGER-NBAR
  match protocol attribute business-relevance business-irrelevant
```

auto qos srnd5 lan-edge

```
policy-map LAN_EDGE-IN
class VOICE-NBAR
  set dscp ef
class BROADCAST_VIDEO-NBAR
  set dscp cs5
class REALTIME_INTERACTIVE-NBAR
  set dscp cs4
class MULTIMEDIA_CONFERENCING-NBAR
  set dscp af41
class MULTIMEDIA_STREAMING-NBAR
  set dscp af31
class SIGNALING-NBAR
  set dscp cs3
class NETWORK_CONTROL-NBAR
  set dscp cs6
class NETWORK_MANAGEMENT-NBAR
  set dscp cs2
class TRANSACTIONAL_DATA-NBAR
  set dscp af21
class BULK_DATA-NBAR
  set dscp af11
class SCAVENGER-NBAR
  set dscp cs1
class class-default
  set dscp default
```

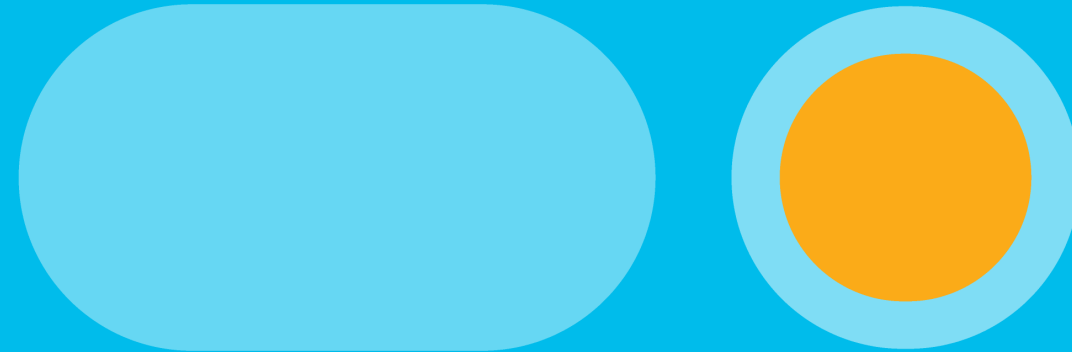
```
class-map match-all VOICE-DSCP
  match dscp ef
class-map match-all BROADCAST_VIDEO-DSCP
  match dscp cs5
class-map match-all REALTIME_INTERACTIVE-DSCP
  match dscp cs4
class-map match-all NETWORK_CONTROL-DSCP
  match dscp cs6
class-map match-all SIGNALING-DSCP
  match dscp cs3
class-map match-all NETWORK_MANAGEMENT-DSCP
  match dscp cs2
class-map match-all MULTIMEDIA_CONFERENCING-DSCP
  match dscp af41
class-map match-all MULTIMEDIA_STREAMING-DSCP
  match dscp af31
class-map match-all BULK_DATA-DSCP
  match dscp af21
class-map match-all SCAVENGER-DSCP
  match dscp cs1
```

auto qos srnd5 wan-edge

```
policy-map WAN_EDGE-OUT
class VOICE-DSCP
  priority percent 10
class BROADCAST_VIDEO-DSCP
  priority percent 10
class REALTIME_INTERACTIVE-DSCP
  priority percent 13
class NETWORK_CONTROL-DSCP
  bandwidth percent 2
class SIGNALING-DSCP
  bandwidth percent 2
class NETWORK_MANAGEMENT-DSCP
  bandwidth percent 3
class MULTIMEDIA_CONFERENCING-DSCP
  bandwidth percent 10
class MULTIMEDIA_STREAMING-DSCP
  bandwidth percent 10
class TRANSACTIONAL_DATA-DSCP
  bandwidth percent 10
class BULK_DATA-DSCP
  bandwidth percent 4
class SCAVENGER-DSCP
  bandwidth percent 1
class class-default
  bandwidth percent 25
  fair-queue
  random-detect dscp-based
```

IOS XE 16.10 2 Lines

APIC-EM EasyQoS / DNA Centre Application Policy



Customer Challenges

- “It takes [us] 4 months and \$1M to push a QoS change...”
- I view the administrator as being a business analyst via a central station without needing to have any understanding of QoS models and low level device attributes”
- —Wall Street Financial Customer

Customer Challenges

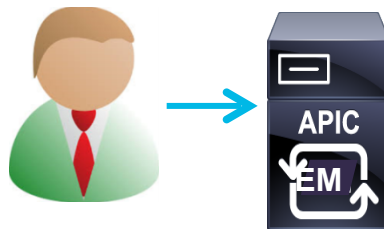
- “It took us 3 months to deploy a 2 line ACL change across 10K devices, which slowed down onboarding of our Jabber application.”
- —Cisco Network Architect

EasyQoS Solution



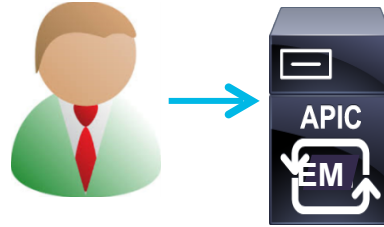
EasyQoS Solution

Network Operators express high-level business-intent to APIC-EM EasyQoS



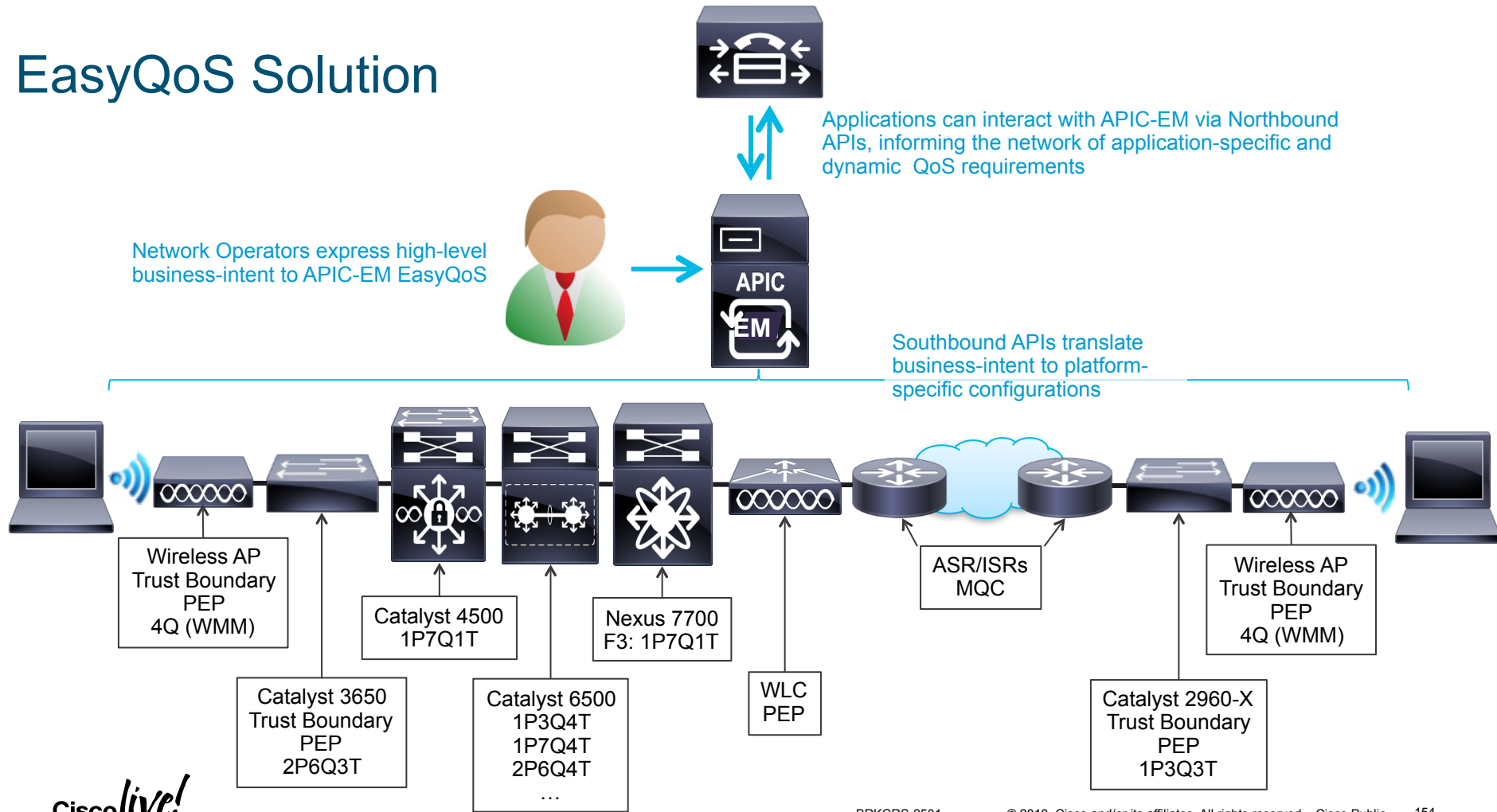
EasyQoS Solution

Network Operators express high-level business-intent to APIC-EM EasyQoS

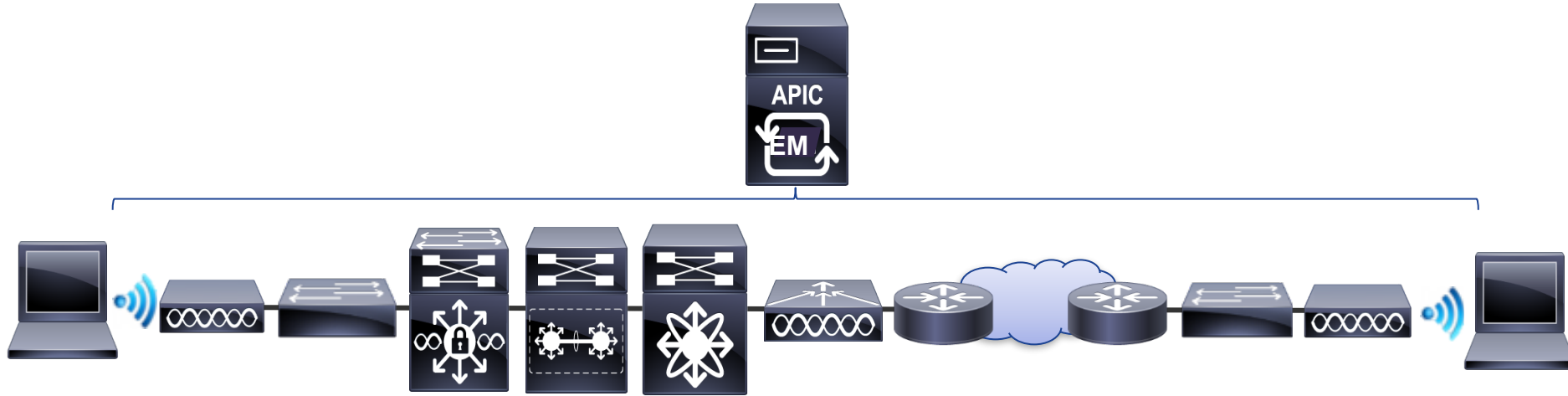


Applications can interact with APIC-EM via Northbound APIs, informing the network of application-specific and dynamic QoS requirements

EasyQoS Solution

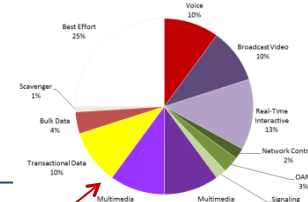
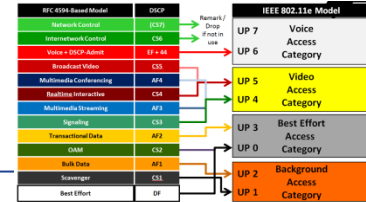
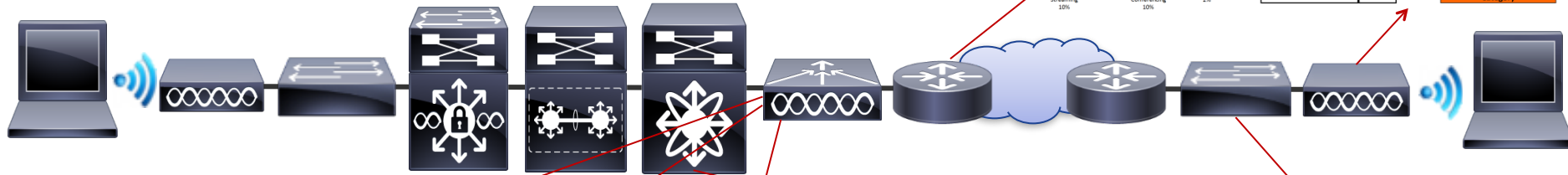


Deploy End-to-End DSCP-Based Queuing Policies



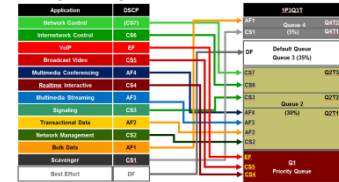
Deploy End-to-End DSCP-Based Queuing Policies

EasyQoS *seamlessly interconnects all types of hardware and software queuing models* to achieve consistent and compatible end-to-end treatments aligned with the expressed business-intent



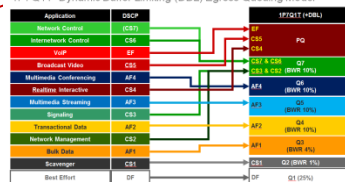
Catalyst 2960-X

1P3Q3T Egress Queuing Model



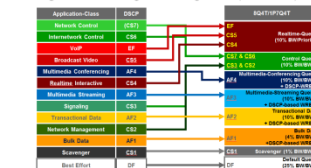
Catalyst 4500

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



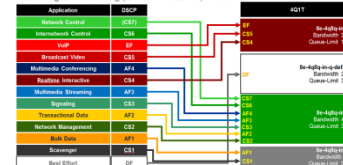
Cisco Catalyst 6500/6800

8Q4T Ingress & 1P7Q4T Egress Queuing Models (6908-10GE)



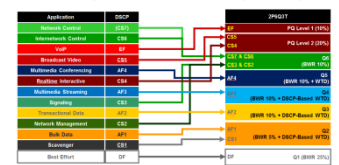
Cisco Nexus 7700 (F3)

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



Catalyst 3650/3850

2P6Q3T with Weighted Tail Drop (WTD) Wired Port Egress Queuing Model



EasyQoS Demo





“QoS rollouts were once 6-month projects costing over \$200K. With Cisco APIC EM Easy QoS, we will go from months to minutes with nominal costs.”

BRIAN MCEVOY

*Symantec
Sr Network Engineer*

Cisco Live Berlin Keynote Video (~21 min in)

https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=93610&backBtn=true

Your Choice:

Manual QoS Policy

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

Intent-Based Application Policy

Your Choice:

Manual QoS Policy

```
match dscp cs4
match dscp af41
match dscp af42
match dscp af43
match dscp cs5
exit
class-map match-any APIC_EM-CONTROL-QUEUE
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
exit
class-map match-any APIC_EM-MM_STREAM-QUEUE
match dscp af31
match dscp af32
match dscp af33
exit
class-map match-any APIC_EM-TRANS_DATA-QUEUE
match dscp af21
match dscp af22
match dscp af23
exit
class-map match-any APIC_EM-BULK_DATA-QUEUE
match dscp af11
match dscp af12
match dscp af13
exit
class-map match-any APIC_EM-SCAVENGER-QUEUE
match dscp cs1
exit
policy-map APIC_EM-QUEUEING-2P6Q3T-OUT
class APIC_EM-VOICE-PQ1
priority level 1 percent 1
queue-buffers ratio 5
class APIC_EM-VIDEO-PQ2
priority level 2 percent 30
queue-buffers ratio 5
class APIC_EM-CONTROL-QUEUE
bandwidth remaining percent 10
queue-buffers ratio 5
class APIC_EM-MM_STREAM-QUEUE
```

Intent-Based Application Policy

Your Choice:

Manual QoS Policy

```
match dscp cs4
match dscp af41
match dscp af42
match dscp af43
match dscp cs5
exit
class-map match-any APIC_EM-CONTROL-QUEUE
match dscp cs2
match dscp cs3
match dscp cs6
match dscp cs7
exit
class-map match-any APIC_EM-MM_STREAM-QUEUE
match dscp af31
match dscp af32
match dscp af33
exit
class-map match-any APIC_EM-TRANS_DATA-QUEUE
match dscp af21
match dscp af22
match dscp af23
exit
class-map match-any APIC_EM-BULK_DATA-QUEUE
match dscp af11
match dscp af12
match dscp af13
exit
class-map match-any APIC_EM-SCAVENGER-QUEUE
match dscp cs1
exit
policy-map APIC_EM-QUEUEING-2P6Q3T-OUT
class APIC_EM-VOICE-PQ1
priority level 1 percent 1
queue-buffers ratio 5
class APIC_EM-VIDEO-PQ2
priority level 2 percent 30
queue-buffers ratio 5
class APIC_EM-CONTROL-QUEUE
bandwidth remaining percent 10
queue-buffers ratio 5
class APIC_EM-MM_STREAM-QUEUE
```

Intent-Based Application Policy

BUSINESS RELEVANT (446)	DEFAULT (348)	BUSINESS IRRELEVANT (388)
<ul style="list-style-type: none">acapactive-directoryMY_CRITICAL_APPalpovertcpagentxalpesaminetandroid-updatesaodvapple-app-storeapple-ios-updates	<ul style="list-style-type: none">3com-amp33com-tsmux3pc3pfsacasaccessbuilderaccessnetworkacpacr-nemaaed-512amanda	<ul style="list-style-type: none">4chan58-cityabc-newsaccuweatheradcashaddthisadobe-connectadweekairplayaliwangwangallrecipes

Apply Policy

APIC-EM EasyQoS At-A-Glance



Cisco APIC-EM QoS

At-A-Glance

The Roles of APIC-EM QoS

QoS is one of the most widely-deployed technologies in the enterprise and needs to be deployed in a holistic, integrated, end-to-end manner to ensure maximum effectiveness. As such, it is a prime candidate technology to showcase the value-add of Software Defined Networking (SDN), which allows for:

- Integrating applications with the network infrastructure
- Capturing business intent of QoS policies so as to articulate an end-to-end QoS strategy
- Abstracting platform-specific implementation details, while maintaining cross-platform consistency
- Dynamic QoS policies based on application requirements and events

Integrating Applications with the Network

A key objective of SDN is to allow for communication between applications and the network. This is done by supporting (Northbound) Application Programming Interfaces (APIs) between software applications and the network controller, such as Cisco's Application Policy Infrastructure Controller-Enterprise Module (APIC-EM). In this manner, the network can adapt policies to application's requirements, as well as provide feedback so that applications can also make intelligent decisions based on dynamic network conditions.

Figure 1 Cisco APIC-EM Architecture



Capturing Business Intent and Articulating QoS Strategy

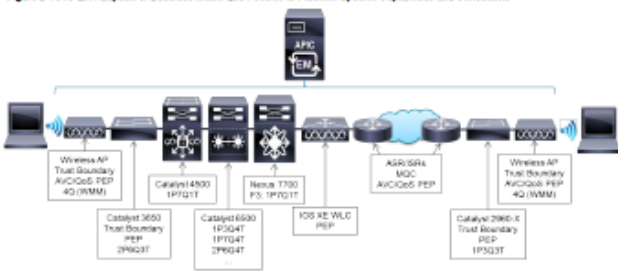
Without a centralized controller, application policies (such as QoS) have to be independently configured on individual network devices and it would be up to the administrator to ensure compatibility and cohesiveness across the network. However, a controller-based approach allows for administrators to centrally define QoS policies, by expressing the business-relevance of applications. With this information, the controller can then articulate an end-to-end strategy that is to be deployed across all network devices in a consistent manner.

Abstracting Platform-Specific Implementation Details

With a central QoS strategy defined, the controller can then apply Cisco Validated Design (CVD) best-practices to translate the policy to device-specific configurations, which it then pushes down to all network devices via (Southbound) APIs, as shown in Figure 2.

In this manner, device-specific details are completely abstracted from the network operator, who can thus focus on business objectives and results.

Figure 2 APIC-EM Adaptation of Business Intent QoS Policies to Platform-Specific Capabilities and Constraints



Three key design principles are followed when translating the strategic (business-intent) QoS policy into tactical (device-specific) configurations:

- The first is that the primary goal of the tactical QoS policy is to express the strategic QoS policy with maximum fidelity, subject to any platform-specific technical constraints.
- The second is that QoS features will not be enabled simply because these exist, but rather only features that directly contribute to the strategic policy will be enabled.
- The third is that all features that are enabled are done in accordance with CVD best-practices.

Cisco APIC-EM QoS

At-A-Glance

Dynamic Application-Based QoS Policies

A unique advantage that a controller-based architecture brings to the network is the ability to deploy dynamic QoS policies in a scalable and virtually instantaneous manner.

For example, APIC-EM can integrate via APIs to collaborative multimedia applications, including Cisco Jabber and Microsoft Lync (now Skype for Business). By means of this integration, QoS policies can be dynamically applied throughout the network to prioritize voice and video flows.

Such dynamic QoS policies allow for these applications to have their flows protected with QoS, regardless of whether:

- the endpoint devices are wired or wireless
- the endpoint devices are IT-managed or BYOD
- the media flows are encrypted or not

There are 5 main steps to these dynamic QoS policies:

Step 1: A network operator enters business-intent into APIC-EM, which then articulates a strategic end-to-end QoS policy, as shown in Figure 3.

Step 2: APIC-EM translates the strategic policy into device-specific tactical policies, including classification, marking and queuing policies.

Note: classification policies for voice and video - which are access-list (ACL) based - do not (initially) include any access-list entries (ACEs) to discretely identify the IP flows to which these should apply.

Note: Queuing policies (not shown in Figure 3, but expressed in Figure 1) are all DSCP-based.

Step 3: APIC-EM is informed (by either Cisco Unified Call Manager or the Microsoft Lync server) of a proceeding call. This includes the 5-tuple information (IP Source / Destination Addresses and UDP Source / Destination Ports) of the voice and video flows, as shown in Figure 4.

Step 4: APIC-EM dynamically pushes out ACEs to the edge switches hosting the endpoints.

Step 5: APIC-EM is informed of a terminated call.

Step 6: APIC-EM removes the ACEs corresponding to the terminated call. (Steps 5 & 6 are not shown).

Figure 3 APIC-EM Dynamic QoS Policies - Steps 1 (Operator Expresses Business Intent) and 2 (Tactical QoS Policies Deployed)

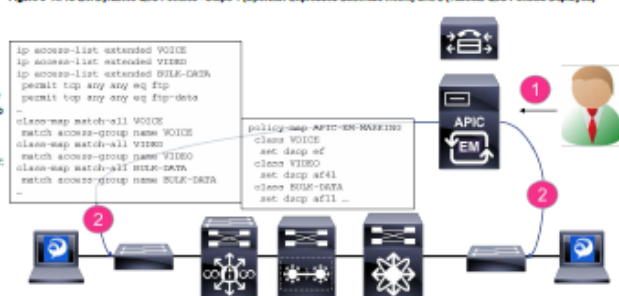
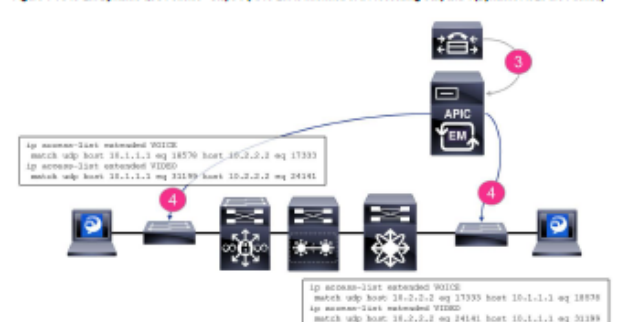


Figure 4 APIC-EM Dynamic QoS Policies - Steps 3 (APIC-EM is informed of a Proceeding Call) and 4 (Dynamic ACEs are Pushed)



Copyright © 2018 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

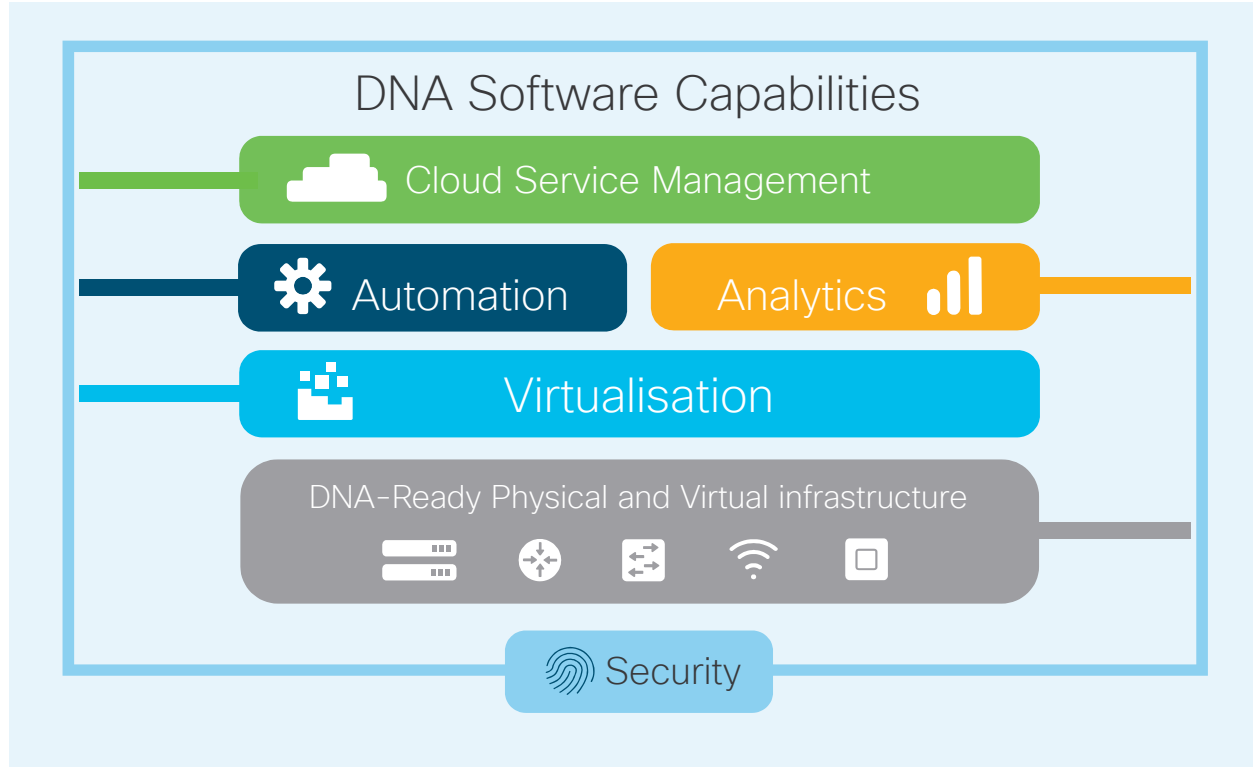
<https://cisco.box.com/v/QoS-AAGs>

Cisco live!

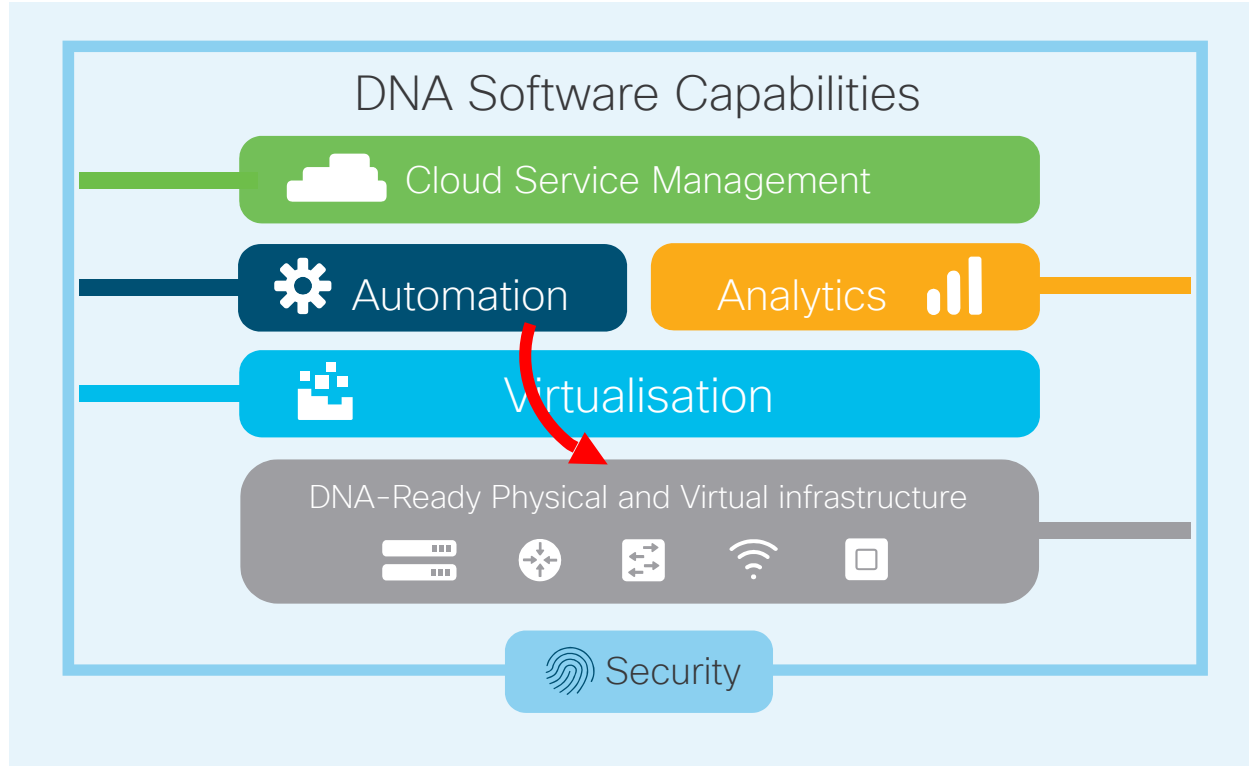
DNA Application Assurance

Tim Szigeti

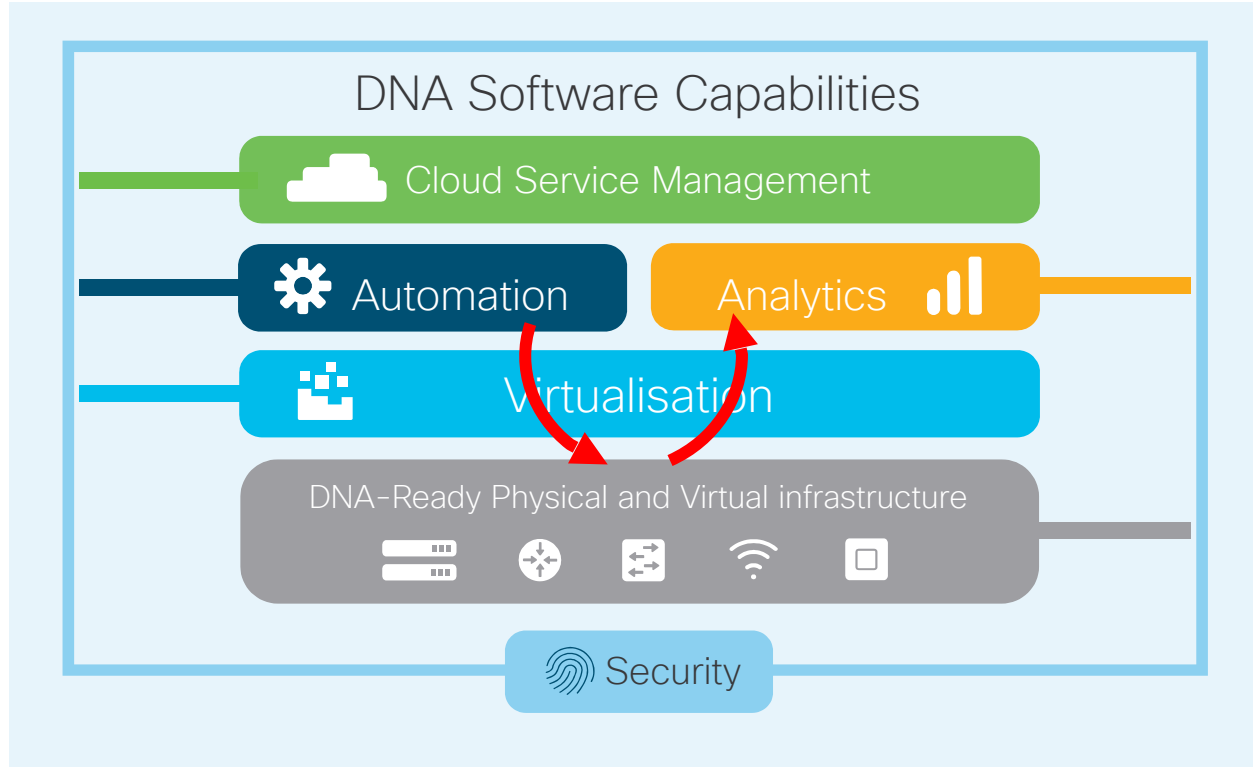
Cisco DNA Architecture



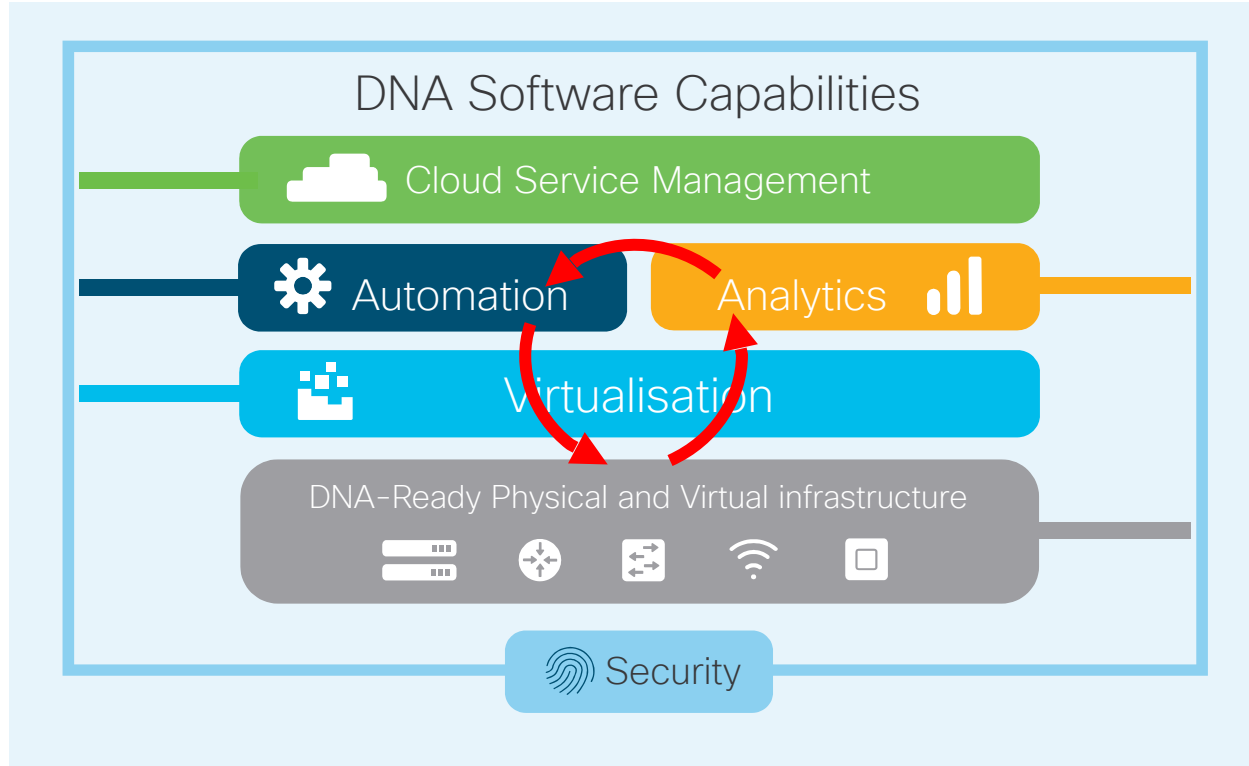
Cisco DNA Architecture



Cisco DNA Architecture



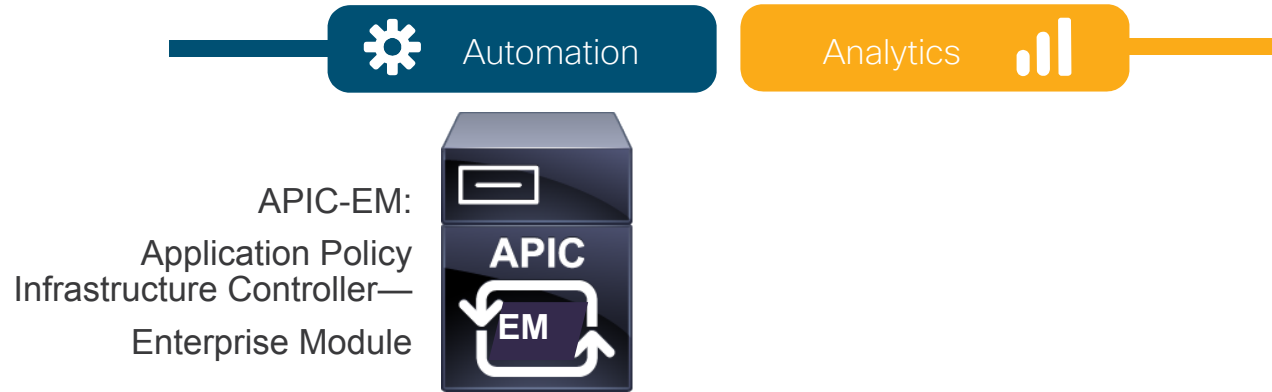
Cisco DNA Architecture



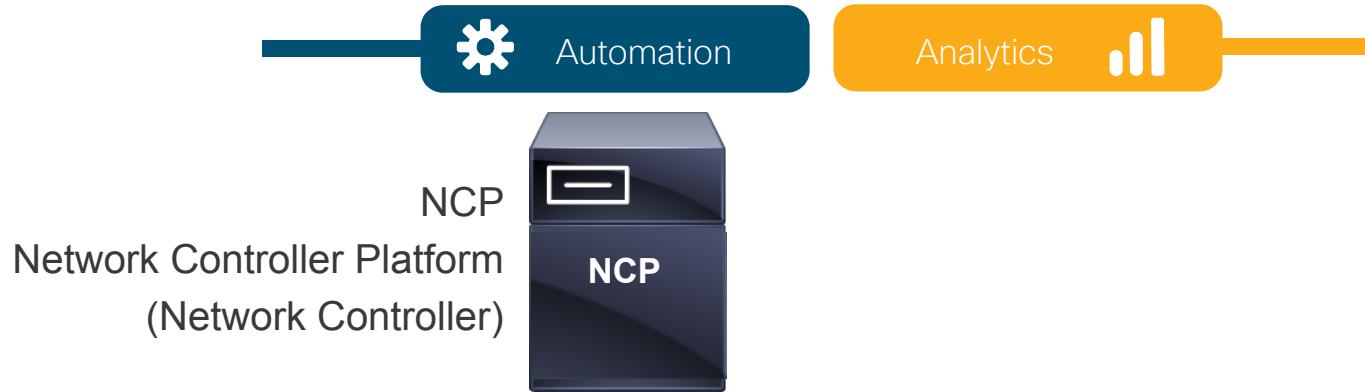
Cisco DNA Architecture—Automation and Analytics



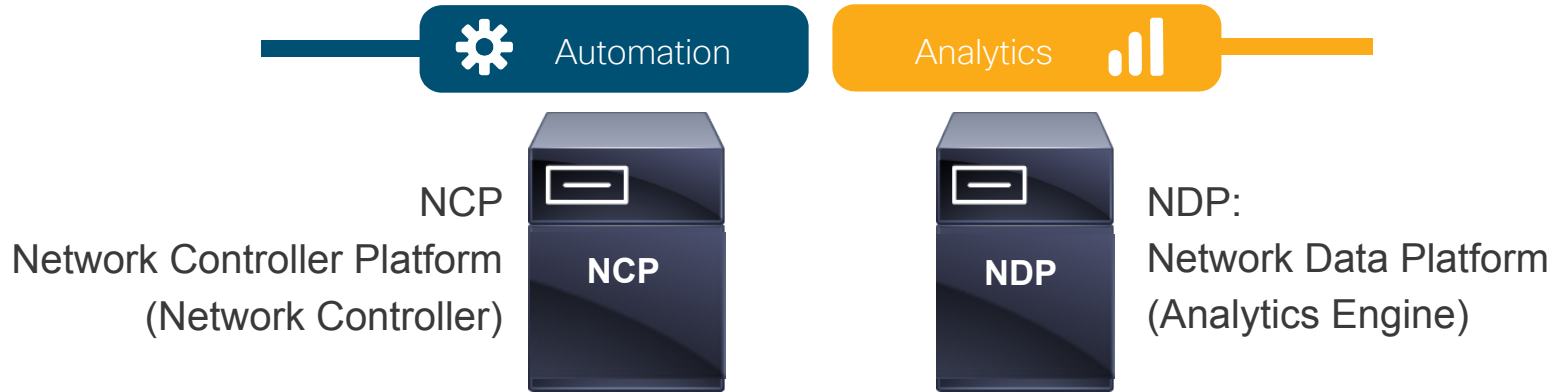
Cisco DNA Architecture—Automation and Analytics



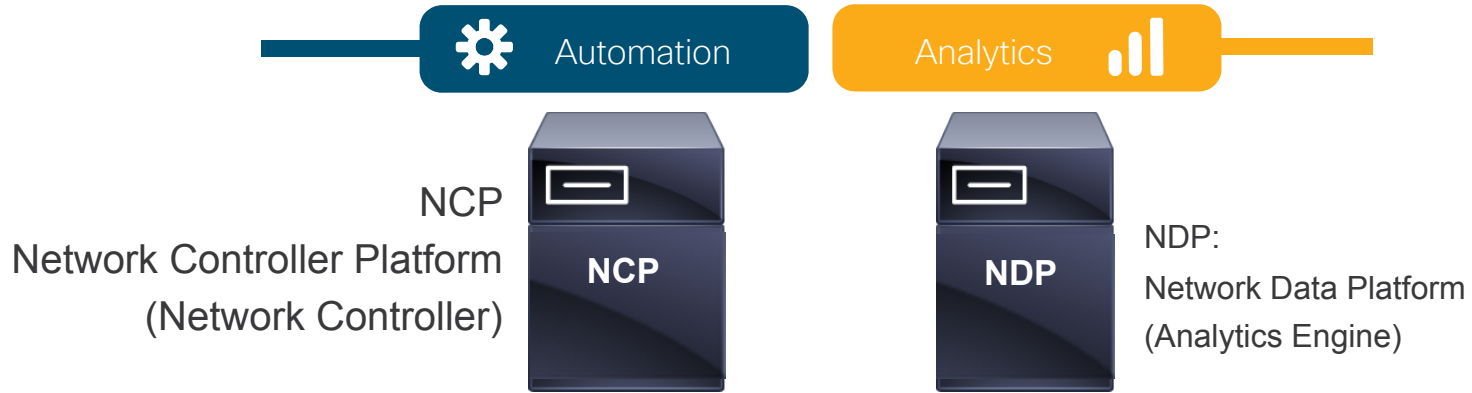
Cisco DNA Architecture—Automation and Analytics



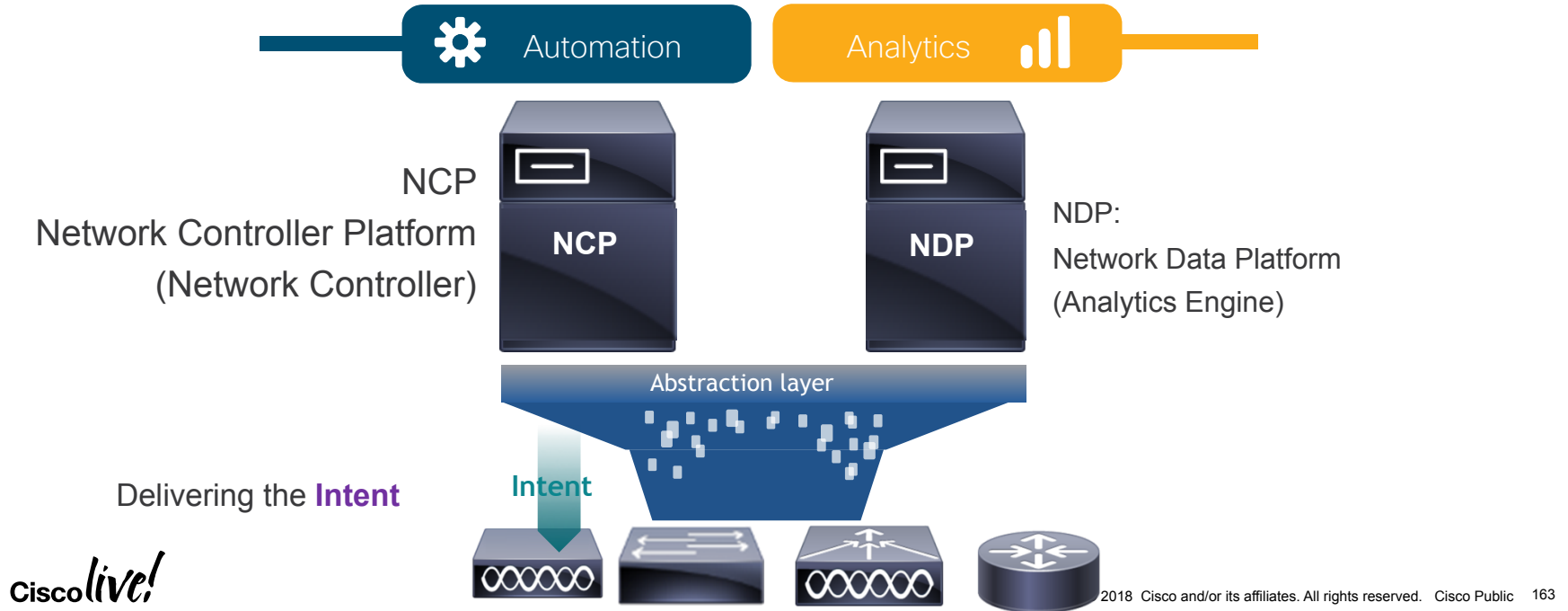
Cisco DNA Architecture—Automation and Analytics



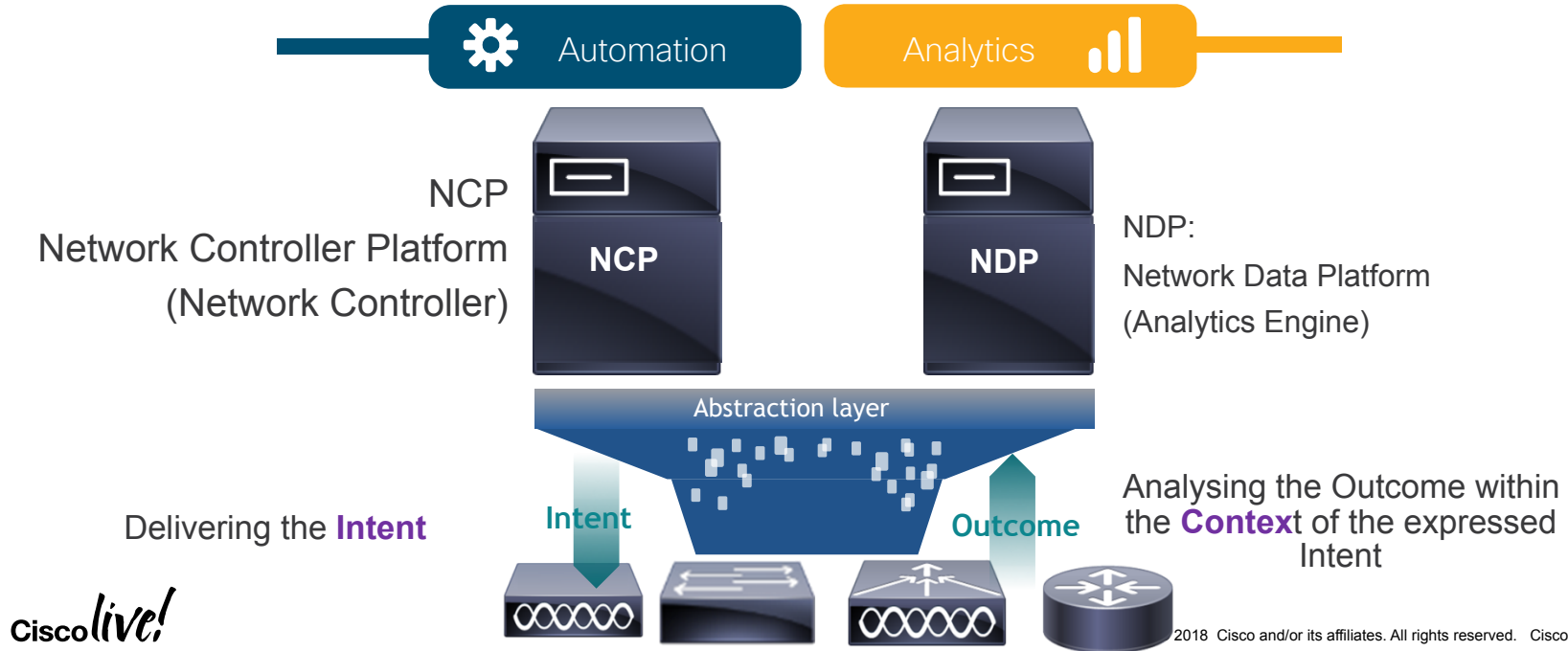
Cisco DNA Architecture—Automation and Analytics



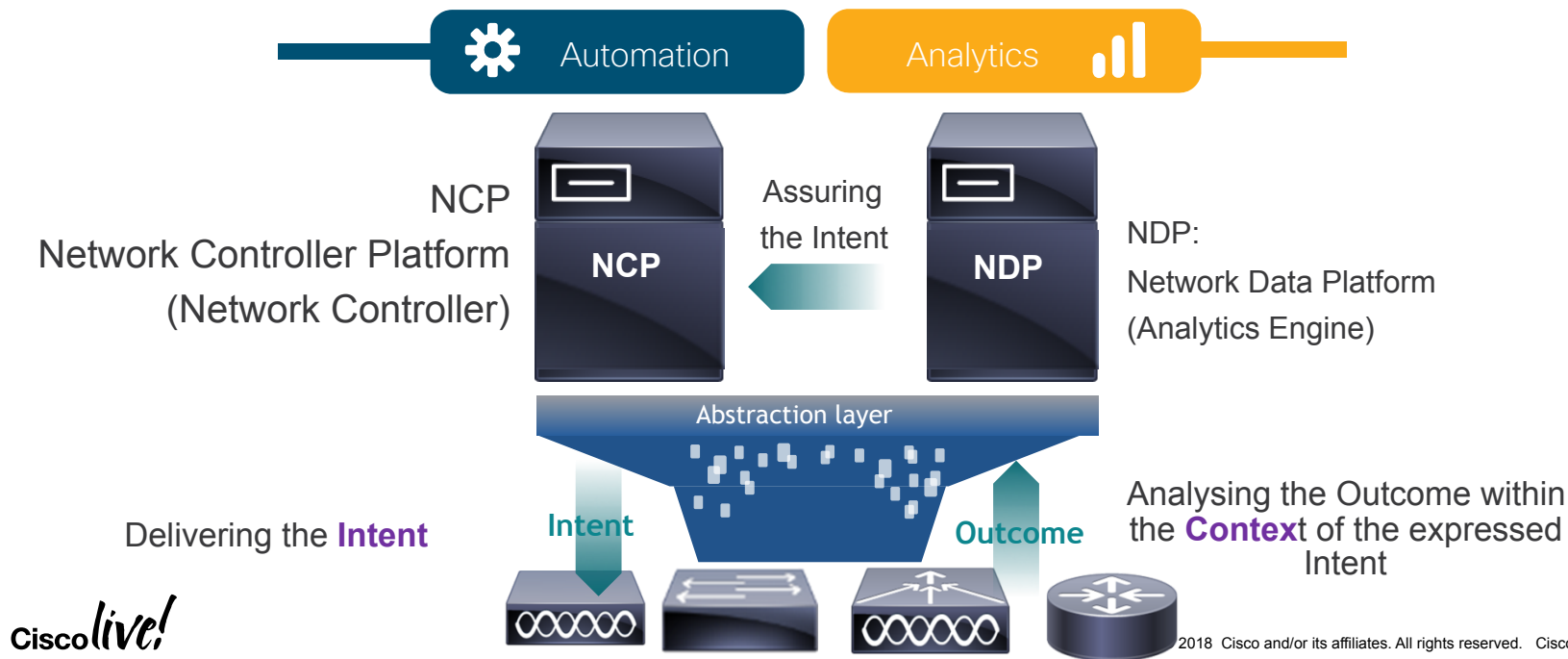
Cisco DNA Architecture—Automation and Analytics



Cisco DNA Architecture—Automation and Analytics



Cisco DNA Architecture—Automation and Analytics



Cisco DNA Architecture—DNA Centre



Cisco DNA Architecture—DNA Centre

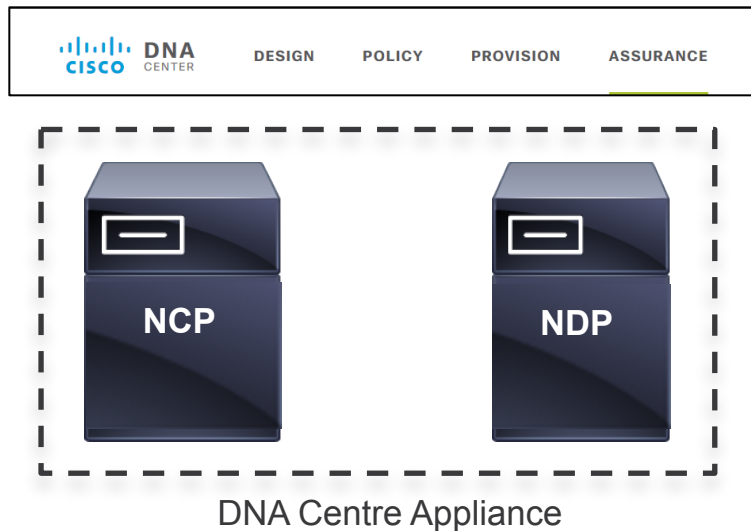


DNA Centre Appliance

Cisco DNA Architecture—DNA Centre

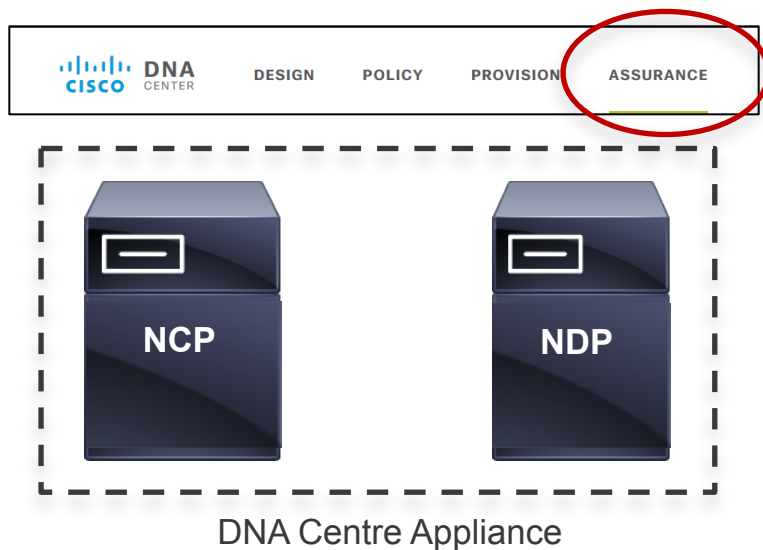
DNA Centre User Interface

A single pane of glass for Design, Policy, Provisioning, and Assurance



Cisco DNA Architecture—DNA Centre

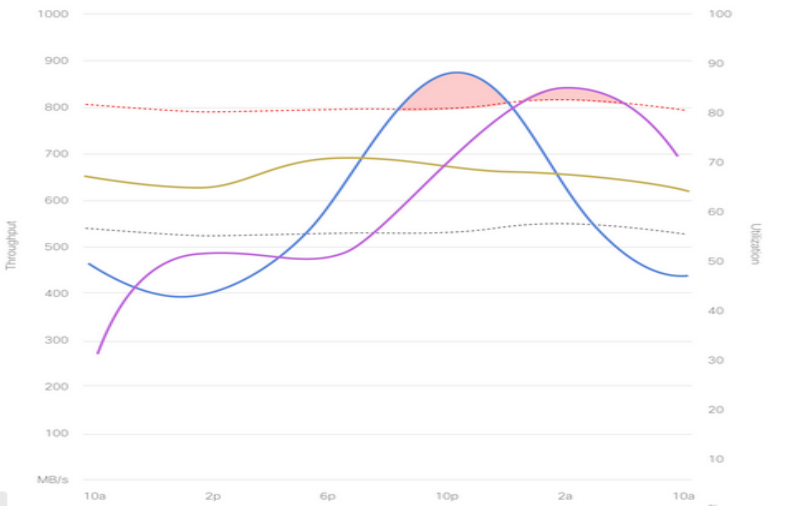
DNA Centre User Interface
A single pane of glass for Design, Policy, Provisioning, and Assurance



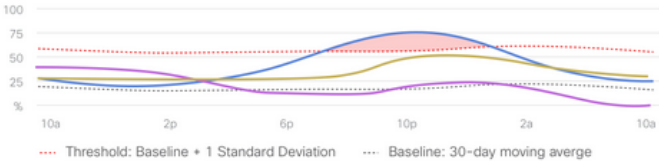
DNA Application Assurance

Business Relevant Default Business Irrelevant

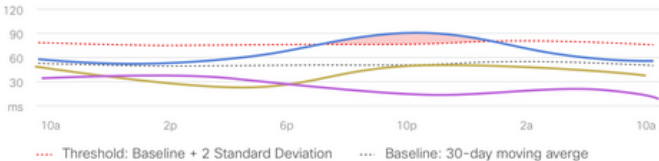
Throughput and Bandwidth Utilization



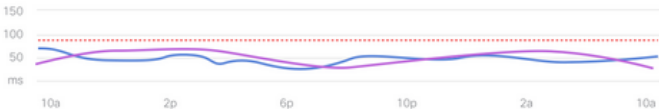
Packet Loss



Delay



Jitter

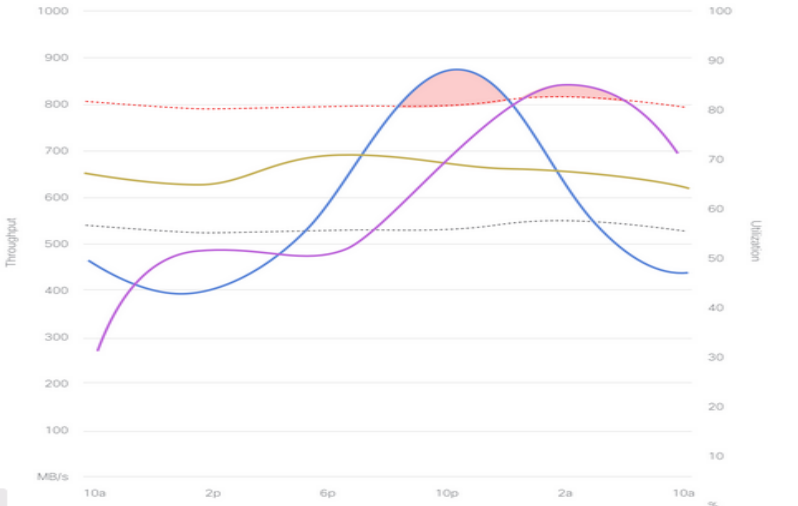


Application		Health		Destination Location	Average Rate (Mbps)	Average Bandwidth Utilization	10a		2p		6p		10p		2a		10a		Jitter (ms)		Path Trace	
Name / IP	Port	Most Recent ▾	Last 24 hours				Engress	Marking	Preservation	Max	Average	Max	Average	Max	Average	Max	Average					
<div><div></div>All Application</div>	---	6	<div></div>	SEA	62	62%	<value>	AF41	Yes		11%	11%	62	62	62	62				---		
<div><div></div>Webex / 192.23.11.4</div>	40	4	<div></div>	SF	25	25%	<value>	AF31	Yes		2%	2%	25	25	25	25				<div></div>		
<div><div></div>192.45.11.25</div>	120	5	<div></div>	SF	92	92%	<value>	AF41	No		25%	25%	92	92	92	92				<div></div>		
<div><div></div>119.192.4.16</div>	44	5	<div></div>	PHX	73	73%	<value>	AF31	Yes		21%	21%	73	73	73	73				<div></div>		
<div><div></div>File Transfer / 122.31.22.1</div>	22	7	<div></div>	LA	92	92%	<value>	EF	No		1%	1%	92	92	92	92				<div></div>		
<div><div></div>11.156.25.122</div>	12	7	<div></div>	LA	92	92%	<value>	EF	No		2%	2%	92	92	92	92				<div></div>		

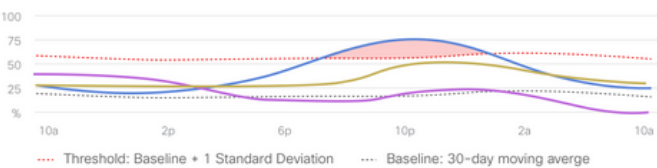
DNA Application Assurance

Business Relevant Default Business Irrelevant

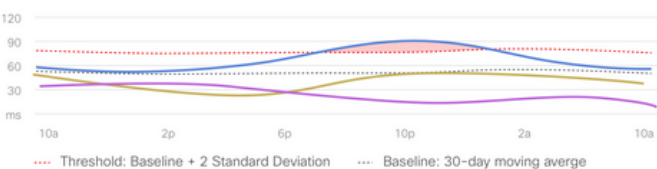
Throughput and Bandwidth Utilization



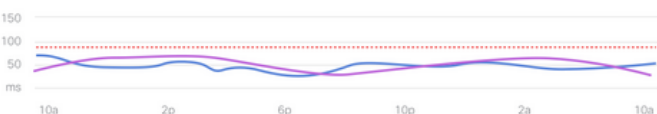
Packet Loss



Delay



Jitter

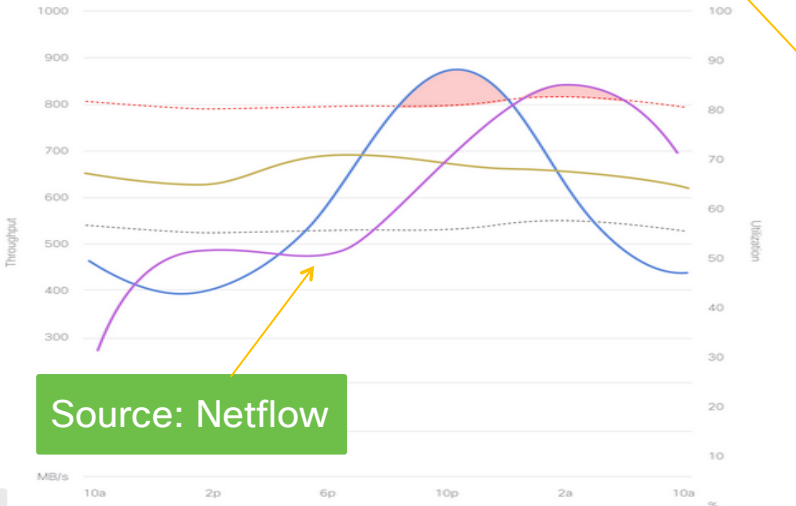


Application		Health		Destination Location	Average Rate (Mbps)	Average Bandwidth Utilization	10a		2p		6p		10p		2a		10a		Jitter (ms)		Path Trace	
Name / IP	Port	Most Recent	Last 24 hours				Engress	Marking	Preservation	Max	Average	Max	Average	Max	Average	Max	Average					
All Application	---	6		SEA	62	62%	<value>	AF41	Yes		11%	11%	62	62	62	62				---		
Webex / 192.23.11.4	40	4		SF	25	25%	<value>	AF31	Yes		2%	2%	25	25	25	25						
192.45.11.25	120	5		SF	92	92%	<value>	AF41	No		25%	25%	92	92	92	92						
119.192.4.16	44	5		PHX	73	73%	<value>	AF31	Yes		21%	21%	73	73	73	73						
File Transfer / 122.31.22.1	22	7		LA	92	92%	<value>	EF	No		1%	1%	92	92	92	92						
11.156.25.122	12	7		LA	92	92%	<value>	EF	No		2%	2%	92	92	92	92						

DNA Application Assurance

Business Relevant Default Business Irrelevant

Throughput and Bandwidth Utilization



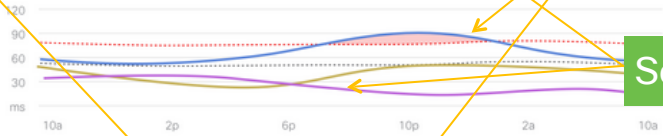
Source: PerfMon

Packet Loss



Source: CB-QoS MIB

Delay



Source: IP SLA

Jitter

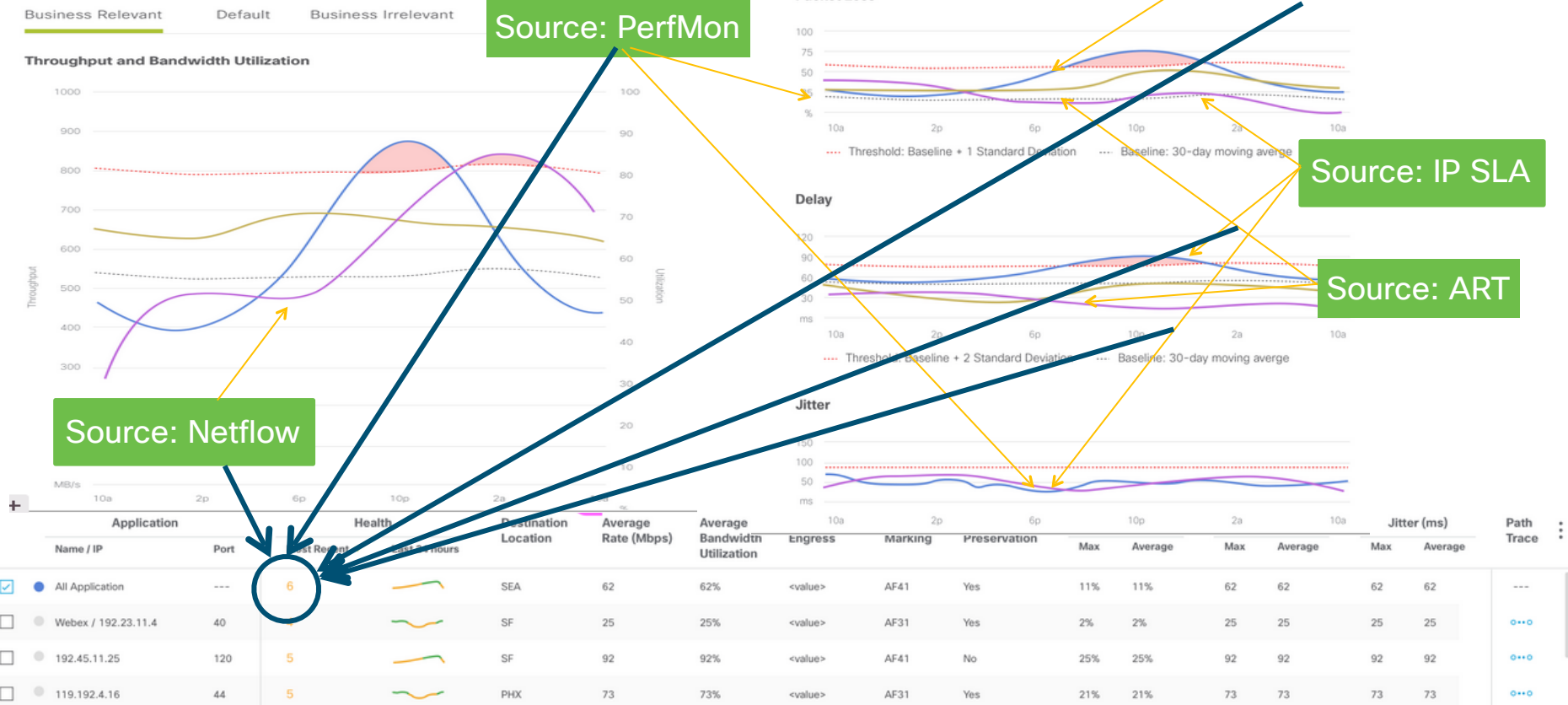


Source: ART

Source: Netflow

Application		Health		Destination Location	Average Rate (Mbps)	Average Bandwidth Utilization	Engress	Marking	Preservation	Max	Average	Max	Average	Jitter (ms)		Path Trace
Name / IP	Port	Most Recent	Last 24 hours											Max	Average	
☒ All Application	---	6		SEA	62	62%	<value>	AF41	Yes	11%	11%	62	62	62	62	---
☐ Webex / 192.23.11.4	40	4		SF	25	25%	<value>	AF31	Yes	2%	2%	25	25	25	25	
☐ 192.45.11.25	120	5		SF	92	92%	<value>	AF41	No	25%	25%	92	92	92	92	
☐ 119.192.4.16	44	5		PHX	73	73%	<value>	AF31	Yes	21%	21%	73	73	73	73	
☐ File Transfer / 122.31.22.1	22	7		LA	92	92%	<value>	EF	No	1%	1%	92	92	92	92	
☐ 11.156.25.122	12	7		LA	92	92%	<value>	EF	No	2%	2%	92	92	92	92	

DNA Application Assurance

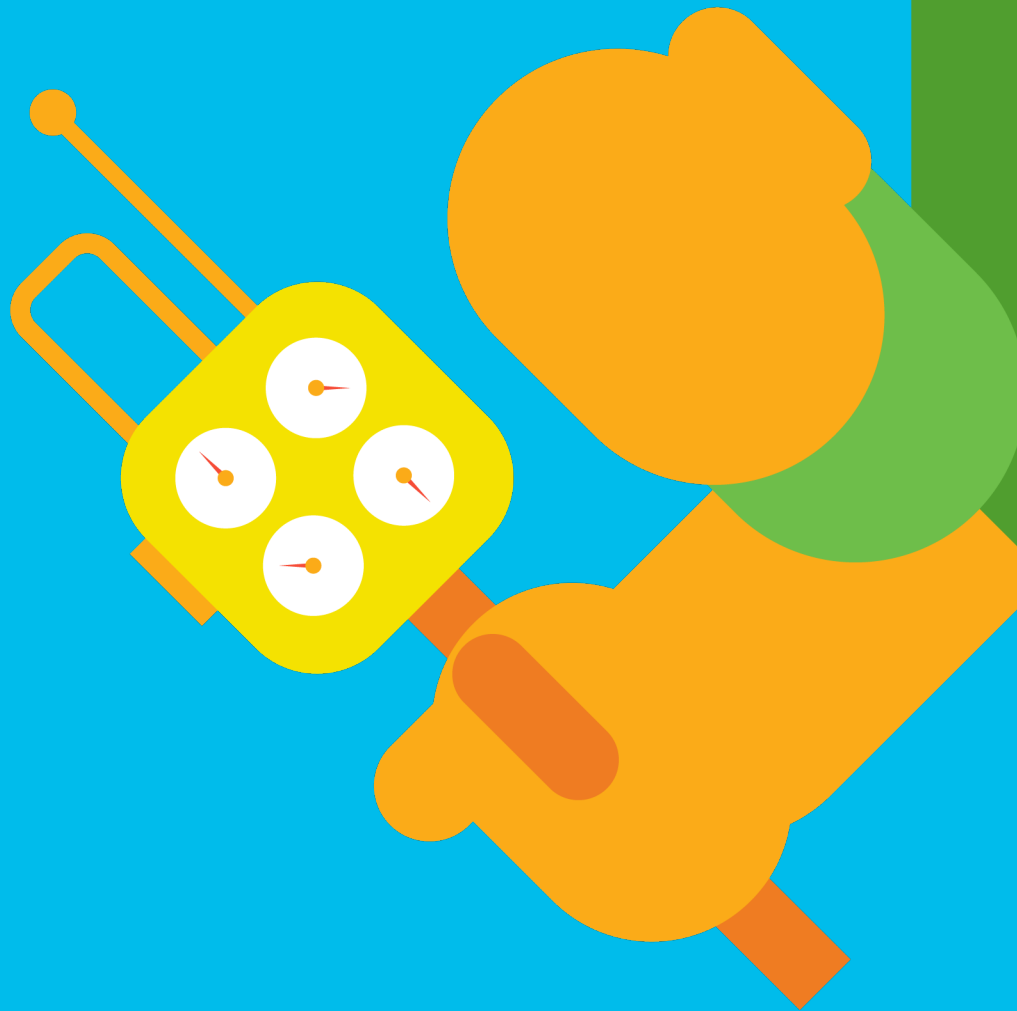


DNA Assurance uses multiple sources of data to generate a multi-dimensional Application Health Score, including network metrics (like packet-loss, latency and jitter), as well as application-specific metrics. 166

Agenda

- Introduction to Strategic QoS Design
- WAN / IWAN QoS Design
- Campus QoS Design
- WLAN QoS Design
- Automating and Assuring QoS
- **Summary and References**
- Appendices

Summary and References



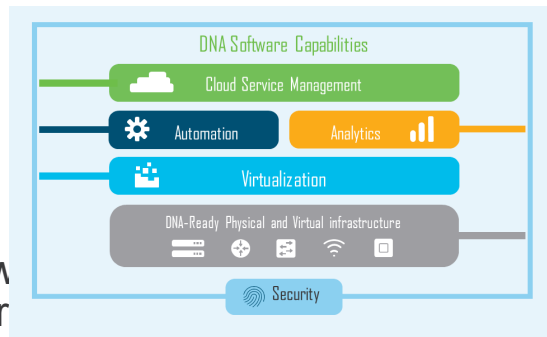
Enterprise QoS Design Summary

Part 1: QoS in DNA

Enterprise QoS Design Summary

Part 1: QoS in DNA

- Cisco has adopted a new paradigm for QoS focusing on policy-abstraction
 - Articulate business intent as a **strategic** end-to-end policy
 - Device-specific **tactical** policies reflect strategic policy with maximum fidelity
- Cisco platform-specific features and controller-based applications all revolve around this paradigm, including:
 - NBAR QoS Attributes (LAN & WAN)
 - IWAN & IWAN App
 - FastLane for iOS for WLAN
 - EasyQoS & DNA Centre Application Policy
 - DNA Assurance
- Cisco's DNA architecture combines hardware, software, and services to deliver



Enterprise QoS Design Summary

Part 2: WAN & IWAN QoS Design

Enterprise QoS Design Summary

Part 2: WAN & IWAN QoS Design

- Use new NBAR2 QoS Attributes (traffic-class and business-relevance) to mark on LAN edges

Enterprise QoS Design Summary

Part 2: WAN & IWAN QoS Design

- Use new NBAR2 QoS Attributes (traffic-class and business-relevance) to mark on LAN edges
- Design WAN/IWAN edge policies to address:
 - QoS Scheduling
 - Aggregate priority load
 - IPSec Anti-Replay
- Know and leverage WAN edge tools, including:
 - Hierarchical QoS policies for sub-line-rate interfaces
 - DMVPN Per-Tunnel QoS for IWAN
 - Enterprise-to-SP Mapping Models
- Or ... just click on the easy button with IWAN App



Enterprise QoS Design Summary

Part 3: Campus QoS Design

Enterprise QoS Design Summary

Part 3: Campus QoS Design

- Campus QoS is key to managing packet loss due to instantaneous buffer overruns which are *very common* in oversubscribed campus networks

Enterprise QoS Design Summary

Part 3: Campus QoS Design

- Campus QoS is key to managing packet loss due to instantaneous buffer overruns which are *very common* in oversubscribed campus networks
- Know your QoS toolset, as hardware features and software syntax vary from platform-to-platform

Enterprise QoS Design Summary

Part 3: Campus QoS Design

- Campus QoS is key to managing packet loss due to instantaneous buffer overruns which are *very common* in oversubscribed campus networks
- Know your QoS toolset, as hardware features and software syntax vary from platform-to-platform
- Cisco provides At-A-Glance Guides to get you up-and-running quickly, as well as detailed Cisco Validated Design Guides

Enterprise QoS Design Summary

Part 3: Campus QoS Design

- Campus QoS is key to managing packet loss due to instantaneous buffer overruns which are *very common* in oversubscribed campus networks
- Know your QoS toolset, as hardware features and software syntax vary from platform-to-platform
- Cisco provides At-A-Glance Guides to get you up-and-running quickly, as well as detailed Cisco Validated Design Guides
- Or ... just click on the easy button with EasyQoS App



Enterprise QoS Design Summary

Part 4: WLAN QoS Design

Enterprise QoS Design Summary

Part 4: WLAN QoS Design

- Design your RF for Voice Efficiency

Enterprise QoS Design Summary

Part 4: WLAN QoS Design

- Design your RF for Voice Efficiency
- Restructure upstream and downstream marking and trust

Enterprise QoS Design Summary

Part 4: WLAN QoS Design

- Design your RF for Voice Efficiency
- Restructure upstream and downstream marking and trust
- Use Platinum for your WLANs

Enterprise QoS Design Summary

Part 4: WLAN QoS Design

- Design your RF for Voice Efficiency
- Restructure upstream and downstream marking and trust
- Use Platinum for your WLANs
- Apply efficient EDCA if possible; CAC if needed

Enterprise QoS Design Summary

Part 4: WLAN QoS Design

- Design your RF for Voice Efficiency
- Restructure upstream and downstream marking and trust
- Use Platinum for your WLANs
- Apply efficient EDCA if possible; CAC if needed
- FastLane is a plus in most cases

Enterprise QoS Design Summary

Part 4: WLAN QoS Design

- Design your RF for Voice Efficiency
- Restructure upstream and downstream marking and trust
- Use Platinum for your WLANs
- Apply efficient EDCA if possible; CAC if needed
- FastLane is a plus in most cases
- Or ... just click on the easy button with EasyQoS App



Enterprise QoS Design Summary

Parts 5: Looking Ahead

Enterprise QoS Design Summary

Parts 5: Looking Ahead

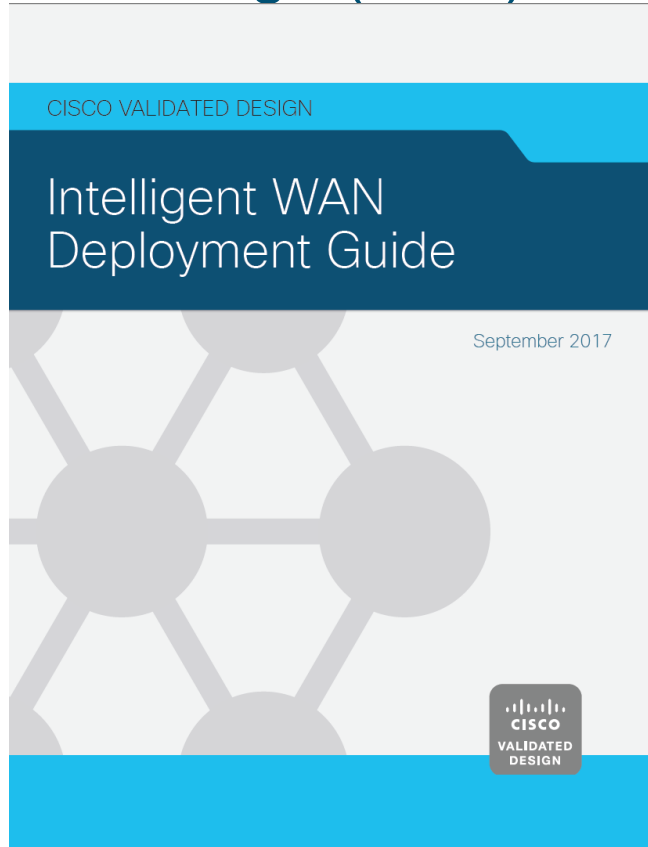
- Cisco campus hardware will converge on UADP
 - this will finally realise the long-held goal of a single hardware queuing model for access, distribution/aggregation and core
- Cisco routing, switching and wireless software will converge on IOS XE
 - All QoS policies will expressed via MQC

Enterprise QoS Design Summary

Parts 5: Looking Ahead

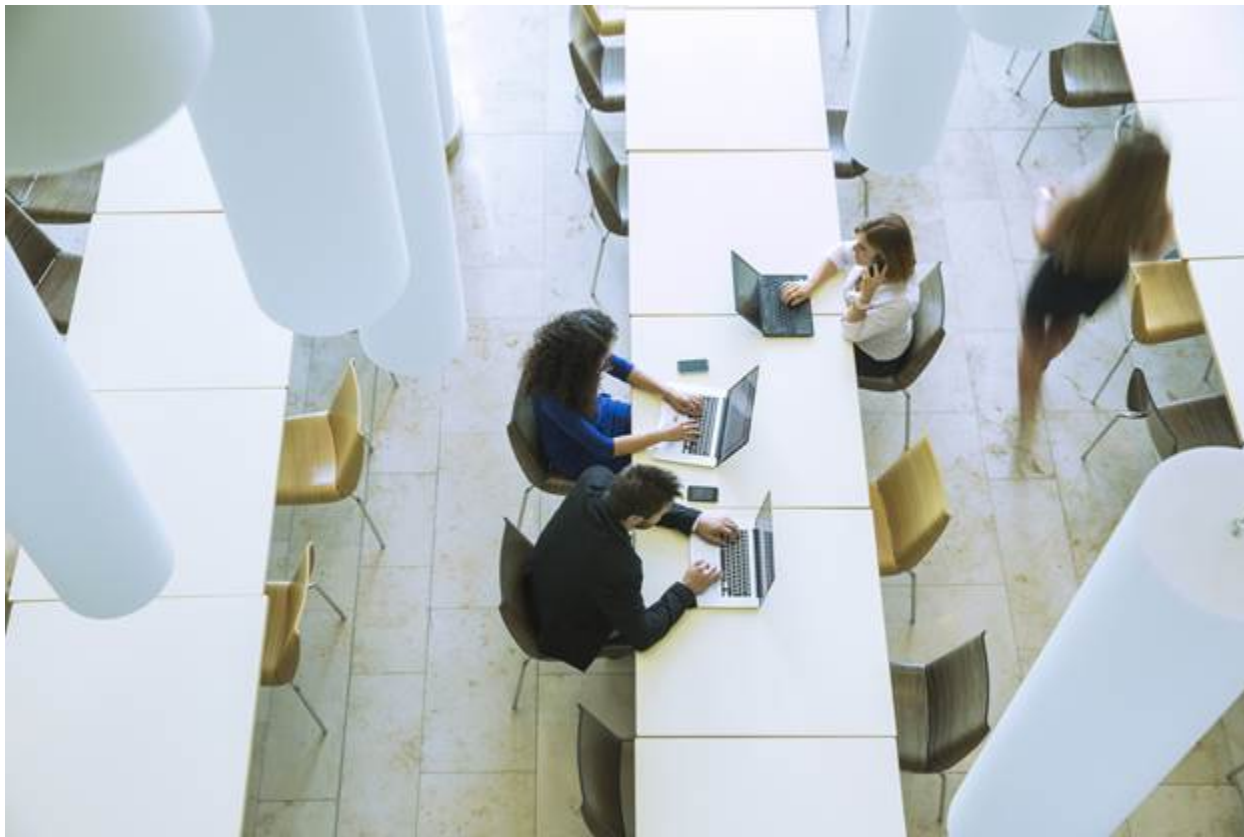
- Cisco campus hardware will converge on UADP
 - this will finally realise the long-held goal of a single hardware queuing model for access, distribution/aggregation and core
- Cisco routing, switching and wireless software will converge on IOS XE
 - All QoS policies will expressed via MQC
- Cisco will continue to simplify the automation of QoS features
 - AutoQoS 5.0
- Cisco is complementing QoS automation with an analytics and assurance to correlate disparate data-sources, identify anomalies and guide the troubleshooting of application quality issues

IWAN Cisco Validated Design (CVD) Guide



<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Sep2017/CVD-IWANDeployment-SEP17.pdf>

EasyQoS Cisco Validated Design (CVD) Guide



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

Recommended Reading

End-to-End QoS (v2)

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

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

Cisco *live!*



End-to-End QoS Network Design

Quality of Service for
Rich-Media & Cloud Networks
Second Edition

ciscopress.com

Copyrighted Material

Tim Szigeti
Christina Hattingh
Robert Barton
Kenneth R. Briley, Jr.

Recommended Reading

End-to-End QoS (v2)

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

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

Cisco *live!*



End-to-End QoS Network Design

Quality of Service for
Rich-Media & Cloud Networks
Second Edition

ciscopress.com

Copyrighted Material

Tim Szigeti
Christina Hattingh
Robert Barton
Kenneth R. Briley, Jr.

Recommended Reading End-to-End QoS (v2)

Amazon.com Overall Rating: ★★★★★

"The best ever book on QoS on the market. Bravo to the author."

"AWESOME RESUME OF QoS TECHNOLOGIES"

"I strongly recommend this book to anyone working with Cisco infrastructure."

"This book is an all-encompassing presentation and tutorial on Cisco Quality of Service (QoS)"

"QoS is intimidating; however, this book is a tremendous resource that will ease your anxiety."

"This book is kept in my cubicle and is already filled with highlights, notes in the margin, and many dog-eared pages."

"QOS is often misunderstood, and he explains it very well. The explanations are thorough to help understand each case"

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

Cisco *live!*



End-to-End QoS Network Design

Quality of Service for
Rich-Media & Cloud Networks
Second Edition

Tim Szigeti
Christina Hattingh
Robert Barton
Kenneth R. Briley, Jr.

ciscopress.com

Copyrighted Material

BRKCF

177

WE NO LONGER Recommended Reading End-to-End QoS (v2) (USE EASYQOS INSTEAD)

Amazon.com Overall Rating: ★★★★★

"The best ever book on QoS on the market. Bravo to the author."

"AWESOME RESUME OF QoS TECHNOLOGIES"

"I strongly recommend this book to anyone working with Cisco infrastructure."

"This book is an all-encompassing presentation and tutorial on Cisco Quality of Service (QoS)"

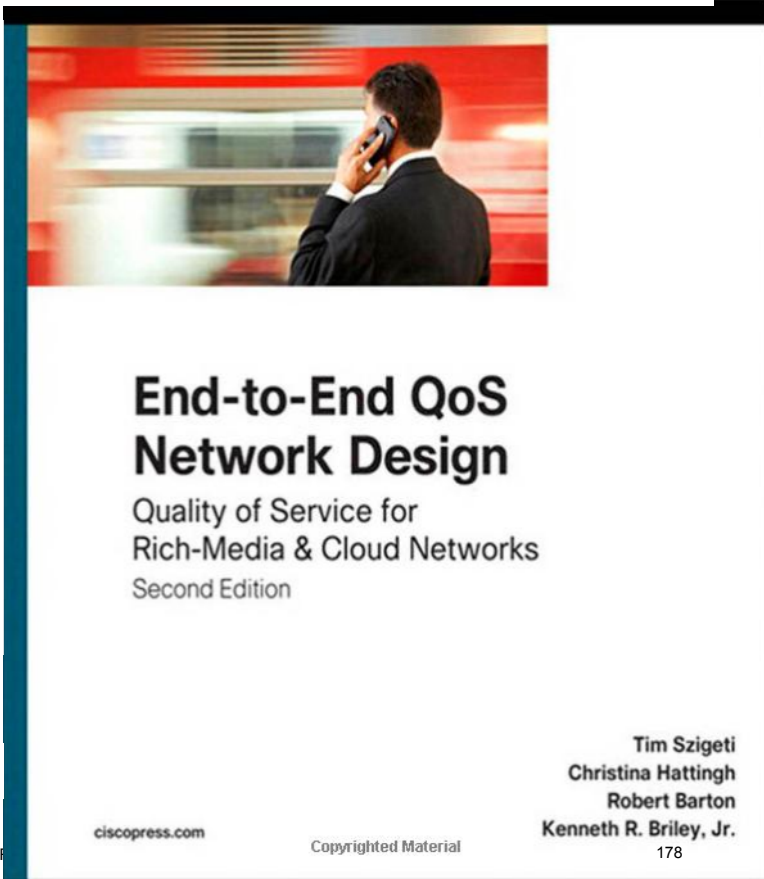
"QoS is intimidating; however, this book is a tremendous resource that will ease your anxiety."

"This book is kept in my cubicle and is already filled with highlights, notes in the margin, and many dog-eared pages."

"QOS is often misunderstood, and he explains it very well. The explanations are thorough to help understand each case"

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

Cisco *live!*



Next Steps: Download APIC-EM (and EasyQOS App)

FREE Download at: cisco.com/go/apicem



Worldwide [change] | Welcome, Saurav Prasad | Account | Log Out | My Cisco

Products & Services | Support | How to Buy | Training & Events | Partners | Employees

Search

Products & Services / Cloud and Systems Management /

Cisco Application Policy Infrastructure Controller Enterprise Module



Automate network configuration and setup

APIC-EM is a central part of Cisco Digital Network Architecture. It delivers software-defined networking to the enterprise branch, campus, and WAN. Its simple user interface lets you automate policy-based application profiles. With this module, IT can respond rapidly to new business opportunities.

[Watch the video](#)[See our DNA offers](#)

Features | Applications | Deploy | Services | Case Studies | News | Support | For partners

Partner Help

What Cisco APIC-EM can do for you

Q & A

Complete Your Online Session Evaluation

- Give us your feedback and receive a **Cisco Live 2018 Cap** by completing the overall event evaluation and 5 session evaluations.
- All evaluations can be completed via the Cisco Live Mobile App.

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at www.CiscoLive.com/Global.

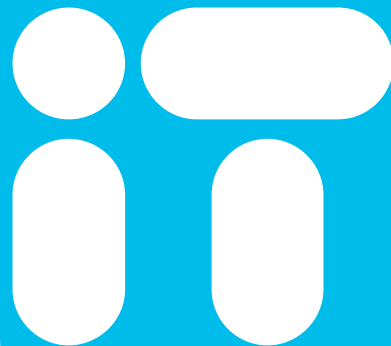




Thank you



You're

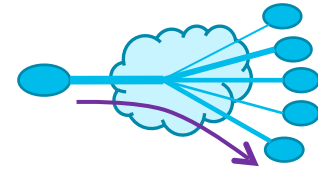
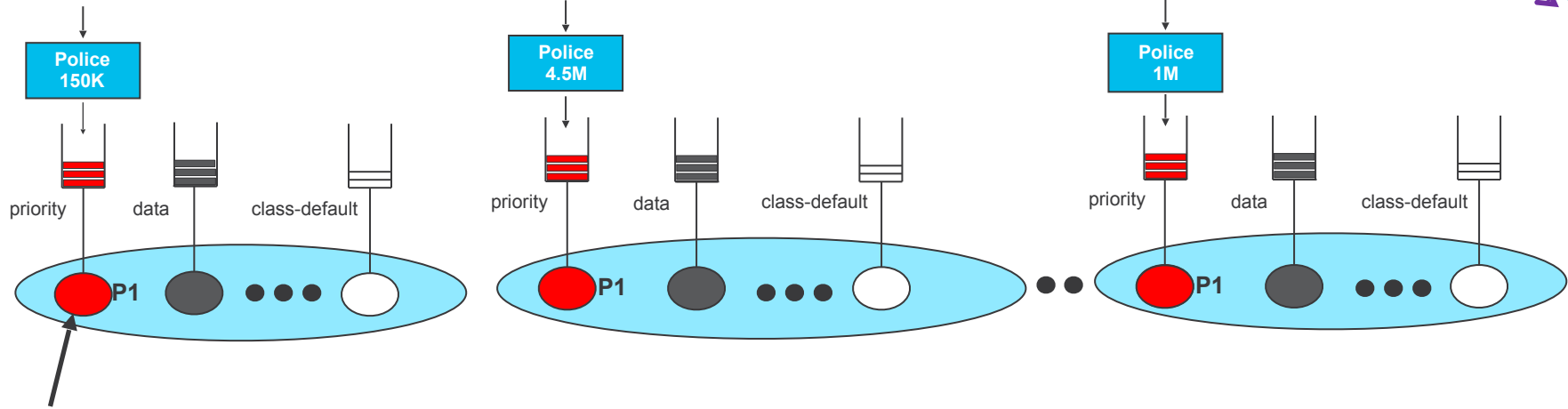


Cisco *live!*

Appendix A—IWAN QoS Design

Aggregate Priority Load

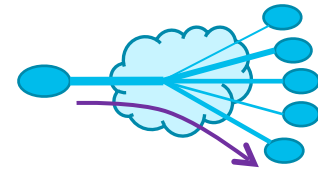
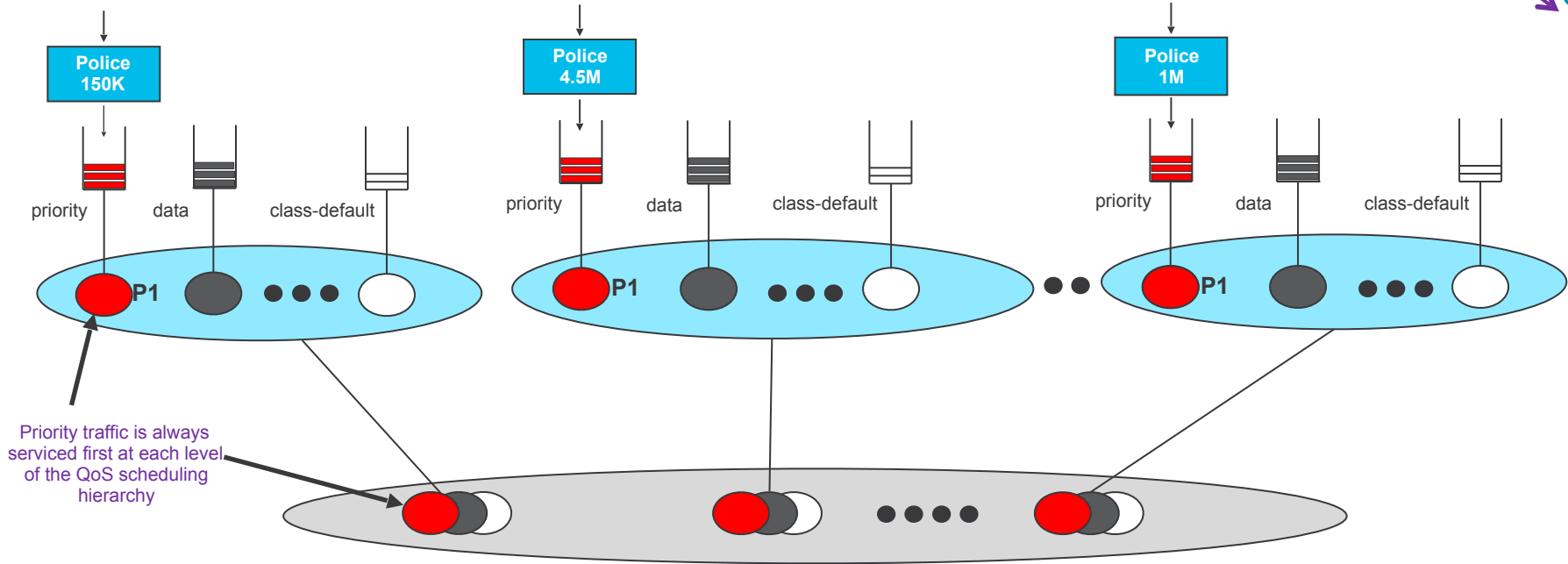
Priority Propagation / Passing Lanes



Priority traffic is always serviced first at each level of the QoS scheduling hierarchy

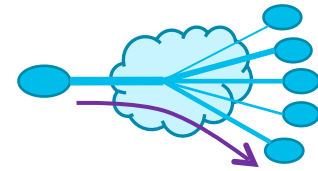
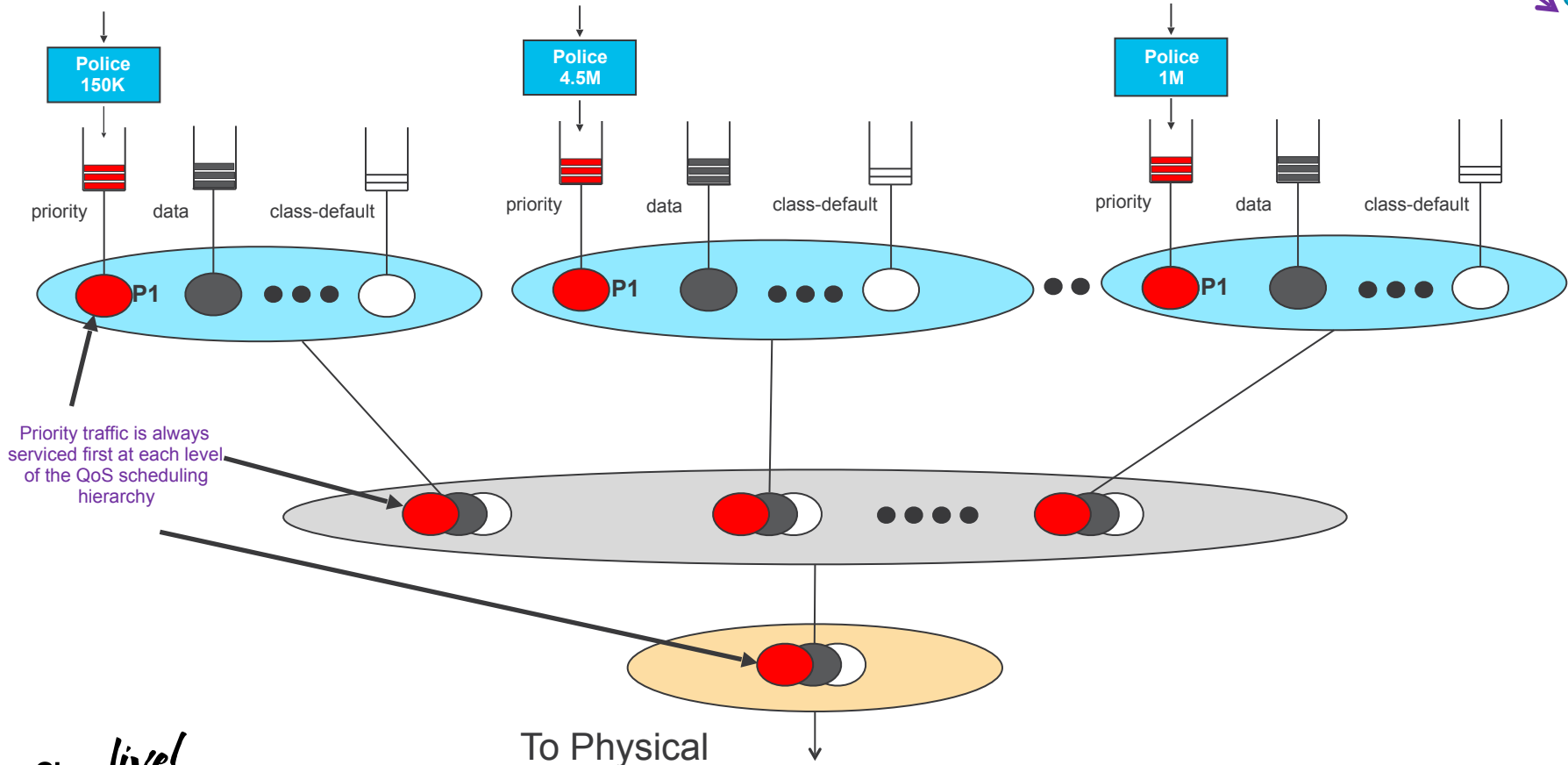
Aggregate Priority Load

Priority Propagation / Passing Lanes



Aggregate Priority Load

Priority Propagation / Passing Lanes

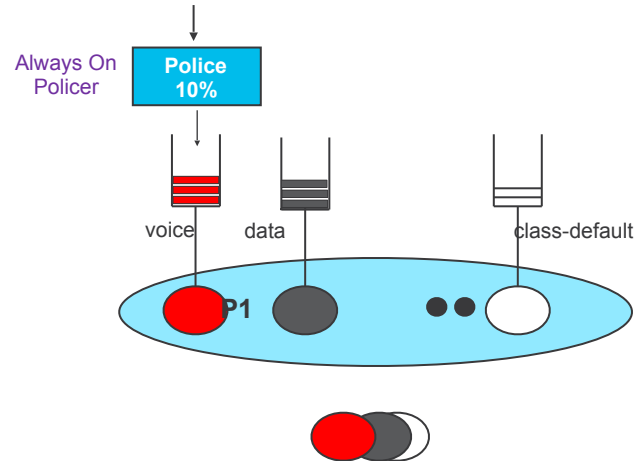
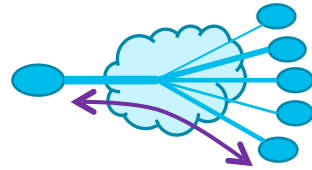


Aggregate Priority Load

IWAN Conclusion

- For Voice, use an **Always On policer**, rather than a Conditional policer

```
class VOICE
  priority level 1
  police cir percent 10
```



Aggregate Priority Load

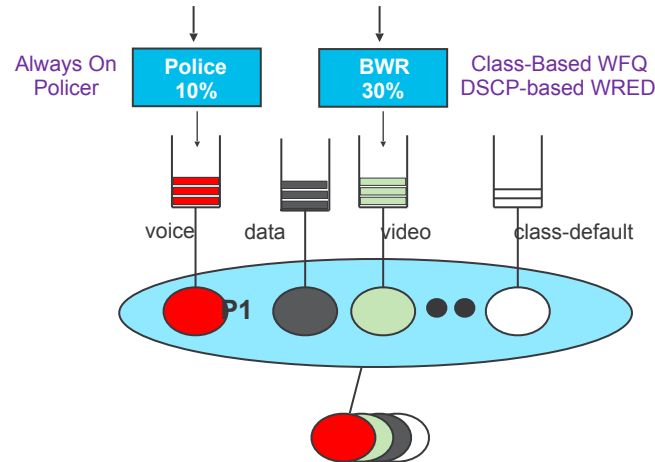
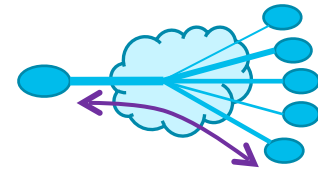
IWAN Conclusion

- For Voice, use an **Always On policer**, rather than a Conditional policer

```
class VOICE
  priority level 1
  police cir percent 10
```

- For Video, use a **Bandwidth Remaining Percent (BWR)** queue with **DSCP-based WRED**, rather than a level 2 Priority queue

```
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
```

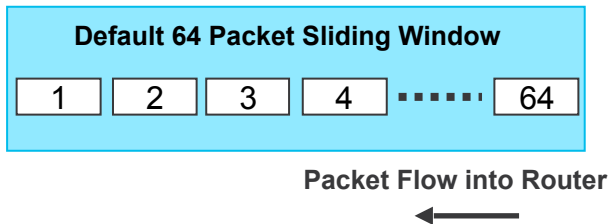


IPsec Anti-Replay

Message Integrity



- Designed to identify packet capture/replay by 3rd party — Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window by default

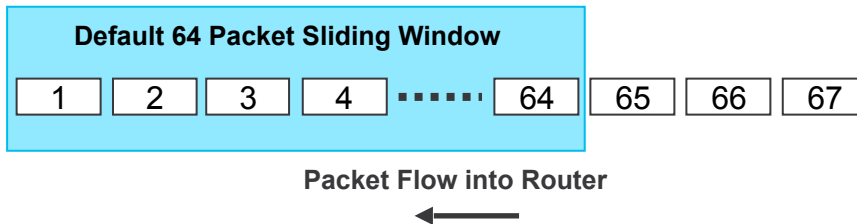


IPsec Anti-Replay

Message Integrity



- Designed to identify packet capture/replay by 3rd party — Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window by default

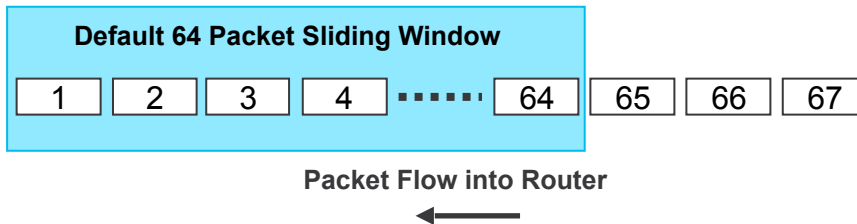


IPsec Anti-Replay

Message Integrity



- Designed to identify packet capture/replay by 3rd party — Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window by default

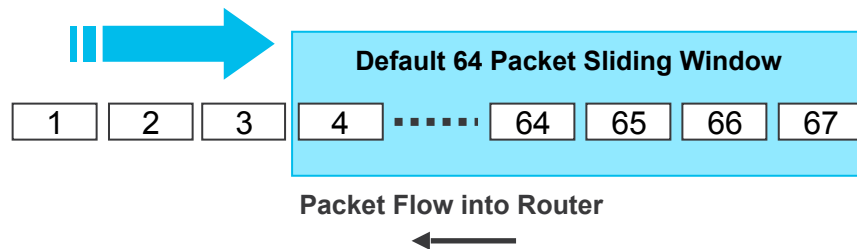


IPsec Anti-Replay

Message Integrity



- Designed to identify packet capture/replay by 3rd party — Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window by default
- Window moves right to include higher sequence numbers
- Window marks packets as received or not

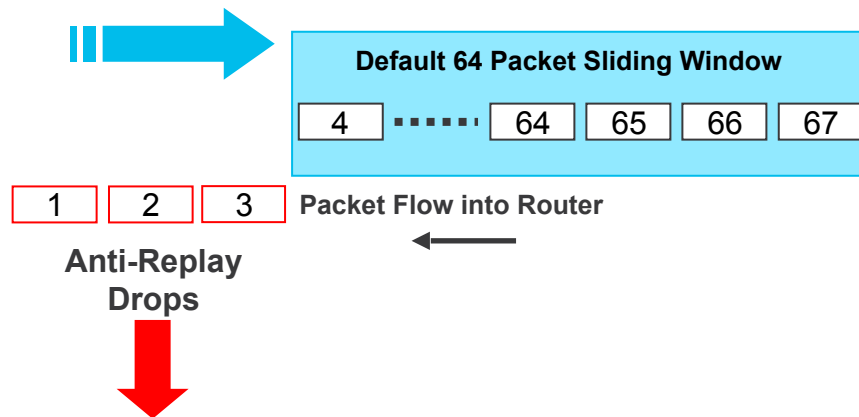


IPsec Anti-Replay

Message Integrity

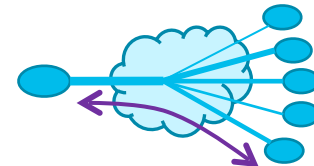


- Designed to identify packet capture/replay by 3rd party — Message Integrity
- Sender assigns sequence number per Security Association (SA) to encrypted packets
- Receiver maintains 64 packet sliding window by default
- Window moves right to include higher sequence numbers
- Window marks packets as received or not
- Packets to the left of the window are dropped



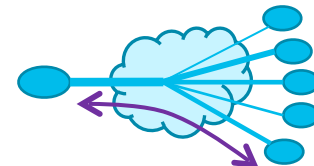
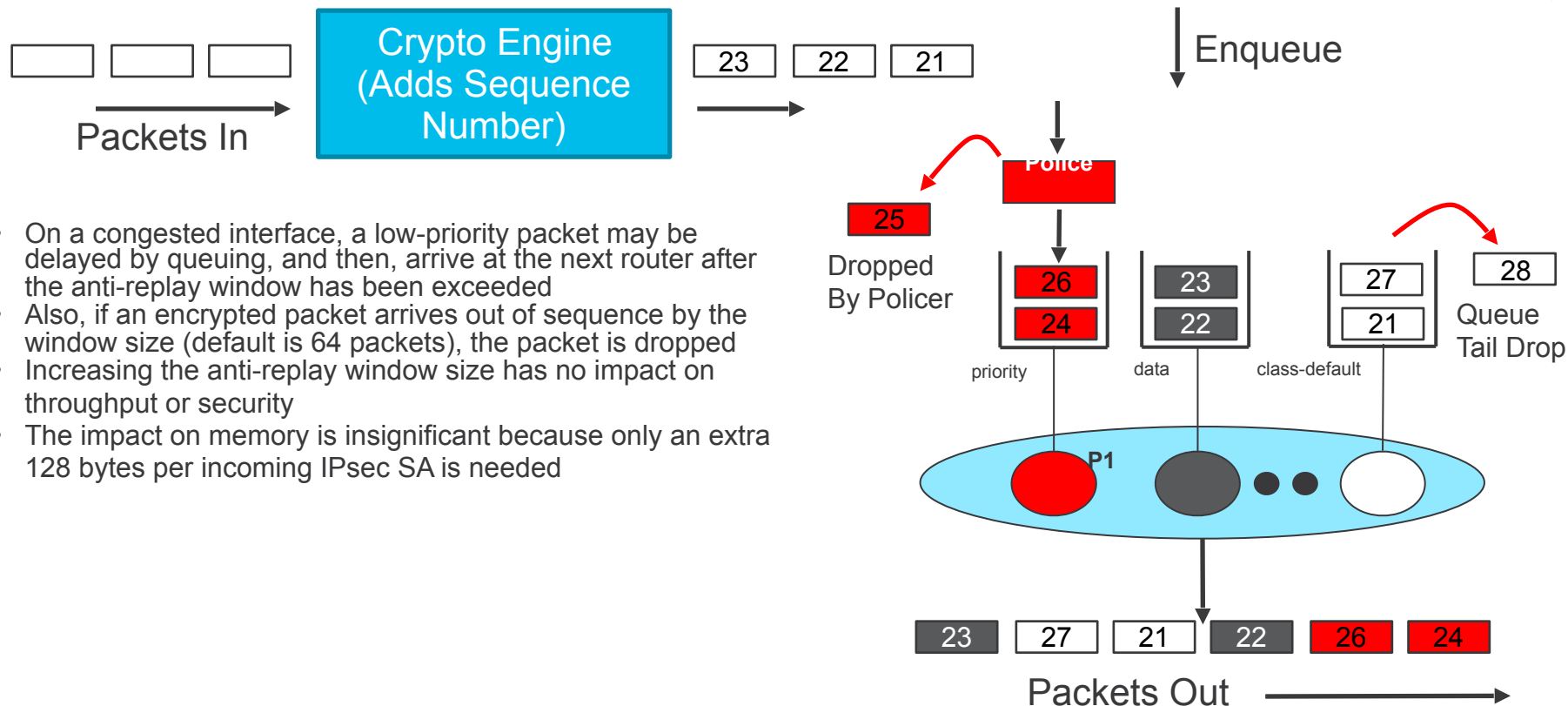
IPsec Anti-Replay and QoS

IWAN Conclusion



IPsec Anti-Replay and QoS

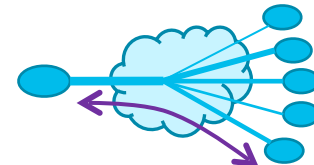
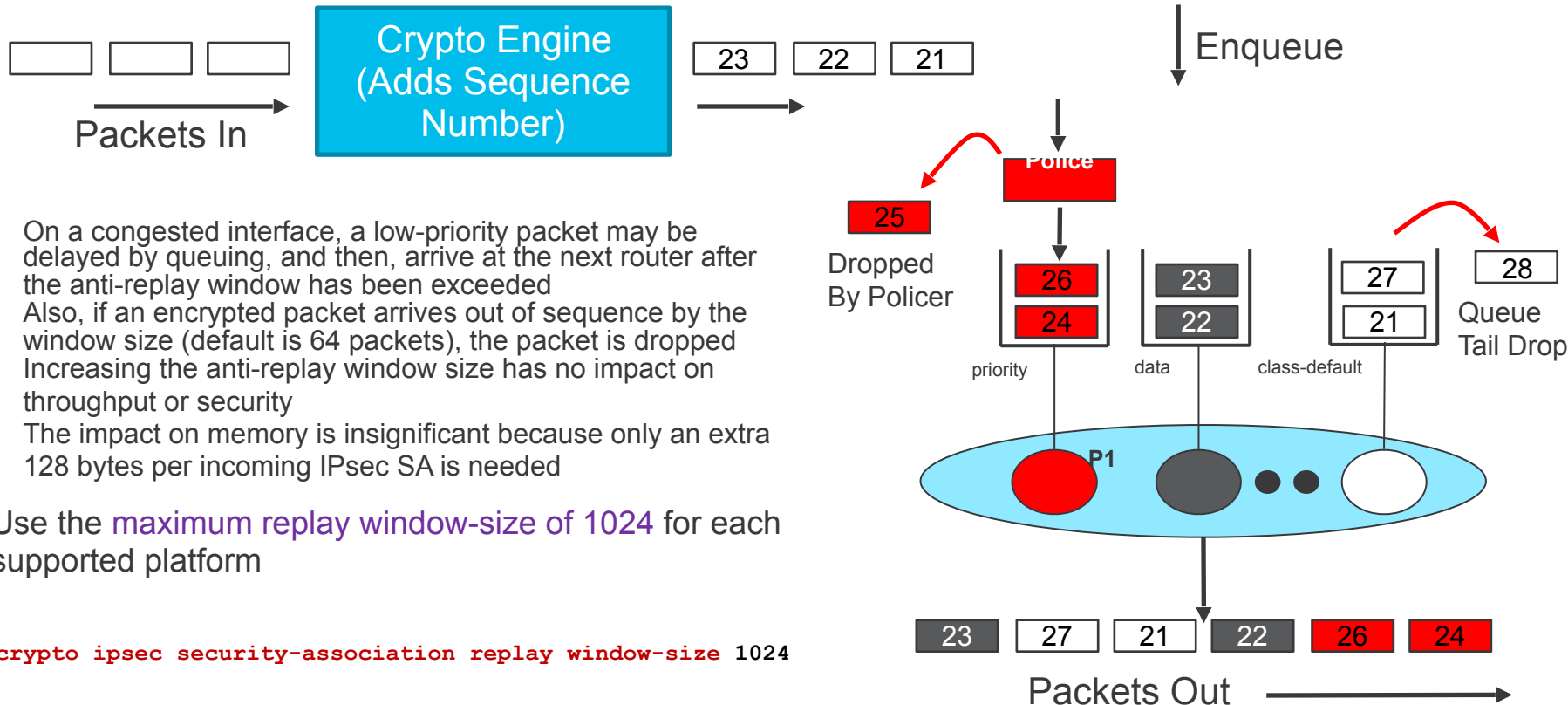
IWAN Conclusion



- On a congested interface, a low-priority packet may be delayed by queuing, and then, arrive at the next router after the anti-replay window has been exceeded
- Also, if an encrypted packet arrives out of sequence by the window size (default is 64 packets), the packet is dropped
- Increasing the anti-replay window size has no impact on throughput or security
- The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed

IPsec Anti-Replay and QoS

IWAN Conclusion



- On a congested interface, a low-priority packet may be delayed by queuing, and then, arrive at the next router after the anti-replay window has been exceeded
- Also, if an encrypted packet arrives out of sequence by the window size (default is 64 packets), the packet is dropped
- Increasing the anti-replay window size has no impact on throughput or security
- The impact on memory is insignificant because only an extra 128 bytes per incoming IPsec SA is needed

Use the **maximum replay window-size of 1024** for each supported platform

```
crypto ipsec security-association replay window-size 1024
```

QoS Tools Review: Queuing & Dropping Tools

Bandwidth Percent vs Bandwidth Remaining Percent

Bandwidth Percent specifies bandwidth allocation as a percentage of the value entered in the bandwidth command on the interface

- Bandwidth percentages have to take into account priority percent values
- They have to be adjusted when priority bandwidth values are changed

QoS Tools Review: Queuing & Dropping Tools

Bandwidth Percent vs Bandwidth Remaining Percent

Bandwidth Percent specifies bandwidth allocation as a percentage of the value entered in the bandwidth command on the interface

- Bandwidth percentages have to take into account priority percent values
- They have to be adjusted when priority bandwidth values are changed

Bandwidth Remaining Percent specifies bandwidth allocation as a percentage of the bandwidth value that has **not** been allocated to priority classes

- Bandwidth remaining percentages must equal 100%
- The bandwidth automatically adjusts when priority bandwidth values are changed

QoS Tools Review: Queuing & Dropping Tools

Bandwidth Percent vs Bandwidth Remaining Percent

Bandwidth Percent specifies bandwidth allocation as a percentage of the value entered in the bandwidth command on the interface

- Bandwidth percentages have to take into account priority percent values
- They have to be adjusted when priority bandwidth values are changed

Bandwidth Remaining Percent specifies bandwidth allocation as a percentage of the bandwidth value that has **not** been allocated to priority classes

- Bandwidth remaining percentages must equal 100%
- The bandwidth automatically adjusts when priority bandwidth values are changed

The two features cannot be used in the same policy map

QoS Tools Review: Queuing & Dropping Tools

Bandwidth Percent vs Bandwidth Remaining Percent

Bandwidth Percent specifies bandwidth allocation as a percentage of the value entered in the bandwidth command on the interface

- Bandwidth percentages have to take into account priority percent values
- They have to be adjusted when priority bandwidth values are changed

Bandwidth Remaining Percent specifies bandwidth allocation as a percentage of the bandwidth value that has **not** been allocated to priority classes

- Bandwidth remaining percentages must equal 100%
- The bandwidth automatically adjusts when priority bandwidth values are changed

The two features cannot be used in the same policy map

Examples:

Bandwidth Percent (BWP)

Service Rate Bandwidth = 10Mbps

Priority Queue 10% = 1 Mbps

BWP of 30% = $10 \times .30 = 3.0$ Mbps

QoS Tools Review: Queuing & Dropping Tools

Bandwidth Percent vs Bandwidth Remaining Percent

Bandwidth Percent specifies bandwidth allocation as a percentage of the value entered in the bandwidth command on the interface

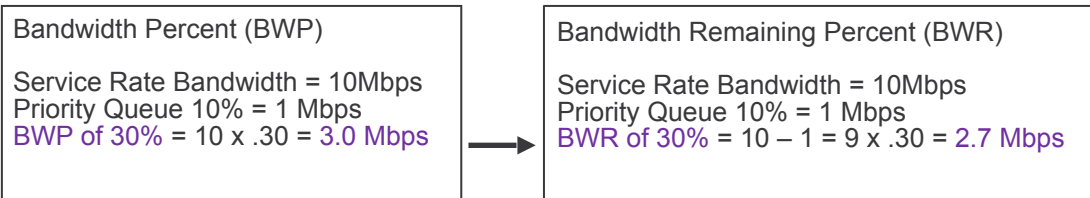
- Bandwidth percentages have to take into account priority percent values
- They have to be adjusted when priority bandwidth values are changed

Bandwidth Remaining Percent specifies bandwidth allocation as a percentage of the bandwidth value that has **not** been allocated to priority classes

- Bandwidth remaining percentages must equal 100%
- The bandwidth automatically adjusts when priority bandwidth values are changed

The two features cannot be used in the same policy map

Examples:



QoS Tools Review: Queuing & Dropping Tools

Bandwidth Percent vs Bandwidth Remaining Percent

Bandwidth Percent specifies bandwidth allocation as a percentage of the value entered in the bandwidth command on the interface

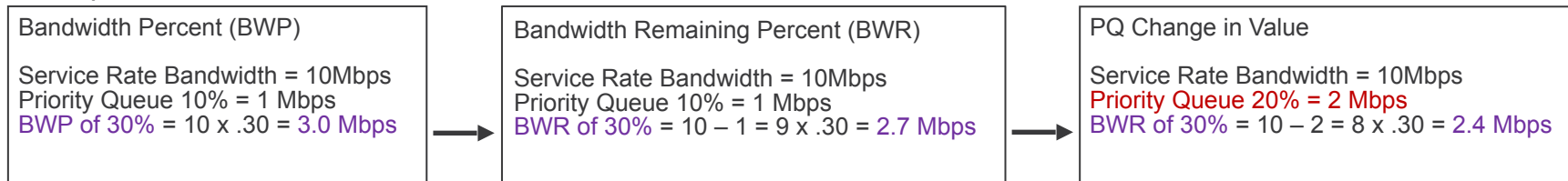
- Bandwidth percentages have to take into account priority percent values
- They have to be adjusted when priority bandwidth values are changed

Bandwidth Remaining Percent specifies bandwidth allocation as a percentage of the bandwidth value that has **not** been allocated to priority classes

- Bandwidth remaining percentages must equal 100%
- The bandwidth automatically adjusts when priority bandwidth values are changed

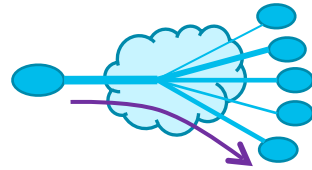
The two features cannot be used in the same policy map

Examples:



Bandwidth Remaining Ratio

IWAN Details



Bandwidth Remaining Ratio (BRR) provides proportional sharing to parent shapers during times of congestion.

If you over-subscribe your hub BR outbound bandwidth with per-tunnel policies that exceed the service rate, the BRR commands on each parent policy means they will get their “fair share” of the remaining bandwidth as compared to the other branch sites.

- If all the per-tunnel BW amounts are 5 Mbps or greater, we use a BRR value of $BW / 1 \text{ Mbps}$. (i.e. 10 Mbps is BRR of 10, 50 Mbps is BRR of 50, etc.)
- If any of the per-tunnel BW values are less than 5 Mbps, we use a BRR value of $BW / 100 \text{ Kbps}$. (i.e. 3 Mbps is BRR of 30, 1.5 Mbps is BRR of 15, etc.)

Bandwidth Remaining Ratio

IWAN Details

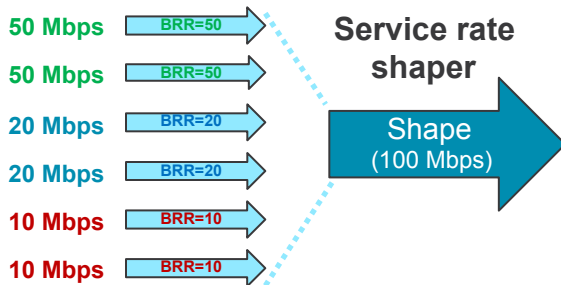


Bandwidth Remaining Ratio (BRR) provides proportional sharing to parent shapers during times of congestion.

If you over-subscribe your hub BR outbound bandwidth with per-tunnel policies that exceed the service rate, the BRR commands on each parent policy means they will get their “fair share” of the remaining bandwidth as compared to the other branch sites.

- If all the per-tunnel BW amounts are 5 Mbps or greater, we use a BRR value of $BW / 1 \text{ Mbps}$. (i.e. 10 Mbps is BRR of 10, 50 Mbps is BRR of 50, etc.)
- If any of the per-tunnel BW values are less than 5 Mbps, we use a BRR value of $BW / 100 \text{ Kbps}$. (i.e. 3 Mbps is BRR of 30, 1.5 Mbps is BRR of 15, etc.)

Per-Tunnel shapers



When the total bandwidth exceeds 100 Mbps, each of the per-tunnel shapers will get their fair share based on their BRR values.

Example:

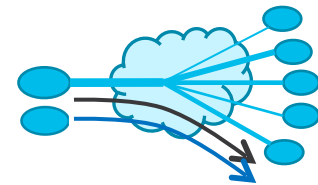
50 Mbps site gets $50 / 160$ or 31.25%

20 Mbps site gets $20 / 160$ or 12.5%

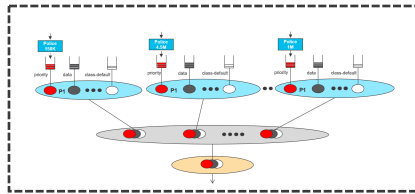
10 Mbps site gets $10 / 160$ or 6.25%

Multiple Sender QoS for Hub Routers

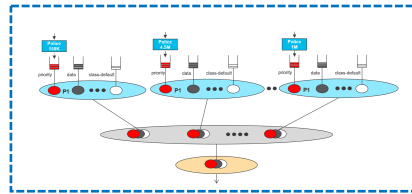
Bandwidth Sharing Between Multiple Senders



Hub BR1 (MNH/MDC)

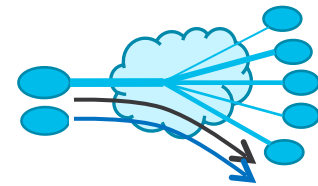
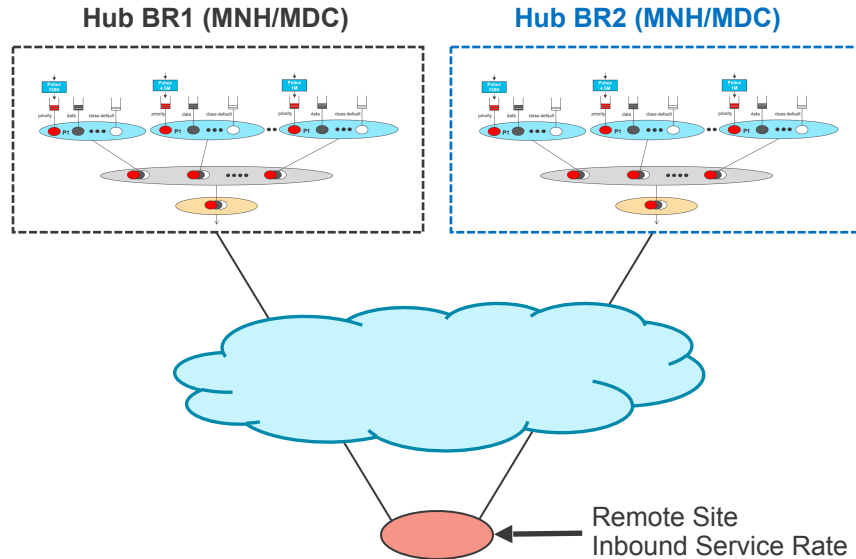


Hub BR2 (MNH/MDC)



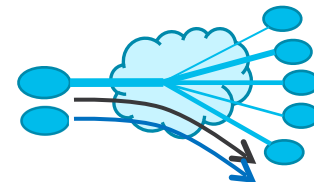
Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

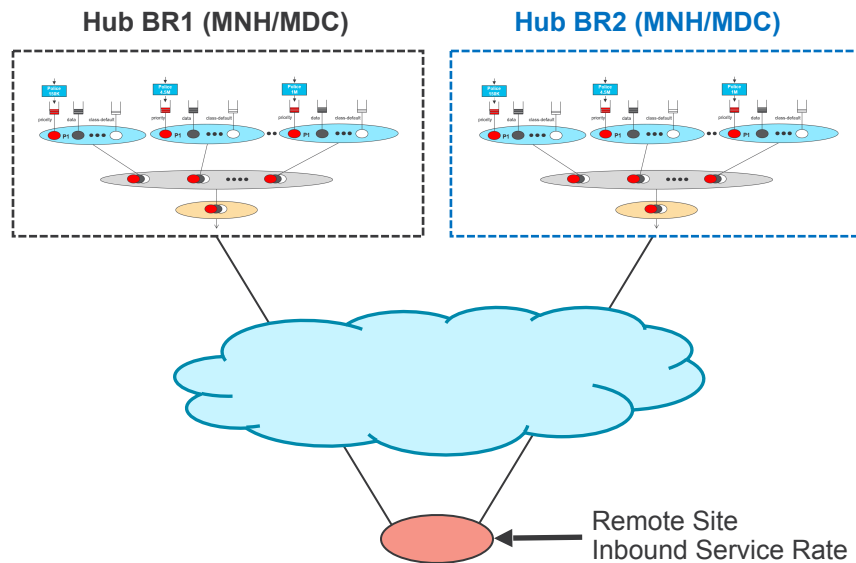


Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

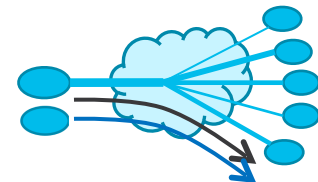


- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for PfR TC channels to establish

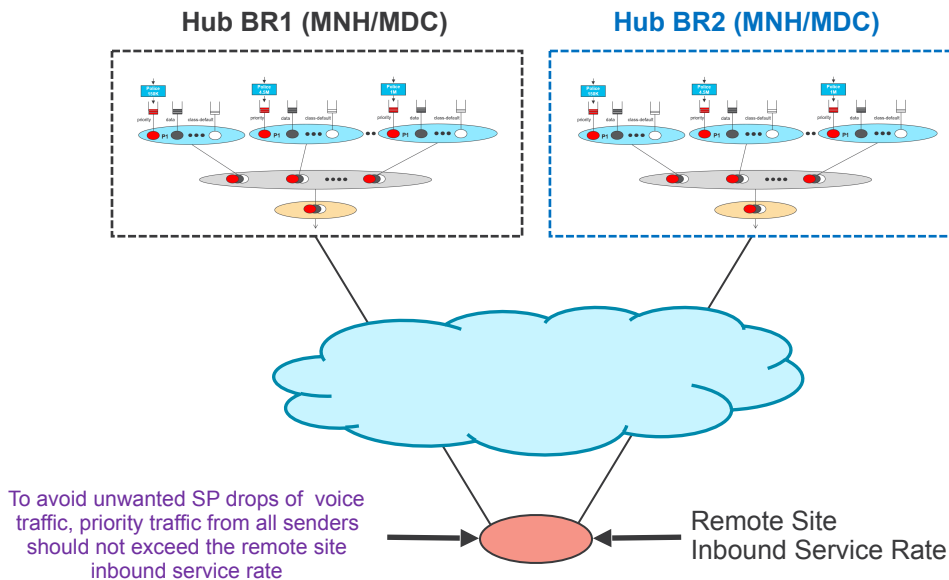


Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

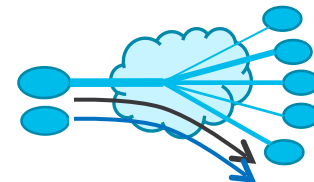


- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for PfR TC channels to establish

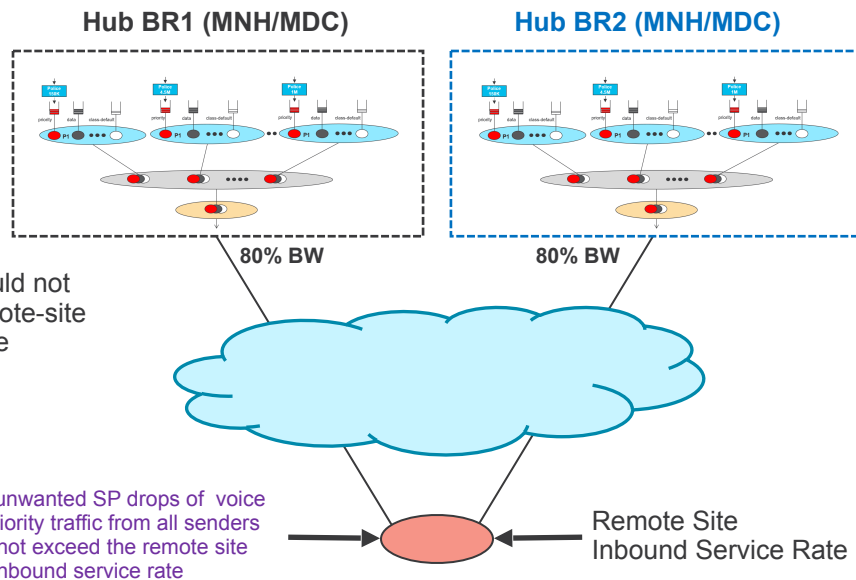


Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

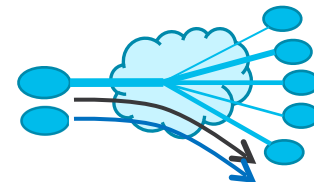


- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for PfR TC channels to establish



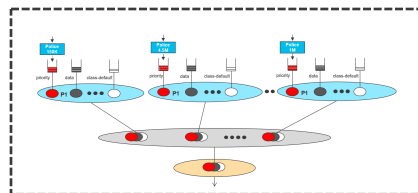
Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

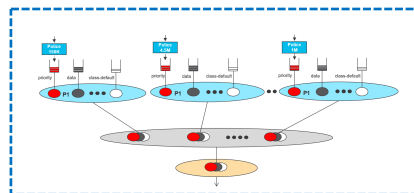


- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for Pfr TC channels to establish
- As the number of senders increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns

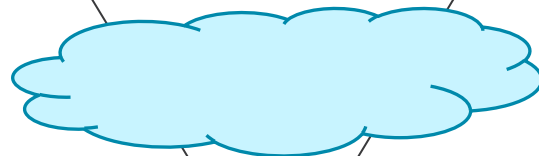
Hub BR1 (MNH/MDC)



Hub BR2 (MNH/MDC)



- Total bandwidth should not exceed 160% of remote-site inbound Service Rate

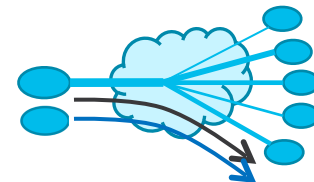


To avoid unwanted SP drops of voice traffic, priority traffic from all senders should not exceed the remote site inbound service rate

Remote Site Inbound Service Rate

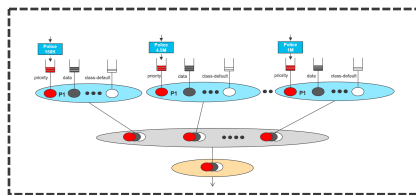
Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

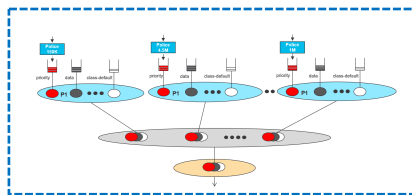


- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for PfR TC channels to establish
- As the number of senders increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns

Hub BR1 (MNH/MDC)

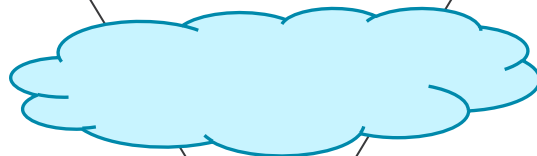


Hub BR2 (MNH/MDC)



Remote Site Example:
 $50 \text{ Mb/s} \times .80 = 40 \text{ Mb/s per Hub BR}$

- Total bandwidth should not exceed 160% of remote-site inbound Service Rate

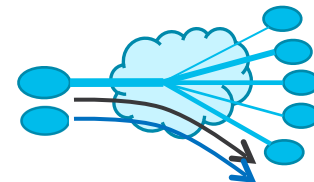


To avoid unwanted SP drops of voice traffic, priority traffic from all senders should not exceed the remote site inbound service rate

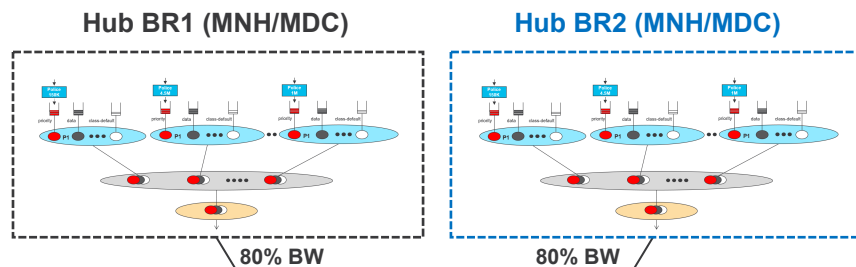
Remote Site
Inbound Service Rate

Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

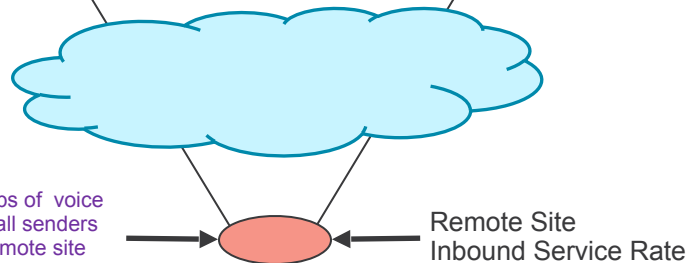


- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for PfR TC channels to establish
- As the number of senders increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns



- Total bandwidth should not exceed 160% of remote-site inbound Service Rate

To avoid unwanted SP drops of voice traffic, priority traffic from all senders should not exceed the remote site inbound service rate



Remote Site Example:
 $50 \text{ Mb/s} * .80 = 40 \text{ Mb/s per Hub BR}$

Branch Tunnel Interface

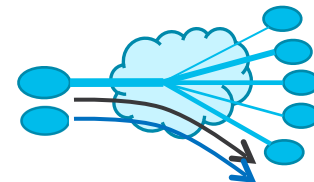
```
interface Tunnel10
bandwidth receive 50000
nhrp nhs 10.6.34.1 nbma 192.168.6.1 multicast
nhrp nhs 10.6.34.2 nbma 192.168.6.41 multicast
nhrp group RS-GROUP-50MBPS-80
```

Hub Policy

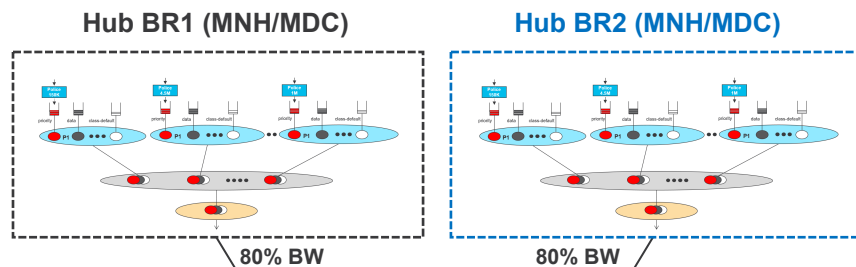
```
policy-map RS-GROUP-50MBPS-80-POLICY
class class-default
description 80% of 50 Mbps
shape average 40 Mbps
bandwidth remaining ratio 40
service-policy WAN
```

Multiple Sender QoS for Hub Routers

Bandwidth Sharing Between Multiple Senders

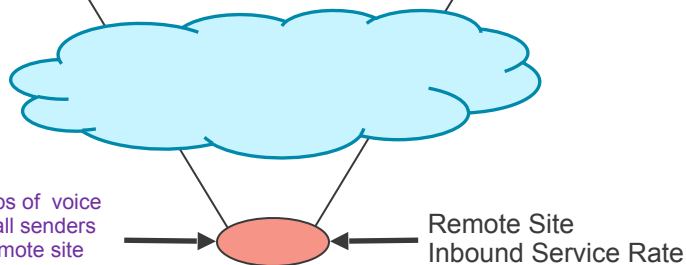


- Bandwidth can exceed 100% of the remote-site inbound Service Rate using a calculated oversubscription of ~ 1.6:1
- Bandwidth has to be divided equally due to one NHRP group
- QoS child policies do not have to be the same per Sender but DSCP markings must match for PfR TC channels to establish
- As the number of senders increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns



- Total bandwidth should not exceed 160% of remote-site inbound Service Rate

To avoid unwanted SP drops of voice traffic, priority traffic from all senders should not exceed the remote site inbound service rate



Remote Site Example:
 $50 \text{ Mb/s} \times 0.80 = 40 \text{ Mb/s}$ per Hub BR

Branch Tunnel Interface

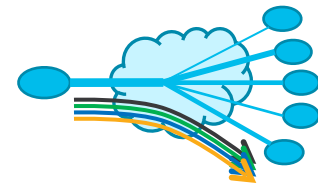
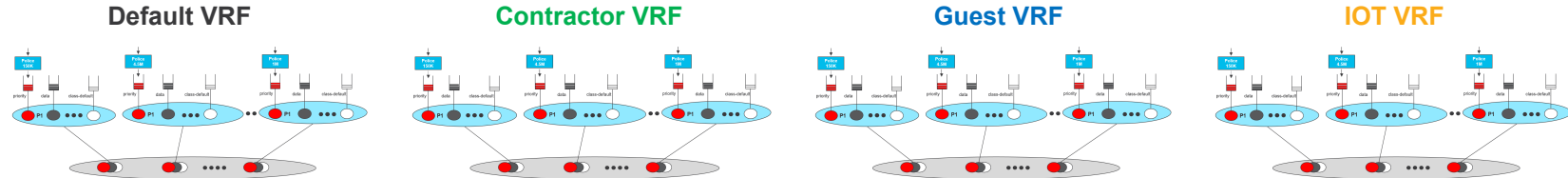
```
interface Tunnel10
bandwidth receive 50000
nhrp nhs 10.6.34.1 noma 192.168.6.1 multicast
nhrp nhs 10.6.34.2 noma 192.168.6.41 multicast
nhrp group RS-GROUP-50MBPS-80
```

Hub Policy

```
policy-map RS-GROUP-50MBPS-80-POLICY
class class-default
description 80% of 50 Mbps
shape average 40 Mbps
bandwidth remaining ratio 40
service-policy WAN
```

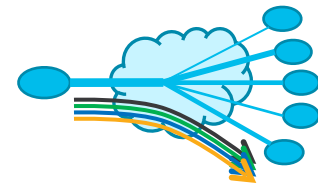
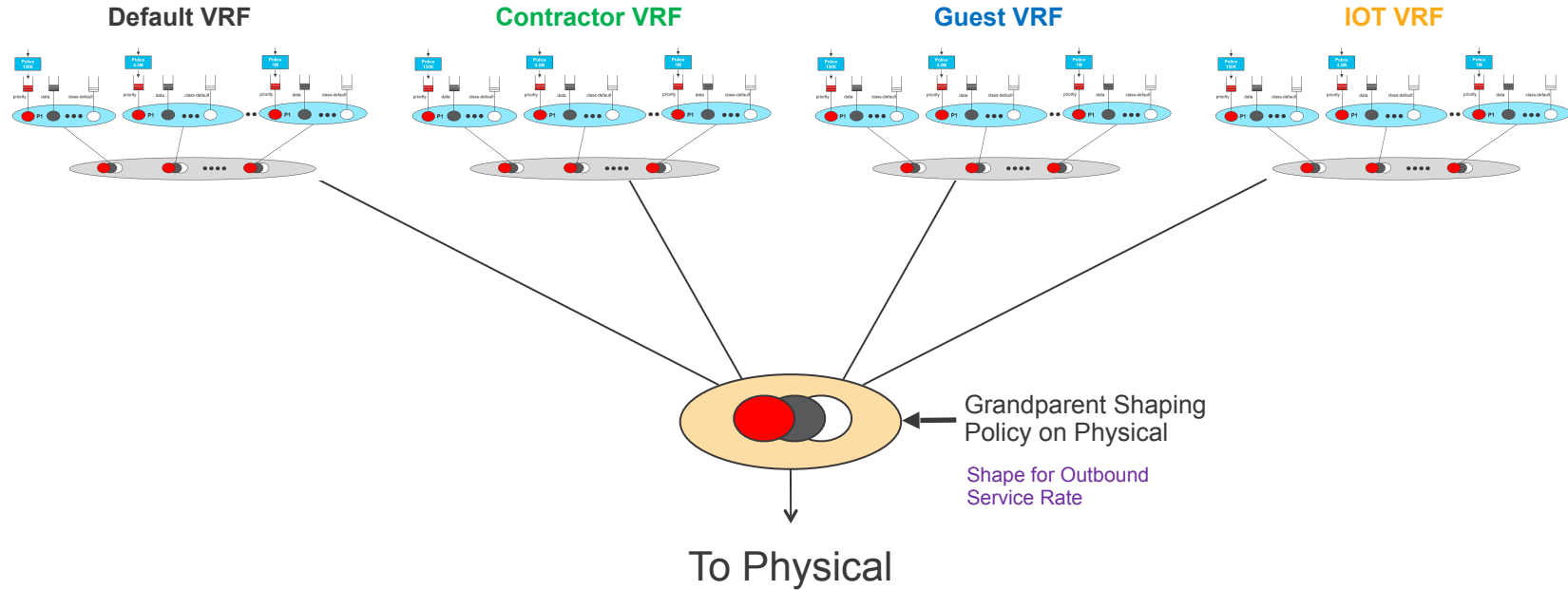
Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels



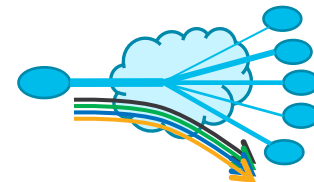
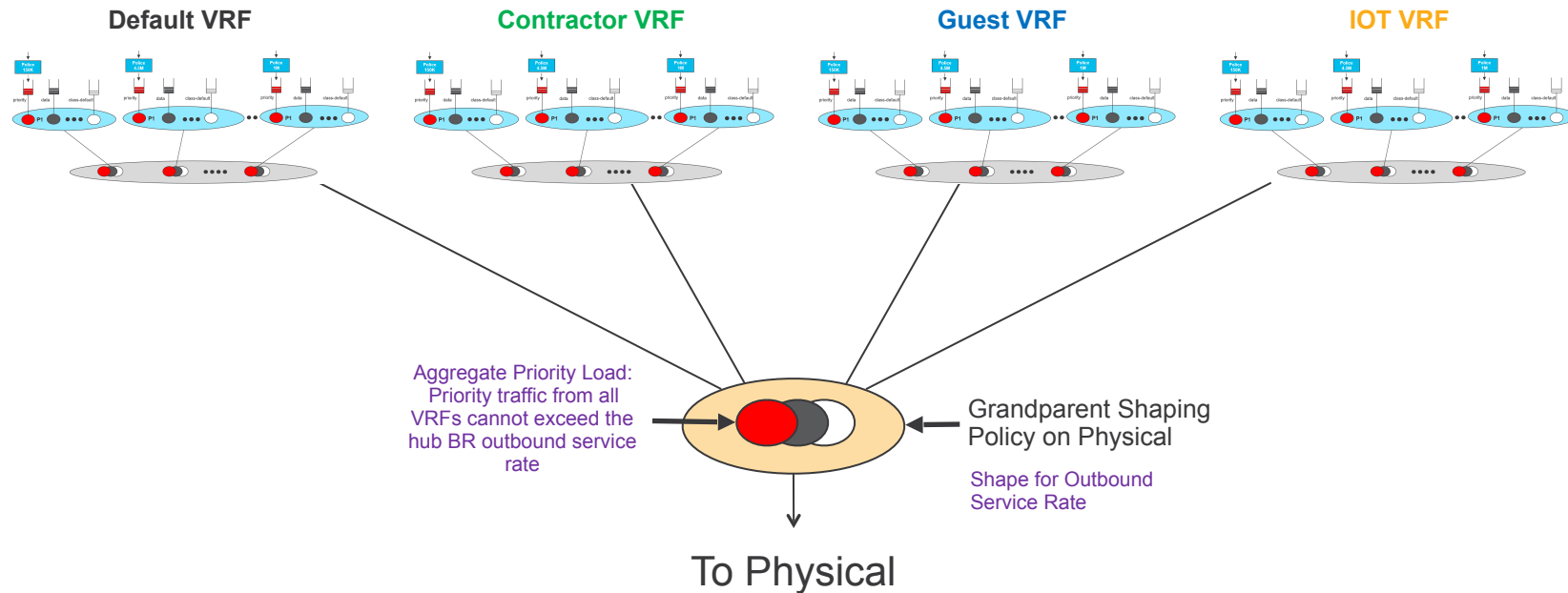
Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels



Multiple VRF QoS for Hub Routers

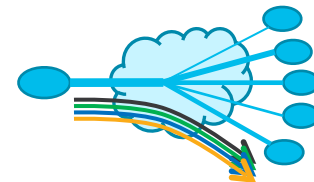
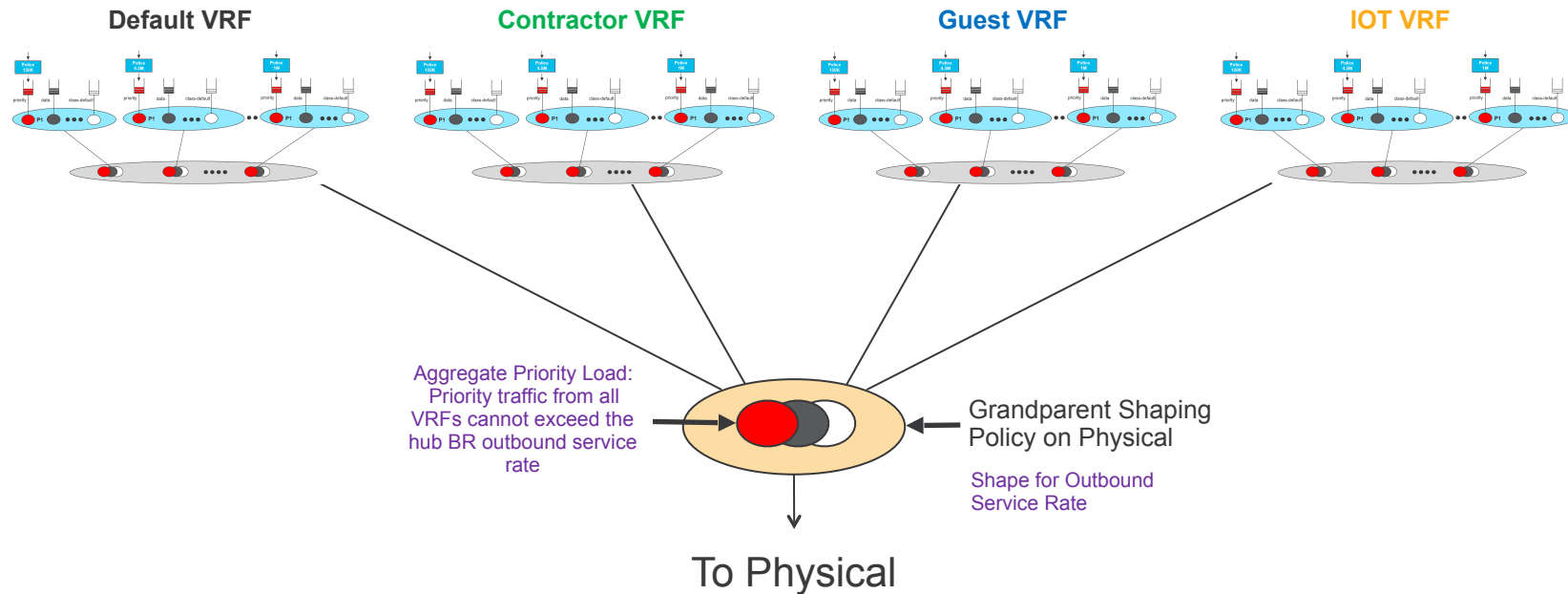
Bandwidth Sharing Between Multiple VRF Tunnels



Multiple VRF QoS for Hub Routers

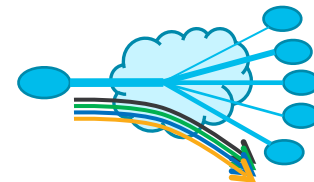
Bandwidth Sharing Between Multiple VRF Tunnels

- Bandwidth can exceed 100% of the remote-site inbound Service Rate using an oversubscription ratio of ~ 2:1
- Bandwidth does not have to be divided equally between VRFs
- QoS policies do not have to be the same per VRF

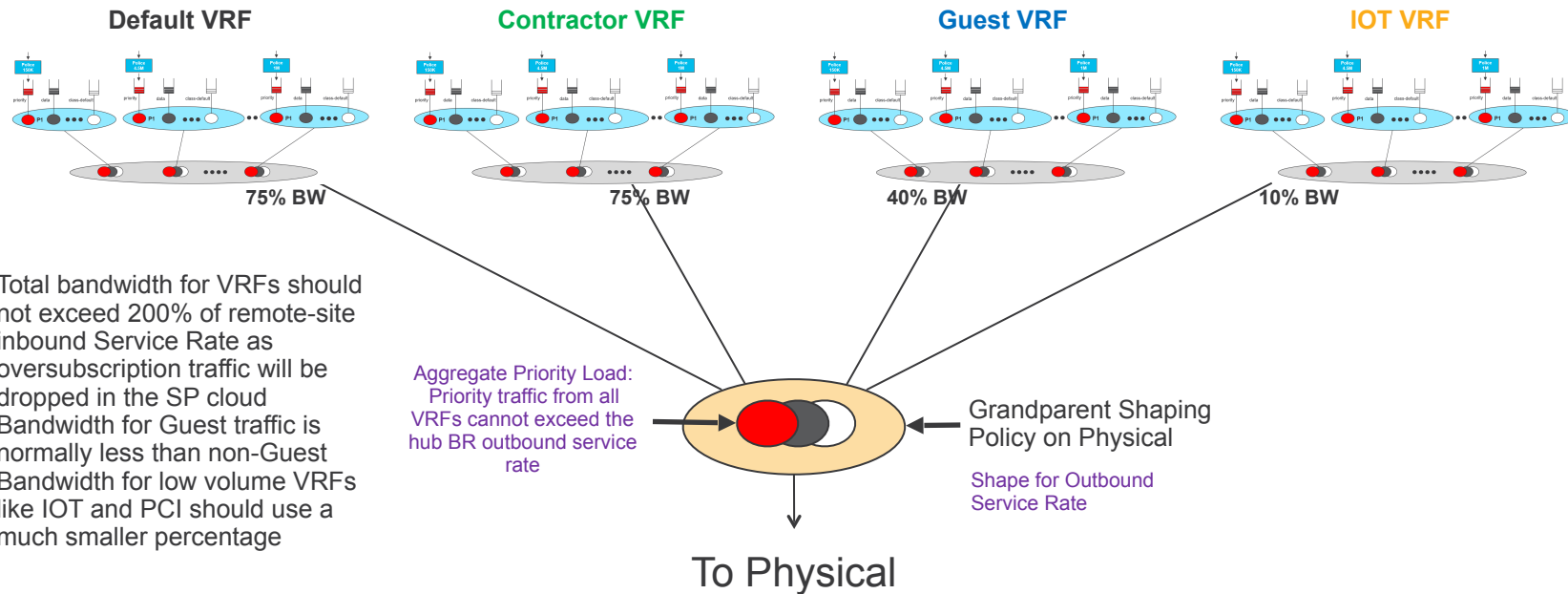


Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels



- Bandwidth can exceed 100% of the remote-site inbound Service Rate using an oversubscription ratio of ~ 2:1
- Bandwidth does not have to be divided equally between VRFs
- QoS policies do not have to be the same per VRF



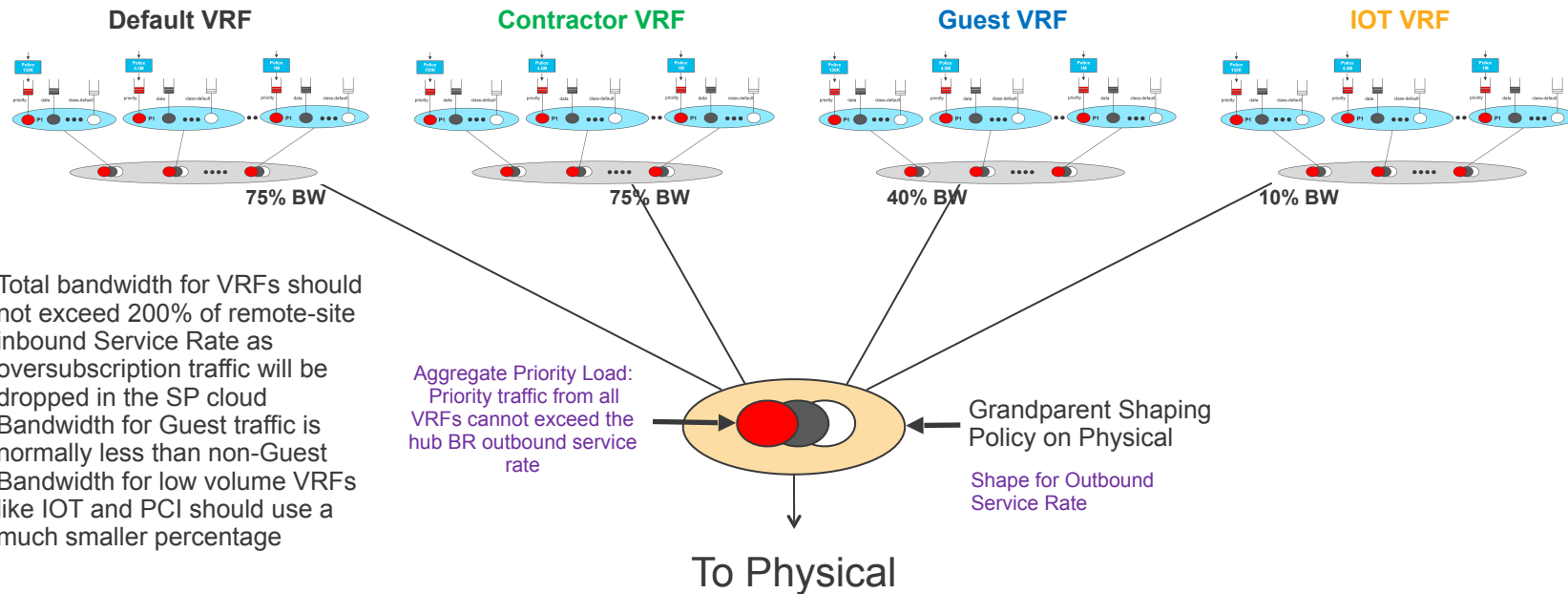
- Total bandwidth for VRFs should not exceed 200% of remote-site inbound Service Rate as oversubscription traffic will be dropped in the SP cloud
- Bandwidth for Guest traffic is normally less than non-Guest
- Bandwidth for low volume VRFs like IOT and PCI should use a much smaller percentage

Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels



- Bandwidth can exceed 100% of the remote-site inbound Service Rate using an oversubscription ratio of ~ 2:1
- Bandwidth does not have to be divided equally between VRFs
- QoS policies do not have to be the same per VRF
- As the number of VRFs increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns



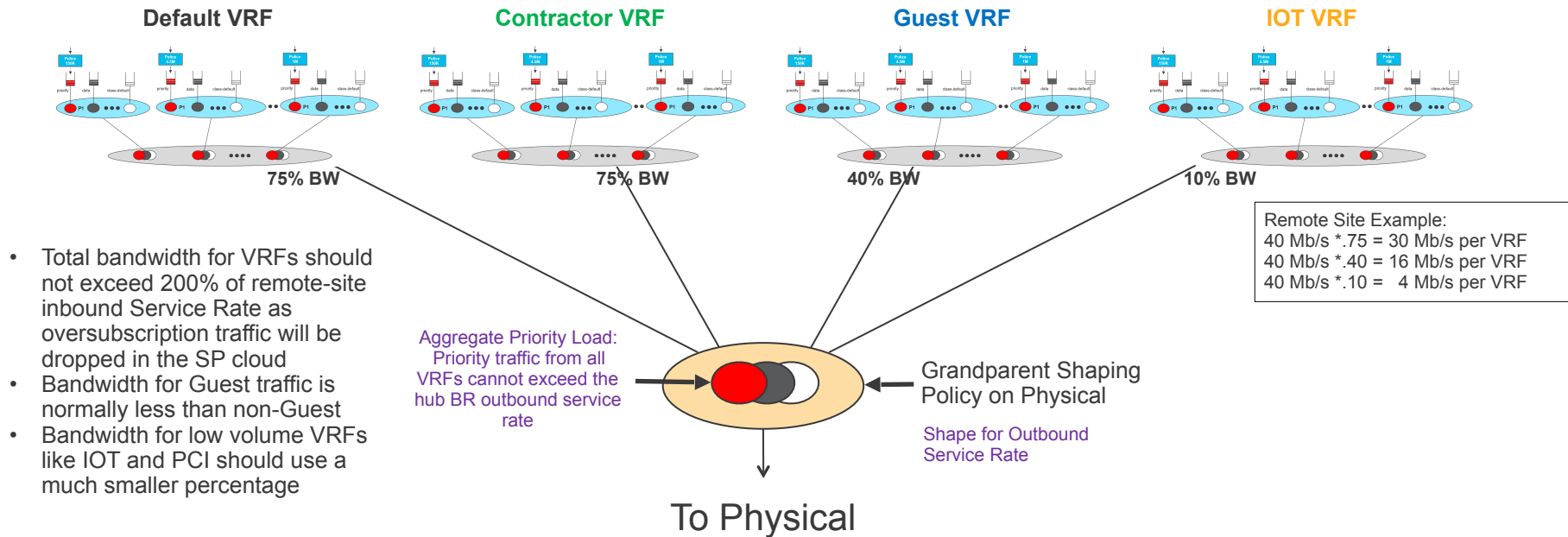
- Total bandwidth for VRFs should not exceed 200% of remote-site inbound Service Rate as oversubscription traffic will be dropped in the SP cloud
- Bandwidth for Guest traffic is normally less than non-Guest
- Bandwidth for low volume VRFs like IOT and PCI should use a much smaller percentage

Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels



- Bandwidth can exceed 100% of the remote-site inbound Service Rate using an oversubscription ratio of ~ 2:1
- Bandwidth does not have to be divided equally between VRFs
- QoS policies do not have to be the same per VRF
- As the number of VRFs increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns

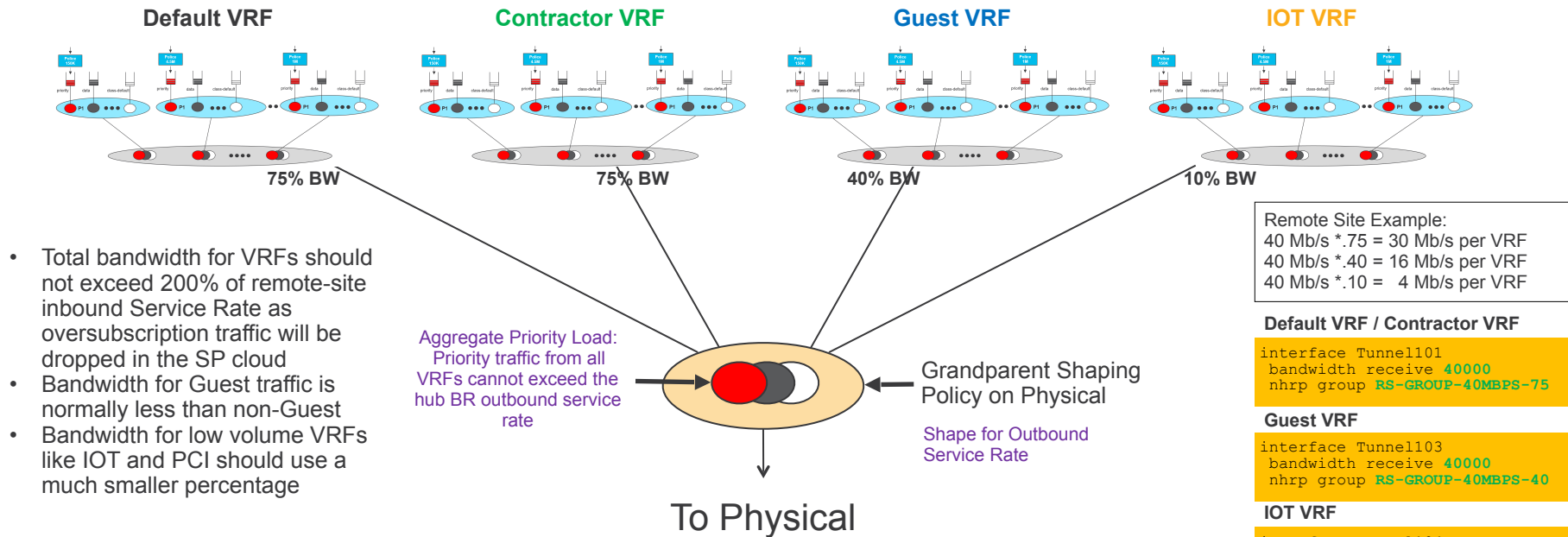


Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels



- Bandwidth can exceed 100% of the remote-site inbound Service Rate using an oversubscription ratio of ~ 2:1
- Bandwidth does not have to be divided equally between VRFs
- QoS policies do not have to be the same per VRF
- As the number of VRFs increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns



Multiple VRF QoS for Branch



Multiple VRF QoS for Branch

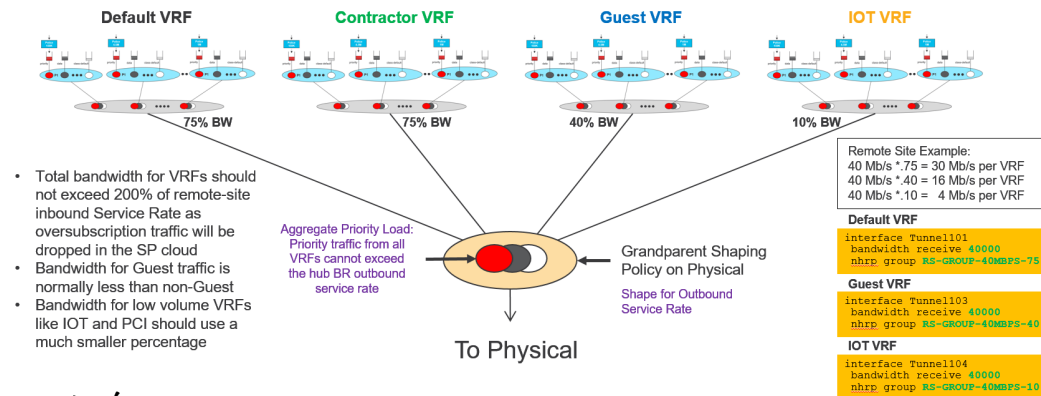


- Using normal IWAN recommendations, QoS policy is applied to the physical interface at an IWAN remote site which means all VRFs share the same QoS policy by default
- If you want to use different QoS policies for each VRF, you can deploy per-tunnel QoS in the spoke to hub direction using the same tools and limitations described on the previous slide

Multiple VRF QoS for Hub Routers

Bandwidth Sharing Between Multiple VRF Tunnels

- Bandwidth can exceed 100% of the remote-site inbound Service Rate using an oversubscription ratio of ~ 2:1
- Bandwidth does not have to be divided equally between VRFs
- QoS policies do not have to be the same per VRF
- As the number of VRFs increase, the percentages need to come down accordingly based on the network administrators knowledge of their traffic patterns



CiscoLive!

VRF = Virtual Routing and Forwarding

BRKRST-2043

© 2017 Cisco and/or its affiliates. All rights reserved. Cisco Public 52

CiscoLive!

BRKCRS-2501

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public

194

Enterprise to SP Mapping

ToS Byte Preservation



The **12-class** view is preserved across the enterprise even though we treat it differently at the egress of the router and send it to different channels within the SP network

The **twelve classes remain intact** on the inner header and the outer tunnel header is remarked as the traffic leaves the tunnel interface

The remarked outer header is discarded after arriving at the tunnel interface on the receiving router, thus leaving the **inner header marking unchanged**

IP Packet



Enterprise to SP Mapping

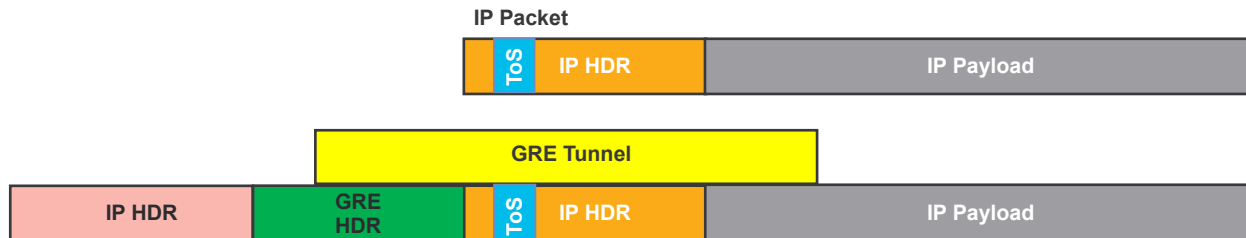
ToS Byte Preservation



The **12-class** view is preserved across the enterprise even though we treat it differently at the egress of the router and send it to different channels within the SP network

The **twelve classes remain intact** on the inner header and the outer tunnel header is remarked as the traffic leaves the tunnel interface

The remarked outer header is discarded after arriving at the tunnel interface on the receiving router, thus leaving the **inner header marking unchanged**



Enterprise to SP Mapping

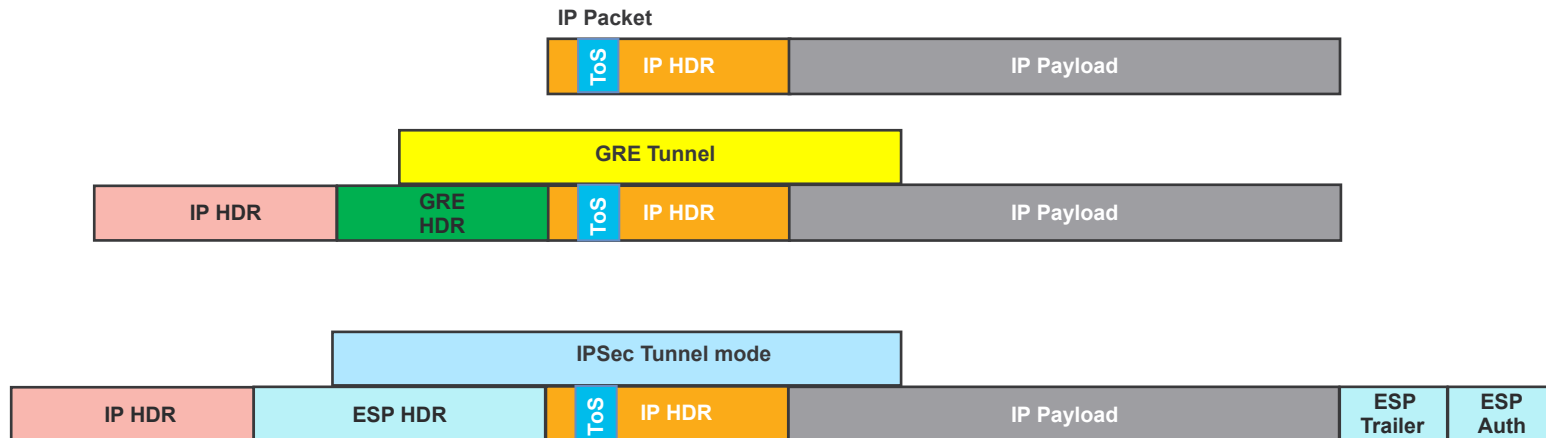
ToS Byte Preservation



The **12-class** view is preserved across the enterprise even though we treat it differently at the egress of the router and send it to different channels within the SP network

The **twelve classes remain intact** on the inner header and the outer tunnel header is remarked as the traffic leaves the tunnel interface

The remarked outer header is discarded after arriving at the tunnel interface on the receiving router, thus leaving the **inner header marking unchanged**



Enterprise to SP Mapping

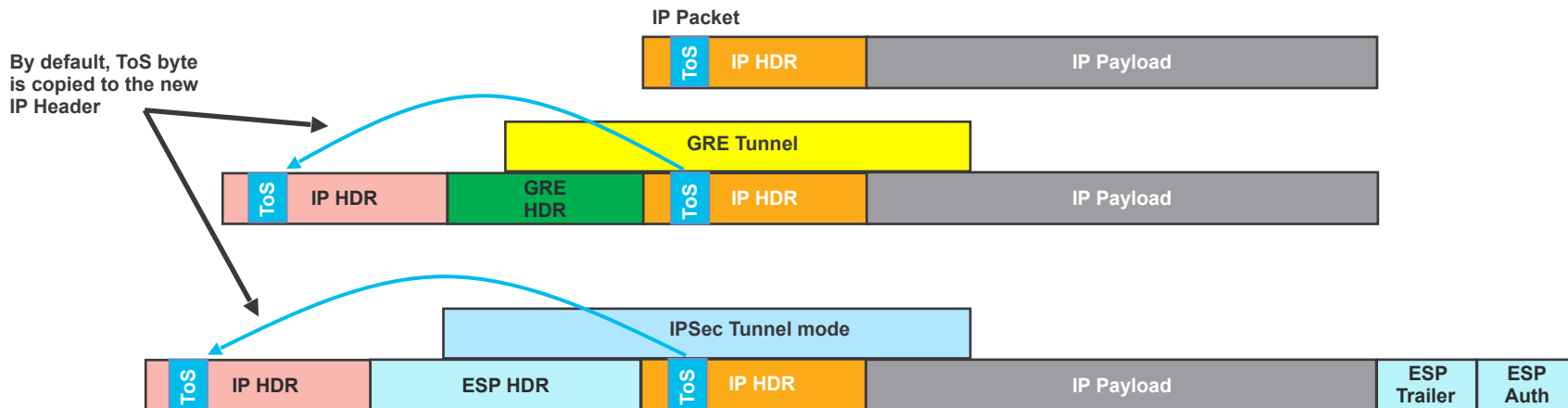
ToS Byte Preservation



The **12-class** view is preserved across the enterprise even though we treat it differently at the egress of the router and send it to different channels within the SP network

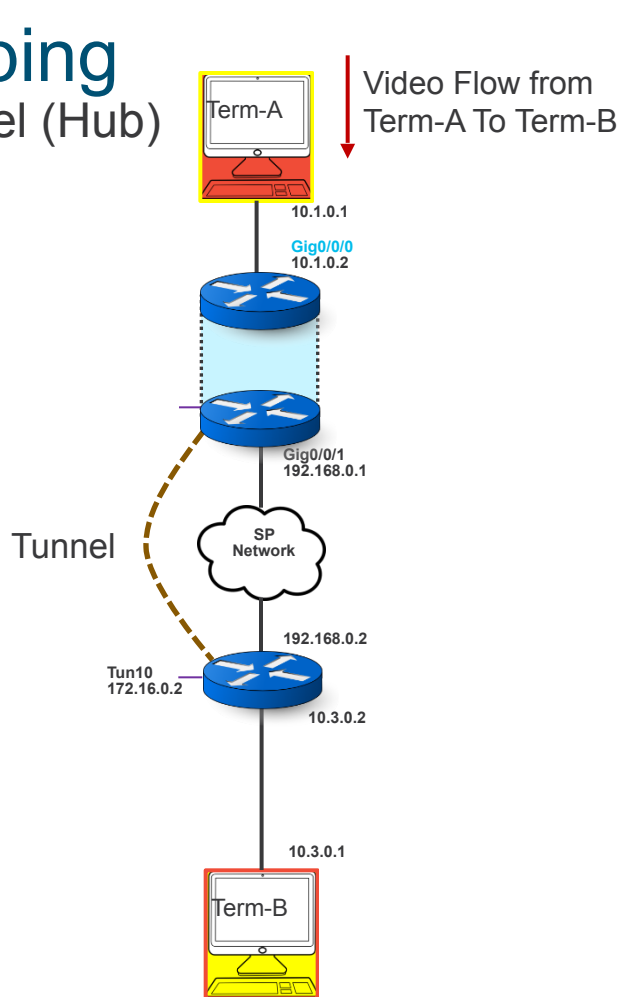
The **twelve classes remain intact** on the inner header and the outer tunnel header is remarked as the traffic leaves the tunnel interface

The remarked outer header is discarded after arriving at the tunnel interface on the receiving router, thus leaving the **inner header marking unchanged**



Enterprise to SP Mapping

Set dscp tunnel outbound on tunnel (Hub)



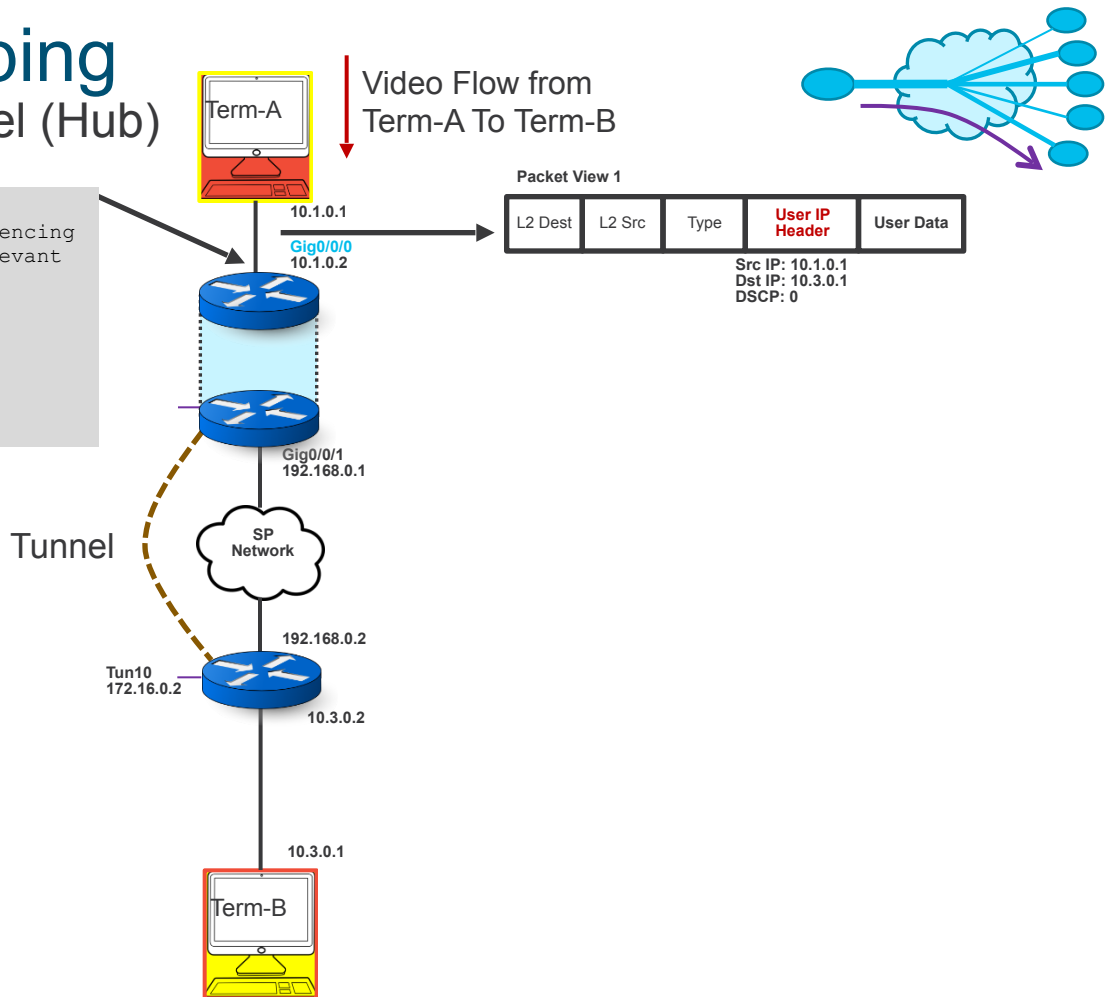
Enterprise to SP Mapping

Set dscp tunnel outbound on tunnel (Hub)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```



Enterprise to SP Mapping

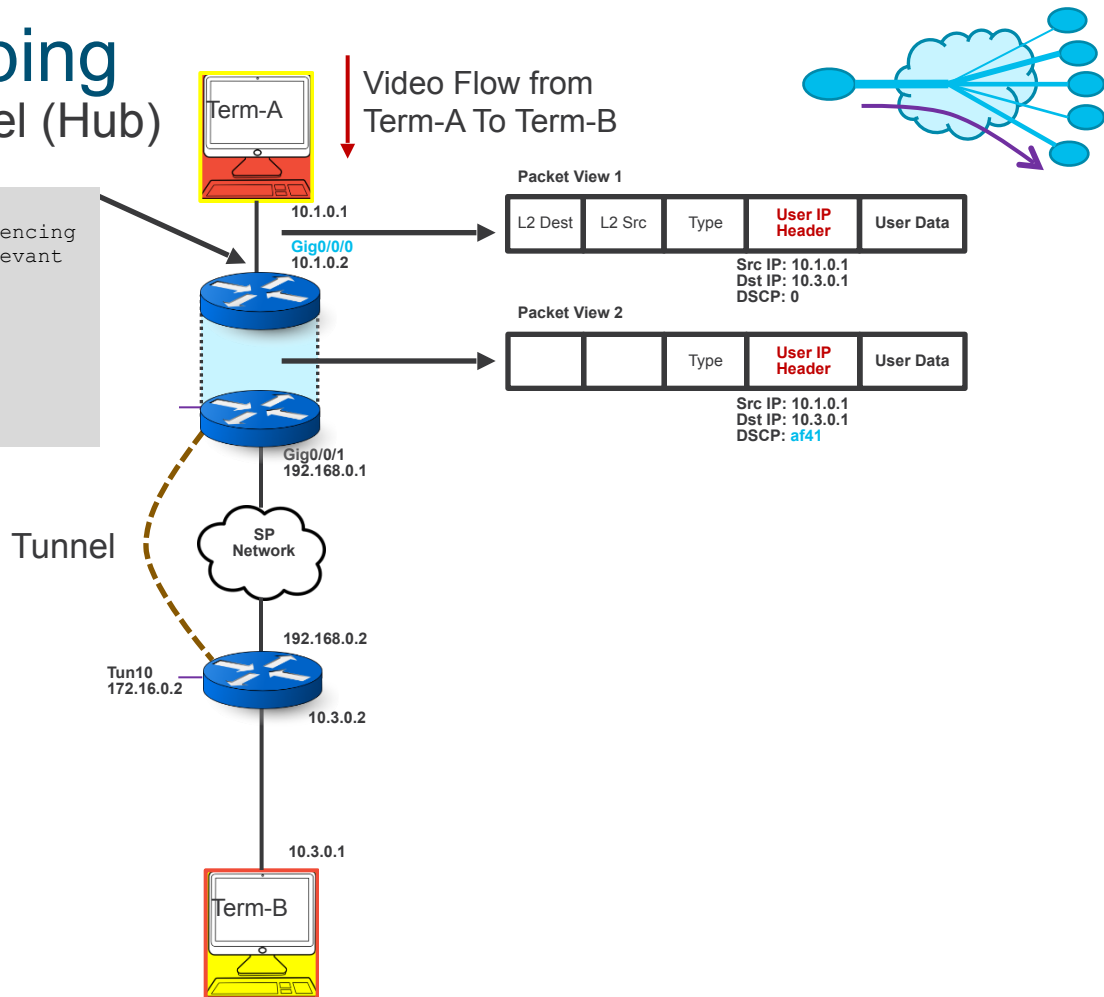
Set dscp tunnel outbound on tunnel (Hub)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the User
IP header



Enterprise to SP Mapping

Set dscp tunnel outbound on tunnel (Hub)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

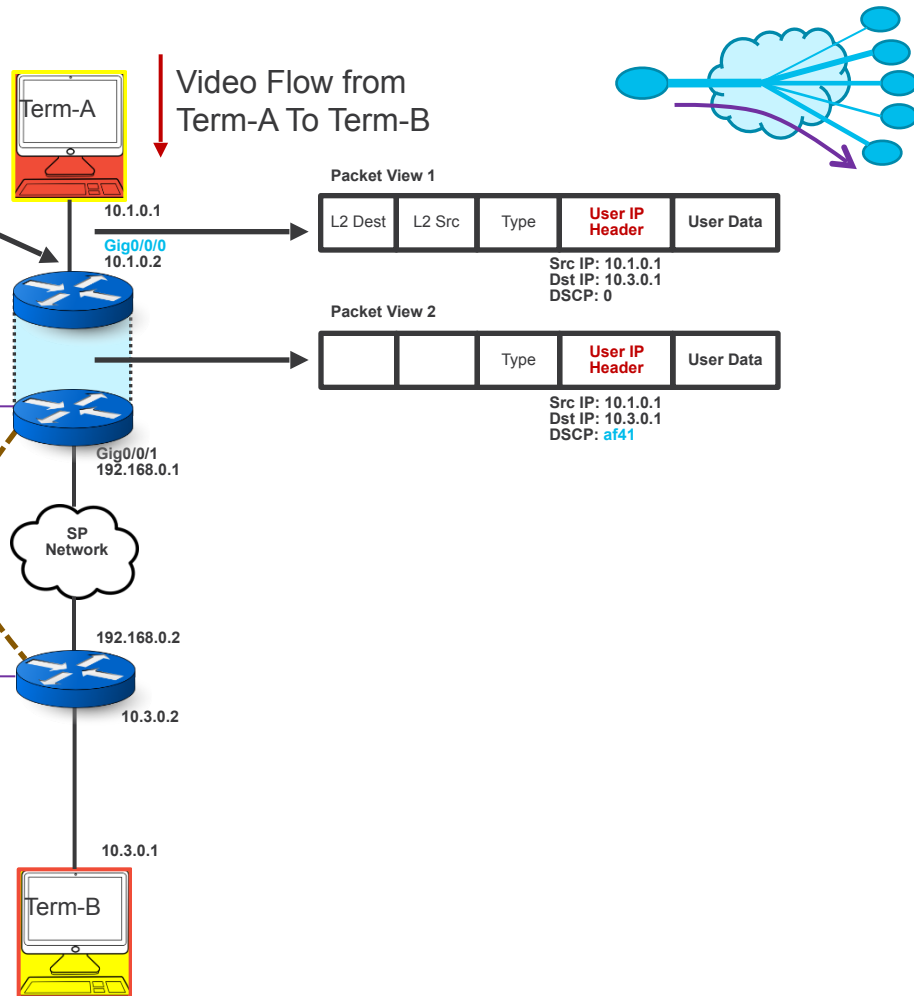
Marking the User
IP header

```
class-map INTERACTIVE-VIDEO
match dscp af41
```

```
policy-map RS-GROUP-10MBPS-POLICY
class INTERACTIVE-VIDEO
set dscp tunnel af31
```

```
interface Tunnel10
nhp map group RS-GROUP-10MBPS service-policy
output RS-GROUP-10MBPS-POLICY
```

Tunnel



Enterprise to SP Mapping

Set dscp tunnel outbound on tunnel (Hub)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the User IP header

```
class-map INTERACTIVE-VIDEO
match dscp af41
```

```
policy-map RS-GROUP-10MBPS-POLICY
class INTERACTIVE-VIDEO
set dscp tunnel af31
```

```
interface Tunnel10
nhp map group RS-GROUP-10MBPS service-policy
output RS-GROUP-10MBPS-POLICY
```

Tunnel



Video Flow from
Term-A To Term-B



10.1.0.1
Gig0/0/0
10.1.0.2

Packet View 1

L2 Dest	L2 Src	Type	User IP Header	User Data
			Src IP: 10.1.0.1 Dst IP: 10.3.0.1 DSCP: 0	

Packet View 2

		Type	User IP Header	User Data
			Src IP: 10.1.0.1 Dst IP: 10.3.0.1 DSCP: af41	

Packet View 3

L2 Dest	L2 Src	Type	Tunnel IP Header	User IP Header	User Data
			Src IP: 10.1.0.1 Dst IP: 10.3.0.1 DSCP: af41		

Tun10
172.16.0.1

Gig0/0/1
192.168.0.1



Tun10
172.16.0.2

192.168.0.2
10.3.0.2

10.3.0.1



Enterprise to SP Mapping

Set dscp tunnel outbound on tunnel (Hub)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the **User IP header**

```
class-map INTERACTIVE-VIDEO
match dscp af41
```

```
policy-map RS-GROUP-10MBPS-POLICY
class INTERACTIVE-VIDEO
set dscp tunnel af31
```

```
interface Tunnel10
nhp map group RS-GROUP-10MBPS service-policy
output RS-GROUP-10MBPS-POLICY
```

Marking the **Tunnel IP header**

Tunnel



Video Flow from
Term-A To Term-B



10.1.0.1
Gig0/0/0
10.1.0.2

Packet View 1

L2 Dest	L2 Src	Type	User IP Header	User Data
			Src IP: 10.1.0.1 Dst IP: 10.3.0.1 DSCP: 0	

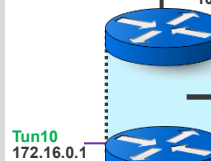
Packet View 2

		Type	User IP Header	User Data
			Src IP: 10.1.0.1 Dst IP: 10.3.0.1 DSCP: af41	

Packet View 3

L2 Dest	L2 Src	Type	Tunnel IP Header	User IP Header	User Data
			Src IP: 172.16.0.1 Dst IP: 172.16.0.2 DSCP: af31	Src IP: 10.1.0.1 Dst IP: 10.3.0.1 DSCP: af41	

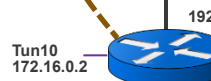
'Set dscp tunnel' means don't copy but instead remember and mark this value once tunnel header is imposed



Tun10
172.16.0.1

Gig0/0/1
192.168.0.1

SP Network



Tun10
172.16.0.2

192.168.0.2

10.3.0.2

10.3.0.1



Enterprise to SP Mapping

Set dscp tunnel outbound on tunnel (Hub)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the **User IP header**

```
class-map INTERACTIVE-VIDEO
match dscp af41
```

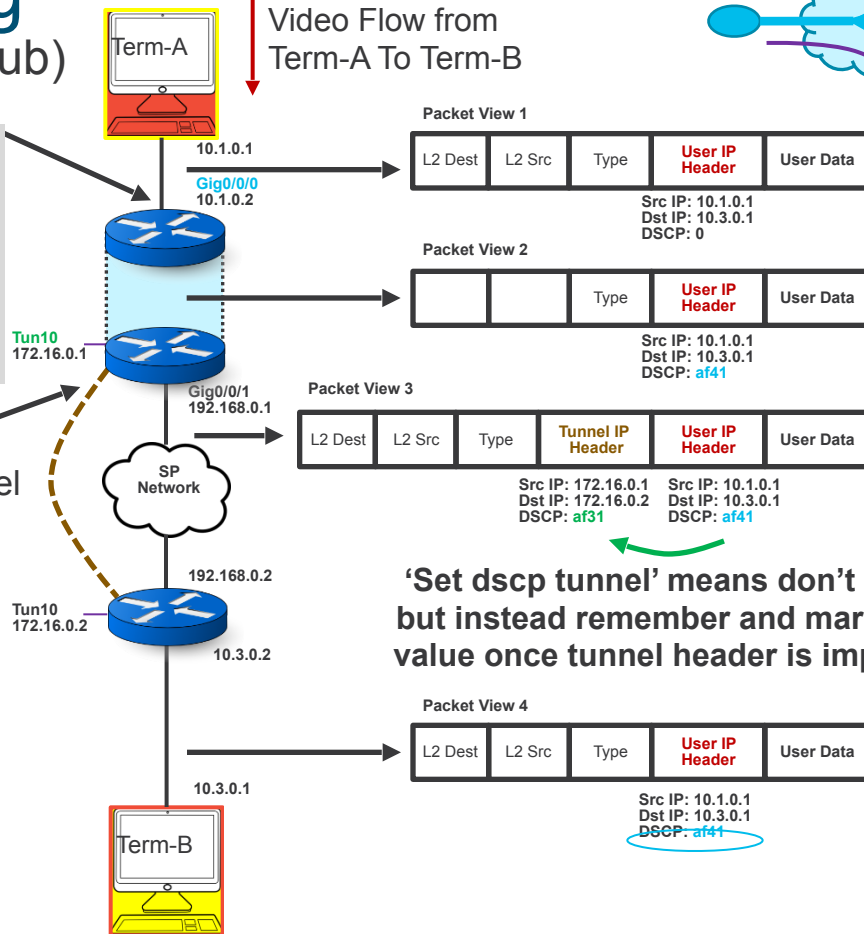
```
policy-map RS-GROUP-10MBPS-POLICY
class INTERACTIVE-VIDEO
set dscp tunnel af31
```

```
interface Tunnel10
nhp map group RS-GROUP-10MBPS service-policy
output RS-GROUP-10MBPS-POLICY
```

Marking the **Tunnel IP header**

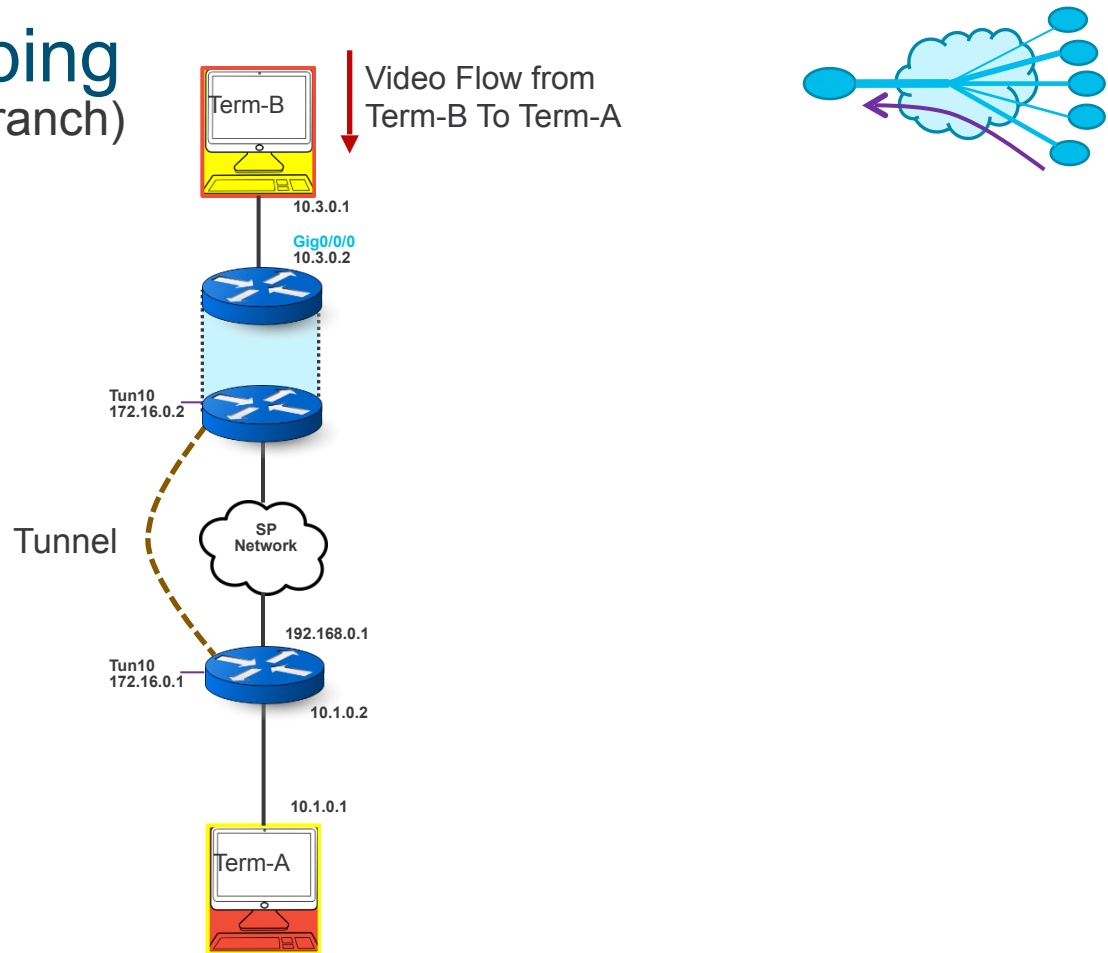
Tunnel

Video Flow from
Term-A To Term-B



Enterprise to SP Mapping

Set dscp outbound on physical (Branch)



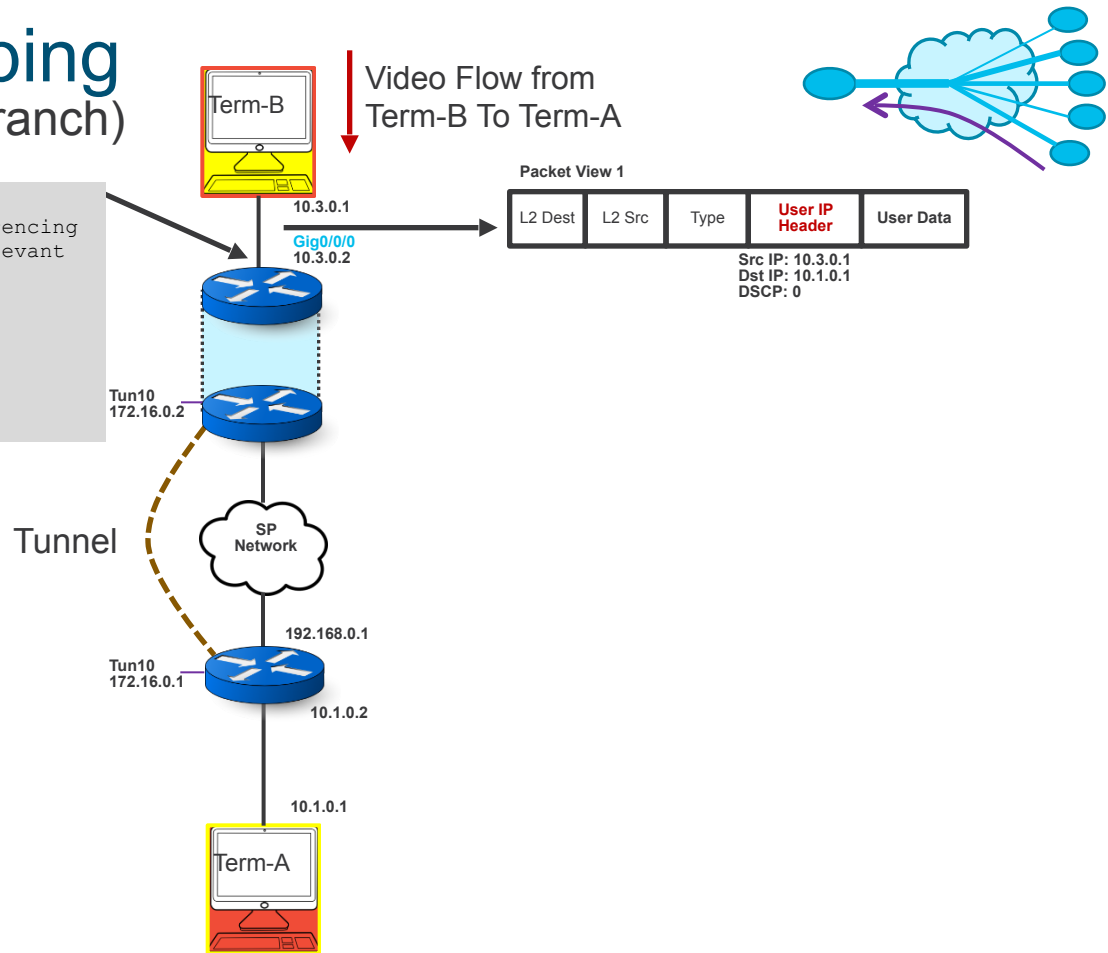
Enterprise to SP Mapping

Set dscp outbound on physical (Branch)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```



Enterprise to SP Mapping

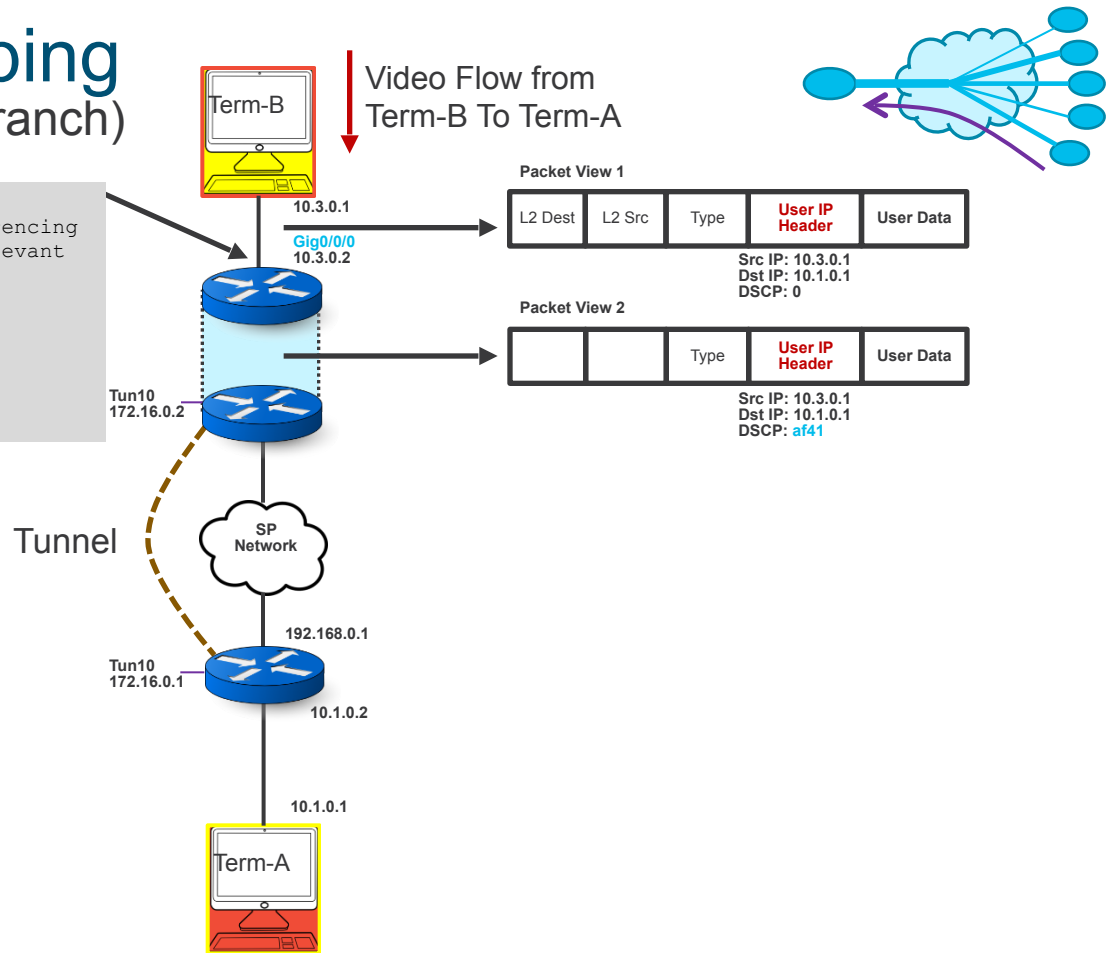
Set dscp outbound on physical (Branch)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the User
IP header



Enterprise to SP Mapping

Set dscp outbound on physical (Branch)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

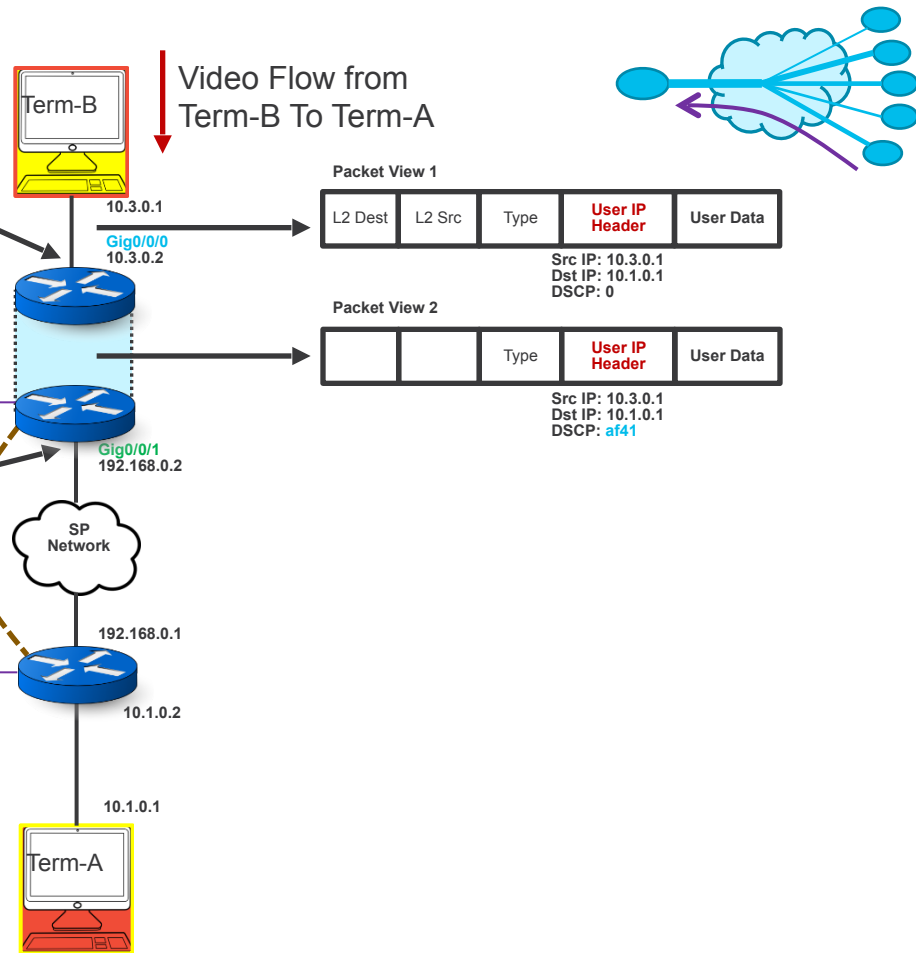
Marking the User IP header

```
class-map INTERACTIVE-VIDEO
match dscp af41
```

```
policy-map POLICY-TRANSPORT-1
class INTERACTIVE-VIDEO
set dscp af31
```

```
interface GigabitEthernet0/0/1
service-policy output POLICY-TRANSPORT-1
```

Tunnel



Enterprise to SP Mapping

Set dscp outbound on physical (Branch)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

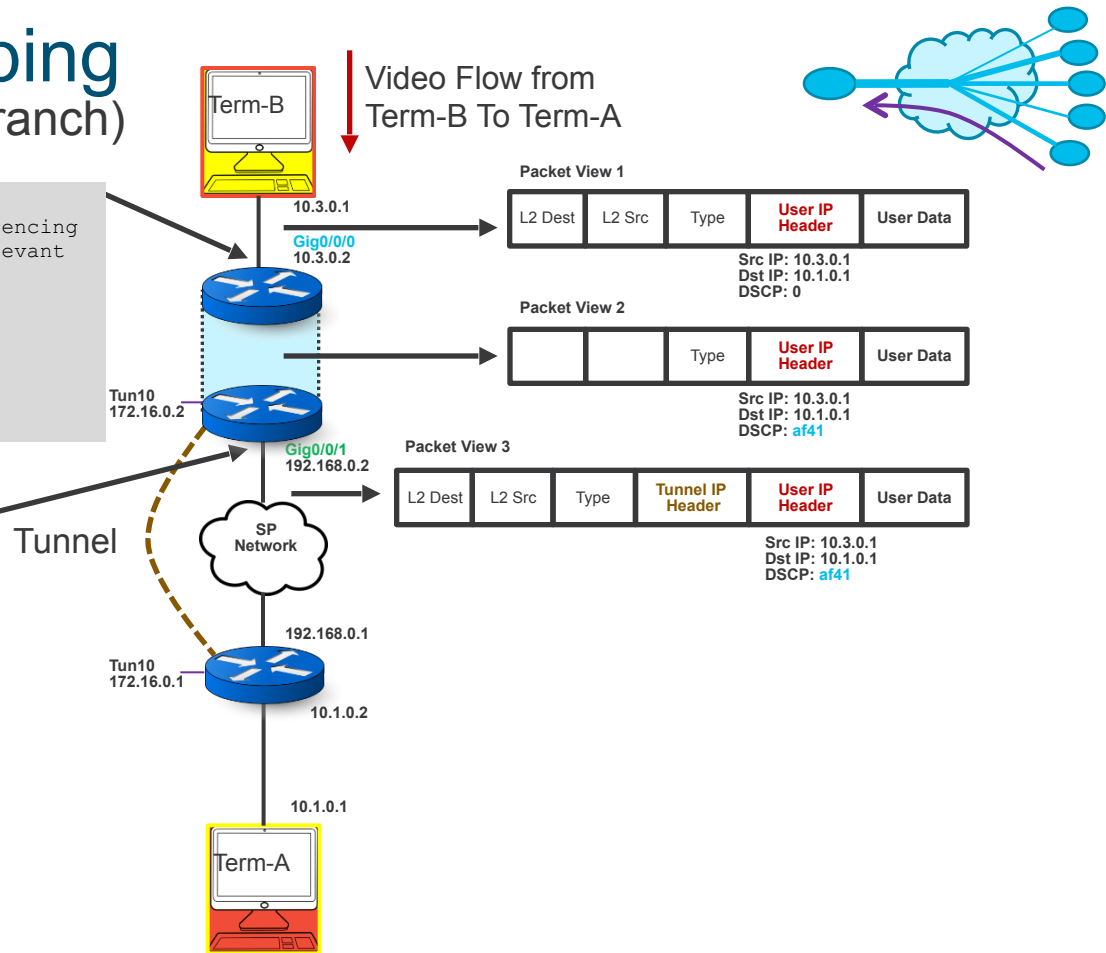
```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the User IP header

```
class-map INTERACTIVE-VIDEO
match dscp af41
```

```
policy-map POLICY-TRANSPORT-1
class INTERACTIVE-VIDEO
set dscp af31
```

```
interface GigabitEthernet0/0/1
service-policy output POLICY-TRANSPORT-1
```



Enterprise to SP Mapping

Set dscp outbound on physical (Branch)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the **User IP header**

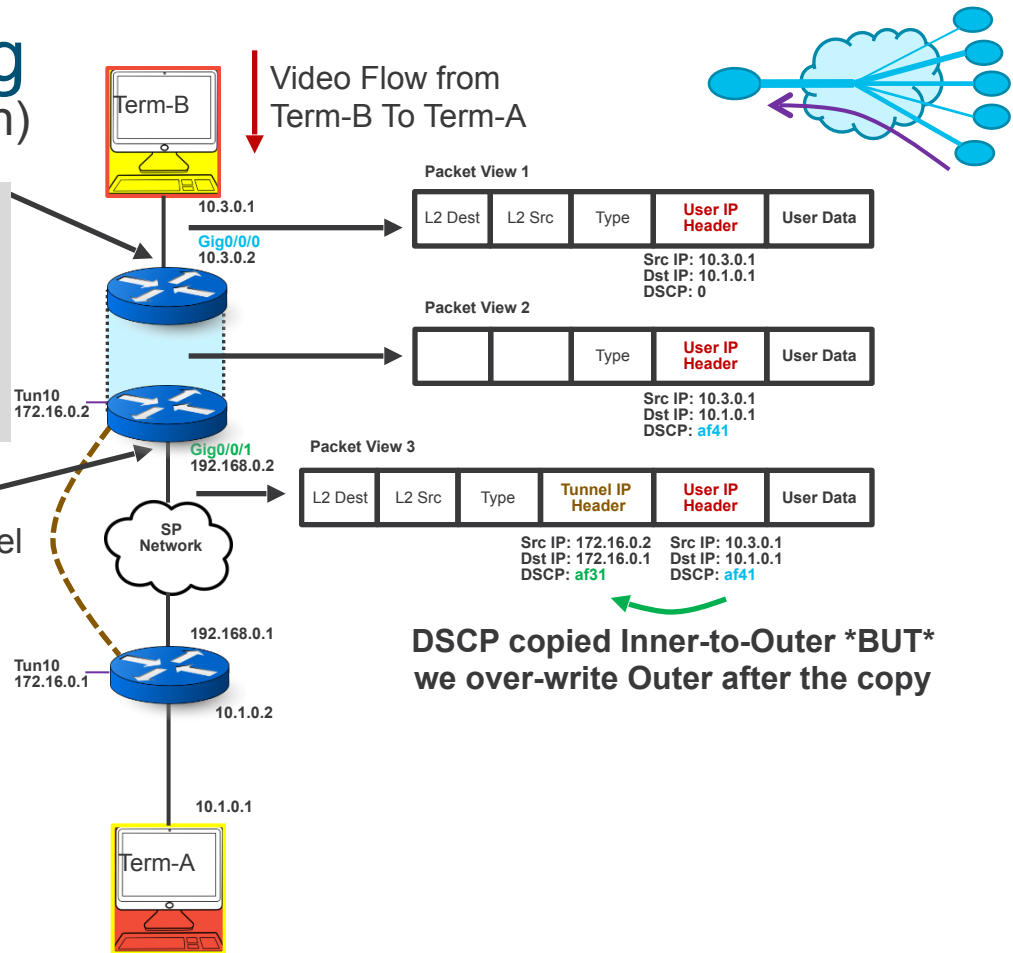
```
class-map INTERACTIVE-VIDEO
match dscp af41
```

```
policy-map POLICY-TRANSPORT-1
class INTERACTIVE-VIDEO
set dscp af31
```

```
interface GigabitEthernet0/0/1
service-policy output POLICY-TRANSPORT-1
```

Marking the **Tunnel IP header**

Tunnel



Enterprise to SP Mapping

Set dscp outbound on physical (Branch)

```
class-map match-all MULTIMEDIA_CONFERENCING-NBAR
match protocol attribute traffic-class multimedia-conferencing
match protocol attribute business-relevance business-relevant
```

```
policy-map INGRESS-MARKING
class MULTIMEDIA_CONFERENCING-NBAR
set dscp af41
```

```
interface GigabitEthernet0/0/0
service-policy input INGRESS-MARKING
```

Marking the **User IP header**

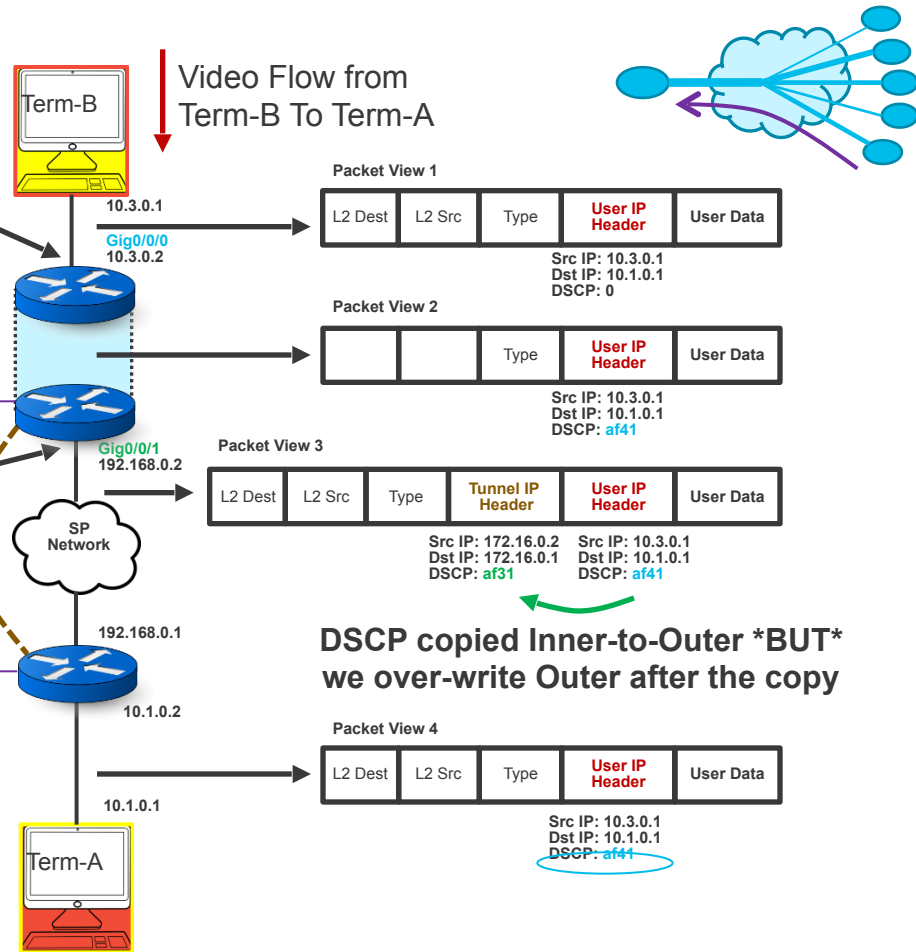
```
class-map INTERACTIVE-VIDEO
match dscp af41
```

```
policy-map POLICY-TRANSPORT-1
class INTERACTIVE-VIDEO
set dscp af31
```

```
interface GigabitEthernet0/0/1
service-policy output POLICY-TRANSPORT-1
```

Marking the **Tunnel IP header**

Tunnel



Enterprise to SP Mapping

Example: 4-Class SP Model

Application	DSCP
Internetwork Control	CS6
VoIP	EF
Broadcast Video	CS5 → AF31
Multimedia Conferencing	AF41 → AF31
Real-Time Interactive	CS4 → AF31
Multimedia Streaming	AF31
Signalling	CS3 → AF21
Transactional Data	AF21
Network Management	CS2 → AF21
Bulk Data	AF11 → AF21
Scavenger	CS1
Best Effort	DF

4-Class Model	
EF	SP-VOICE
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
DF	SP-DEFAULT

Enterprise to SP Mapping

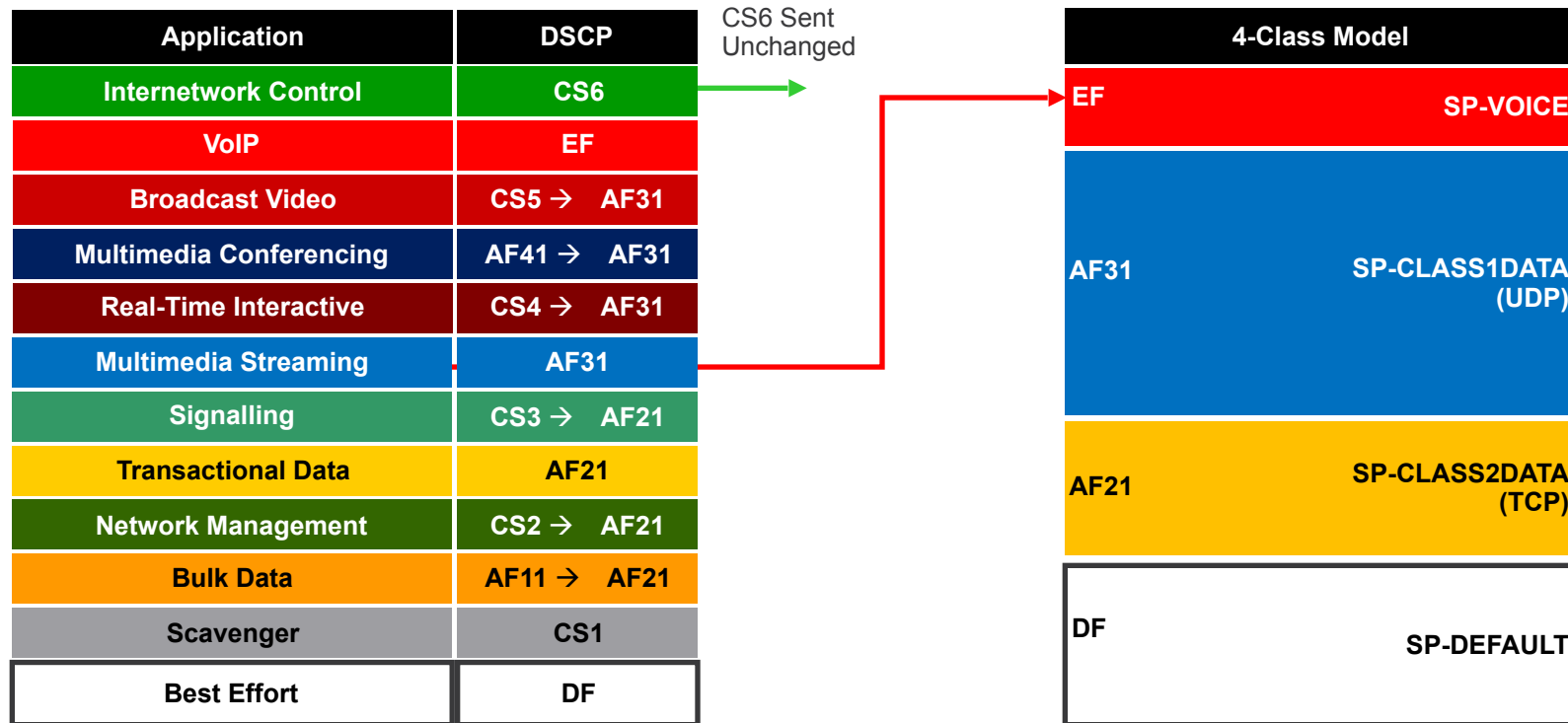
Example: 4-Class SP Model

Application	DSCP	CS6 Sent Unchanged
Internetwork Control	CS6	
VoIP	EF	→
Broadcast Video	CS5 → AF31	
Multimedia Conferencing	AF41 → AF31	
Real-Time Interactive	CS4 → AF31	
Multimedia Streaming	AF31	
Signalling	CS3 → AF21	
Transactional Data	AF21	
Network Management	CS2 → AF21	
Bulk Data	AF11 → AF21	
Scavenger	CS1	
Best Effort	DF	

4-Class Model	
EF	SP-VOICE
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
DF	SP-DEFAULT

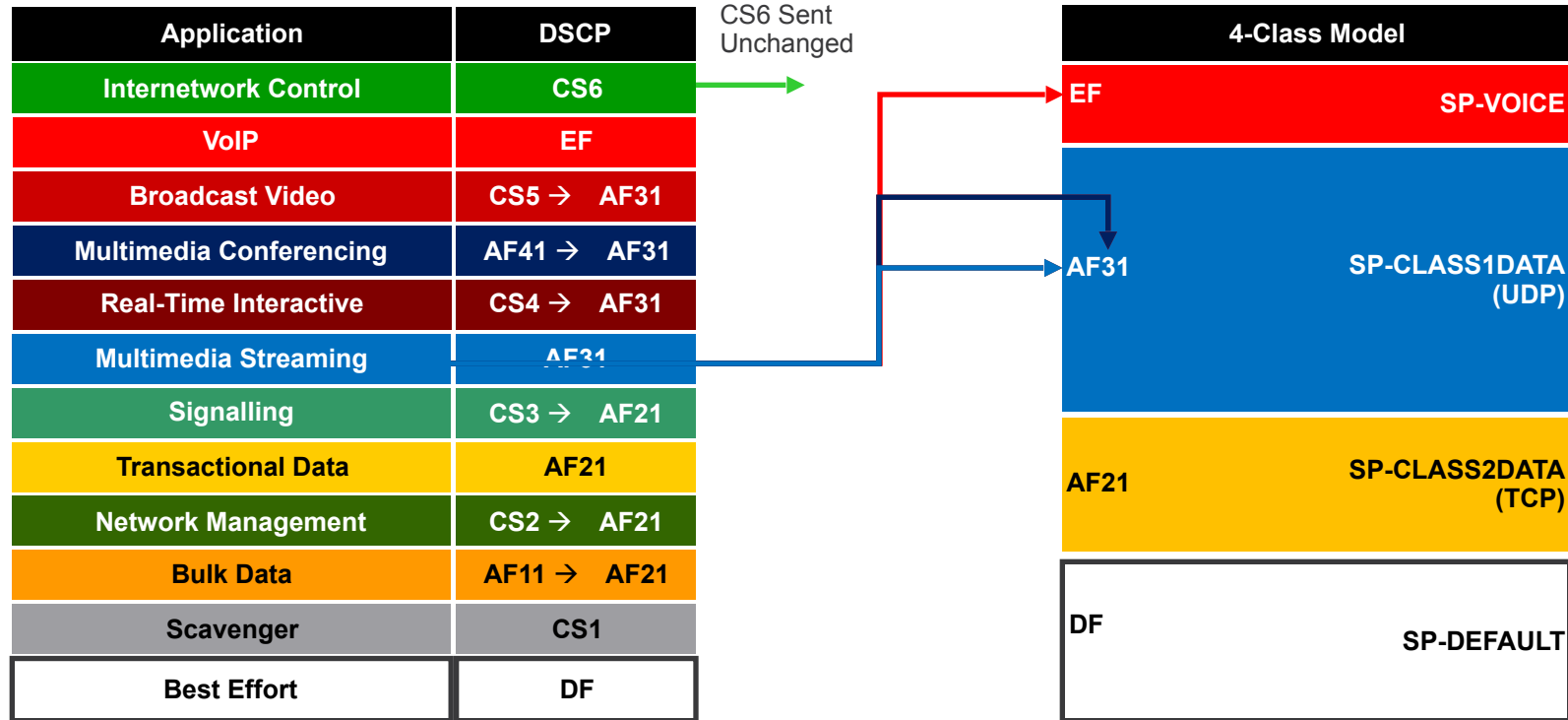
Enterprise to SP Mapping

Example: 4-Class SP Model



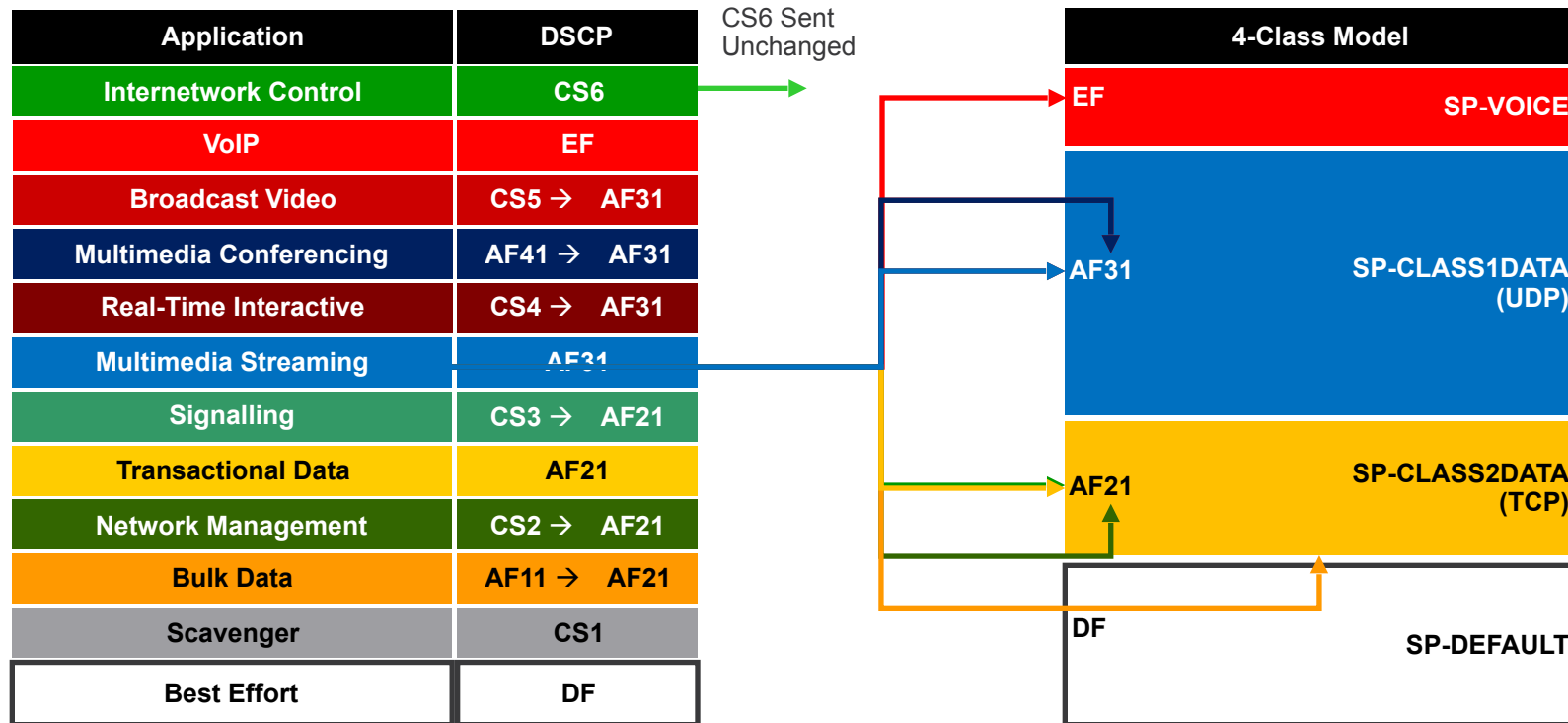
Enterprise to SP Mapping

Example: 4-Class SP Model



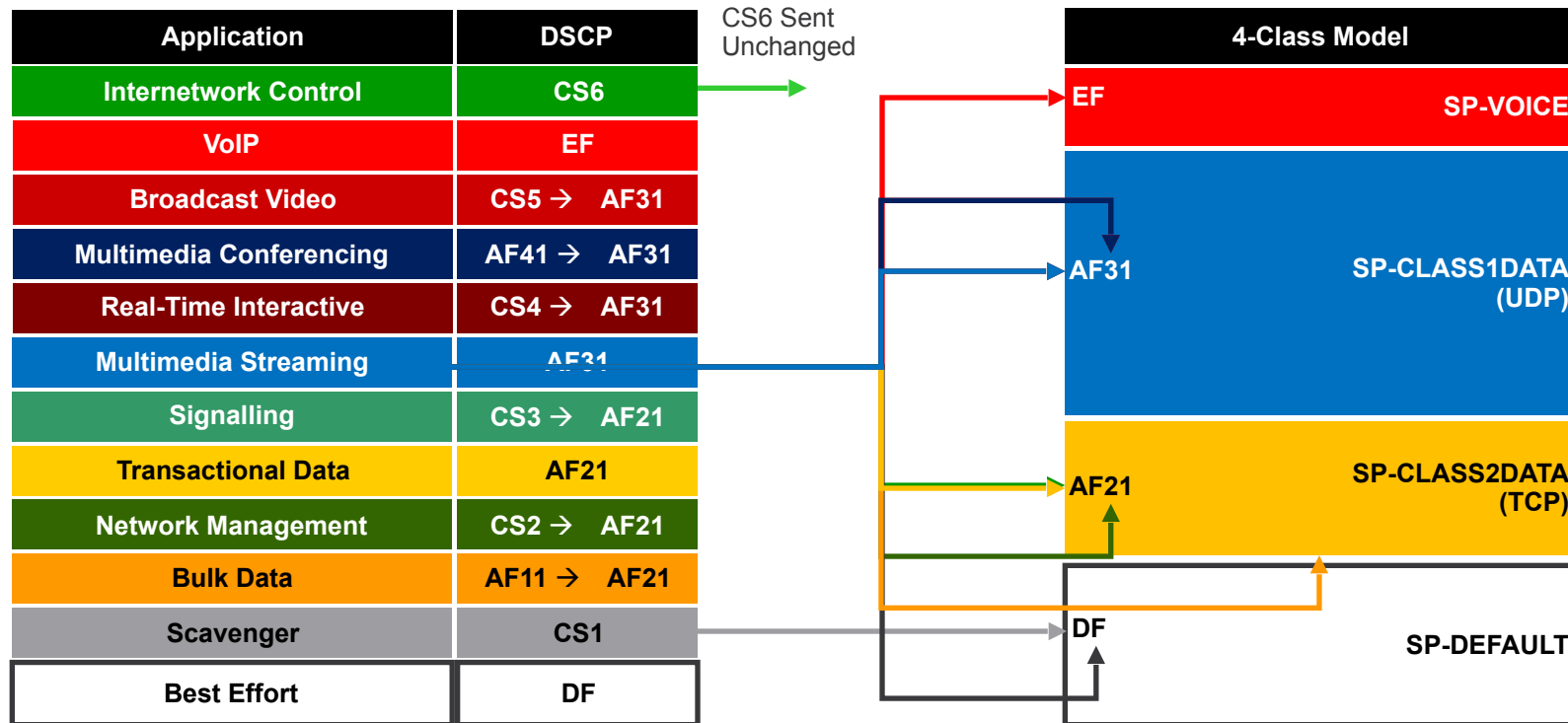
Enterprise to SP Mapping

Example: 4-Class SP Model



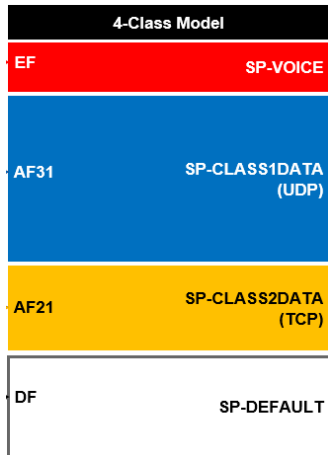
Enterprise to SP Mapping

Example: 4-Class SP Model



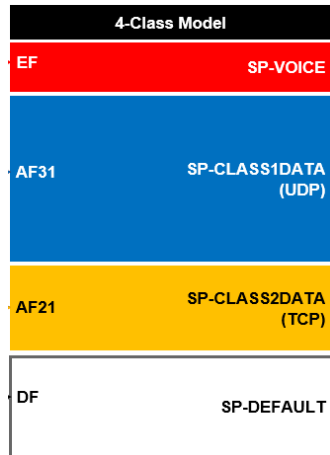
4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



4-Class SP QoS Model Configuration

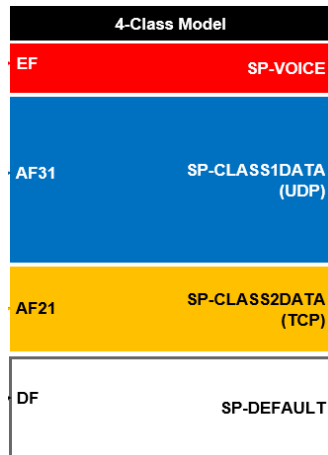
Tunnel Interface
IWAN Hub BR



```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel default
class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



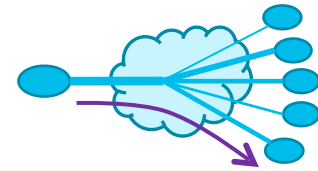
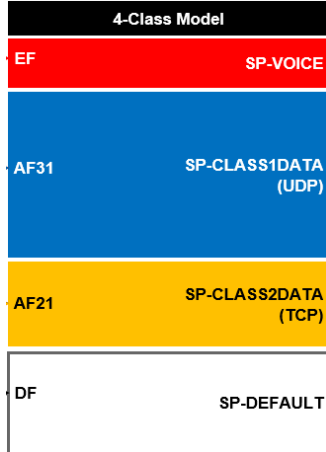
```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel default
class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy WAN
```

4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



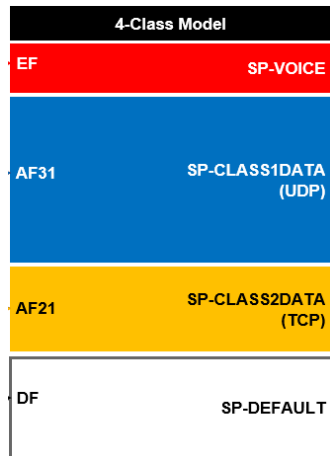
```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel default
class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy WAN
```


4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



```
policy-map WAN
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af31
class NET-CTRL-MGMT
bandwidth remaining percent 5
set dscp tunnel cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dscp tunnel af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af21
class SCAVENGER
bandwidth remaining percent 1
set dscp tunnel default
class VOICE
priority level 1
police cir percent 10
set dscp tunnel ef
class class-default
bandwidth remaining percent 25
random-detect
random-detect exponential-weighting-constant 9
set dscp tunnel default
```

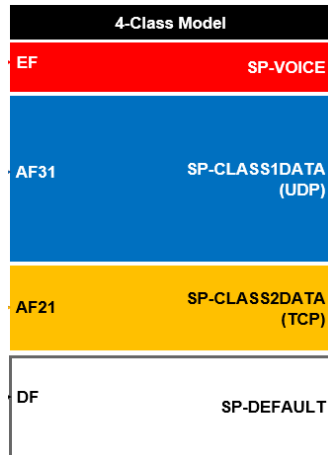
Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
shape average 10 Mbps
bandwidth remaining ratio 10
service-policy WAN
```

```
interface Tunnel10
bandwidth <service-rate>
nhp map group RS-GROUP-10MBPS service-policy
output RS-GROUP-10MBPS-POLICY
```

4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp tunnel af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp tunnel af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp tunnel cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp tunnel af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp tunnel af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp tunnel default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp tunnel ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    random-detect exponential-weighting-constant 9
    set dscp tunnel default
```

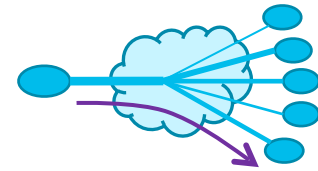
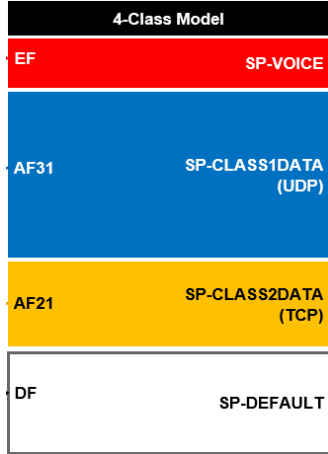
Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
  class class-default
    shape average 10 Mbps
    bandwidth remaining ratio 10
    service-policy WAN
```

```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group RS-GROUP-10MBPS service-policy
  output RS-GROUP-10MBPS-POLICY
```

4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel default
class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

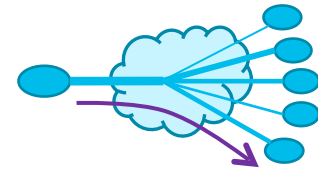
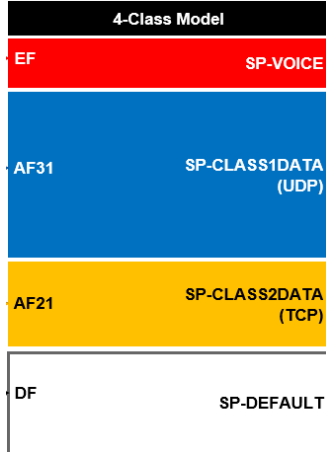
Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy WAN
```

```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group RS-GROUP-10MBPS service-policy
  output RS-GROUP-10MBPS-POLICY
```

4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel default
class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy WAN
```

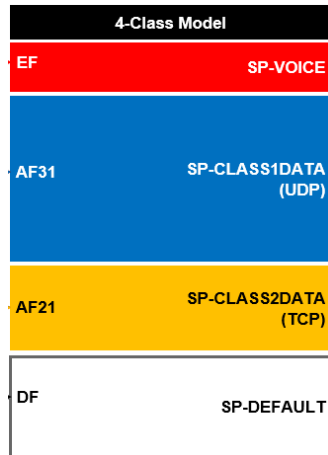
```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group RS-GROUP-10MBPS service-policy
  output RS-GROUP-10MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group RS-GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Tunnel Interface
IWAN Hub BR



```
policy-map WAN
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af31
class NET-CTRL-MGMT
bandwidth remaining percent 5
set dscp tunnel cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dscp tunnel af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af21
class SCAVENGER
bandwidth remaining percent 1
set dscp tunnel default
class VOICE
priority level 1
police cir percent 10
set dscp tunnel ef
class class-default
bandwidth remaining percent 25
random-detect
random-detect exponential-weighting-constant 9
set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
shape average 10 Mbps
bandwidth remaining ratio 10
service-policy WAN
```

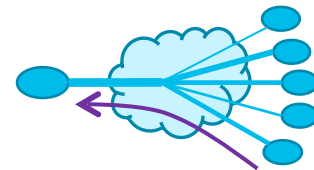
```
interface Tunnell0
bandwidth <service-rate>
nhp map group RS-GROUP-10MBPS service-policy
output RS-GROUP-10MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
bandwidth 10000
service-policy output POLICY-TRANSPORT-1
!
interface Tunnell0
bandwidth 10000
nhp group RS-GROUP-10MBPS
tunnel source GigabitEthernet0/0
tunnel vrf IWAN-TRANSPORT-1
```

4-Class SP QoS Model Configuration

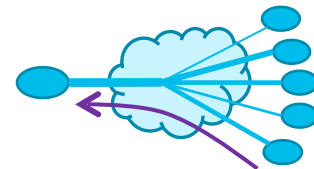
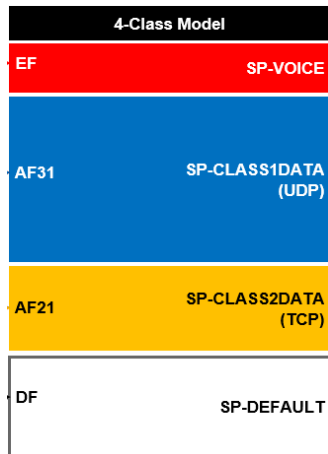
Physical Interface
IWAN Branch



4-Class Model	
EF	SP-VOICE
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
DF	SP-DEFAULT

4-Class SP QoS Model Configuration

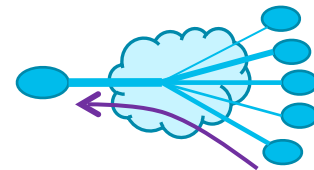
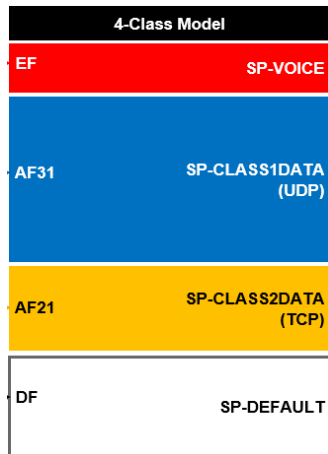
Physical Interface IWAN Branch



```
policy-map WAN
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp af31
class NET-CTRL-MGMT
bandwidth remaining percent 5
set dscp cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dscp af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp af21
class SCAVENGER
bandwidth remaining percent 1
set dscp default
class VOICE
priority level 1
police cir percent 10
set dscp ef
class class-default
bandwidth remaining percent 25
random-detect
random-detect exponential-weighting-constant 9
set dscp default
```

4-Class SP QoS Model Configuration

Physical Interface IWAN Branch



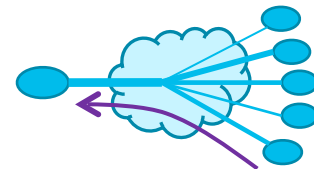
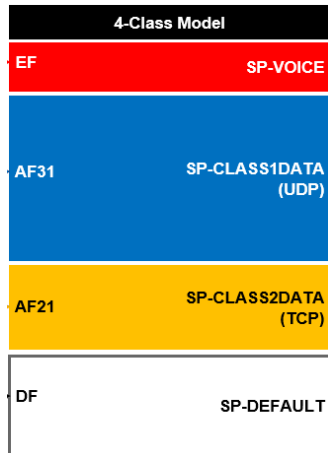
```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    random-detect exponential-weighting-constant 9
    set dscp default
```

Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN
```


4-Class SP QoS Model Configuration

Physical Interface IWAN Branch



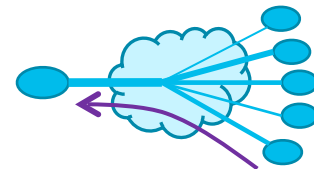
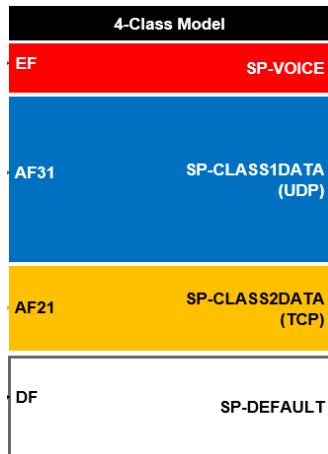
```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    random-detect exponential-weighting-constant 9
    set dscp default
```

Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN
```

4-Class SP QoS Model Configuration

Physical Interface IWAN Branch



```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    random-detect exponential-weighting-constant 9
    set dscp default
```

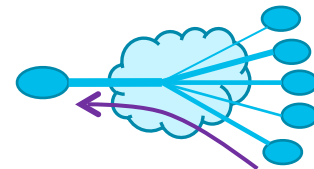
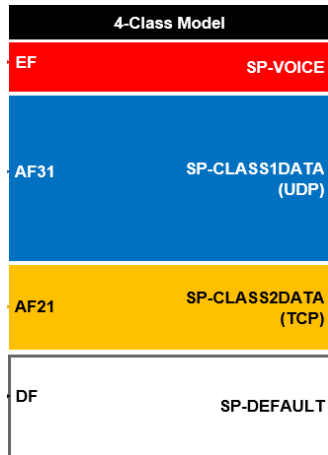
Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN
```

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Physical Interface IWAN Branch



```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    random-detect exponential-weighting-constant 9
    set dscp default
```

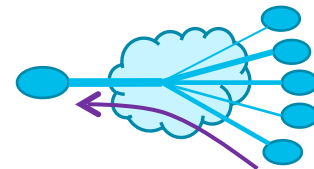
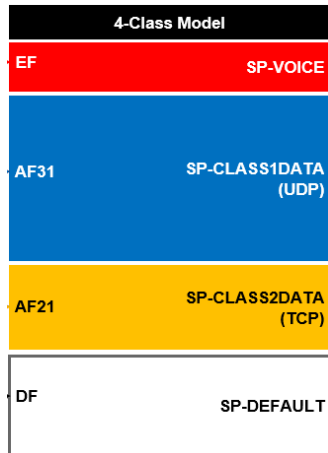
Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN
```

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Physical Interface IWAN Branch



```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    random-detect exponential-weighting-constant 9
    set dscp default
```

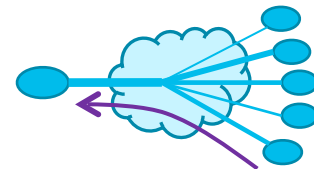
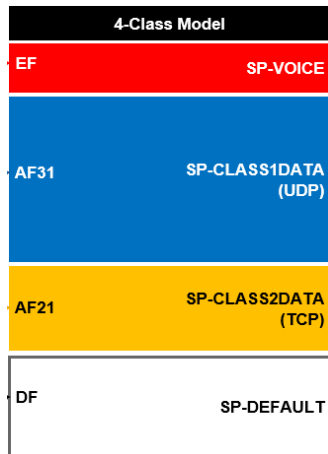
Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN
```

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```

4-Class SP QoS Model Configuration

Physical Interface IWAN Branch



```
policy-map WAN
  class INTERACTIVE-VIDEO
    bandwidth remaining percent 30
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class STREAMING-VIDEO
    bandwidth remaining percent 10
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af31
  class NET-CTRL-MGMT
    bandwidth remaining percent 5
    set dscp cs6
  class CALL-SIGNALING
    bandwidth remaining percent 4
    set dscp af21
  class CRITICAL-DATA
    bandwidth remaining percent 25
    random-detect dscp-based
    random-detect exponential-weighting-constant 9
    set dscp af21
  class SCAVENGER
    bandwidth remaining percent 1
    set dscp default
  class VOICE
    priority level 1
    police cir percent 10
    set dscp ef
  class class-default
    bandwidth remaining percent 25
    random-detect
    random-detect exponential-weighting-constant 9
    set dscp default
```

Branch Router:

```
policy-map POLICY-TRANSPORT-1
  class class-default
    shape average 10 Mbps
    service-policy WAN
```

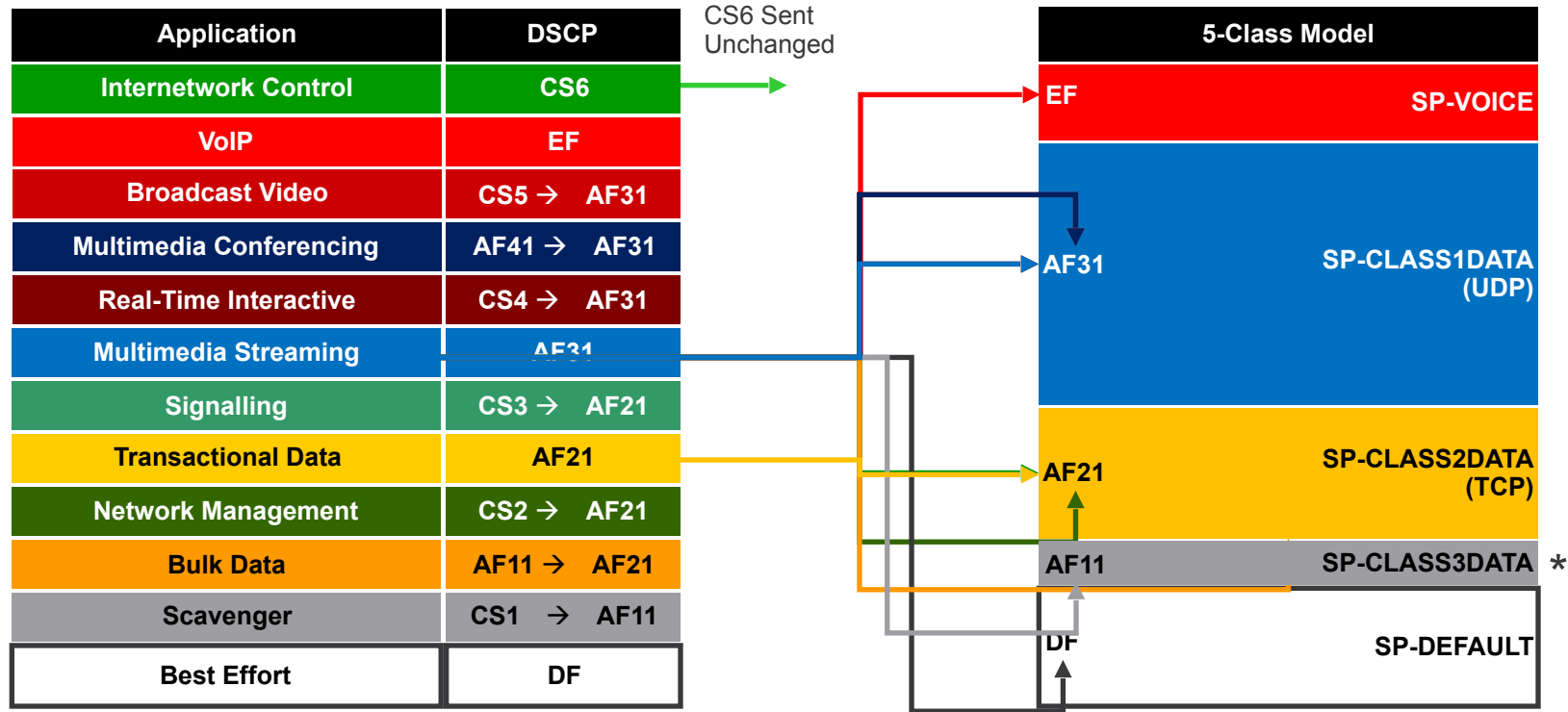
```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```

The PfR Traffic Class channels will not establish if the DSCP values from the hub and branch routers do not match

Enterprise to SP Mapping

Reference

Example: 5-Class SP Model

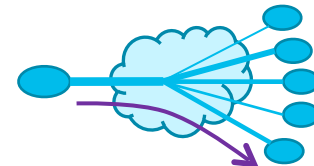


* - Specified by ISP

5-Class QoS Model Configuration

Tunnel Interface
IWAN Hub BR

Reference



5-Class Model	
EF	SP-VOICE
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
class INTERACTIVE-VIDEO
bandwidth remaining percent 30
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af31
class STREAMING-VIDEO
bandwidth remaining percent 10
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af31
class NET-CTRL-MGMT
bandwidth remaining percent 5
set dscp tunnel cs6
class CALL-SIGNALING
bandwidth remaining percent 4
set dscp tunnel af21
class CRITICAL-DATA
bandwidth remaining percent 25
random-detect dscp-based
random-detect exponential-weighting-constant 9
set dscp tunnel af21
class SCAVENGER
bandwidth remaining percent 1
set dscp tunnel af11
class VOICE
priority level 1
police cir percent 10
set dscp tunnel ef
class class-default
bandwidth remaining percent 25
random-detect
random-detect exponential-weighting-constant 9
set dscp tunnel default
```

Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
shape average 10 Mbps
bandwidth remaining ratio 10
service-policy WAN
```

```
interface Tunnell0
bandwidth <service-rate>
nhp map group RS-GROUP-10MBPS service-policy
output RS-GROUP-10MBPS-POLICY
```

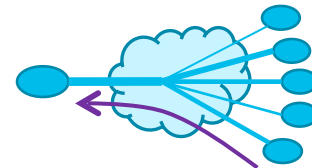
Branch Router:

```
interface GigabitEthernet0/0
bandwidth 10000
service-policy output POLICY-TRANSPORT-1
!
interface Tunnell0
bandwidth 10000
nhp group RS-GROUP-10MBPS
tunnel source GigabitEthernet0/0
tunnel vrf IWAN-TRANSPORT-1
```

5-Class QoS Model Configuration

Physical Interface
IWAN Branch

Reference



5-Class Model	
EF	SP-VOICE
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp af11
class VOICE
  priority level 1
  police cir percent 10
  set dscp ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp default
```

Branch Router:

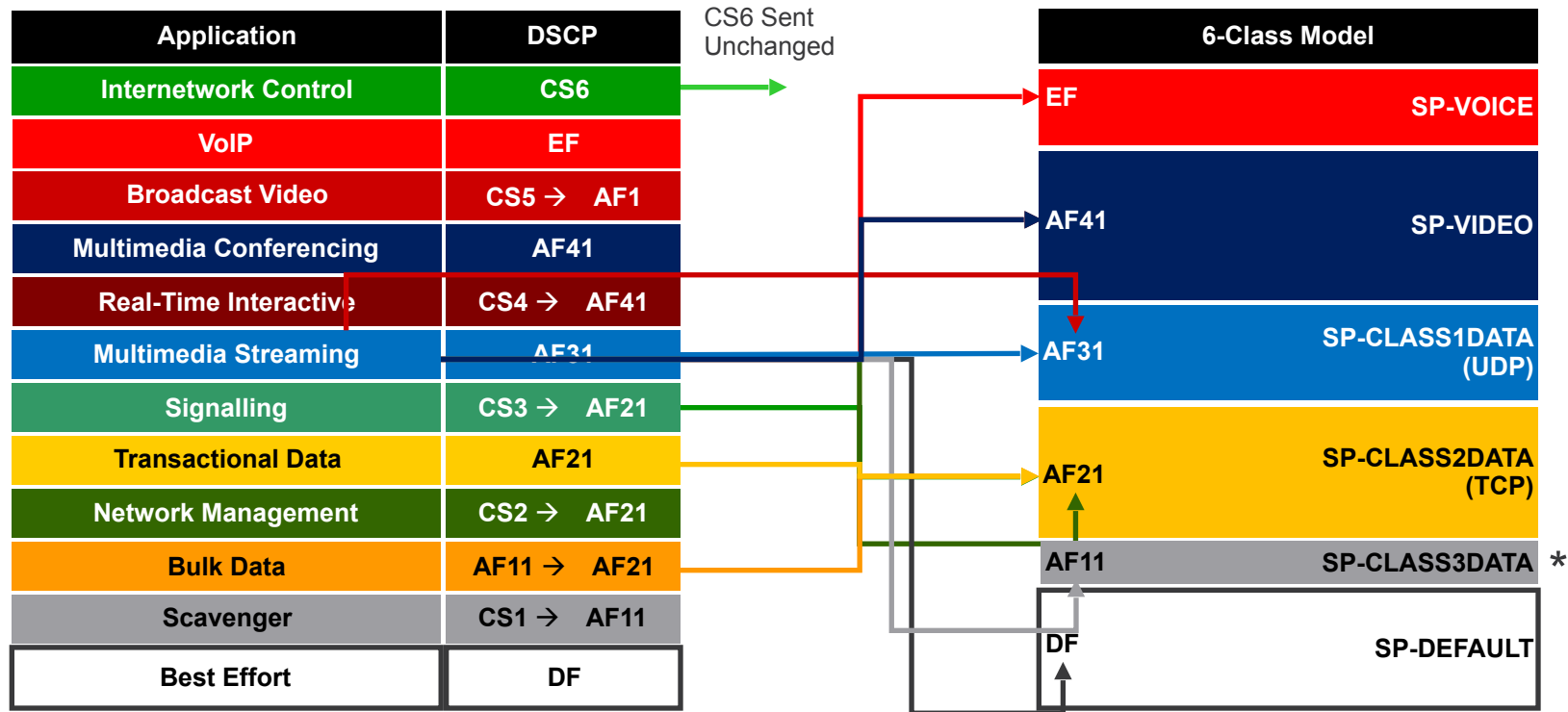
```
policy-map POLICY-TRANSPORT-1
class class-default
  shape average 10 Mbps
  service-policy WAN
```

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```


Enterprise to SP Mapping

Example: 6-Class SP Model

Reference



* - Specified by ISP

6-Class QoS Model Configuration

Tunnel Interface
IWAN Hub BR

6-Class Model	
EF	SP-VOICE
AF41	SP-VIDEO
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af41
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp tunnel cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp tunnel af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp tunnel af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp tunnel af11
class VOICE
  priority level 1
  police cir percent 10
  set dscp tunnel ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp tunnel default
```

Reference



Hub Router:

```
policy-map RS-GROUP-10MBPS-POLICY
class class-default
  shape average 10 Mbps
  bandwidth remaining ratio 10
  service-policy WAN
```

```
interface Tunnel10
  bandwidth <service-rate>
  nhrp map group RS-GROUP-10MBPS service-policy
  output RS-GROUP-10MBPS-POLICY
```

Branch Router:

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
!
interface Tunnel10
  bandwidth 10000
  nhrp group RS-GROUP-10MBPS
  tunnel source GigabitEthernet0/0
  tunnel vrf IWAN-TRANSPORT-1
```

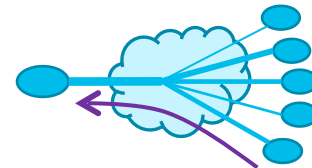
6-Class QoS Model Configuration

Physical Interface IWAN Branch

6-Class Model	
EF	SP-VOICE
AF41	SP-VIDEO
AF31	SP-CLASS1DATA (UDP)
AF21	SP-CLASS2DATA (TCP)
AF11	SP-CLASS3DATA
DF	SP-DEFAULT

```
policy-map WAN
class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af41
class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af31
class NET-CTRL-MGMT
  bandwidth remaining percent 5
  set dscp cs6
class CALL-SIGNALING
  bandwidth remaining percent 4
  set dscp af21
class CRITICAL-DATA
  bandwidth remaining percent 25
  random-detect dscp-based
  random-detect exponential-weighting-constant 9
  set dscp af21
class SCAVENGER
  bandwidth remaining percent 1
  set dscp af11
class VOICE
  priority level 1
  police cir percent 10
  set dscp ef
class class-default
  bandwidth remaining percent 25
  random-detect
  random-detect exponential-weighting-constant 9
  set dscp default
```

Reference



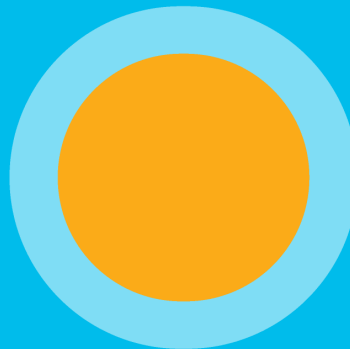
Branch Router:

```
policy-map POLICY-TRANSPORT-1
class class-default
  shape average 10 Mbps
  service-policy WAN
```

```
interface GigabitEthernet0/0
  bandwidth 10000
  service-policy output POLICY-TRANSPORT-1
```

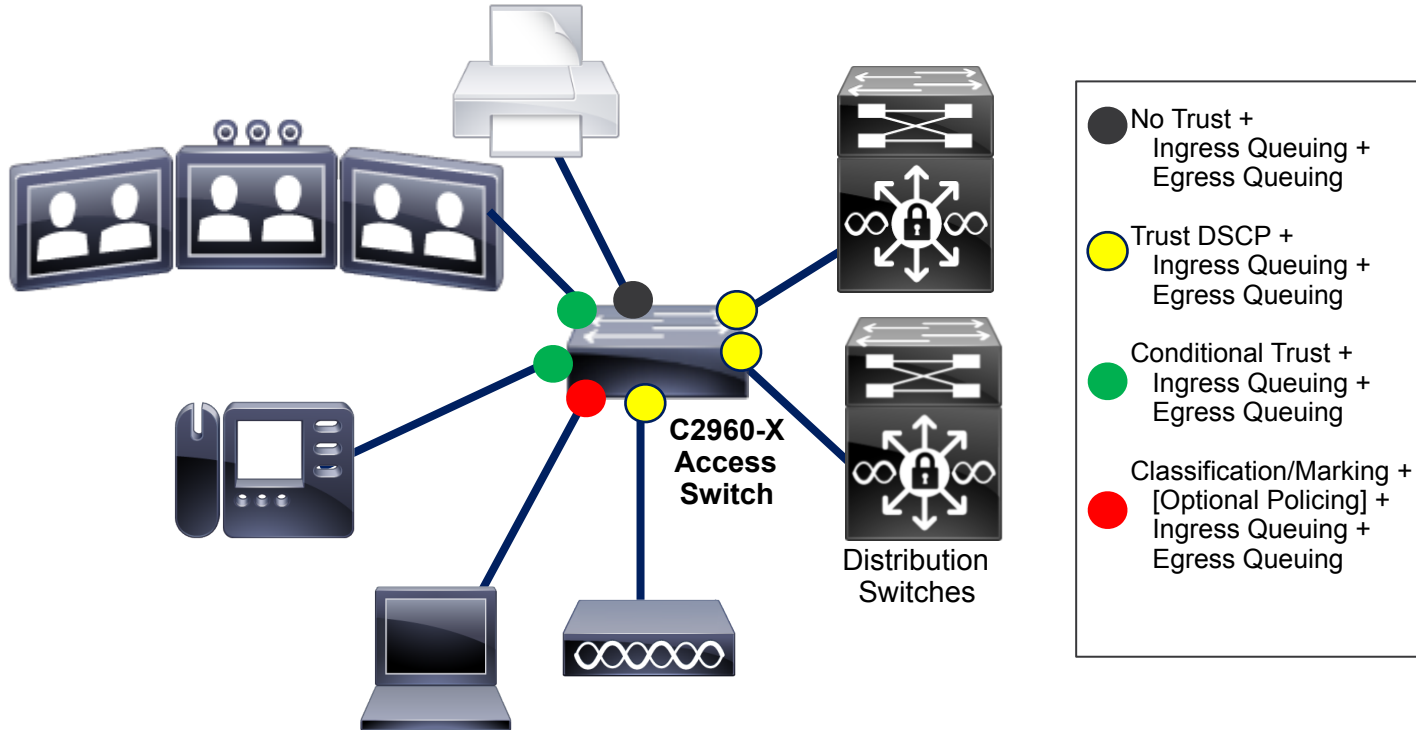
Appendix B— Campus Qos Design

Cisco Catalyst 2960-X QoS Design



Catalyst 2960-X

QoS Roles in the Campus Access



Catalyst 2960-X

QoS Design Steps

1. Enable QoS

2. Configure Ingress QoS Model(s):

- ❑ Trust Models
- ❑ Conditional Trust Model
- ❑ Service Policy Models

3. Configure Egress Queuing

Note: Catalyst 2960-X is QoS compatible with the Catalyst 3560-X & 3750-X, with the following exceptions:

- The Catalyst 3560-X & 3750-X support ingress queuing policies, but the 2960-X does not.
- Similarly, the Catalyst 3560-X & 3750-X support VLAN-based QoS policies, but the 2960-X does not.

Note: Catalyst 2960-X must be running a LAN Base image to support the following QoS features

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

Catalyst 2960-X

Enabling QoS and Trust Models

Catalyst 2960-X

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Shaded commands are global

Catalyst 2960-X

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Shaded commands are global

Trust-CoS Model Example:

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

Key commands/parameters in **RED**

```
mls qos trust cos
```

Highlighted commands are interface specific

Catalyst 2960-X

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Shaded commands are global

Trust-CoS Model Example:

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

Key commands/parameters in **RED**

```
mls qos trust cos
```

Highlighted commands are interface specific

Note: CoS 5 which is explicitly mapped to DSCP 46

Catalyst 2960-X

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Shaded commands are global

Trust-CoS Model Example:

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

Key commands/parameters in **RED**

```
mls qos trust cos
```

Highlighted commands are interface specific

Trust-DSCP Model Example:

```
mls qos trust dscp
```

Note: CoS 5 which is explicitly mapped to DSCP 46

Catalyst 2960-X

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Shaded commands are global

Trust-CoS Model Example:

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

Key commands/parameters in **RED**

```
mls qos trust cos
```

Highlighted commands are interface specific

Trust-DSCP Model Example:

```
mls qos trust dscp
```

Note: CoS 5 which is explicitly mapped to DSCP 46

Conditional-Trust Model Example:

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

Catalyst 2960-X

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Shaded commands are global

Trust-CoS Model Example:

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

Key commands/parameters in **RED**

```
mls qos trust cos
```

Highlighted commands are interface specific

Trust-DSCP Model Example:

```
mls qos trust dscp
```

Note: CoS 5 which is explicitly mapped to DSCP 46

Conditional-Trust Model Example:

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

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

Catalyst 2960-X

Conditional Trust Model Example

Conditional Trust Policy to a Cisco IP Phone:

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

```
mls qos trust device cisco-phone
```

```
mls qos trust cos
```

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

Catalyst 2960-X

Conditional Trust Model Example

Conditional Trust Policy to a Cisco IP Phone:

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

```
mls qos trust device cisco-phone
```

```
mls qos trust cos
```

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

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

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

Catalyst 2960-X

Marking Policy Model Example – Policy-Map & Class-Maps

```
class-map match-all VOIP
  match access-group name VOIP
class-map match-all MULTIMEDIA-CONFERENCING
  match access-group name MULTIMEDIA-CONFERENCING
class-map match-all SIGNALING
  match access-group name SIGNALING
class-map match-all TRANSACTIONAL-DATA
  match access-group name TRANSACTIONAL-DATA
class-map match-all BULK-DATA
  match access-group name BULK-DATA
class-map match-all SCAVENGER
  match access-group name SCAVENGER
```

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

```
service-policy input MARKING-POLICY
```

Catalyst 2960-X

Marking Policy Model Example – Access Control List

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

Catalyst 2960-X

Marking & Policing Policy Example

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

```
[class-maps omitted for brevity]
```

```
policy-map MARKING&POLICING
```

```
class VVLAN-VOIP
```

```
set dscp ef
```

```
police 128k 8000 exceed-action drop
```

```
class VVLAN-SIGNALING
```

```
set dscp cs3
```

```
police 32k 8000 exceed-action drop
```

```
class MULTIMEDIA-CONFERENCING
```

```
set dscp af41
```

```
police 5m 8000 exceed-action drop
```

```
class SIGNALING
```

```
set dscp cs3
```

```
police 32k 8000 exceed-action drop
```

```
class TRANSACTIONAL-DATA
```

```
set dscp af21
```

```
police 10m 8000 exceed-action policed-dscp-transmit
```

```
...
```

```
[continued]
```

```
class BULK-DATA
```

```
set dscp af11
```

```
police 10m 8000 exceed-action policed-dscp-transmit
```

```
class SCAVENGER
```

```
set dscp cs1
```

```
police 10m 8000 exceed-action drop
```

```
class DEFAULT
```

```
set dscp default
```

```
police 10m 8000 exceed-action policed-dscp-transmit
```

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

Catalyst 2960-X

Marking & Policing Policy Example

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

In this example exceeding:

- Best Effort (DSCP 0)
- Bulk (AF11 / DSCP 10)
- Transactional Data (AF21 / DSCP 18) are remarked to Scavenger (CS1 / DSCP 8).

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

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

[continued]

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

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

Catalyst 2960-X

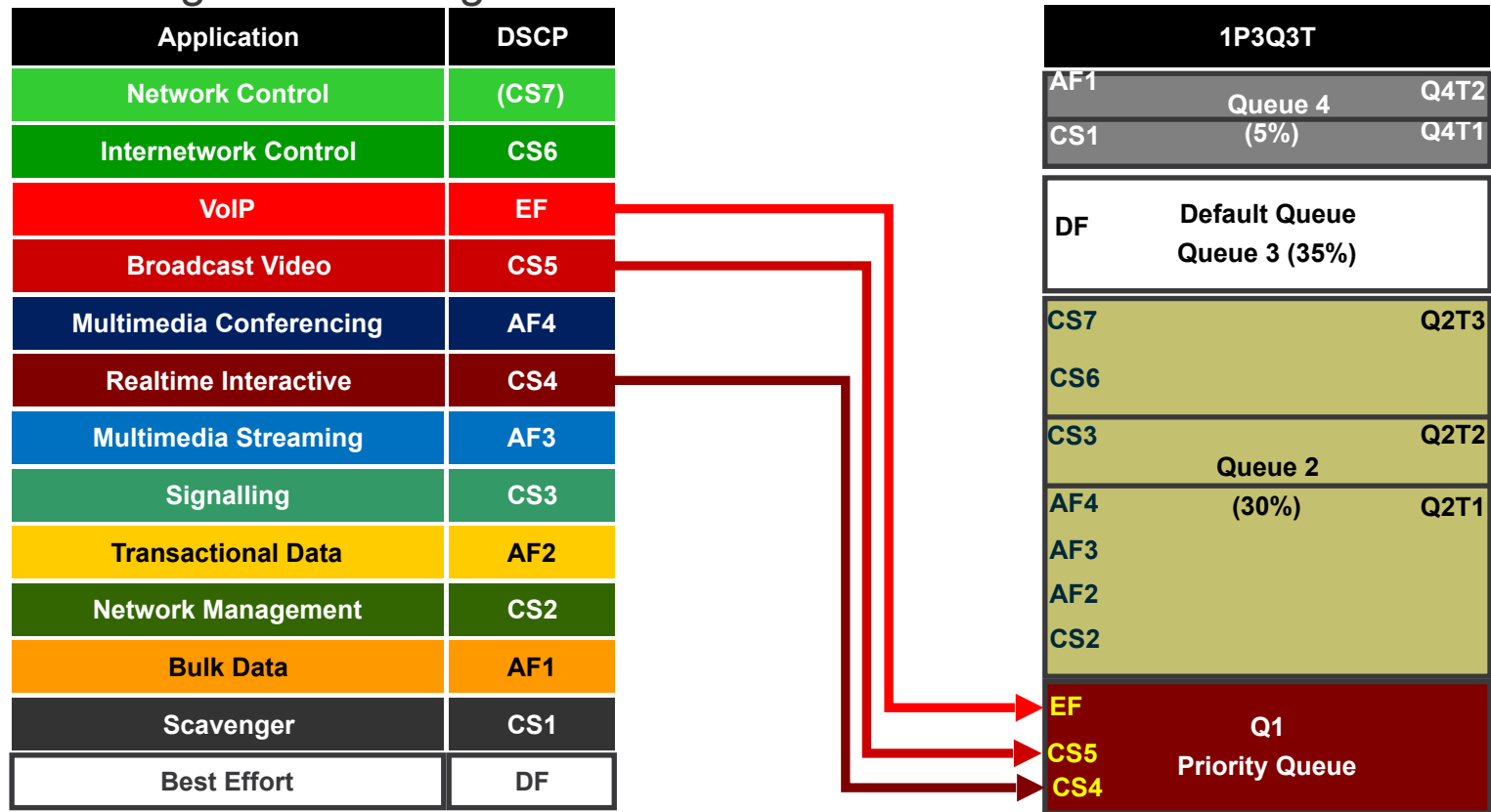
1P3Q3T Egress Queuing Model

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

1P3Q3T		
AF1	Queue 4	Q4T2
CS1	(5%)	Q4T1
DF	Default Queue Queue 3 (35%)	
CS7		Q2T3
CS6		
CS3	Queue 2	Q2T2
AF4	(30%)	Q2T1
AF3		
AF2		
CS2		
EF CS5 CS4	Q1 Priority Queue	

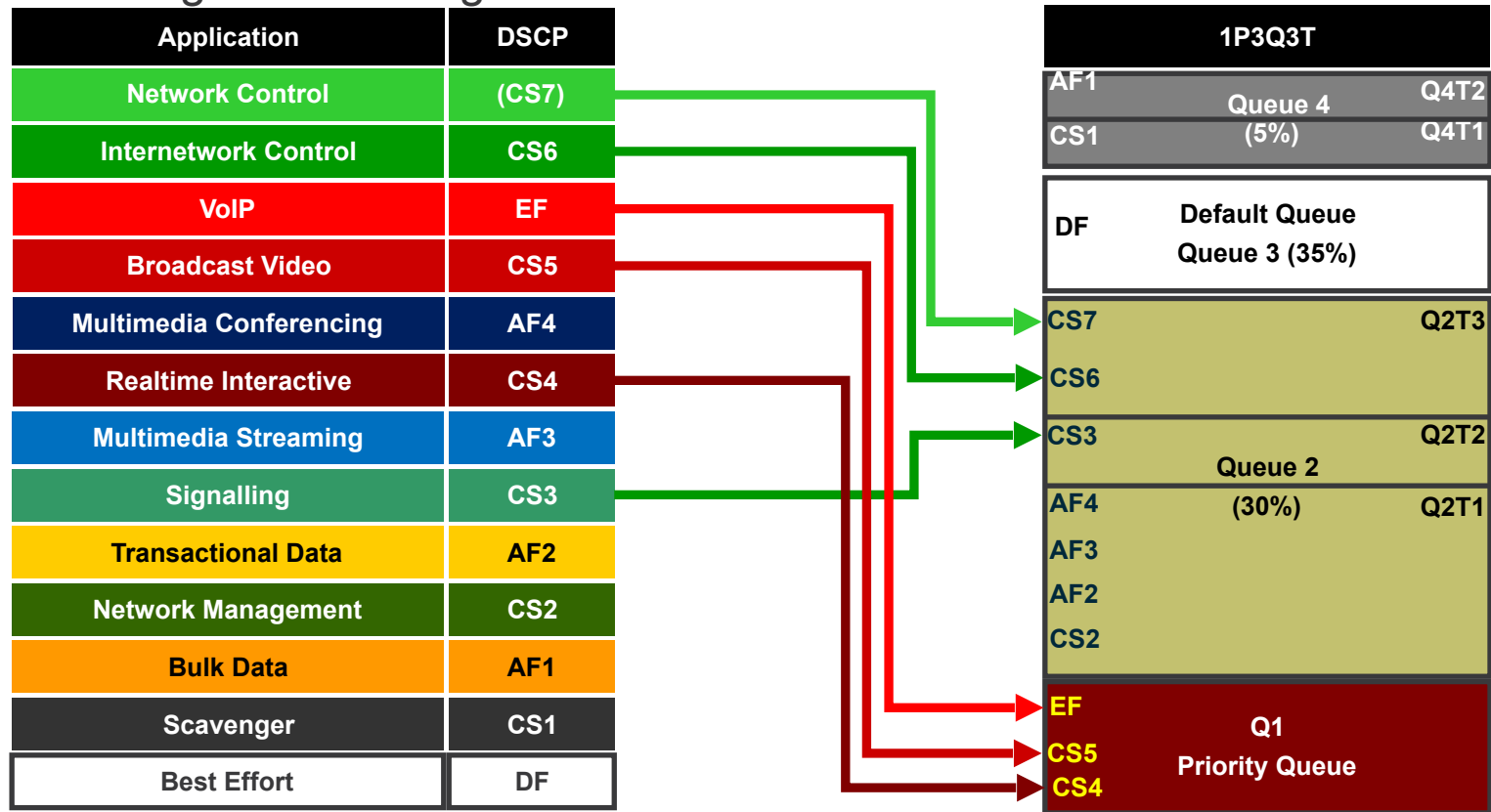
Catalyst 2960-X

1P3Q3T Egress Queuing Model



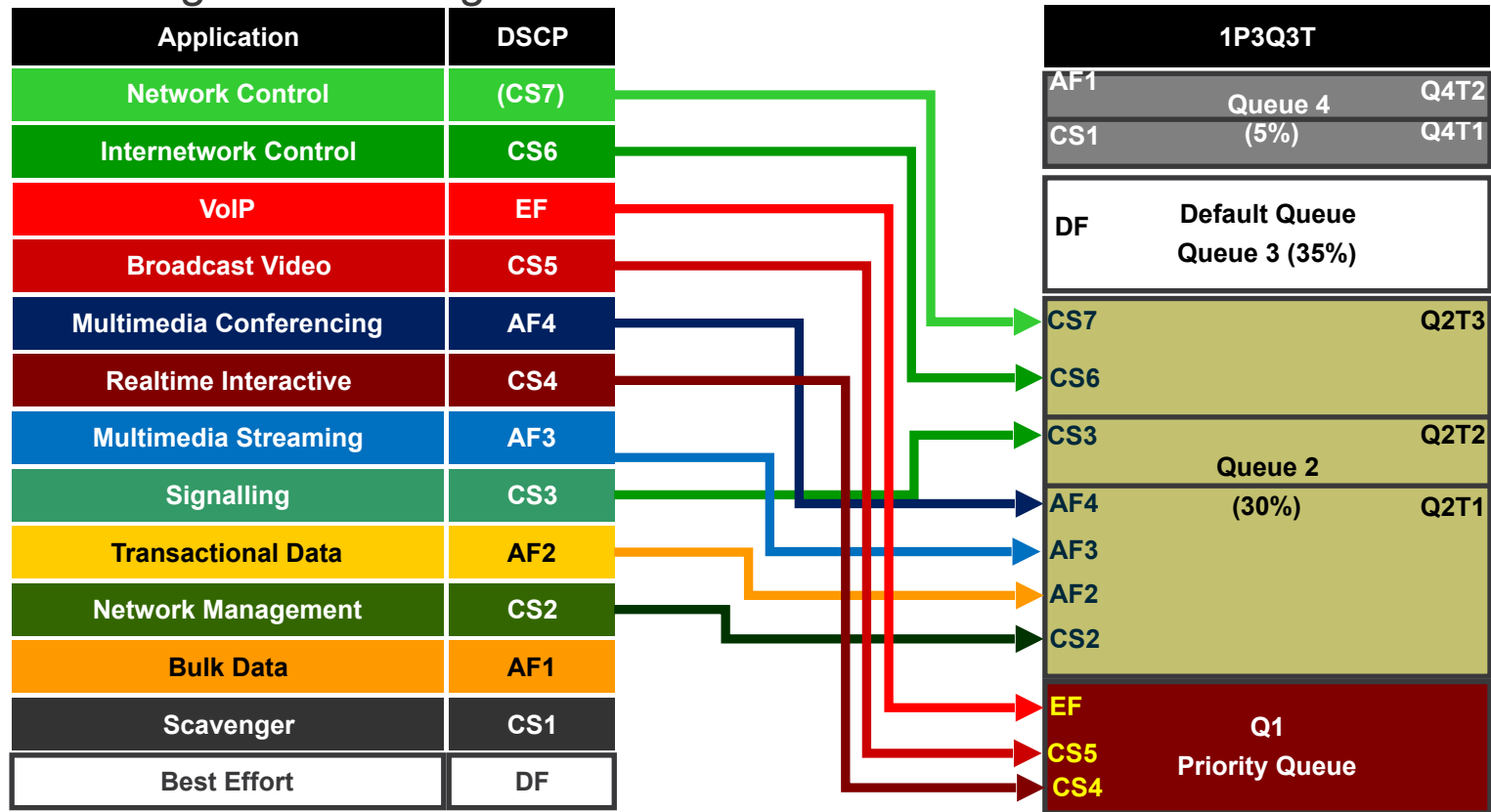
Catalyst 2960-X

1P3Q3T Egress Queuing Model



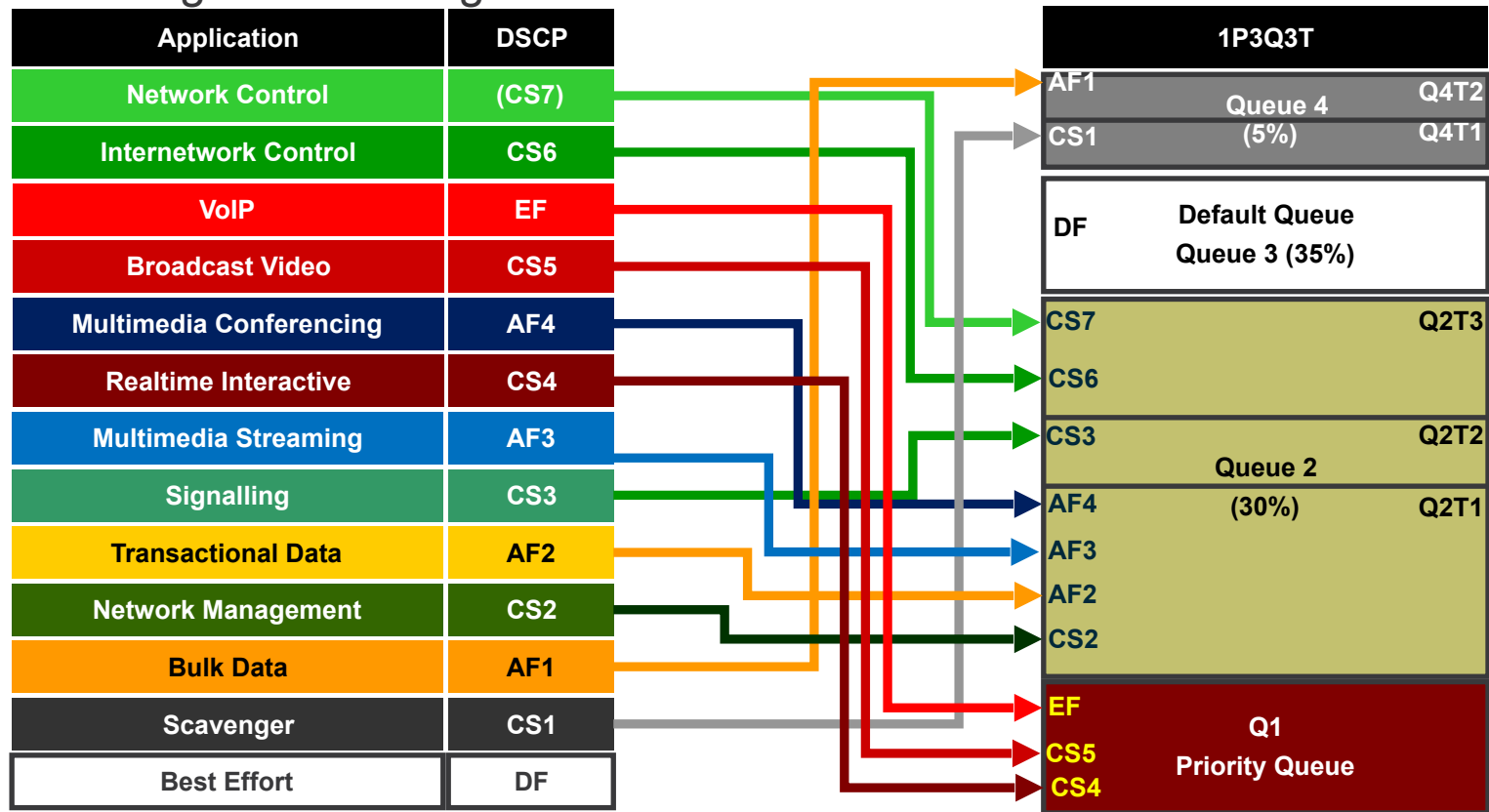
Catalyst 2960-X

1P3Q3T Egress Queuing Model



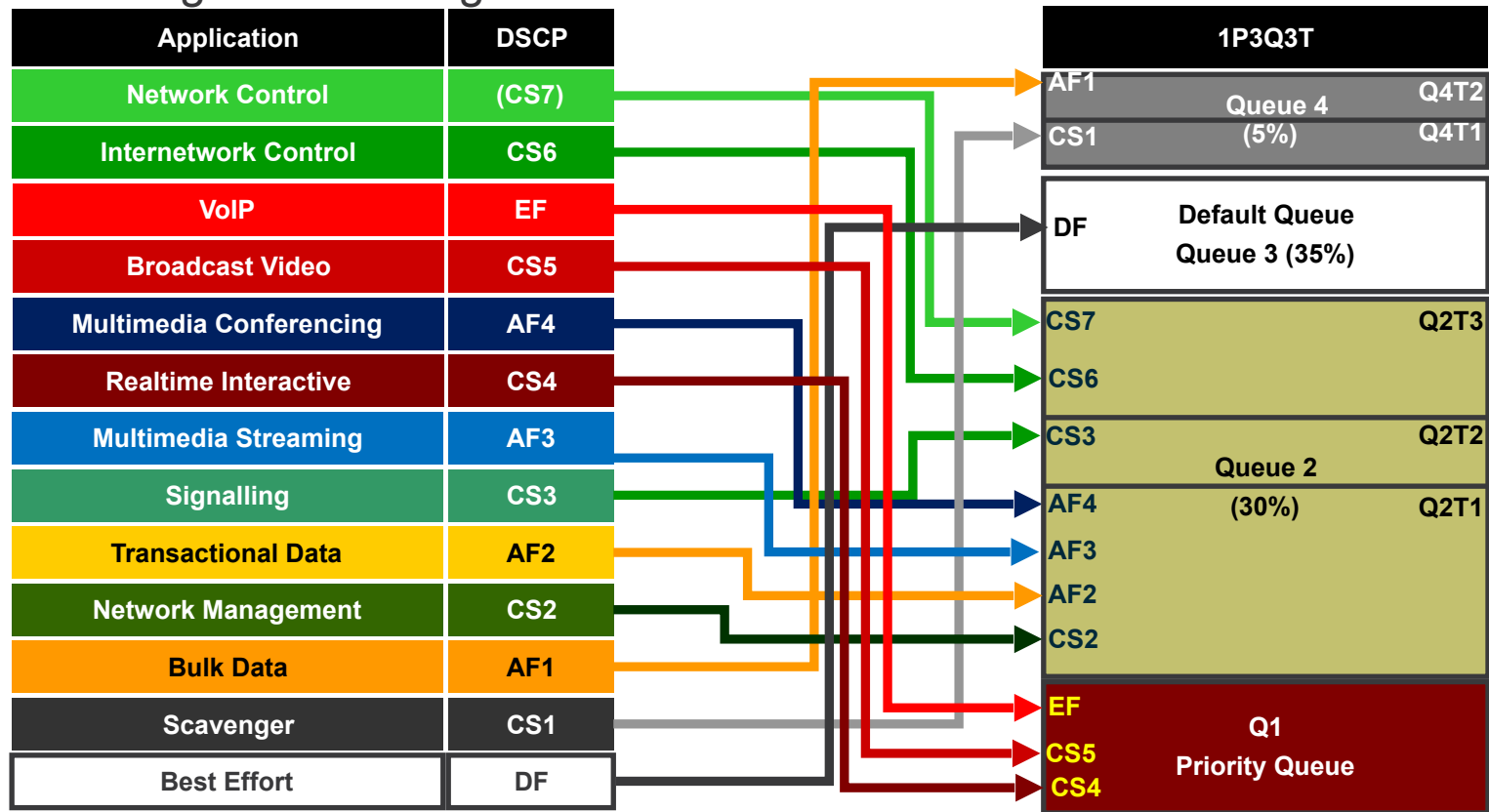
Catalyst 2960-X

1P3Q3T Egress Queuing Model



Catalyst 2960-X

1P3Q3T Egress Queuing Model



Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 1 of 2

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 1 of 2

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

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 1 of 2

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

```
! This section configures egress buffers and thresholds
```

```
mls qos queue-set output 1 buffers 15 30 35 20
```

```
mls qos queue-set output 1 threshold 1 100 100 100 100
```

```
mls qos queue-set output 1 threshold 2 80 90 100 3200
```

```
mls qos queue-set output 1 threshold 3 100 100 100 3200
```

```
mls qos queue-set output 1 threshold 4 60 100 100 3200
```

```
! This section configures egress CoS-to-Queue mappings
```

```
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
```

```
mls qos srr-queue output cos-map queue 2 threshold 1 2
```

```
mls qos srr-queue output cos-map queue 2 threshold 2 3
```

```
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
```

```
mls qos srr-queue output cos-map queue 3 threshold 3 0
```

```
mls qos srr-queue output cos-map queue 4 threshold 3 1
```

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 1 of 2

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

! This section configures egress buffers and thresholds

```
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 3200
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 100 100 3200
```

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

! This section configures egress CoS-to-Queue mappings

```
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
```

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 1 of 2

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

! This section configures egress buffers and thresholds

```
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 3200
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 100 100 3200
```

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

! This section configures egress CoS-to-Queue mappings

```
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
```

Each queue has 4 thresholds:

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

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 1 of 2

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

! This section configures egress buffers and thresholds

```
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 3200
mls qos queue-set output 1 threshold 3 100 100 100 3200
mls qos queue-set output 1 threshold 4 60 100 100 3200
```

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

! This section configures egress CoS-to-Queue mappings

```
mls qos srr-queue output cos-map queue 1 threshold 3 4 5
mls qos srr-queue output cos-map queue 2 threshold 1 2
mls qos srr-queue output cos-map queue 2 threshold 2 3
mls qos srr-queue output cos-map queue 2 threshold 3 6 7
mls qos srr-queue output cos-map queue 3 threshold 3 0
mls qos srr-queue output cos-map queue 4 threshold 3 1
```

Each queue has 4 thresholds:

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

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

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 2 of 2

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

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

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 2 of 2

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

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

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

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 2 of 2

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

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

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

Enables the PQ

Catalyst 2960-X

1P3Q3T Egress Queuing Model Config—Part 2 of 2

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

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

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

Enables the PQ

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

Catalyst 2960-X

EtherChannel QoS Design

All QoS policies are configured on the **physical port-member interfaces only**

Platform	QoS Policies Applied to the (Logical) Port-Channel Interface	QoS Policies Applied to the (Physical) Port-Member Interfaces
Catalyst 2960/3560/3750		<ul style="list-style-type: none">Classification & Marking (Ingress) and Queuing (Egress)

Catalyst 2960-X QoS Design At-A-Glance



Cisco Catalyst 2960-X QoS Design

At-A-Glance

Role in Campus Network

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

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



QoS Design Steps

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

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

Step 1: Globally Enable QoS

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

Step 2: Configure Ingress QoS Model(s)

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

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

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

Trust DSCP Model

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

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

Conditional Trust Model

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

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

Service Policy Models

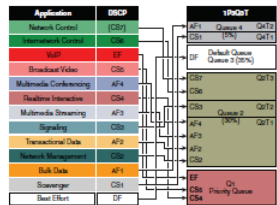
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

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

Step 3: Configure Egress Queuing

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

Figure 2 Catalyst 2960-X Egress Queuing Model



EtherChannel QoS

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

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

At-A-Glance

Cisco Validated Design

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

Step 1: Enable QoS:

```
mls qos
```

Step 2: Configure Ingress QoS Model:

Trust DSCP Model:

```
mls qos trust dscp
```

Conditional Trust Model:

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

Service Policy Models:

```
[class-maps omitted for brevity]

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

service-policy input MARKING-POLICY

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

Step 3: Configure Egress Queuing

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

queue-set 1

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

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

For more details, see Campus QoS Design 4.0:

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoS_Campus_40.html

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



Copyright © 2011 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

<https://cisco.app.box.com/v/QoS-AAGs>

Cisco live!

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



Cisco Catalyst 3560-X/3750-X QoS Design

At-A-Glance

Role in Campus Network

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

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



QoS Design Steps

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

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

Step 1: Globally Enable QoS

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

Step 2: Configure Ingress QoS Model(s)

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

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

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

Trust DSCP Model

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

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

Conditional Trust Model

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

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

Service Policy Models

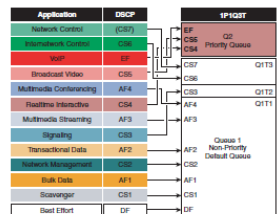
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

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

Step 3: Configure Ingress Queuing

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

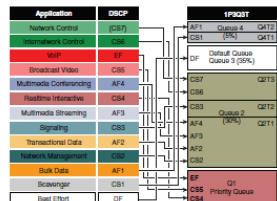
Figure 2 Catalyst 3560-X/3750-X Ingress Queuing Model



Step 4: Configure Egress Queuing

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

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



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

At-A-Glance

EtherChannel QoS

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

Cisco Validated Design

The Cisco Validated Design for Cisco Catalyst 3560-X and 3750-X series switches in the role of an access switch in a campus network is presented below.

Step 1: Enable QoS:

```
mls qos
```

Step 2: Configure Ingress QoS Model:

Trust DSCP Model:

```
mls qos trust dscp
```

Conditional Trust Model:

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

Service Policy Models:
(class-maps omitted for brevity)

policy-map MARKING-POLICY

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

service-policy input MARKING-POLICY

Step 3: Configure Ingress Queuing

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

Step 4: Configure Egress Queuing

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

queue-set 1

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

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

For more details, see Campus QoS Design 4.0.

http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoS_Campus_40.html

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

Copyright © 2011 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

<https://cisco.app.box.com/v/QoS-S-AAGs>

Cisco live!

Catalyst 6500/6800 Queuing Models

Catalyst 65xx-E / 6807-XL with Sup2T/6T

Ingress & Egress Queueing Models

- Ingress Queue Structures

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

- Ingress & Egress Queue Structures

- | | | |
|----------|-----------------------|-----------------|
| • 2P6Q4T | DSCP to Queue Mapping | DSCP-based WRED |
|----------|-----------------------|-----------------|

- Egress Queue Structures

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

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

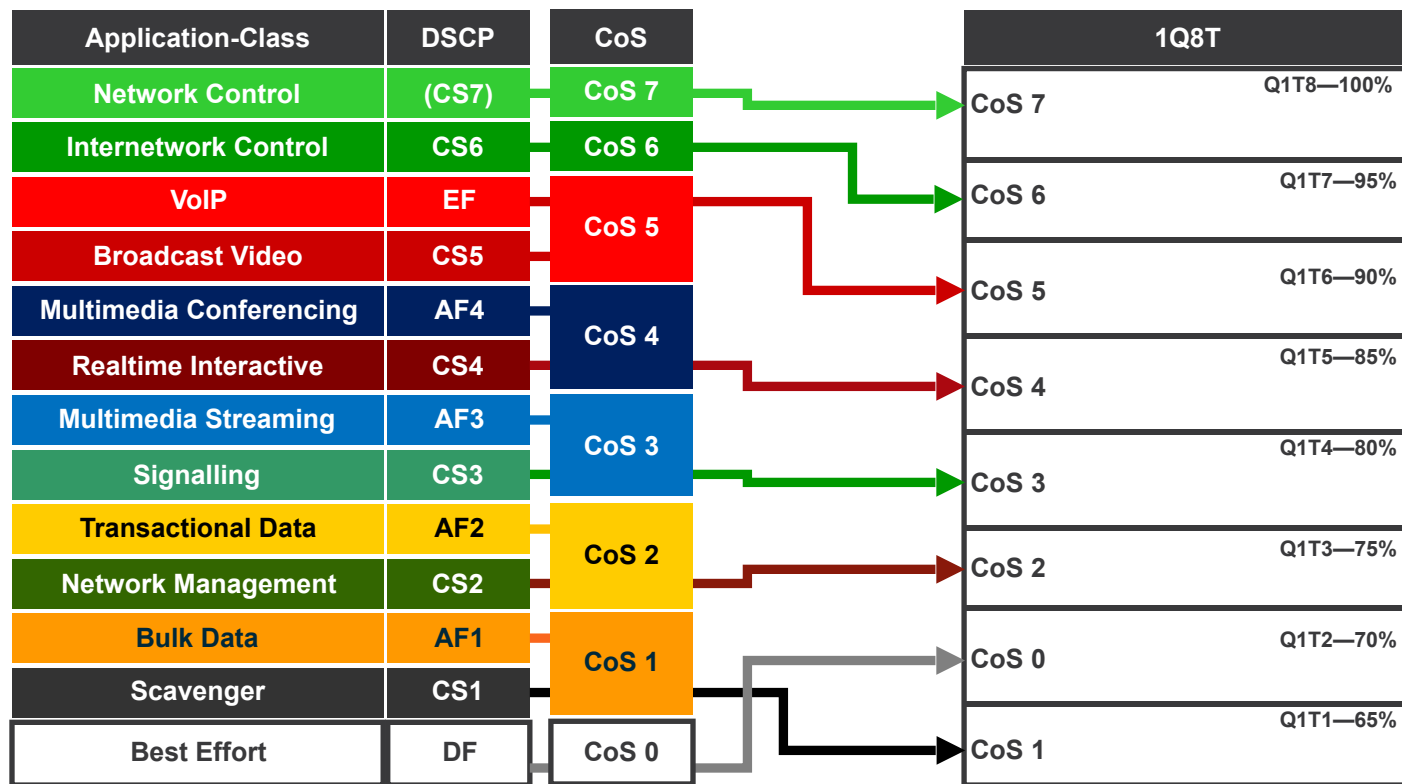
1Q8T – Ingress Queueing CoS to Queue Mapping CoS-based Tail-Drop

1Q8T Ingress Queueing Linecards

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

Catalyst 65xx-E/6807-XL with Sup2T/6T

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



All noted thresholds are tail-drop thresholds

Catalyst 65xx-E/6807-XL—1Q8T Ingress Model

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

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

Recommend to explicitly configure it.

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

2Q4T – Ingress Queueing

CoS to Queue Mapping

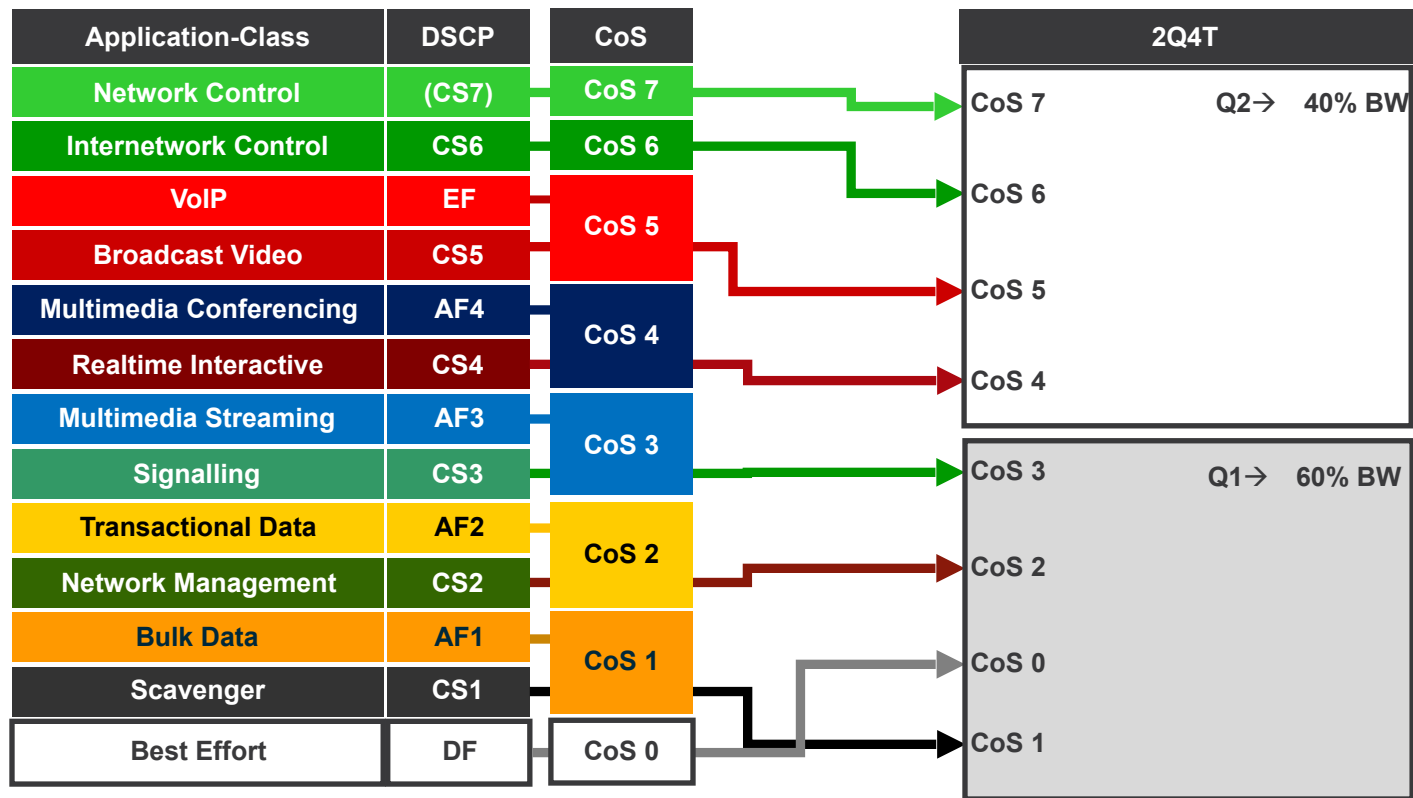
CoS-based Tail-Drop

2Q4T Ingress Queueing Linecards

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

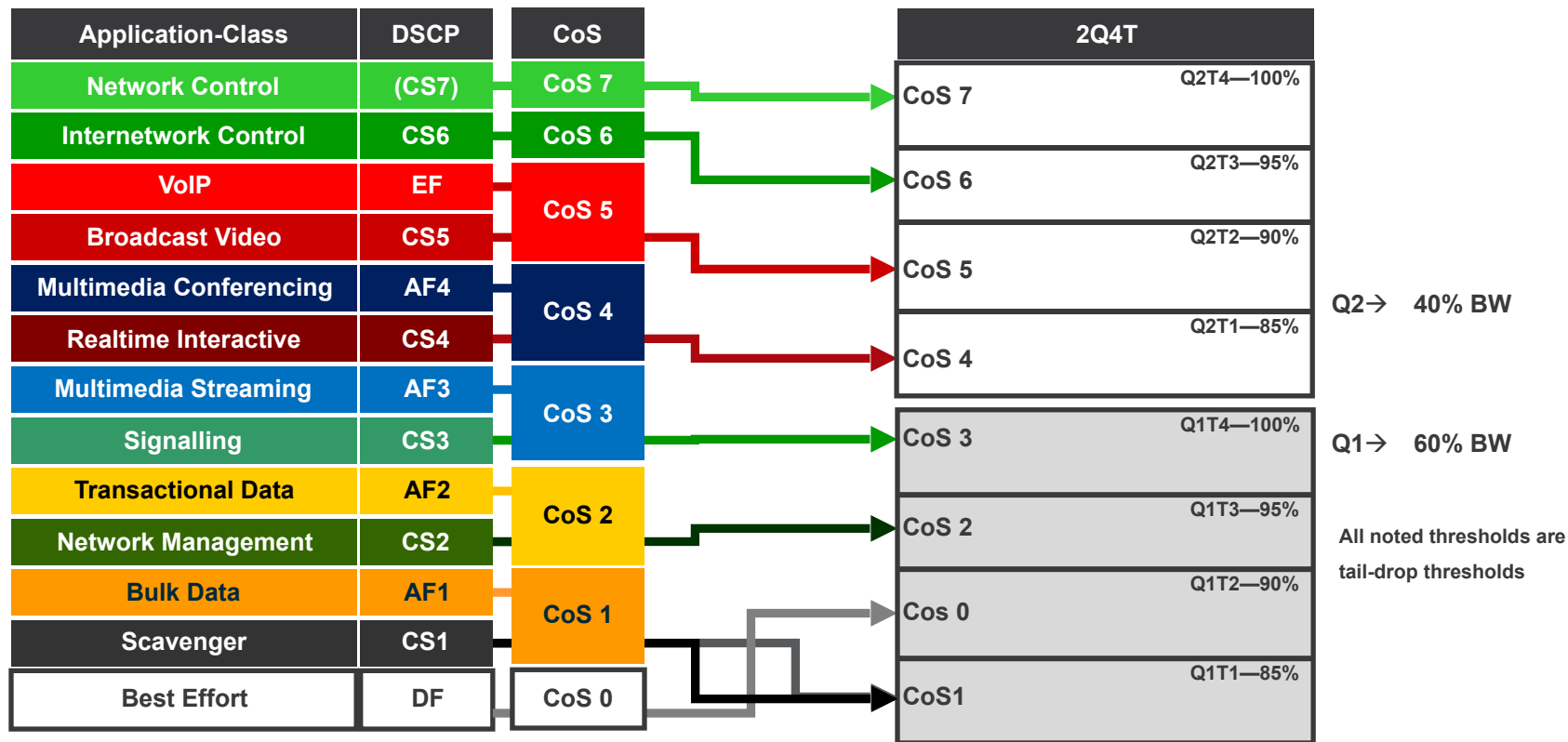
Catalyst 65xx-E/6807-XL with Sup2T

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



Catalyst 65xx-E/6807-XL with Sup2T

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



Catalyst 65xx-E/6807-XL—2Q4T Ingress Model

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

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

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

Recommend explicitly configuring thresholds however.

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

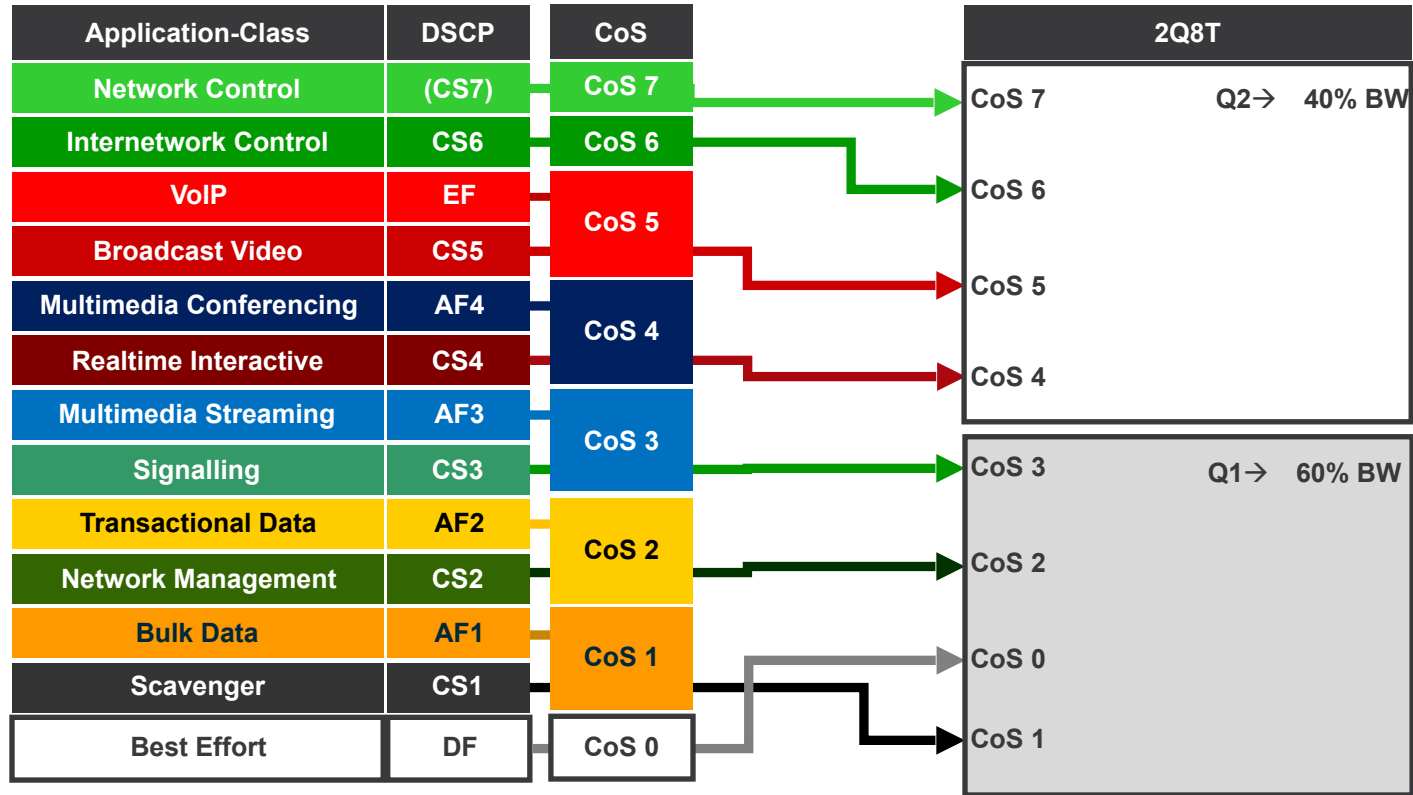
2Q8T – Ingress Queueing CoS to Queue Mapping CoS-based Tail-Drop

2Q8T Ingress Queueing Linecards

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

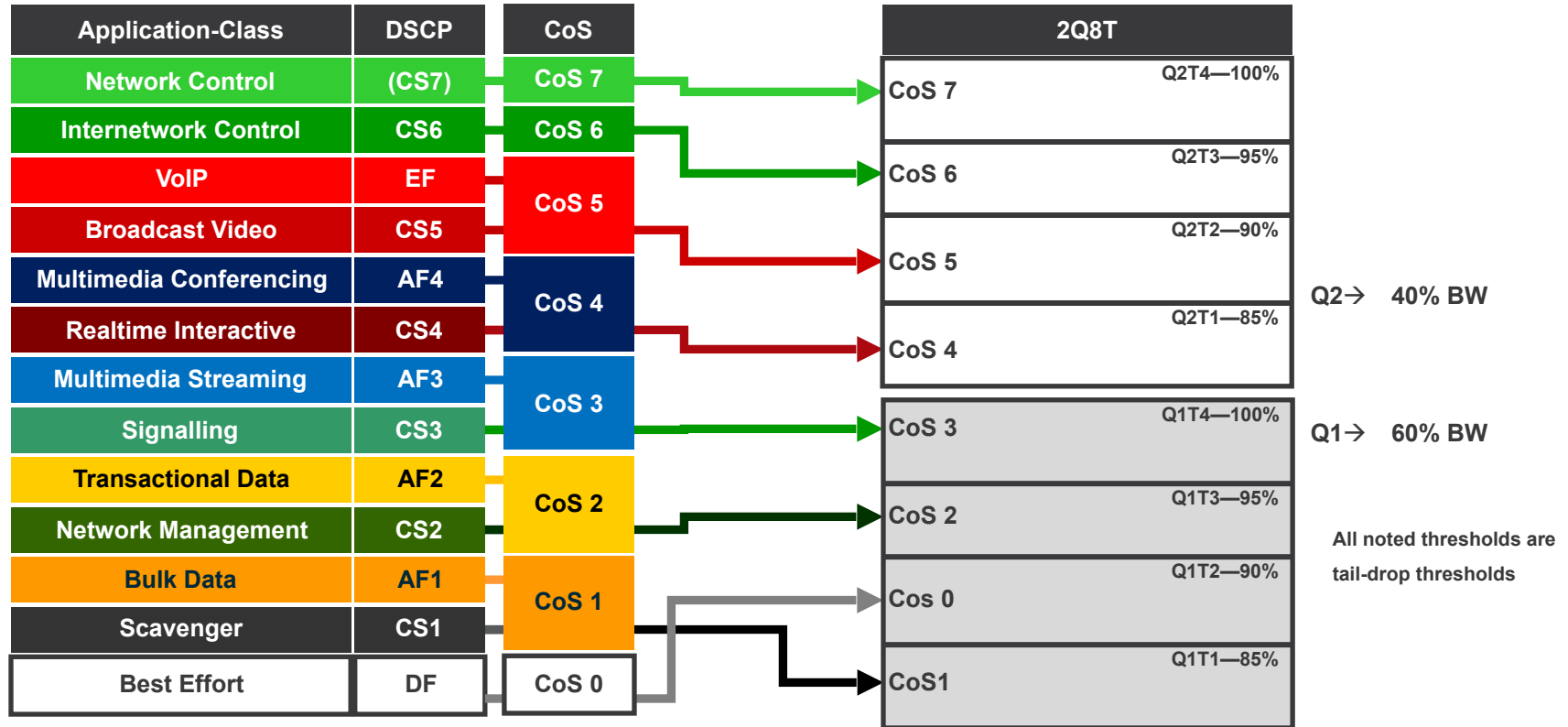
Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Catalyst 65xx-E/6807-XL—2Q8T Ingress Model

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

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

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

Recommend explicitly configuring thresholds

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

8Q4T – Ingress Queueing

DSCP to Queue Mapping

DSCP-based WRED

8Q4T Ingress Queueing Linecards

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

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

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

Global command disables GigabitEthernet interfaces on the Sup2T.

```
o23-6500-1#show platform qos module 3
```

```
QoS is enabled globally
Port QoS is enabled globally
QoS serial policing mode enabled globally
Distributed Policing is Disabled
Secondary PUPs are enabled
QoS Trust state is DSCP on the following interface:
```

Global command to show whether the GigabitEthernet interfaces on the Sup2T are enabled or disabled

```
E00/2 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 Vll
```

```
QoS 10g-only mode supported: Yes [Current mode: Off]
```

```
Global Policy-map: ingress[]
```

GigabitEthernet interfaces on the Sup2T are currently enabled

How to Enable or Display Performance Mode on Linecards

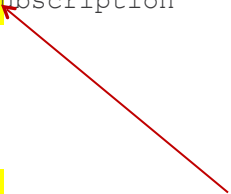
```
o23-6500-1(config)#no hw-module slot 5 oversubscription port-group 4
```

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



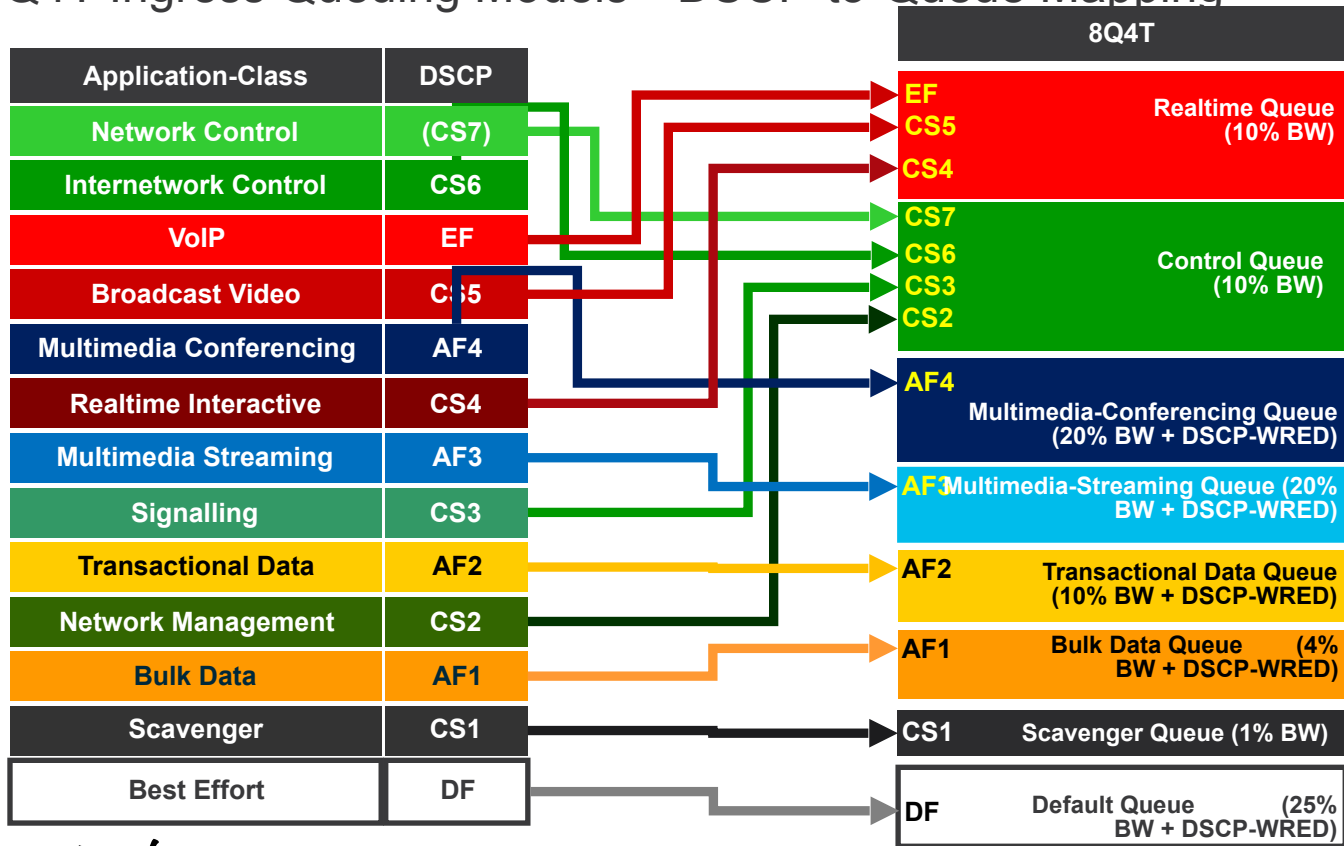
```
o23-6500-1#show hw-module slot 5 oversubscription
port-group      oversubscription-mode
1               enabled
2               enabled
3               enabled
4               disabled
```

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



Cisco Catalyst 65xx-E/6807-XL with Sup2T

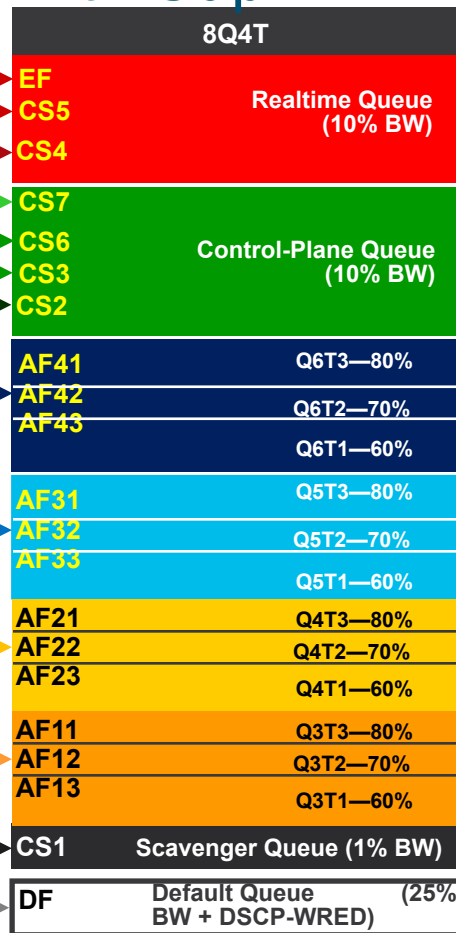
8Q4T Ingress Queuing Models—DSCP-to-Queue Mapping



Cisco Catalyst 65xx-E/6807-XL with Sup2T

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

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



All noted thresholds are
Min WRED thresholds

All max WRED thresholds
Are set to 100%

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

Multimedia-Streaming Queue (20%
BW + DSCP-WRED)

Transactional Data Queue
(10% BW + DSCP-WRED)

Bulk Data Queue (4%
BW + DSCP-WRED)

Catalyst 65xx-E/6807-XL —8Q4T Ingress Model

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

Catalyst 65xx-E/6807-XL —8Q4T Ingress Model

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

Catalyst 65xx-E/6807-XL —8Q4T Ingress Model

[continued]

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

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


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

8Q8T Ingress Queueing Linecards

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

```
o23-6500-1#show module
```

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

...

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

8Q8T Ingress Queueing Linecards

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

```
o23-6500-1#show module
```

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

...

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

8Q8T Ingress Queueing Linecards

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

```
o23-6500-1#show module
```

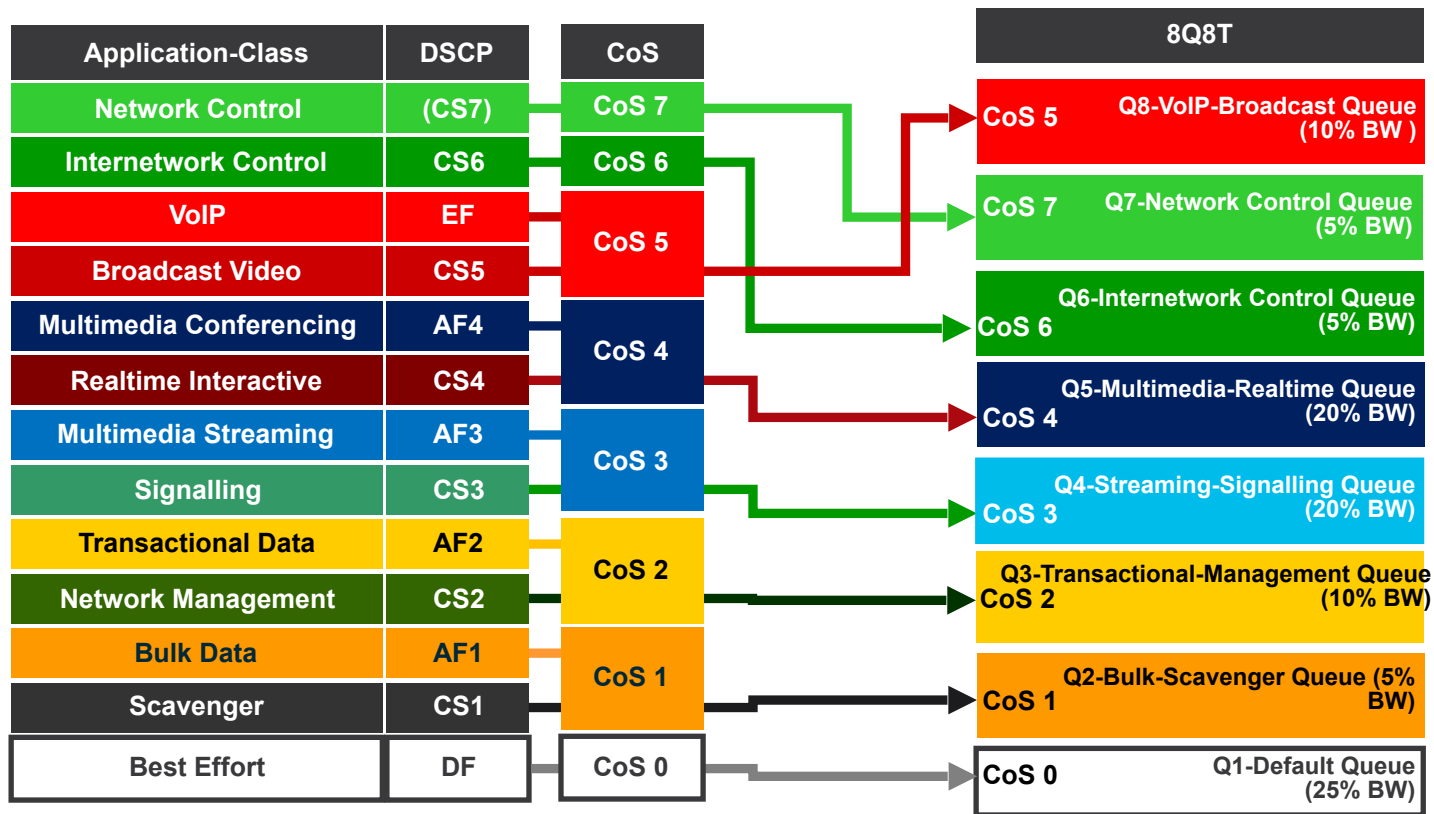
Mod	Ports	Card Type	Model	Serial No.
1	48	CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	SAL10478SWP
2	8	DCEF2T 8 port 10GE	WS-X6908-10G	SAL172682AK
3	5	Supervisor Engine 2T 10GE w/ CTS (Acti	VS-SUP2T-10G	SAL1702WNR0
5	16	CEF720 16 port 10GE	WS-X6716-10GE	SAL1228WYB7
6	4	CEF720 4 port 10-Gigabit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

...

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

Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Catalyst 65xx-E/6807-XL —8Q8T Ingress Model

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

Catalyst 65xx-E/6807-XL —8Q8T Ingress Model

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

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

1P7Q2T – Ingress Queueing

DSCP to Queue Mapping

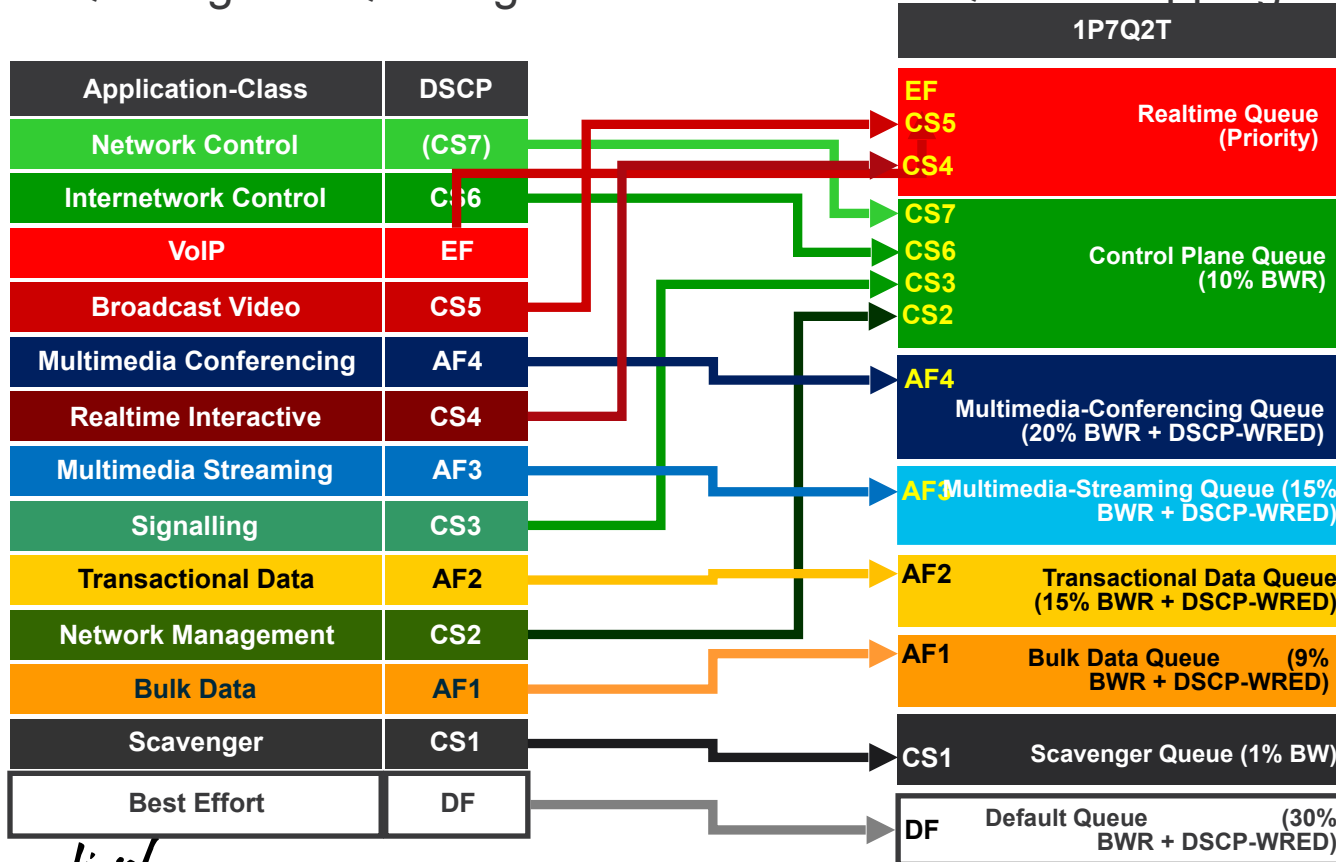
DSCP-based WRED

1P7Q2T Ingress Queueing Linecards

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

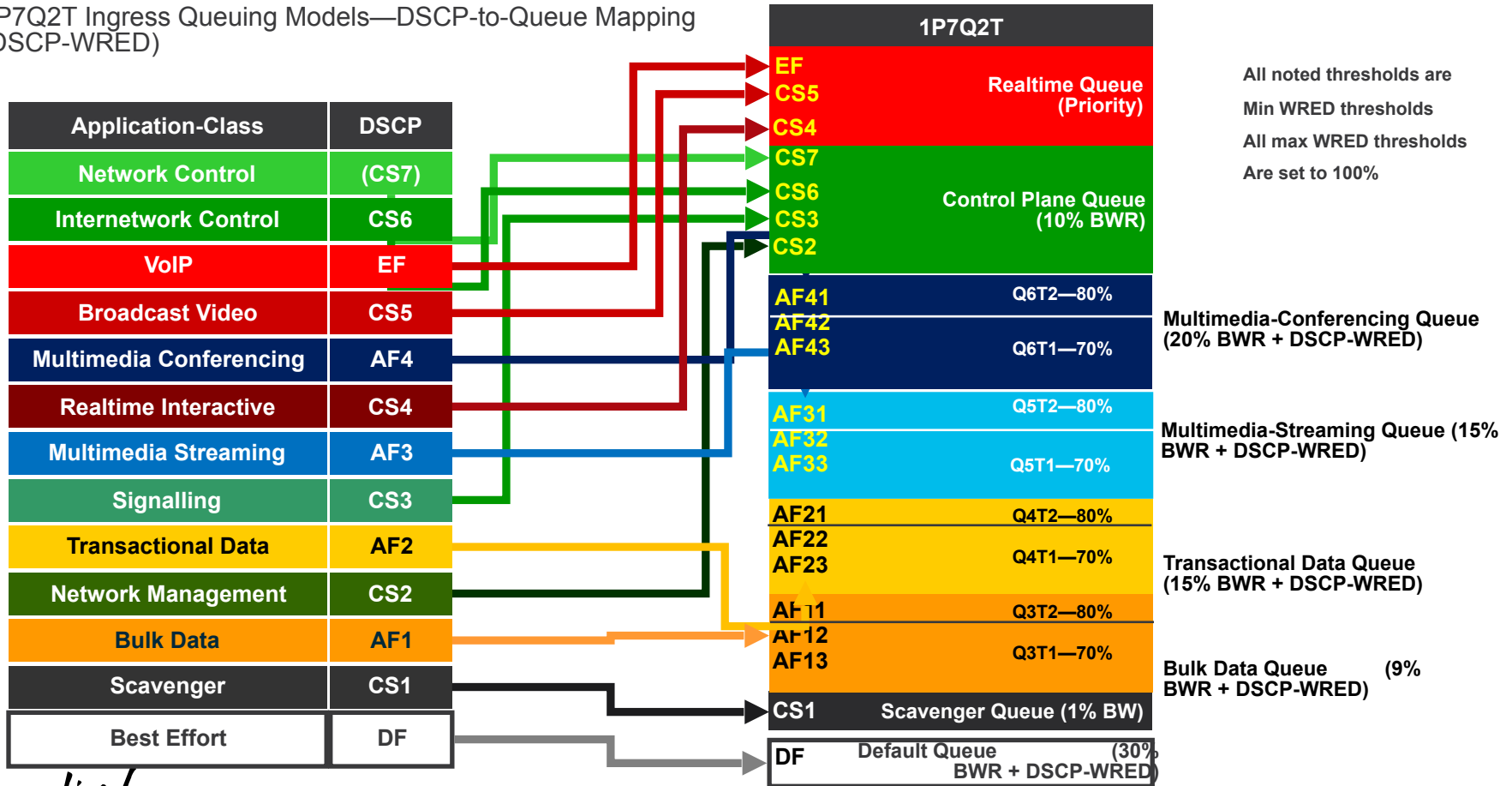
Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL - 1P7Q2T Ingress Model

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

Catalyst 65xx-E/6807-XL —1P7Q2T Ingress Model

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

Catalyst 65xx-E/6807-XL - 1P7Q2T Ingress Model

[continued]

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

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

2P6Q4T Ingress & Egress Queueing

DSCP to Queue Mapping

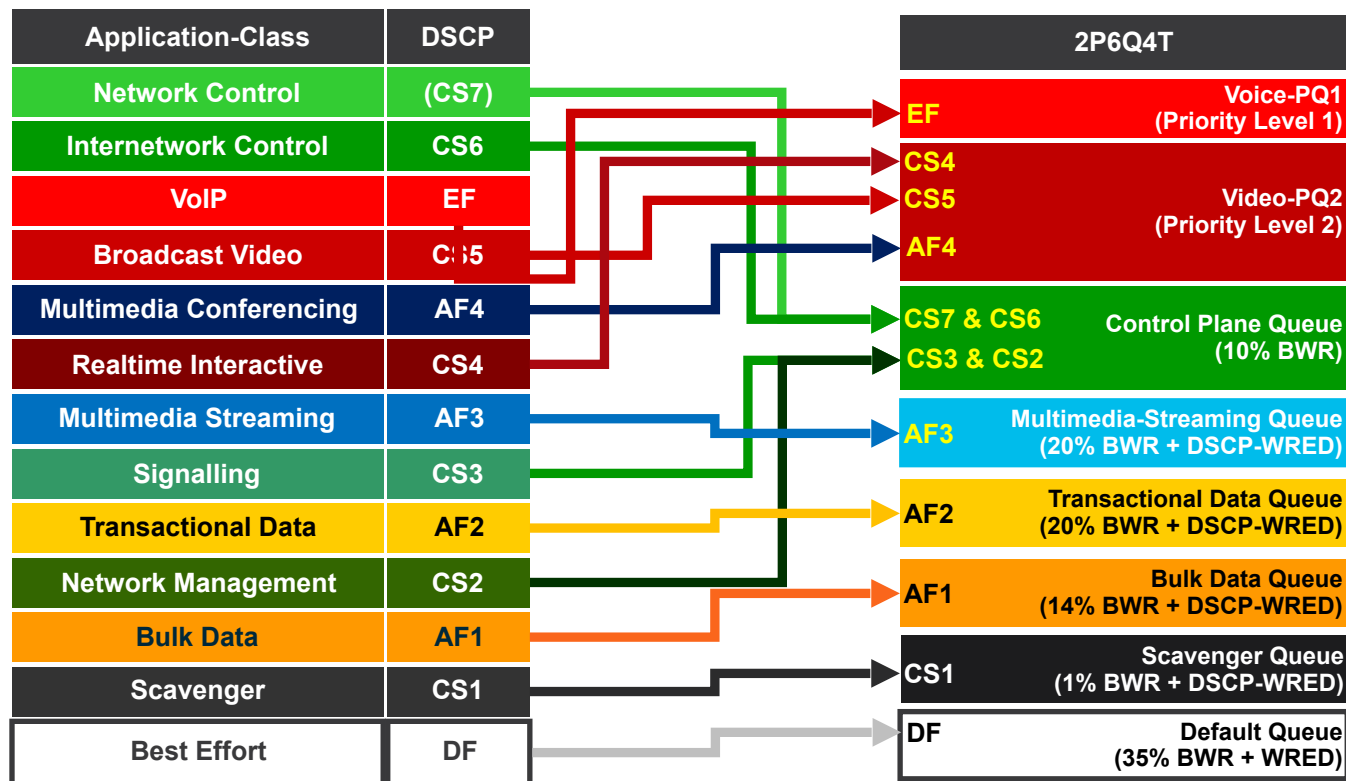
DSCP-based WRED

2P6Q4T Ingress Queueing Linecards

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

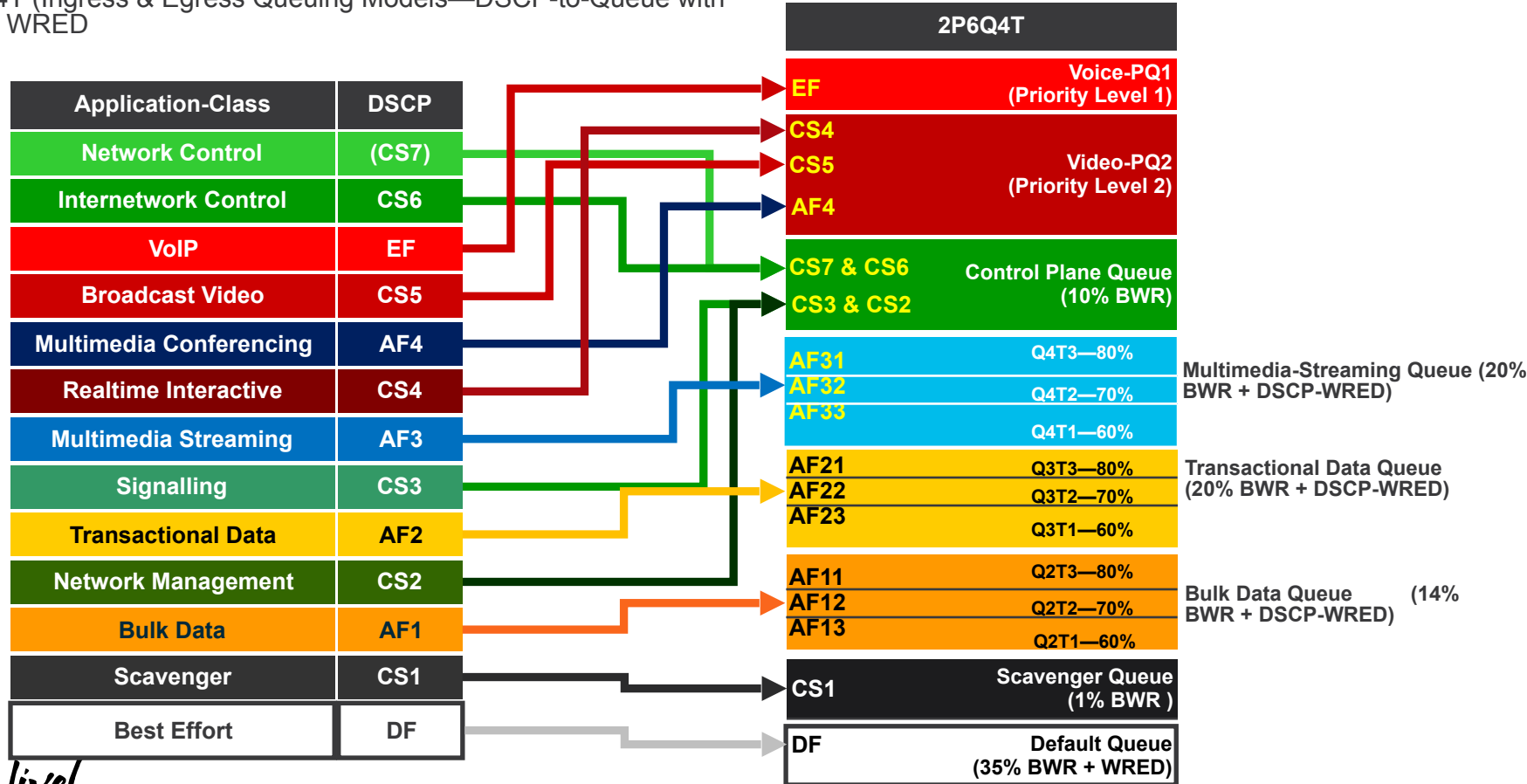
Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL—2P6Q4T Model

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

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

Cisco Catalyst 65xx-E/6807-XL—2P6Q4T Model

Part 2 of 3—2P6Q4T Queuing Policy-Map

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

Cisco Catalyst 65xx-E/6807-XL—2P6Q4T Model

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

[continued]

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

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

1P3Q8T – Egress Queueing

CoS to Queue Mapping

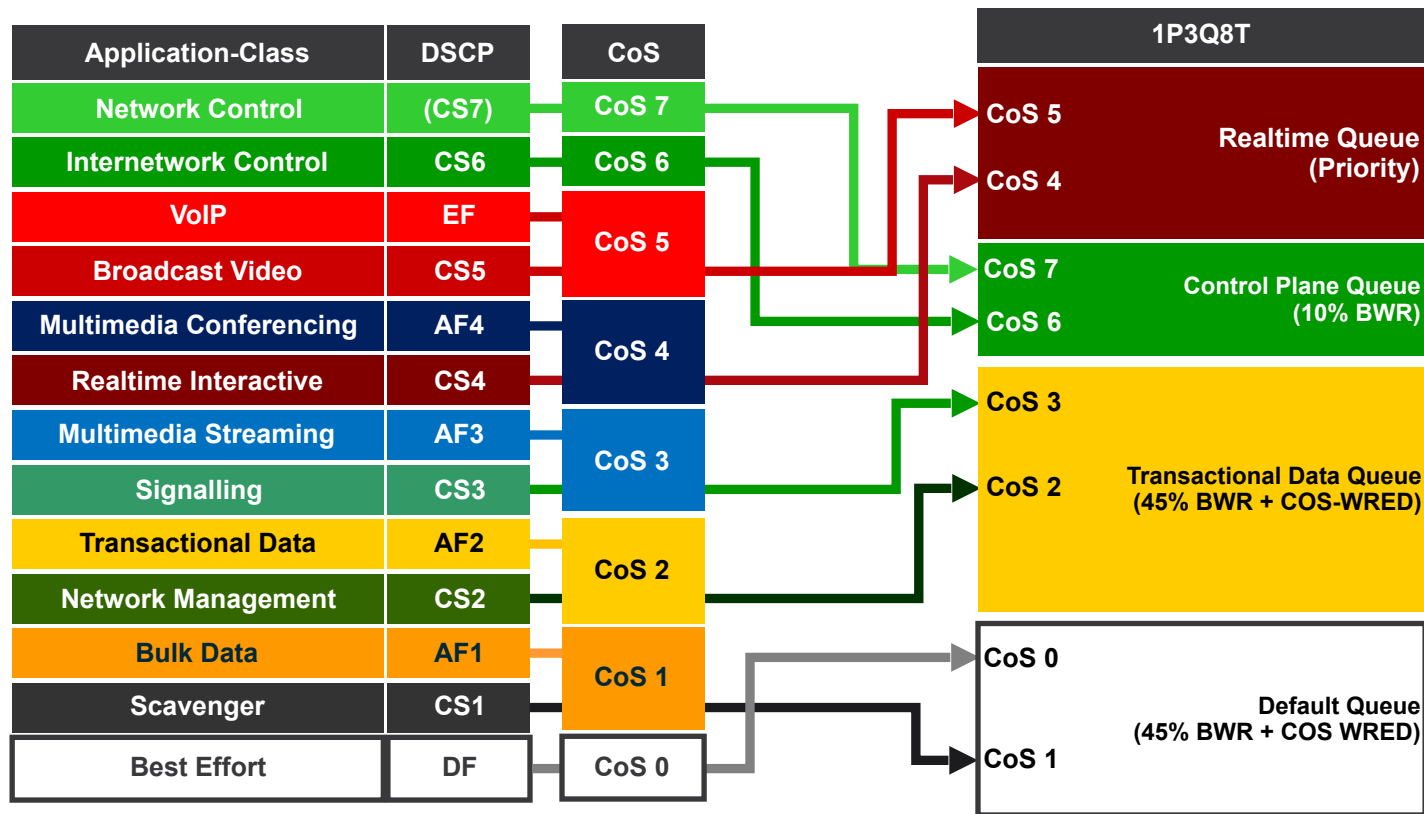
CoS-based Tail-Drop

1P3Q8T Egress Queueing Linecards

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

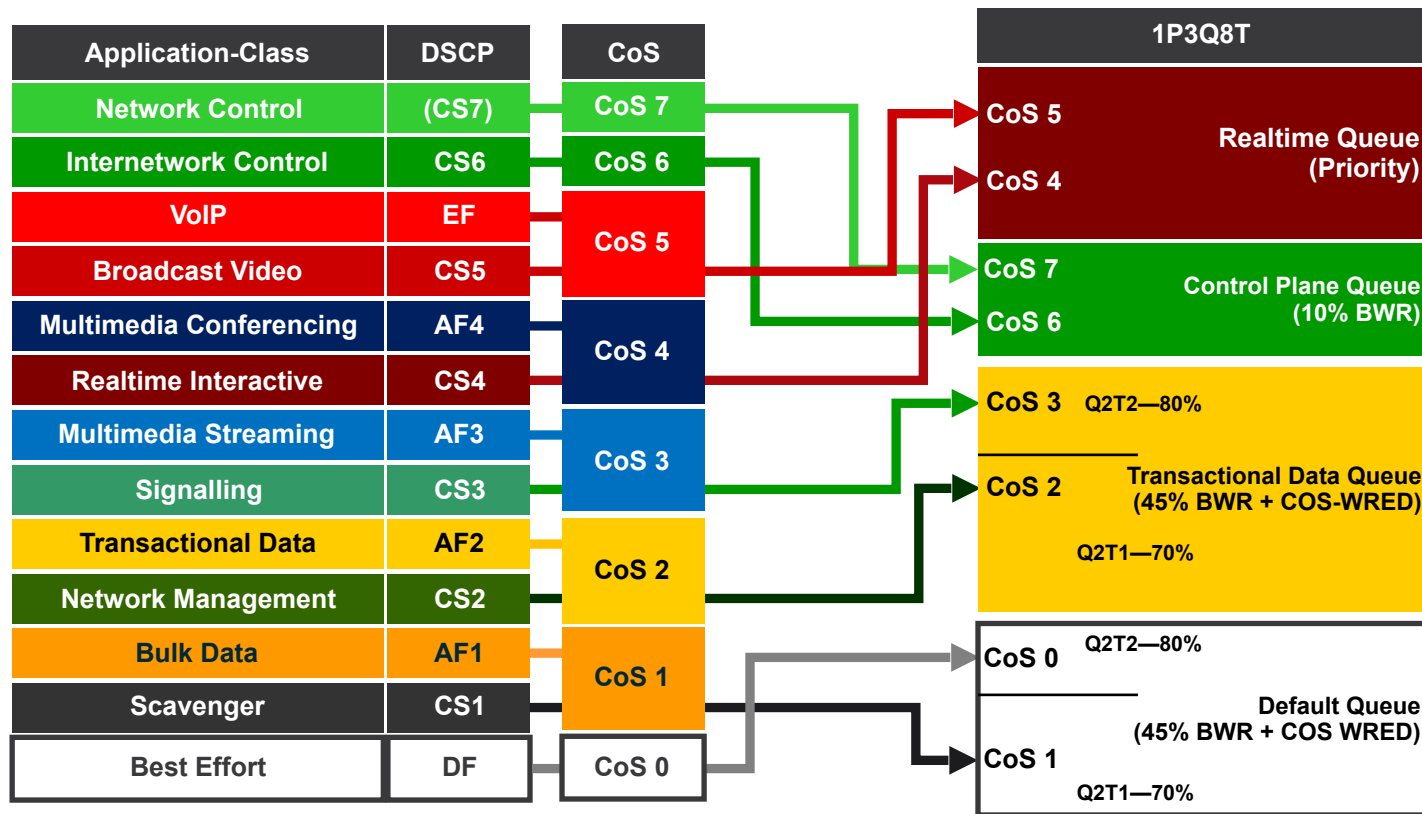
Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



All noted thresholds are
Min WRED thresholds

All max WRED thresholds
Are set to 100%

Catalyst 65xx-E/6807-XL—1P3Q8T Egress Model

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

Cisco Catalyst 65xx-E/6807-XL —1P3Q8T Egress Model

```
policy-map type lan-queuing APIC_EM-QUEUING-1P3Q8T-OUT
```

```
class APIC_EM-REALTIME-1P3Q8T-QUEUE
```

```
priority
```

```
class APIC_EM-CONTROL-1P3Q8T-QUEUE
```

```
bandwidth remaining percent 5
```

```
class APIC_EM-TRANS_DATA-1P3Q8T-QUEUE
```

```
bandwidth remaining percent 45
```

```
random-detect cos-based
```

```
random-detect cos 3 percent 80 100
```

```
random-detect cos 2 percent 70 100
```

```
class class-default
```

```
random-detect cos-based
```

```
random-detect cos 0 percent 80 100
```

```
random-detect cos 1 percent 70 100
```

```
interface GigabitEthernet1/3/2
```

```
service-policy type lan-queuing output APIC_EM-QUEUING-1P3Q8T-OUT
```

1P3Q4T – Egress Queueing

CoS to Queue Mapping

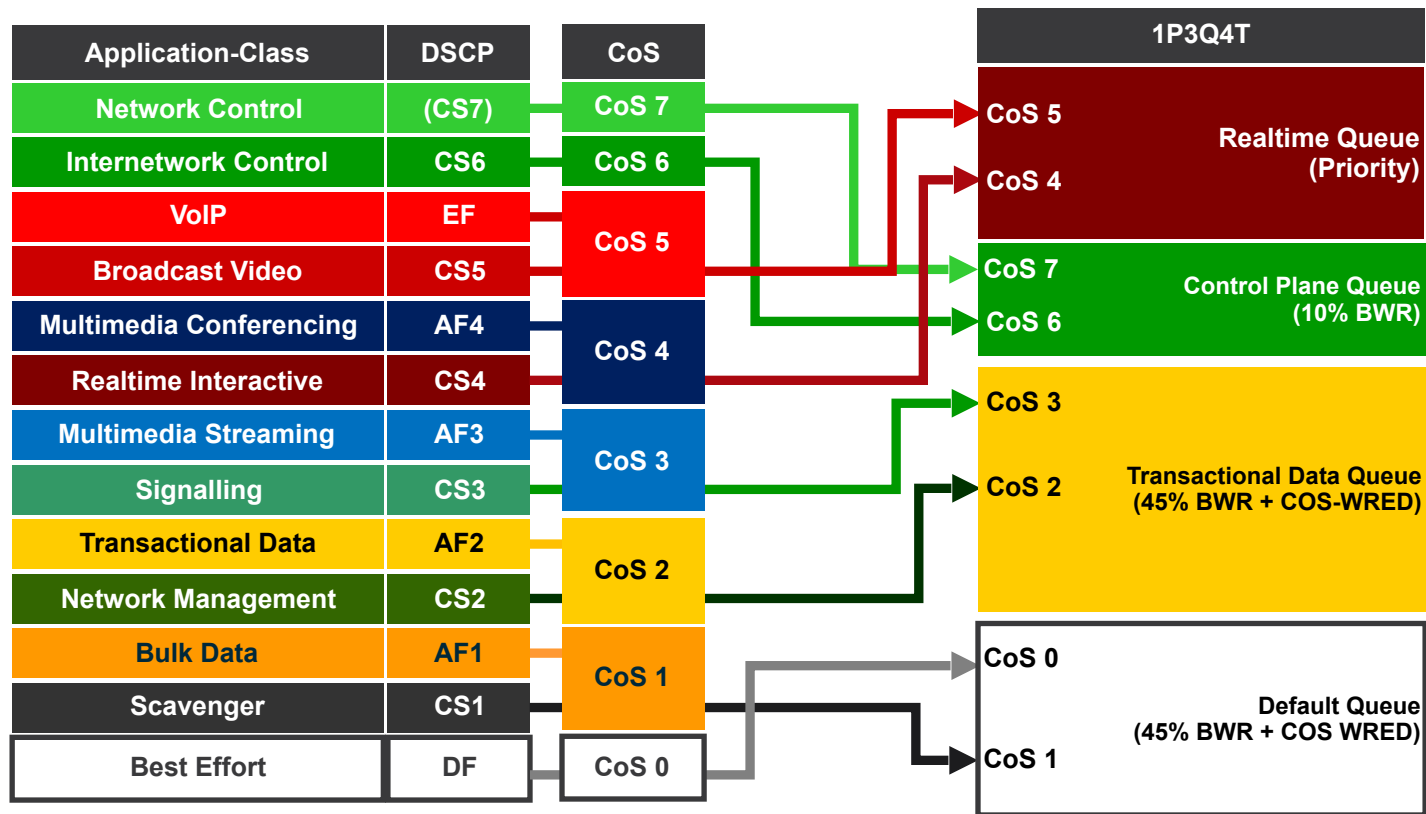
CoS-based Tail-Drop

1P3Q4T Egress Queueing Linecards

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

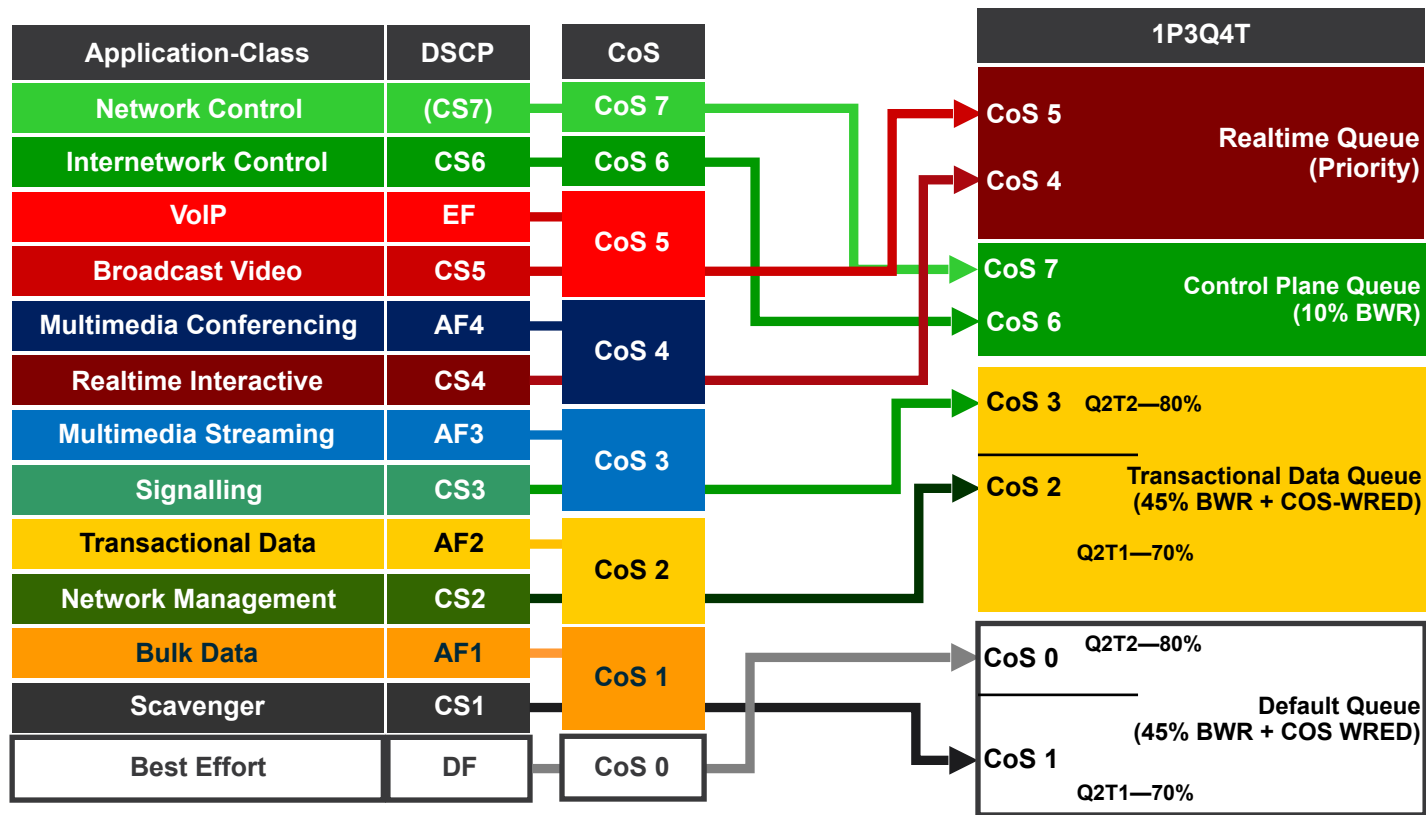
Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



All noted thresholds are
Min WRED thresholds

All max WRED thresholds
Are set to 100%

Catalyst 65xx-E/6807-XL —1P3Q4T Egress Model

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


Catalyst 65xx-E/6807-XL —1P3Q4T Egress Model

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

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

1P7Q4T –Egress Queueing

DSCP to Queue Mapping

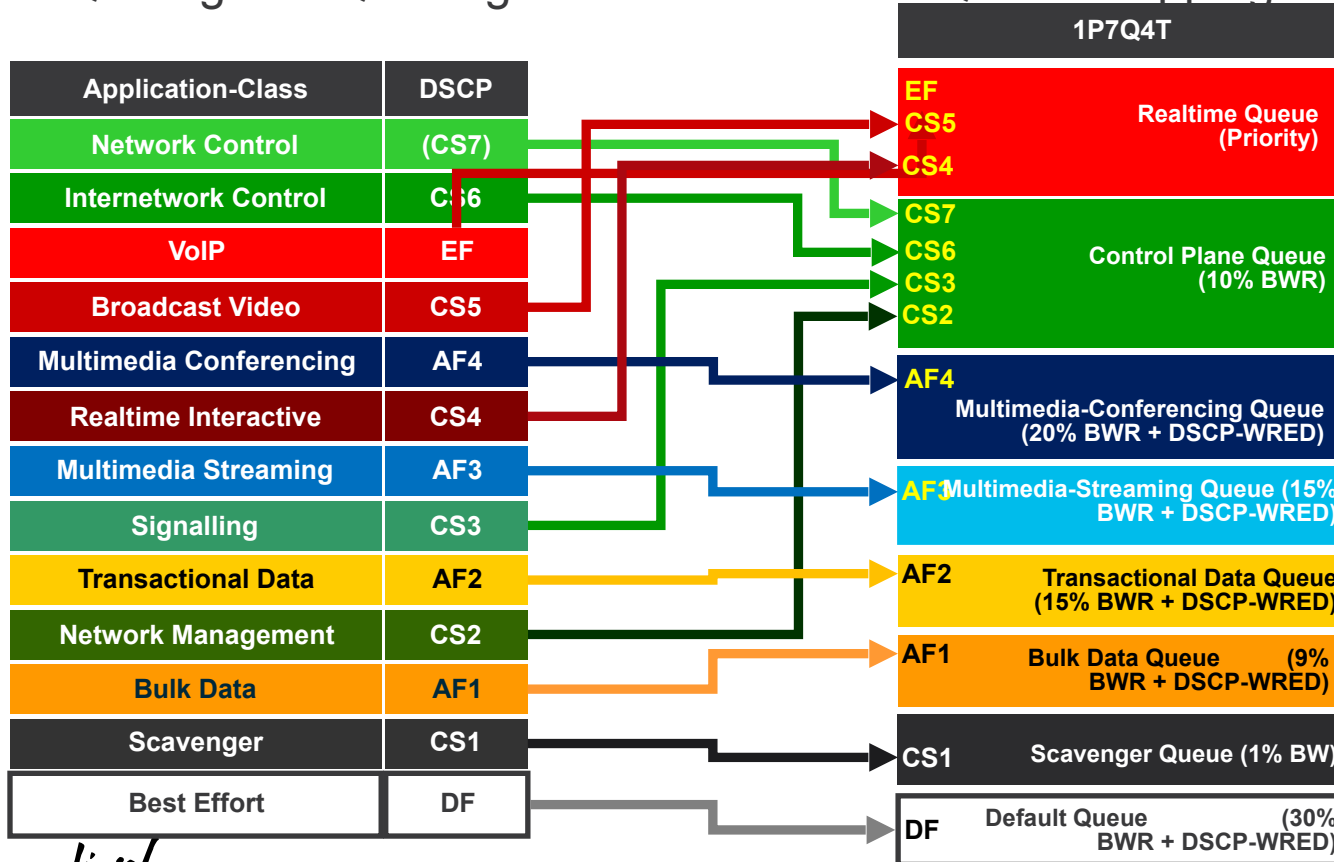
DSCP-based WRED

1P7Q4T Egress Queueing Linecards

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

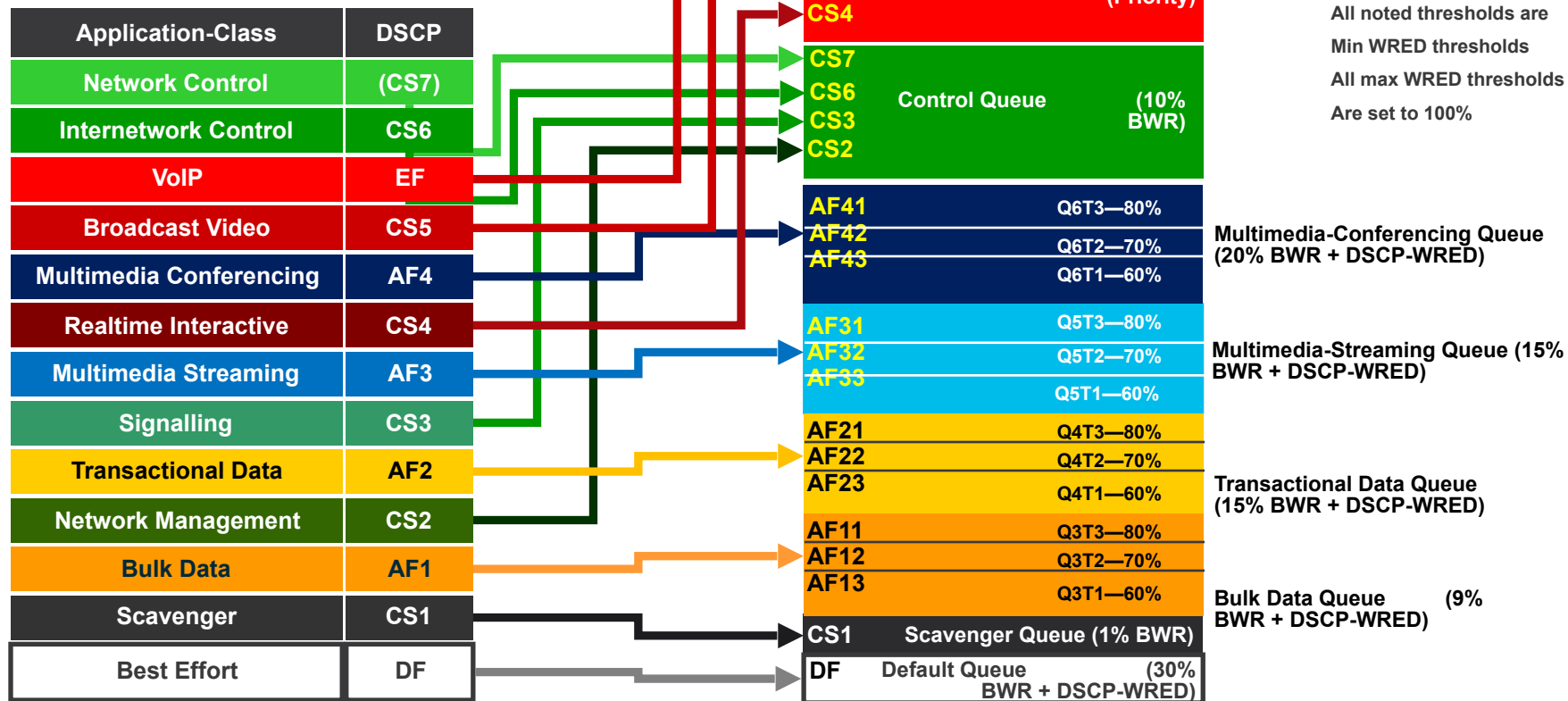
Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



All noted thresholds are
Min WRED thresholds
All max WRED thresholds
Are set to 100%

Catalyst 65xx-E/6807-XL —1P7Q4T Egress Model

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

Cisco Catalyst 65xx-E/6807-XL —1P7Q4T Egress Model

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

Cisco Catalyst 65xx-E/6807-XL —1P7Q4T Egress Model

[continued]

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

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


1P7Q8T – Egress Queueing

CoS to Queue Mapping

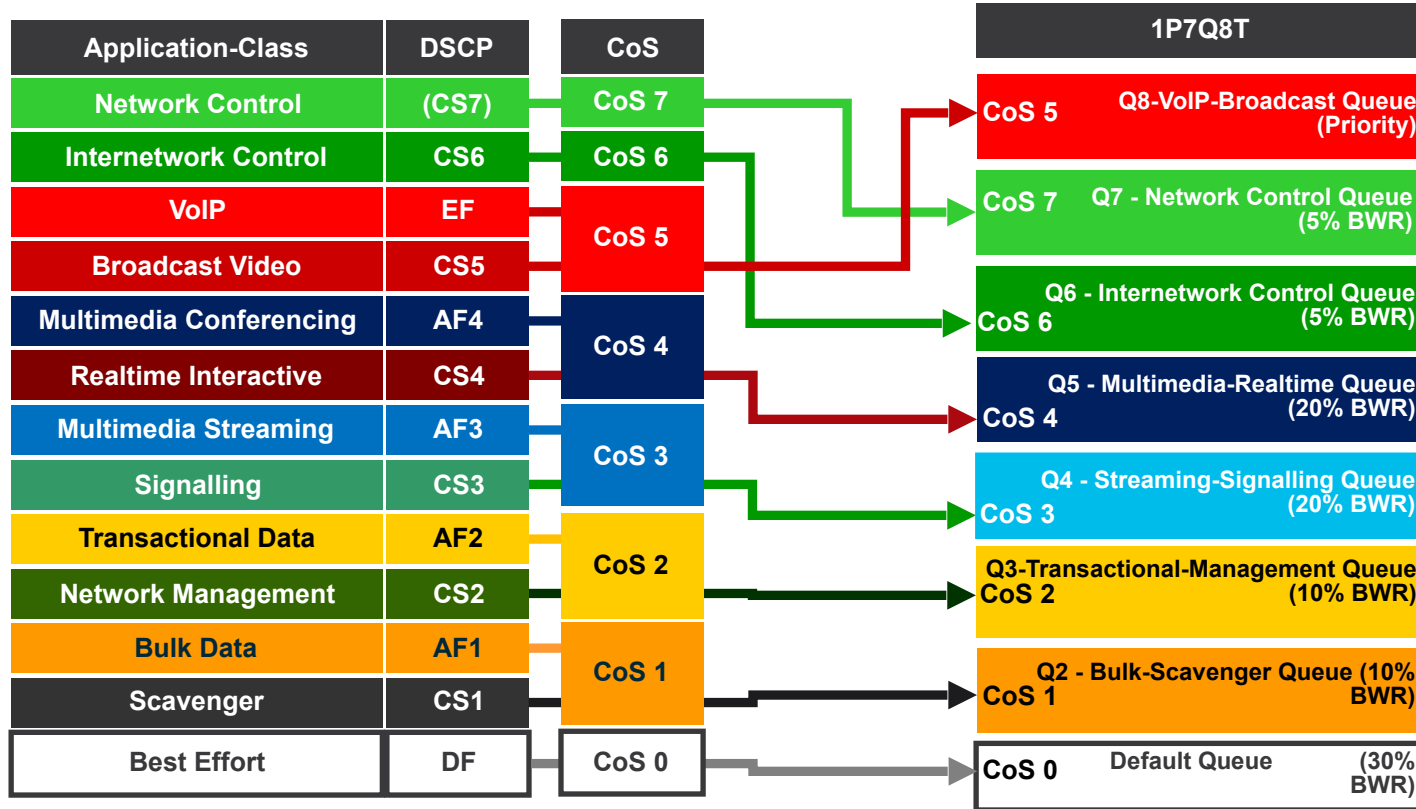
CoS-based Tail-Drop

1P7Q8T Egress Queueing Linecards

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

Cisco Catalyst 65xx-E/6807-XL with Sup2T

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



Catalyst 65xx-E/6807-XL —1P7Q8T Egress Model

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

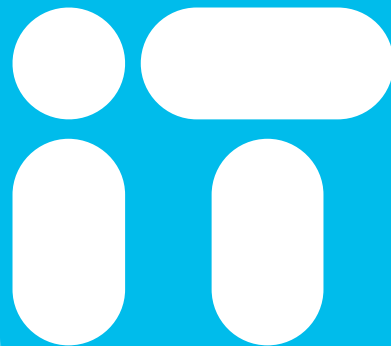
Catalyst 65xx-E/6807-XL —1P7Q8T Egress Model

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

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



You're



Cisco *live!*