QoS и Multicast в классической LAN сети

Юрий Дышлевой

Системный инженер, CCIE

25.03.2021

Agenda

- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

Agenda

- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

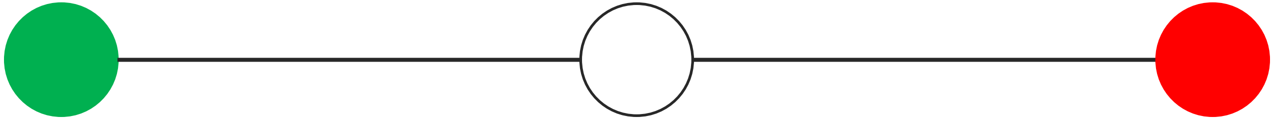
Where to Begin?

Where to Begin?

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

Determining Business Relevance

How Important is an Application to Your Business?



Relevant

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

RFC 4594

Default

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

RFC 2474

Irrelevant

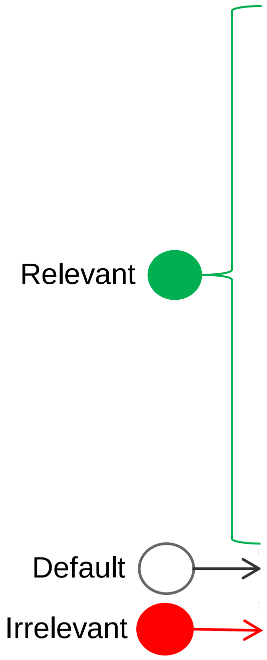
- These applications do not support business objectives and are typically consumer-oriented
- Applications of this type should be treated with a “less-than Best Effort” service

RFC 3662

Translating Business-Relevance to QoS Policies

Apply RFC 4594-based Marking / Queuing / Dropping

Application Class	Per-Hop Behavior	Queuing & Dropping	Application Examples



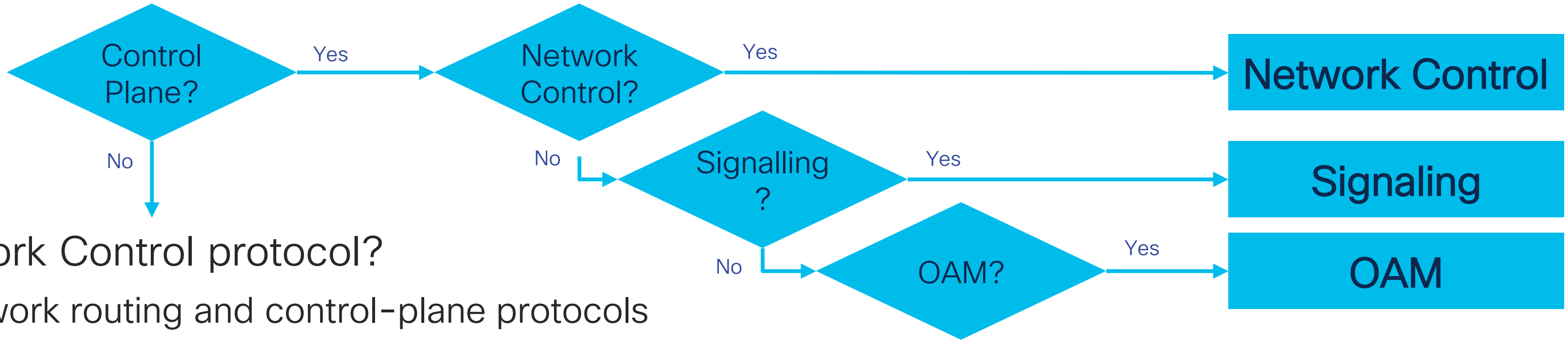
Translating Business-Relevance to QoS Policies

Apply RFC 4594-based Marking / Queuing / Dropping

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

Application Classification Rules

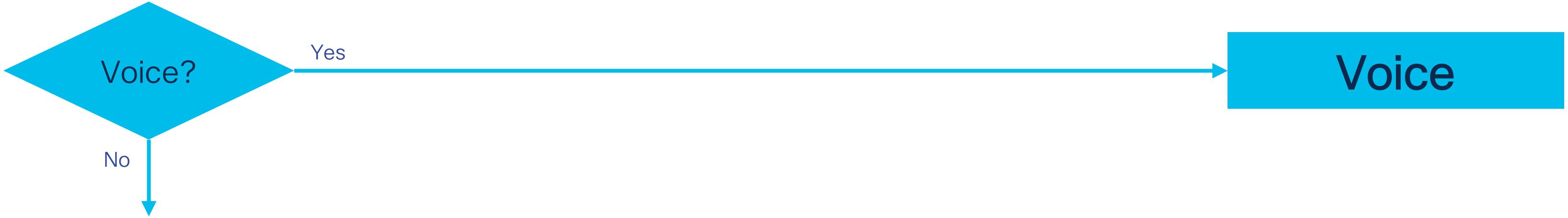
Is the Protocol a Control Plane Protocol?



- 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 (continued)

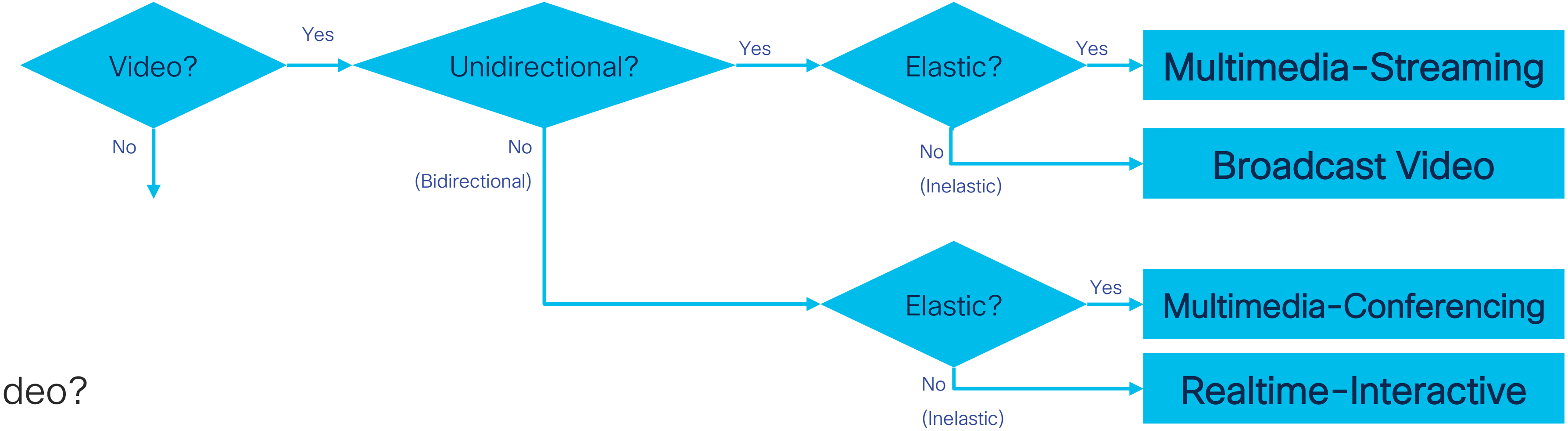
Is the Application Voice?



- 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 Webex; 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 (continued)

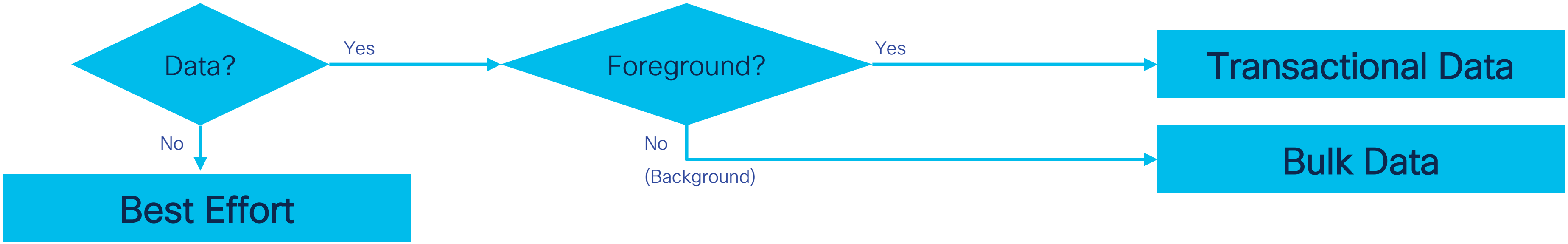
Is the Application Video?



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

Application Classification Rules (continued)

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)

Agenda

- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

Campus LAN QoS Design Considerations and Best Practices

The Case for Campus QoS

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

Why Is Video So Sensitive to Packet Loss?

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

1080 lines of Horizontal Resolution

1080p60

1080 x 1920 lines =

2,073,600 pixels per frame

x 24 bits of color per pixel

x 60 frames per second

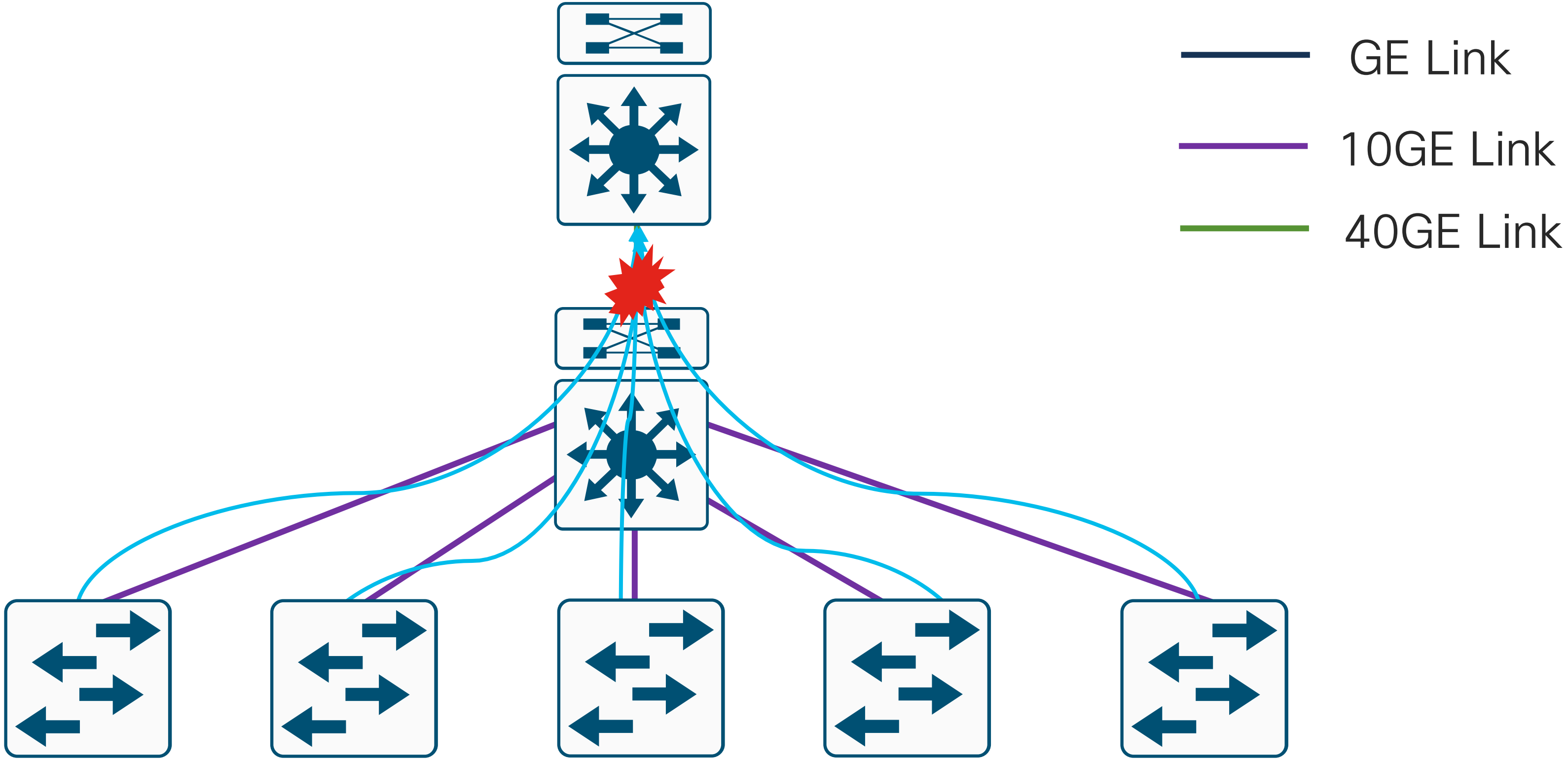
= 2,985,984,000 bps

or 3 Gbps Uncompressed!

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

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

Oversubscription in 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

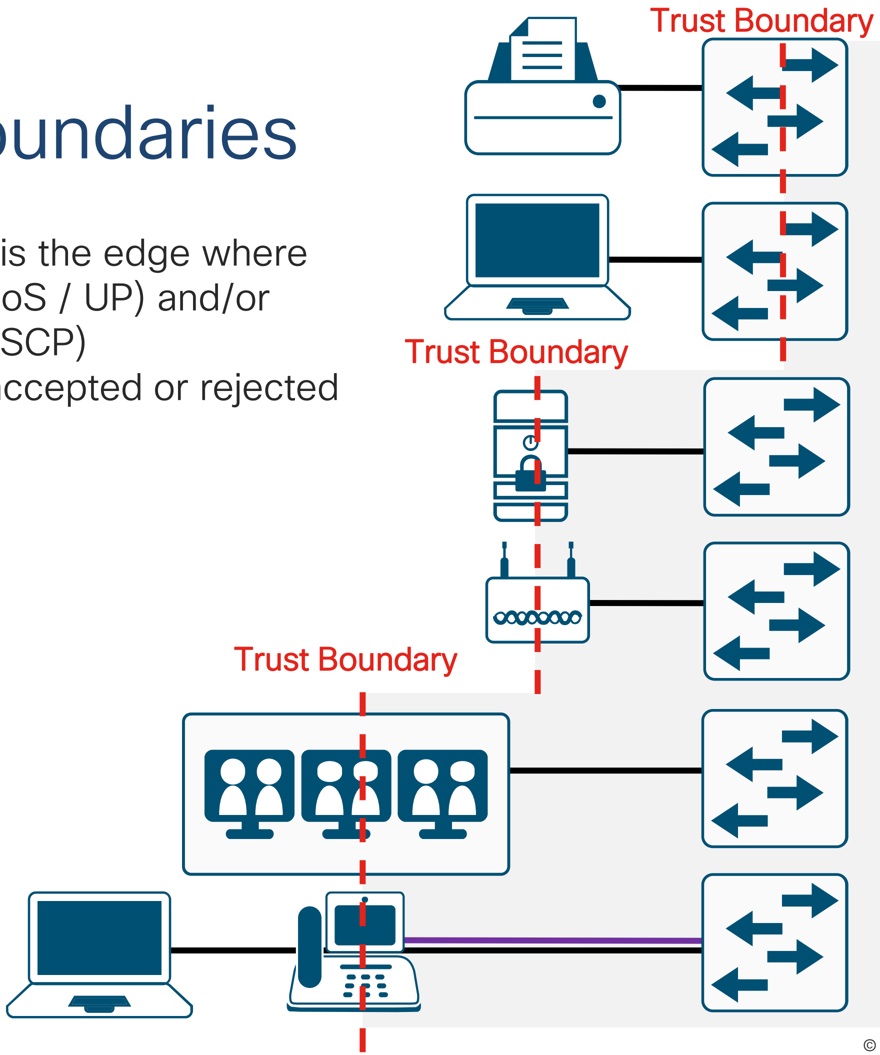
Hardware Varies

Trust Boundaries

The trust boundary is the edge where

- Layer 2 (CoS / UP) and/or
- Layer 3 (DSCP)

QoS markings are accepted or rejected



Untrusted / User-Administered Devices
`no mls qos trust*`

Trusted Centrally-Administered Devices
`mls qos trust dscp*`

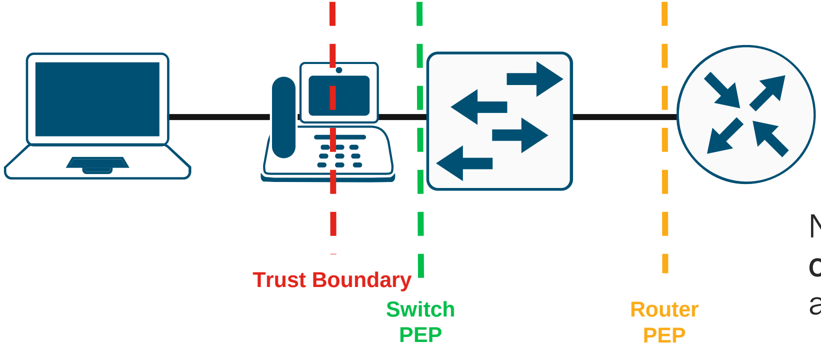
Centrally-Administered & Conditionally-Trusted Devices
`mls qos trust device*`

- `cisco-phone`
- `cts`
- `ip-camera`
- `media-player`

*MLS QoS syntax

Policy Enforcement Points (PEPs)

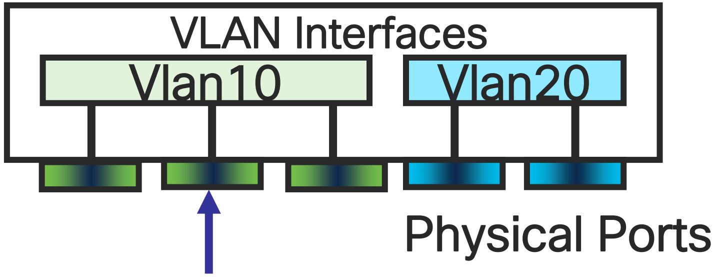
- The Policy Enforcement Point (PEP) is the edge where classification and marking policies are enforced
- The PEP may or ***may not be the same as the trust boundary***
- Multiple PEPs may exist for different types of network devices



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

Per-Port QoS vs. Per-VLAN QoS

Per-Port QoS

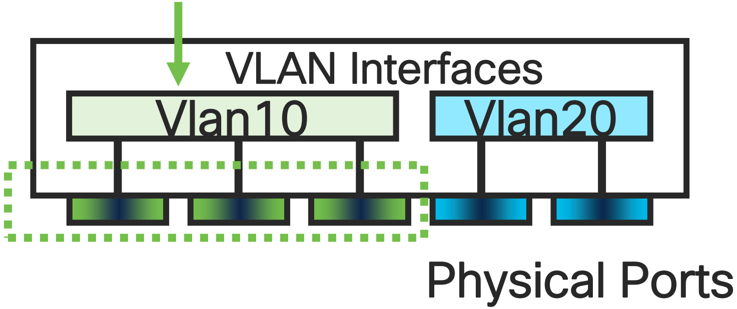


Policy map is applied to the physical switch port

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

Per-VLAN QoS

Policy map is applied to the logical VLAN interface



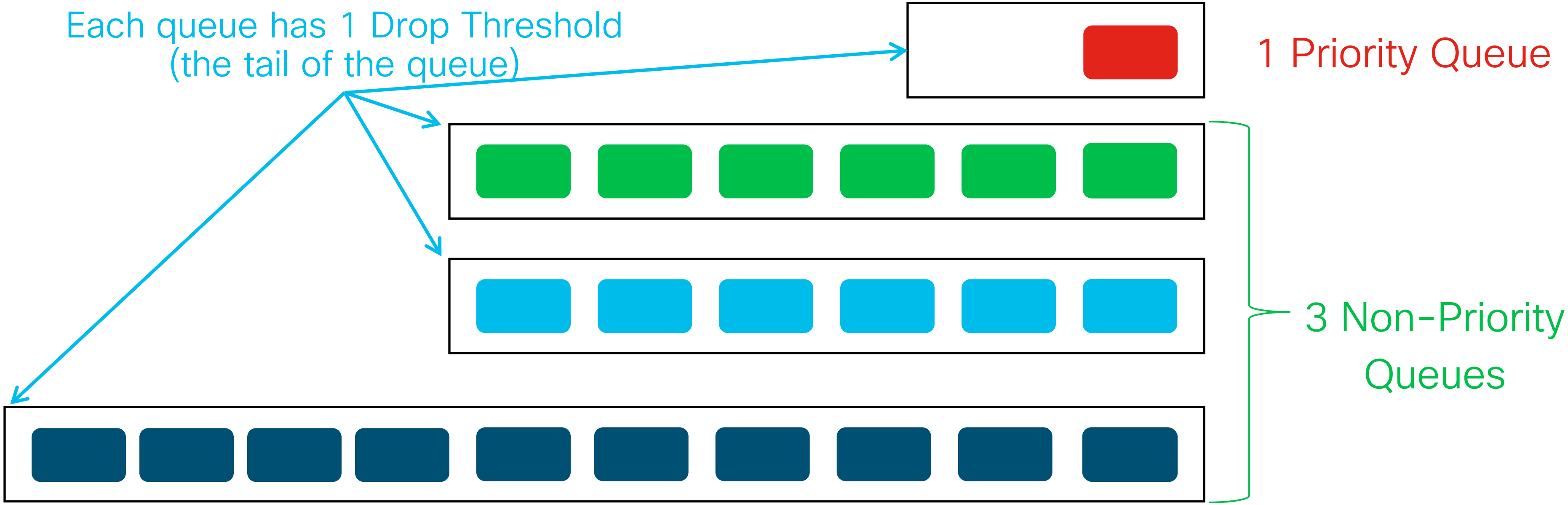
```
interface gig 1/1-48
 mls qos vlan-based

interface Vlan 10
 service-policy input MARKING
```

NBAR2 in Hardware–Today

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

Catalyst Hardware Queuing

1P3Q1T Example



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

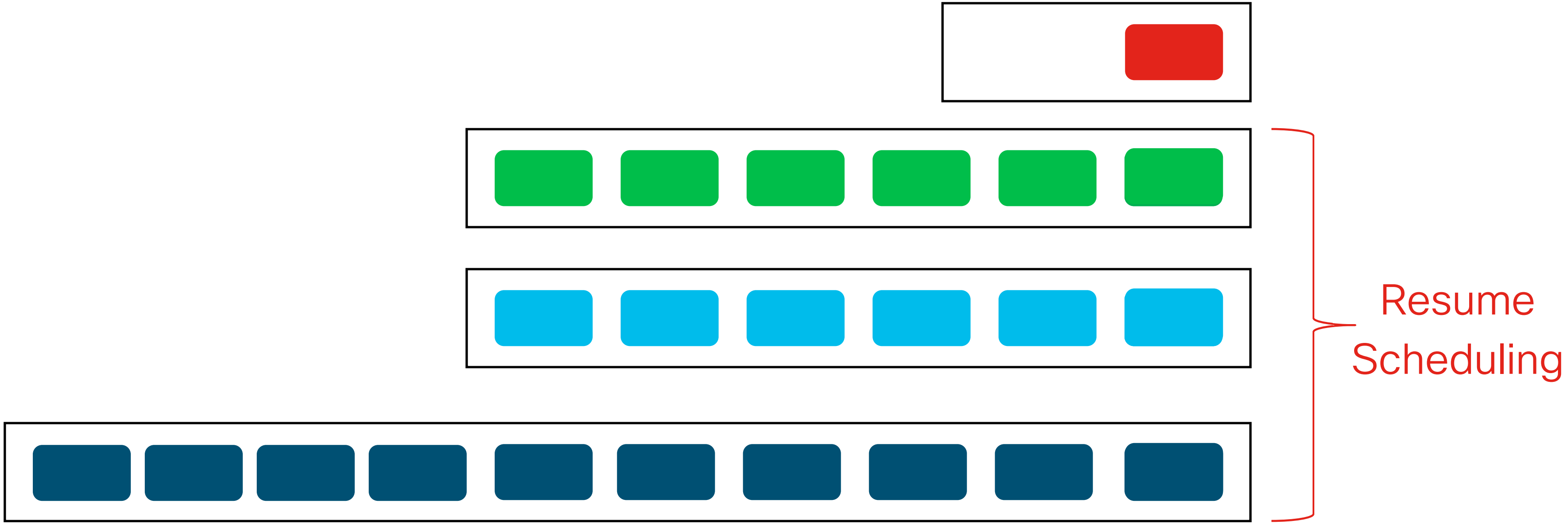
1 Priority Queue

3 Non-Priority Queues

1P3Q1T

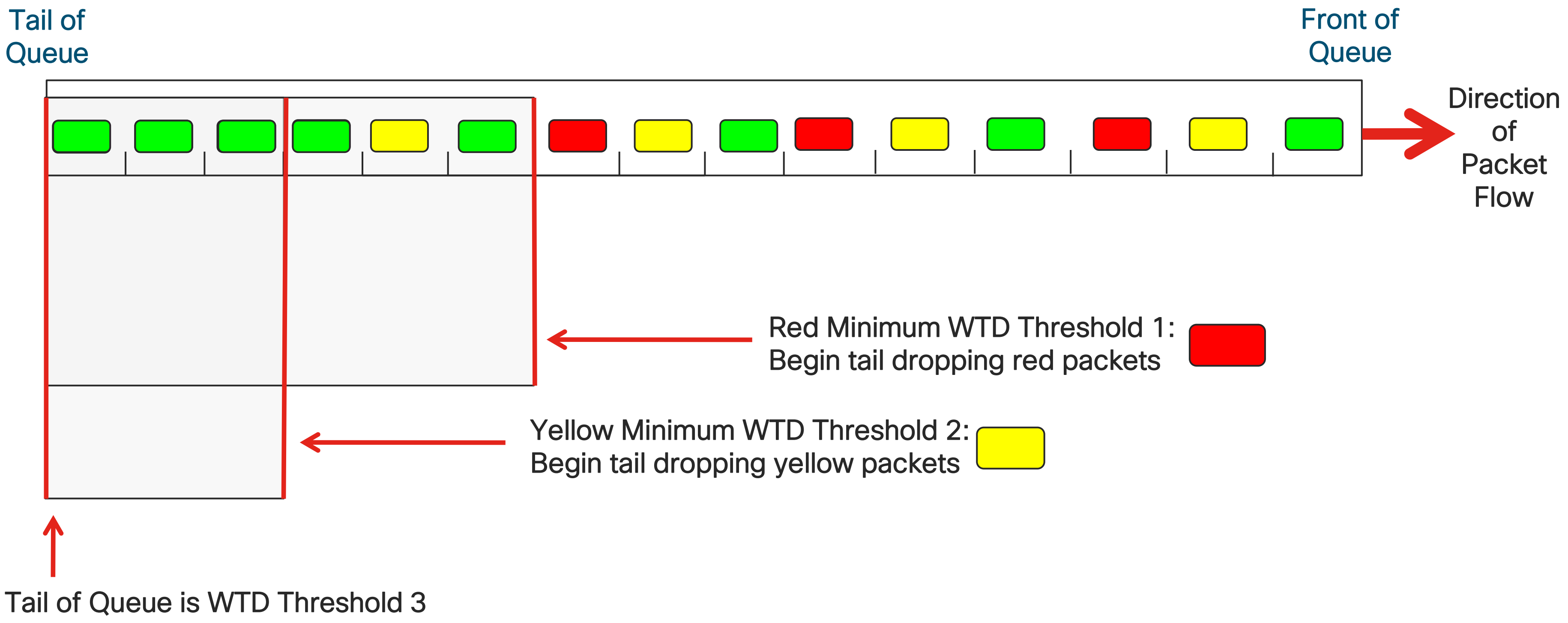
Catalyst Hardware Queuing

1P3Q1T Example



Weighted Tail Drop (WTD) Operation

3T WTD Example



Tail of Queue

Front of Queue

Direction of Packet Flow

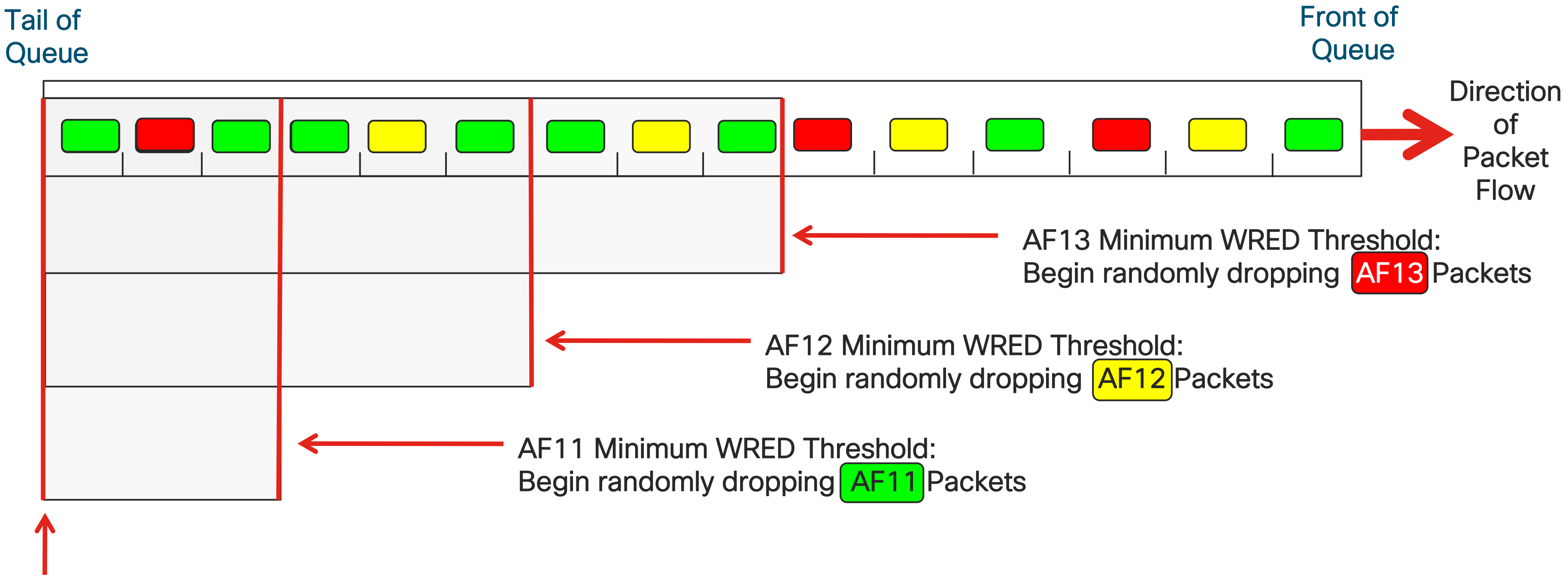
Red Minimum WTD Threshold 1: Begin tail dropping red packets 🟥

Yellow Minimum WTD Threshold 2: Begin tail dropping yellow packets 🟨

Tail of Queue is WTD Threshold 3

Weighted Random Early Detect (WRED) Operation

3T WRED Example



AF13 Minimum WRED Threshold:
Begin randomly dropping AF13 Packets

AF12 Minimum WRED Threshold:
Begin randomly dropping AF12 Packets

AF11 Minimum WRED Threshold:
Begin randomly dropping AF11 Packets

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

Auto QoS

- Auto QoS is a macro which provisions pre-defined ingress classification & marking and queuing (egress and/or ingress) policies to switch ports
- Eleven forms of the interface-level Auto QoS command
  - auto qos voip {cisco-phone | cisco-softphone | trust}
  - auto qos video {cts | ip-camera | media-player}
  - auto qos classify [police]
  - auto qos trust [cos | dscp]
- To remove Auto QoS on an interface preface the command with a “no” (i.e. no auto qos voip cisco-phone)
  - It is not recommended to modify the configuration provisioned by the Auto QoS commands because it may affect the ability of the switch to remove the configuration at the interface-level or globally when removing Auto QoS
- The global command “auto qos srnd4” must be configured to use the current version of Auto QoS on Catalyst 3750-X / 3560-X / 2960-X platforms.

Campus QoS Design Best Practices

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

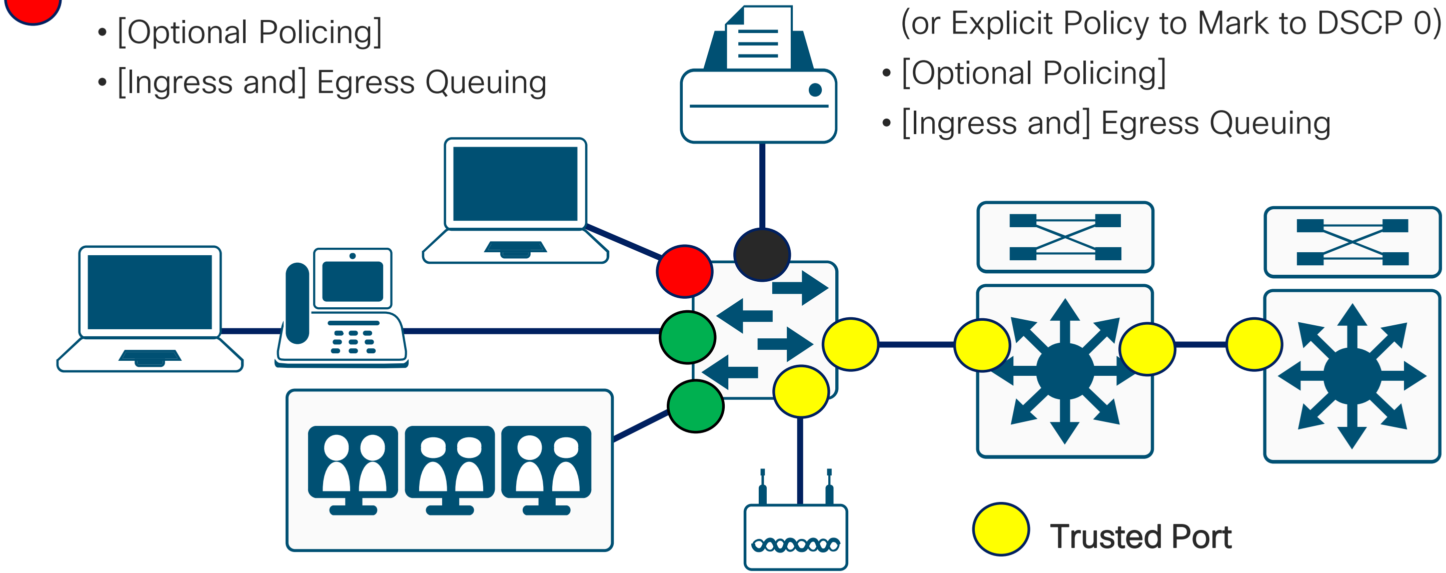
Campus Port QoS Roles

🔴 **Untrusted Endpoint:**

- Ingress Classification and Marking
- [Optional Policing]
- [Ingress and] Egress Queuing

⚫ **Untrusted Endpoint:**

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



🟢 **Conditionally-Trusted Endpoint**

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

🟡 **Trusted Port**

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

Agenda

- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

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

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

QoS Design Steps

1. Enable QoS
2. Configure Ingress QoS Model(s):
   - Trust Models
   - Conditional Trust Model
   - Service Policy Models
3. Configure Egress Queuing
4. Configure Ingress Queuing (Catalyst 3560-X & 3750-X)

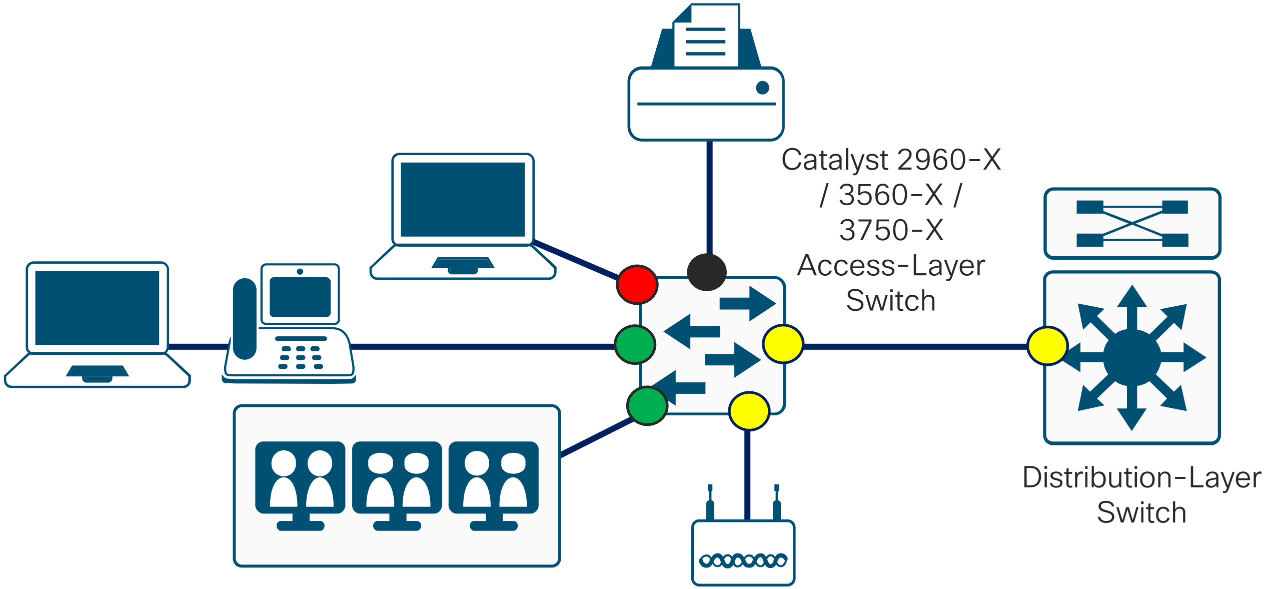
Note: The Catalyst 3560-X & 3750-X support VLAN-based QoS policies, but the 2960-X does not.

Note: Catalyst 2960-X must be running a LAN Base image to support the following QoS features

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

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

QoS Roles in the Campus Access


Catalyst 2960-X / 3560-X / 3750-X Access-Layer Switch
Distribution-Layer Switch

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

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

Enabling QoS and Trust Models

Enabling QoS:

```
mls qos
```

Grey shaded commands are global

Trust-CoS Model Example:

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

Key commands/parameters are in RED

```
mls qos trust cos
```

Yellow shaded commands are interface specific

Trust-DSCP Model Example:

```
mls qos trust dscp
```

Note: CoS 5 which is explicitly mapped to DSCP 46

Conditional-Trust Model Example:

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

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

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

Conditional Trust Model Example

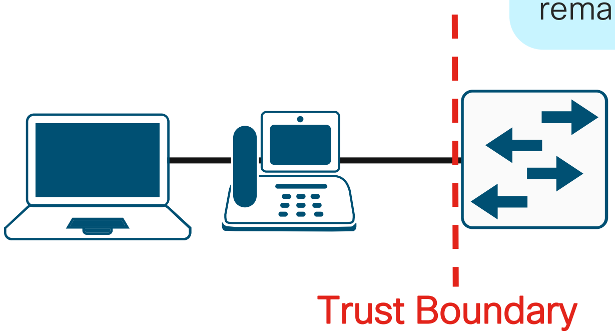
Conditional Trust Policy to a Cisco IP

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

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

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

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



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

Ingress Classification & Marking Policy Example – Policy-Map

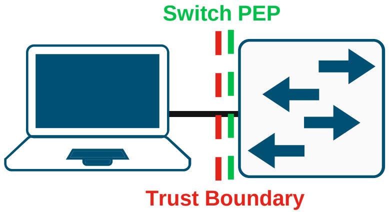
The policy-map definition specifies an ordered list of classes, each with an action, with a default class at the bottom

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

```
[continued]
 class BULK-DATA
  set dscp af11
 class SCAVENGER
  set dscp cs1
 class class-default
  set dscp default
```

```
service-policy input MARKING-POLICY
```

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



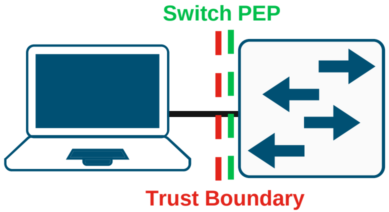
Catalyst 2960-X / 3560-X / 3750-X

Ingress Classification & Marking Policy Example – Class-Maps

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

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

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



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

Ingress Classification & Marking Policy Model Example – Access Control List

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

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

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

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

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

Catalyst 2960-X

Marking & Policing Policy Example

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

In this example exceeding:

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

are remarked to Scavenger (CS1 / DSCP 8).

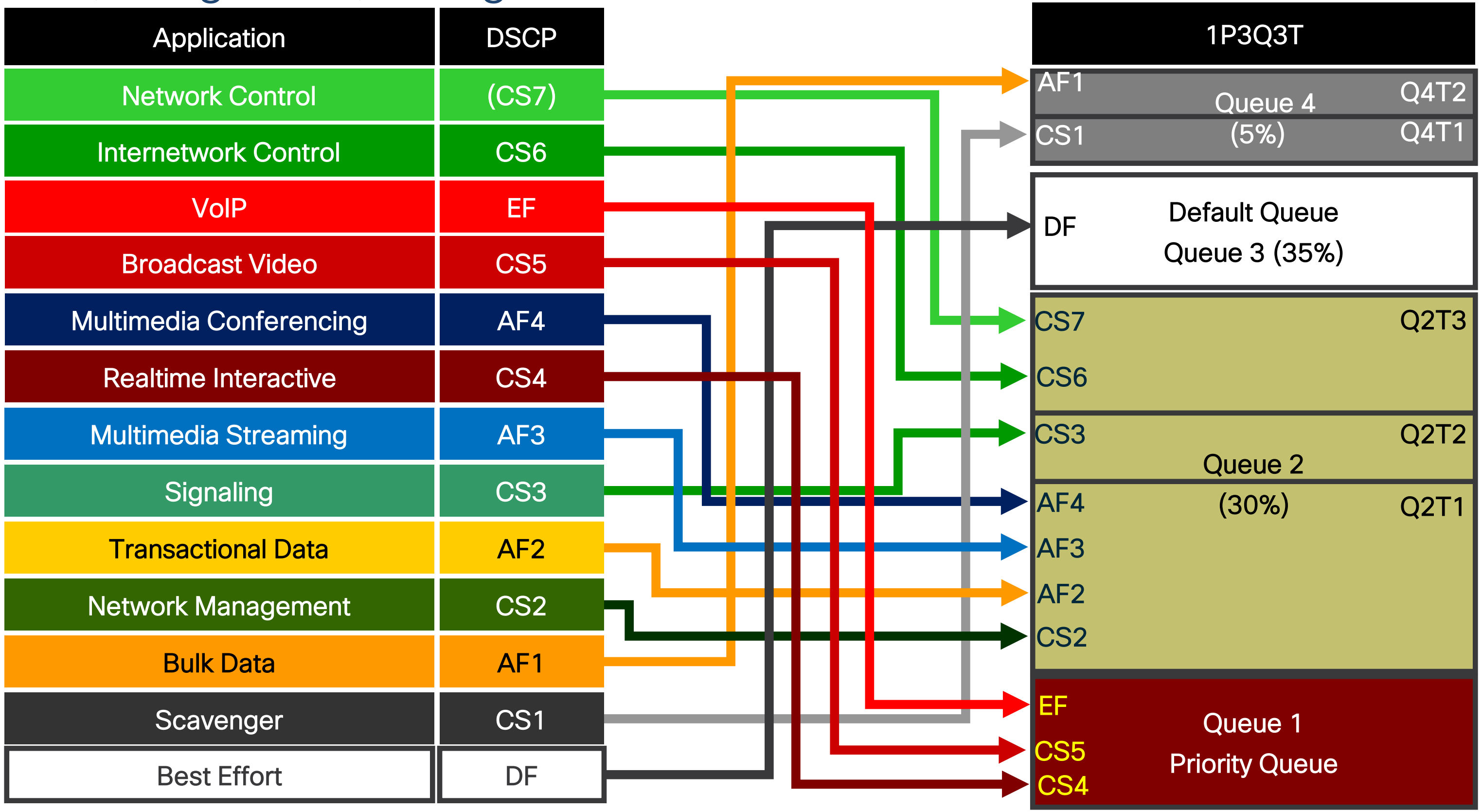
```
mls qos map policed-dscp 0 10 18 to 8

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

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

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

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

1P3Q3T Egress Queuing Model



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

1P3Q3T

AF1 Queue 4 Q4T2
CS1 (5%) Q4T1

DF Default Queue
Queue 3 (35%)

CS7 Q2T3
CS6

CS3 Q2T2
Queue 2

AF4 (30%) Q2T1
AF3
AF2
CS2

EF Queue 1
CS5 Priority Queue
CS4

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

1P3Q3T Egress Queuing Model Config—Part 1 of 2

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

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

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

Each queue has 4 thresholds:

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

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

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

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

1P3Q3T Egress Queuing Model Config—Part 2 of 2

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

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

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

Enables the PQ

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

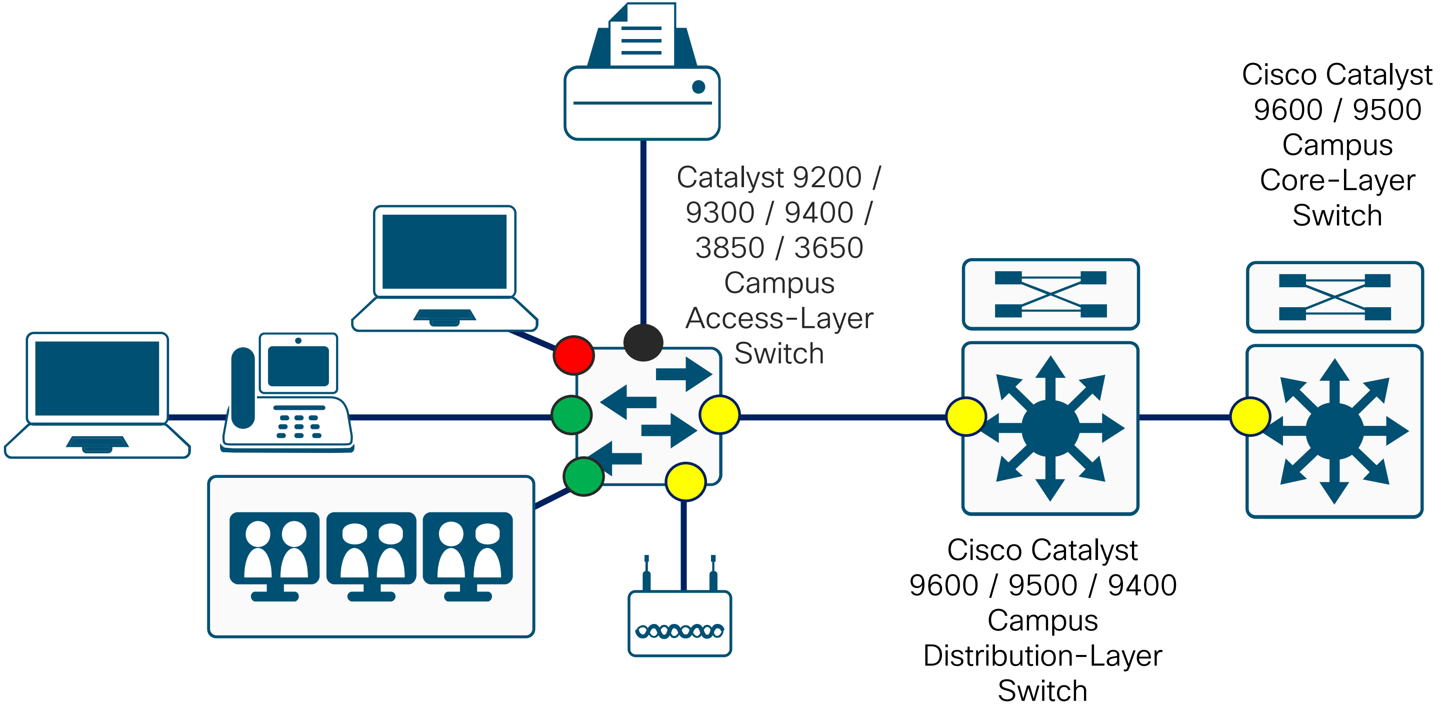
Agenda

- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design

Catalyst 9000 / 3850 / 3650 Series

QoS Roles in the Campus



Catalyst 9200 / 9300 / 9400 / 3850 / 3650 Campus Access-Layer Switch
Cisco Catalyst 9600 / 9500 Campus Core-Layer Switch
Cisco Catalyst 9600 / 9500 / 9400 Campus Distribution-Layer Switch

⚫ No Trust +
Ingress Queuing +
Egress Queuing

🟡 Trust DSCP +
Ingress Queuing +
Egress Queuing

🟢 Conditional Trust +
Ingress Queuing +
Egress Queuing

🔴 Classification/Marking +
[Optional Policing] +
Ingress Queuing +
Egress Queuing

Catalyst 9000 / 3850 / 3650 Series

QoS Design Steps

Access-Layer Switch Role

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

Core or Distribution-Layer Switch Role

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

Catalyst 9000 / 3850 / 3650 Series

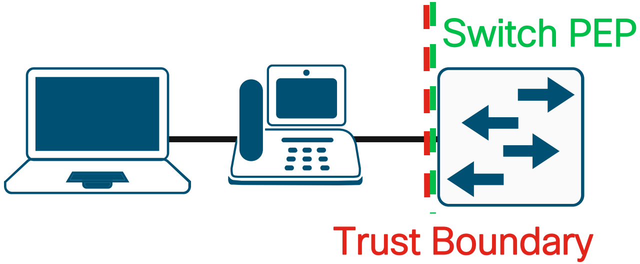
Conditional Trust Models

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

Conditional-Trust Models:

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

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



Conditional-Trust (Cisco IP Phone) Example:

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

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

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

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

Catalyst 9000 / 3850 / 3650 Series

Classification Options

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

Catalyst 9000 / 3850 / 3650 Series

Configuring NBAR2 QoS Policies

```
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
…
```

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

```
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
```

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

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

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

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

Catalyst 9000 / 3850 / 3650

Marking & Policing Policy Example

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

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

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

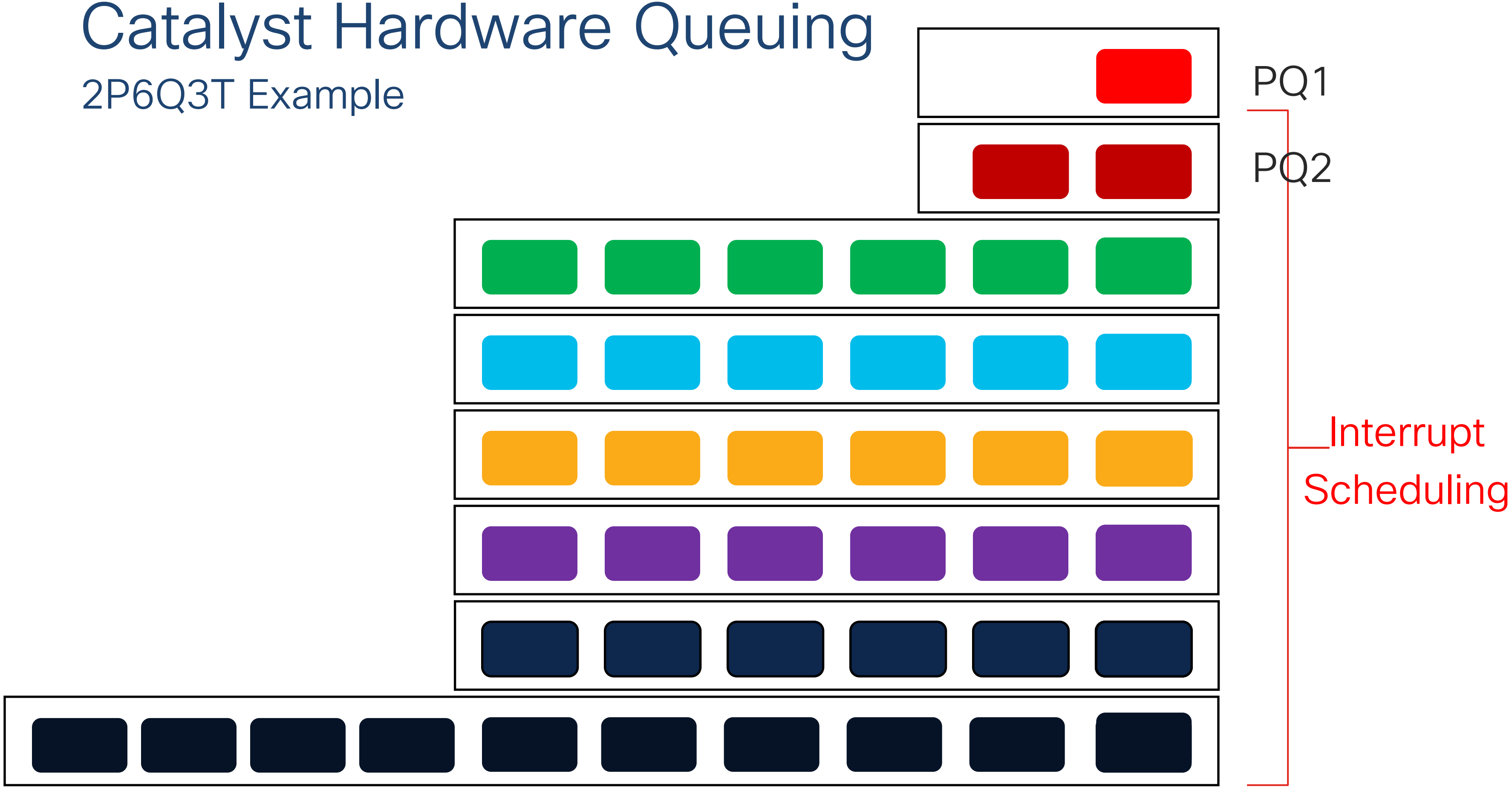
All markdown and/or mapping operations are configured through **table-maps**

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

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

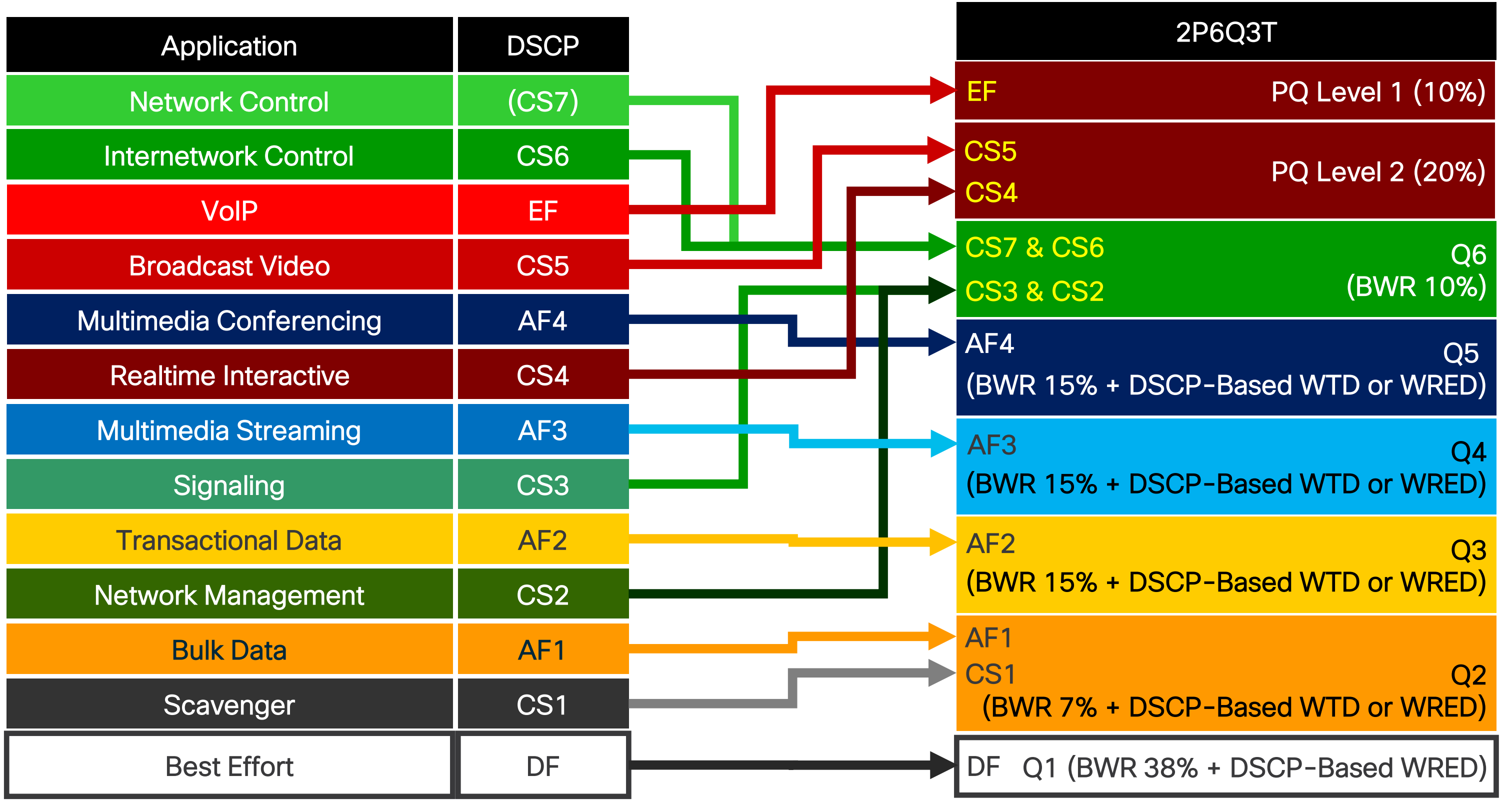
Catalyst Hardware Queuing

2P6Q3T Example



Catalyst 9000 / 3850 / 3650

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



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

2P6Q3T	
EF	PQ Level 1 (10%)
CS5 CS4	PQ Level 2 (20%)
CS7 & CS6 CS3 & CS2	Q6 (BWR 10%)
AF4	Q5 (BWR 15% + DSCP-Based WTD or WRED)
AF3	Q4 (BWR 15% + DSCP-Based WTD or WRED)
AF2	Q3 (BWR 15% + DSCP-Based WTD or WRED)
AF1 CS1	Q2 (BWR 7% + DSCP-Based WTD or WRED)
DF	Q1 (BWR 38% + DSCP-Based WRED)

BWR = Bandwidth Remaining

WTD = Weighted Tail Drop

WRED = Weighted Random Early Detect

WRED supported on Catalyst 9000 Series only

Catalyst 9000 / 3850 / 3650

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

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

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

Catalyst 9000 / 3850 / 3650

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

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

Two-levels of priority queuing are supported

Policer is always unconditional regardless of form

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

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

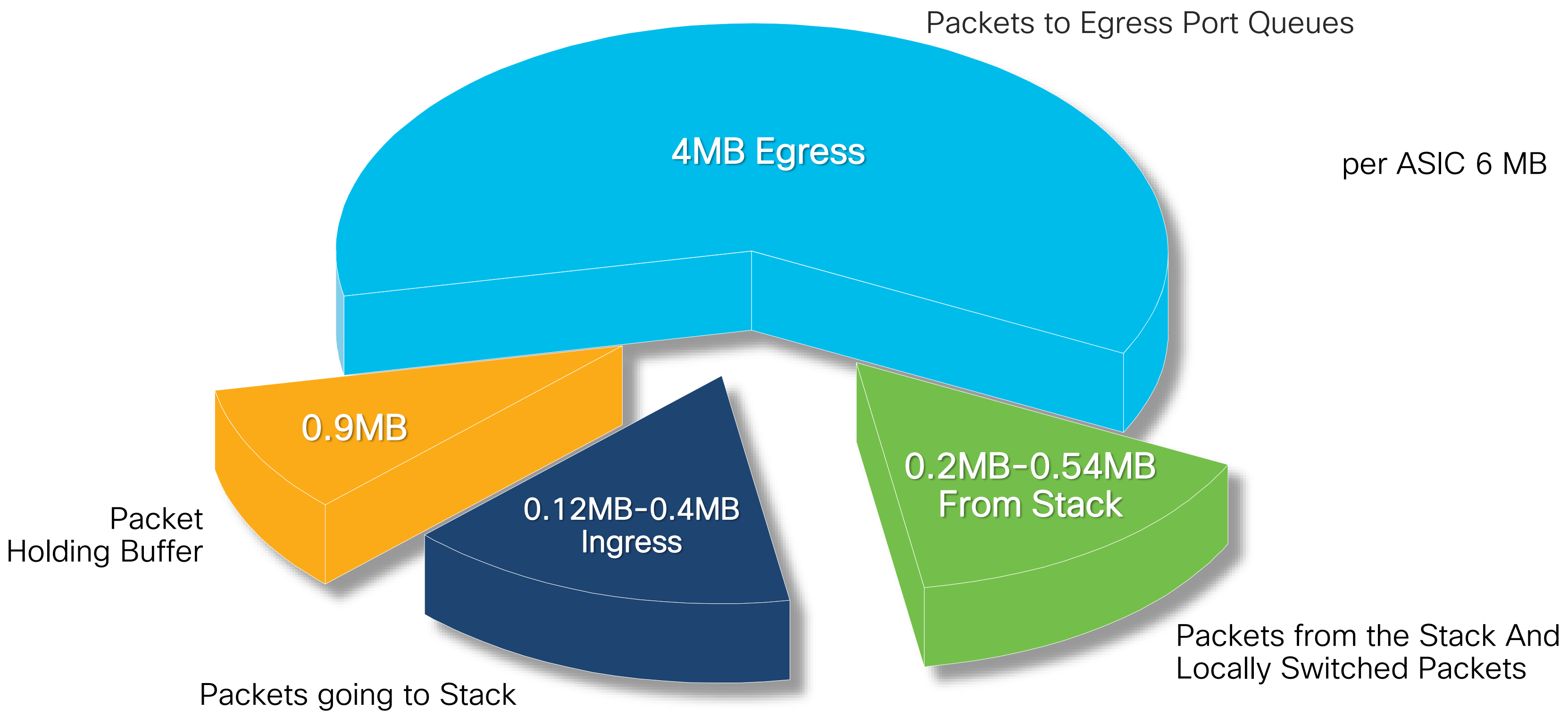
If a PQ is enabled then non-PQs must use **bandwidth remaining**

Allocates buffers to queues

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

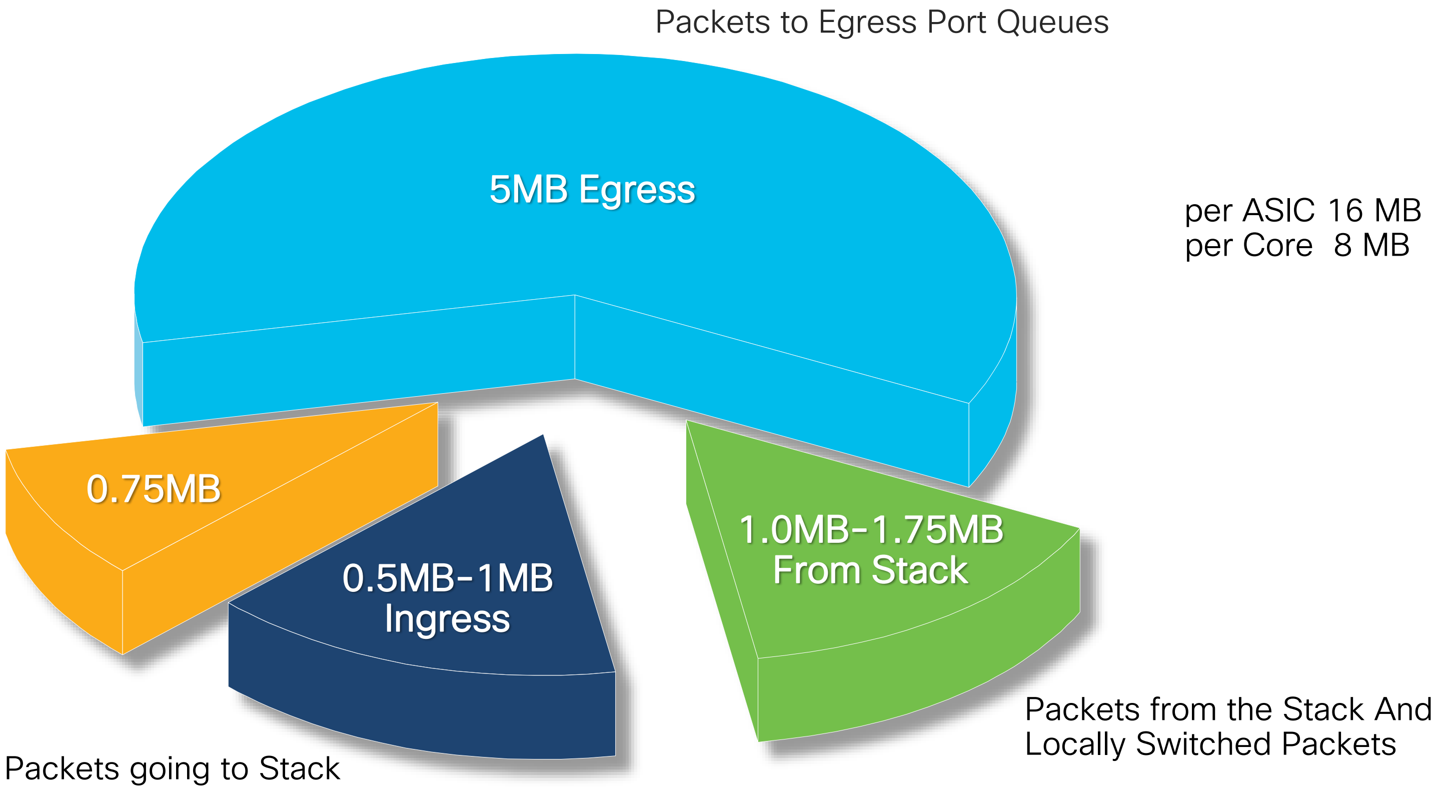
Cisco Catalyst 9200 Series

UADP 2.0 Mini Buffer size



Cisco Catalyst 9300 Series

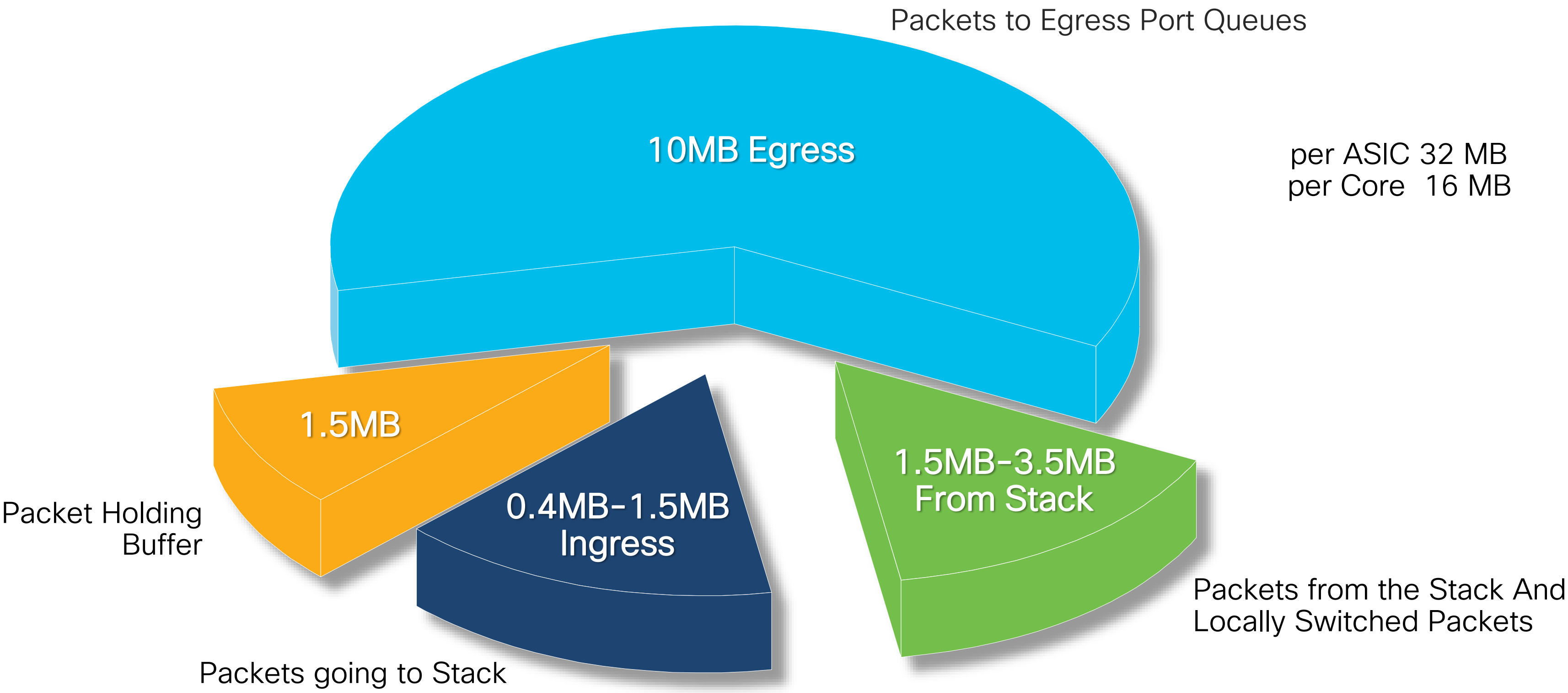
UADP 2.0 Buffer size



per ASIC 16 MB
per Core 8 MB

Cisco Catalyst 9400/9500 Series

UADP 2.0 XL Buffer size

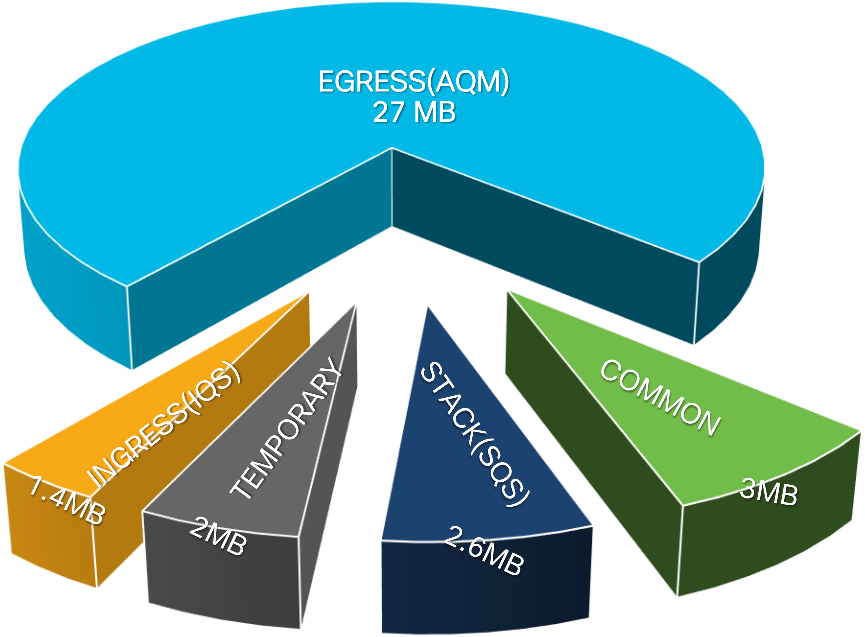


per ASIC 32 MB
per Core 16 MB

Cisco Catalyst 9500-H

UADP 3.0 Buffer size

- A total of 36MB of single buffer is shared by I/O data



Catalyst 9000 (ONLY)

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

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

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

Enables DSCP-based WRED for the queue

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

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

Catalyst 9000 / 3850 / 3650

Hierarchical QoS Policies–Queuing within Shaped Rate Example

```
policy-map 50MBPS-SHAPER
 class class-default
  shape average 50000000
  service-policy 2P6Q3T
interface GigabitEthernet 1/0/1
 service-policy output 50MBPS-SHAPER
```

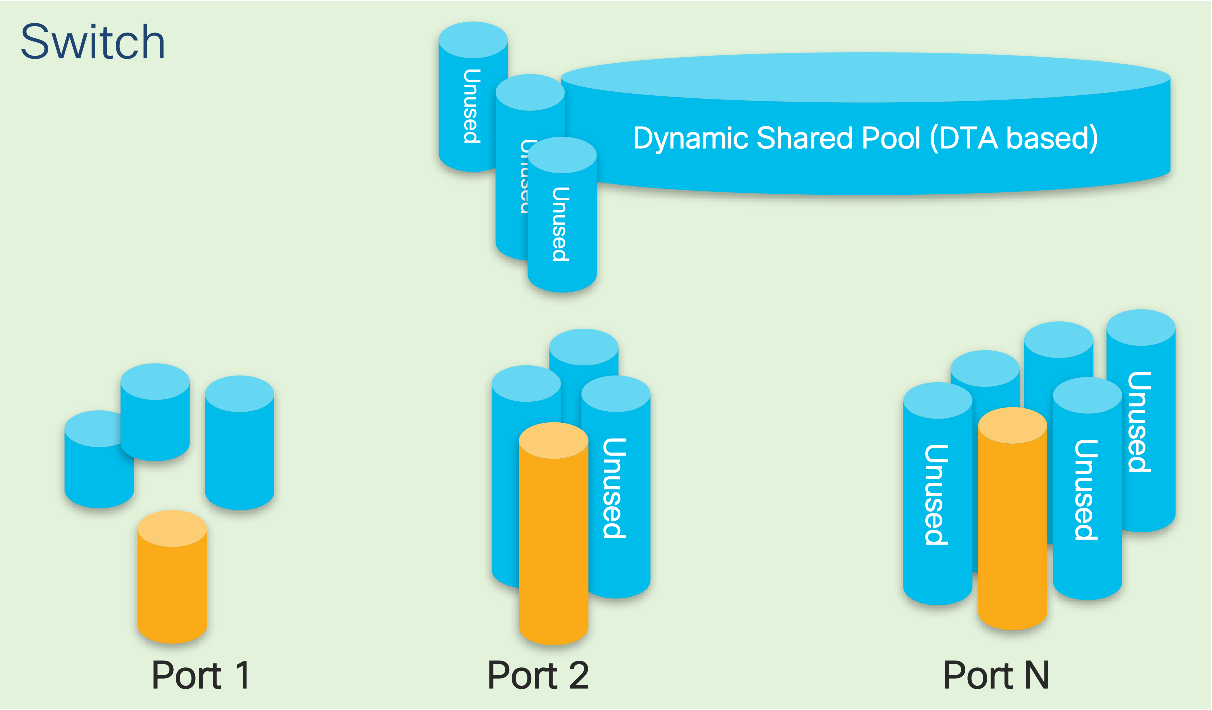
Defines the sub-line rate (CIR)

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

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

Automatic adjustment of buffer allocation

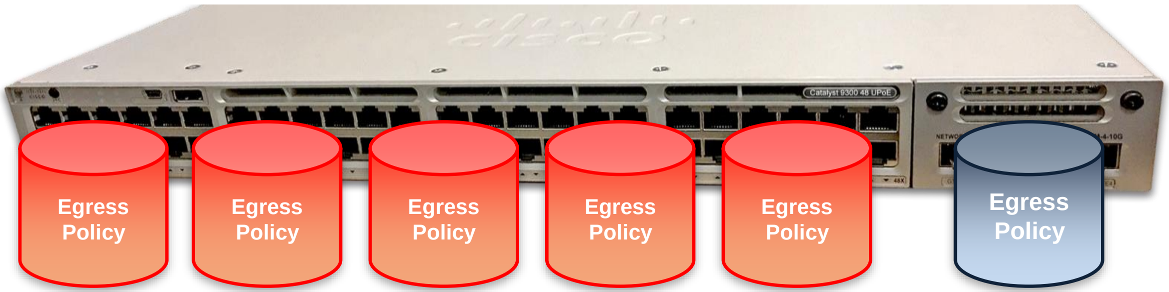
Dynamic Threshold and Scaling(DTS)



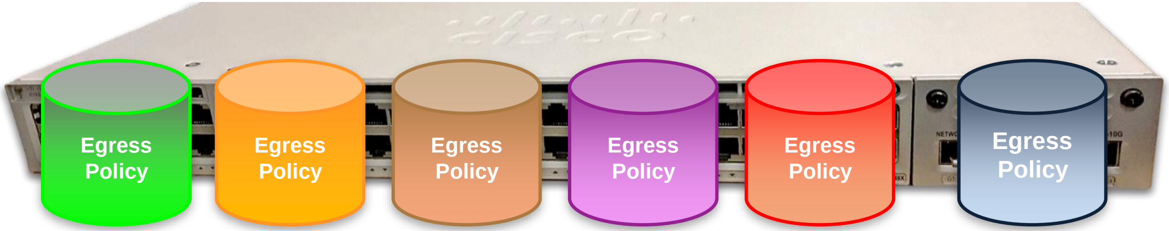
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-3/configuration_guide/qos/b_173_qos_9300_cg/configuring_qos.html

- An algorithm called DTS is automatically applied as a function to allocate soft buffer resources fairly and efficiently.
- In the event of congestion, incoming data is flexibly allocated with shared buffers (soft buffers) based on global / port resource occupancy.
- The maximum value of the shared buffer can be expanded by changing the global settings.

Catalyst 9000 Series Per-port Policy Allocation

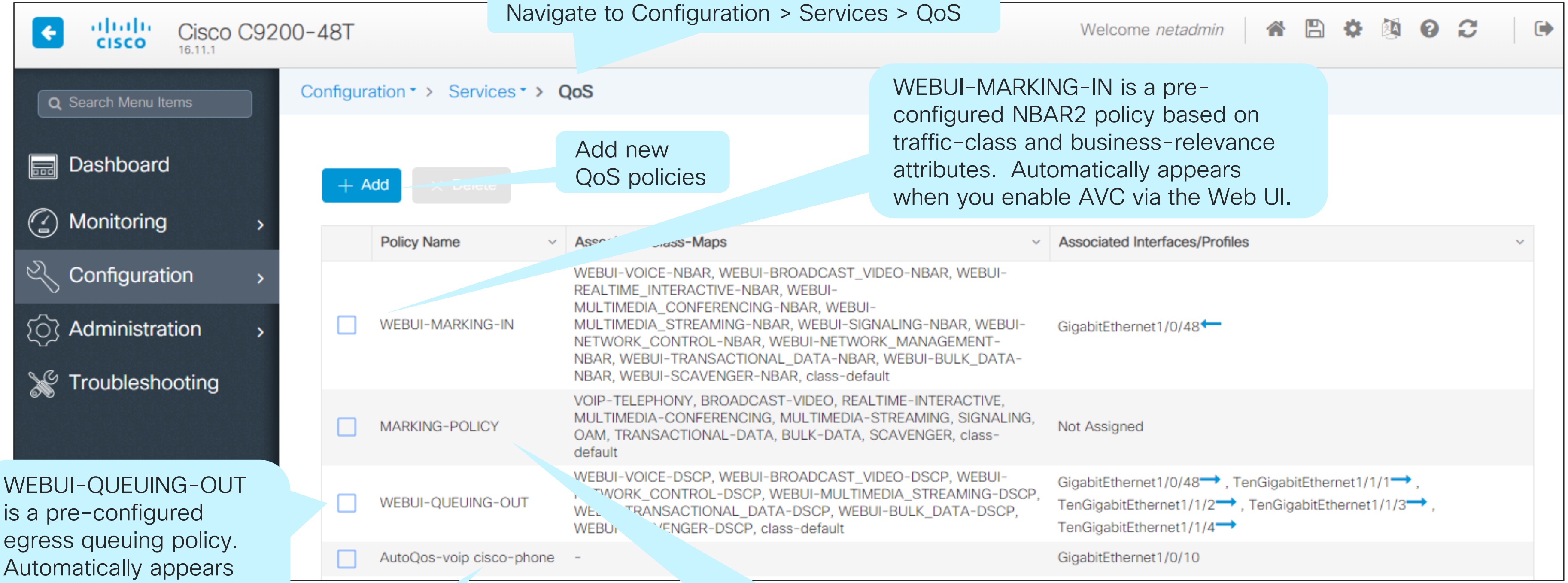


- Catalyst 3850 / 3650 Series supports two egress policies
  - All built-in front panel ports need to share the same egress queueing policy
  - All ports on network modules need to share the same egress queueing policy



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

QoS Policy via the Catalyst 9000 Series Web UI



Configuration > Services > QoS

	Policy Name	Associated Class-Maps	Associated Interfaces/Profiles
□	WEBUI-MARKING-IN	WEBUI-VOICE-NBAR, WEBUI-BROADCAST_VIDEO-NBAR, WEBUI-REALTIME_INTERACTIVE-NBAR, WEBUI-MULTIMEDIA_CONFERENCING-NBAR, WEBUI-MULTIMEDIA_STREAMING-NBAR, WEBUI-SIGNALING-NBAR, WEBUI-NETWORK_CONTROL-NBAR, WEBUI-NETWORK_MANAGEMENT-NBAR, WEBUI-TRANSACTIONAL_DATA-NBAR, WEBUI-BULK_DATA-NBAR, WEBUI-SCAVENGER-NBAR, class-default	GigabitEthernet1/0/48←
□	MARKING-POLICY	VOIP-TELEPHONY, BROADCAST-VIDEO, REALTIME-INTERACTIVE, MULTIMEDIA-CONFERENCING, MULTIMEDIA-STREAMING, SIGNALING, OAM, TRANSACTIONAL-DATA, BULK-DATA, SCAVENGER, class-default	Not Assigned
□	WEBUI-QUEUING-OUT	WEBUI-VOICE-DSCP, WEBUI-BROADCAST_VIDEO-DSCP, WEBUI-NETWORK_CONTROL-DSCP, WEBUI-MULTIMEDIA_STREAMING-DSCP, WEBUI-TRANSACTIONAL_DATA-DSCP, WEBUI-BULK_DATA-DSCP, WEBUI-SCAVENGER-DSCP, class-default	GigabitEthernet1/0/48→ , TenGigabitEthernet1/1/1→ , TenGigabitEthernet1/1/2→ , TenGigabitEthernet1/1/3→ , TenGigabitEthernet1/1/4→
□	AutoQos-voip cisco-phone	-	GigabitEthernet1/0/10

Navigate to Configuration > Services > QoS

Add new QoS policies

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

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

Auto QoS policies

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

Agenda

- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
  - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
  - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

MLS to MQC Migration

Difference between platforms

	MLS	MQC
QoS default	Disabled	Enabled
Global config	Support MLS QoS Support some of MQC at ingress	Does not support MLS QoS Support MQC [class-map, policy-map]
Interface config	Support MLS QoS config and some of MQC CLI at ingress	Attach the policy to the interface
Port trust default	Disabled	Enabled
Port Ingress	Classification/Policing/Marking/ Queuing	Classification/Policing/marking [NO Iingress Queuing !]
Port Egress	Queuing	Classification/Policing/marking/queuing
Switch Virtual Interface (SVI) Ingress	Classification/Policing/Marking	Classification/Marking
SVI Egress	None	Classification/Marking

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3850-series-switches/118629-technote-qos-00.html

Feature Detail Comparison

Ingress

Feature	MLS (based on 3750)	MQC (based on 3850/9000)
Classification	Class-map match Differentiated Services Code Point (DSCP), Precedence (Prec), Access Control List (ACL)	Class-map Class of Service (CoS), Prec, DSCP, ACL And VLAN, NBAR2
Marking [unconditional set]	Set DSCP and Prec	Set CoS, Prec, DSCP and QoS-group
Marking [conditional marking]	DSCP mutation	Class-default table-map
Policing	1r2c	1r2c and 2r3c
Policing markdown	Policing exceeds mark-down [Only supports DSCP]	Policing exceeds and violates mark-down [Supports CoS, DSCP, Prec]
Aggregate Policing	Supports	Agg-policing [one type of HQoS]
Ingress Queuing	Supports only on 3750 but does not support on 3750x	Does not support
Hierarchical QoS (HQoS)	VLAN based HQoS only	Port-based Agg-policing and Per-VLAN (PV)

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3850-series-switches/118629-technote-qos-00.html

Feature Detail Comparison

Egress

Feature	MLS (based on 3750)	MQC (based on 3850/9000)
Classification support for none queuing action	Does not support	CoS, Prec, DSCP, QoS-group, ACL and VLAN
Classification support for queuing action	CoS and DSCP	CoS, Prec, DSCP and QoS-group
Marking	Does not support	Set CoS, Prec, and DSCP
Policing	Does not support	1r2c , 2r3c with exceed/violate mark down through table-map
Max number of queues and queue types	1P3Q3T [4 queues] Expedite queue-> Priority queue	2P6Q3T [up to 8 queues]
Egress Queuing	Share mode, shape mode, queue-limit, priority and queue-buffer	Bandwidth, bandwidth remaining, shaping, queue-limit, priority and queue-buffer
HQoS	Does not support	HQoS: Agg-policing, PV, Port-shaper and Parent user shaper with child non-queuing action

https://www.cisco.com/c/en/us/support/docs/switches/catalyst-3850-series-switches/118629-technote-qos-00.html

Example: Police-markdown

MLS

Default policed-dscp map:

```
MLS-SW#show mls qos map policed-dscp
Policed-dscp map:
d1 : d2 0 1 2 3 4 5 6 7 8 9
----------------------------------
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
```

User define policed-dscp map:

```
MLS-SW(config)#mls qos map policed-dscp 0 10 18 24 46 to 8
MLS-SW#show mls qos map policed-dscp
Policed-dscp map:
d1 : d2 0 1 2 3 4 5 6 7 8 9
---------------------------------------
0 : 08 01 02 03 04 05 06 07 08 09
1 : 08 11 12 13 14 15 16 17 08 19
2 : 20 21 22 23 08 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 08 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
```

```
Policy config:
class-map match-all policed-dscp
match access-group 2
class policed-dscp
police 8000 8000 exceed-action policed-dscp-transmit
```

Example: Police-markdown

MQC

```
MQC-SW(config)#table-map policed-dscp
MQC-SW(config-tablemap)#map from 0 to 8
MQC-SW(config-tablemap)#map from 10 to 8
MQC-SW(config-tablemap)#map from 18 to 8
MQC-SW(config-tablemap)#map from 24 to 8
MQC-SW(config-tablemap)#map from 46 to 8
MQC-SW  #show table-map policed-dscp
Table Map policed-dscp
from 0 to 8
from 10 to 8
from 18 to 8
from 24 to 8
from 46 to 8
default copy
```

```
MQC-SW#show policy-map policed-dscp
Policy Map policed-dscp
Class class-default
police cir percent 10
conform-action transmit
exceed-action set-dscp-transmit dscp table policed-dscp
```

Example: MLS QoS Enable with Aggregate Policing

MLS

Global:

```
mls qos aggregate-policer AG_POLICER 8000 8000
exceed-action drop
```

Access-list:

```
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 2 …
```

Class-map:

```
class-map match-all AG1
 match access-group 1
class-map match-all AG2
 match access-group 2
```

→

Policy-map:

```
policy-map AG_POLICER
 class AG1
  set dscp 40
  police aggregate AG_POLICER
 class AG2
  set dscp 55
  police aggregate AG_POLICER
```

Example: MLS QoS Enable with Aggregate Policing

MQC

Access-list:

```
access-list 1 permit 10.0.0.0 0.255.255.255
access-list 2 …
```

Class-map:

```
class-map match-all AG1
 match access-group 1
class-map match-all AG2
 match access-group 2
```

```
policy-map AG_POLICER
 class class-default
  police cir  8000
  service-policy CHILD

policy-map CHILD
 class AG1
  set dscp 40
 class AG2
  set dscp 55
```

Example: QoS Bandwidth Configuration

MLS

Default share and shape mode:

```
MLS-SW#show mls qos interface gig 1/0/1
queueing
GigabitEthernet1/0/1
Egress Priority Queue : disabled
Shaped queue weights (absolute) : 25 0 0 0
Shared queue weights : 25 25 25 25
The port bandwidth limit : 100 (Operational
Bandwidth:100.0)
The port is mapped to qset : 1
```

User config share mode under interface:

```
interface GigabitEthernet1/0/1
 srr-queue bandwidth share 40 30 20 10
 srr-queue bandwidth shape 0 0 0 0
```

→

```
MLS-SW#show mls qos interface gig1/0/1 queueing
GigabitEthernet1/0/1
Egress Priority Queue : disabled
Shaped queue weights (absolute) : 0 0 0 0
Shared queue weights : 40 30 20 10
The port bandwidth limit : 100 (Operational
Bandwidth:100.0)
The port is mapped to qset : 1
```

Example: QoS Bandwidth Configuration

MQC

```
MQC-SW#show class-map COS1
 Class Map match-any COS1

   Match cos  1

3850#show class-map COS2
 Class Map match-any COS2

   Match cos  2

3850#show class-map COS3
 Class Map match-any COS3

   Match cos  3
```

→

```
MQC-SW#show policy-map  BANDWIDTH
  Policy Map bandwidth
    Class COS1
      bandwidth percent 40
    Class COS2
      bandwidth percent 30
    Class COS3
      bandwidth percent 20
    Class class-default
      bandwidth percent 10
```

Agenda

- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
    - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
    - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

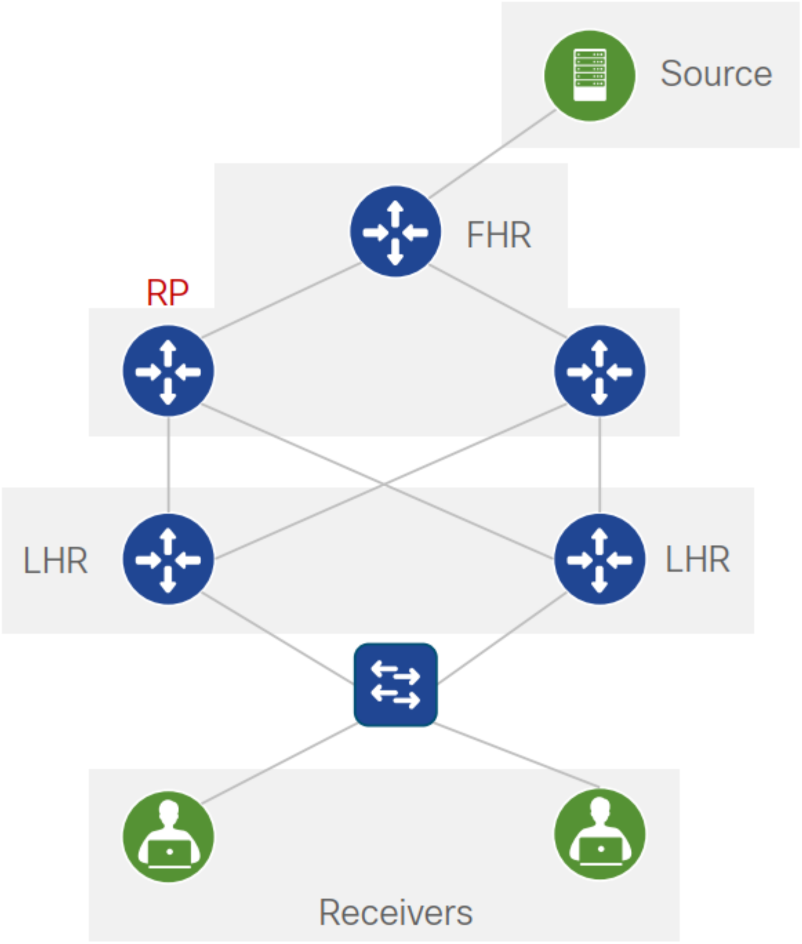
Multicast for modern tasks

Use cases

Multicast Routing Terminology

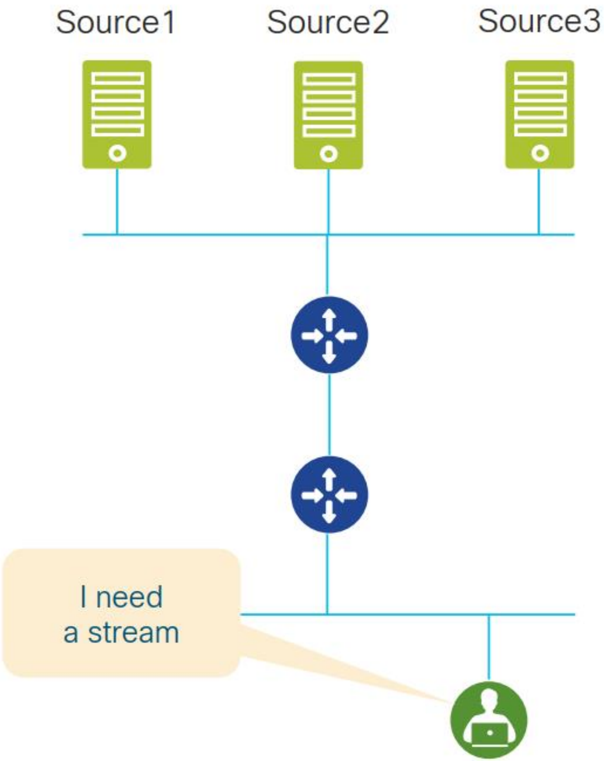
- Source – Device sending multicast traffic
- Receiver – Device receiving multicast traffic

- First-Hop Router – FHR attached to source network segment
- Last-Hop Router – LHR attached to receiver network segment
- Multicast Router – Router enabled for multicast traffic



Any-Source Multicast

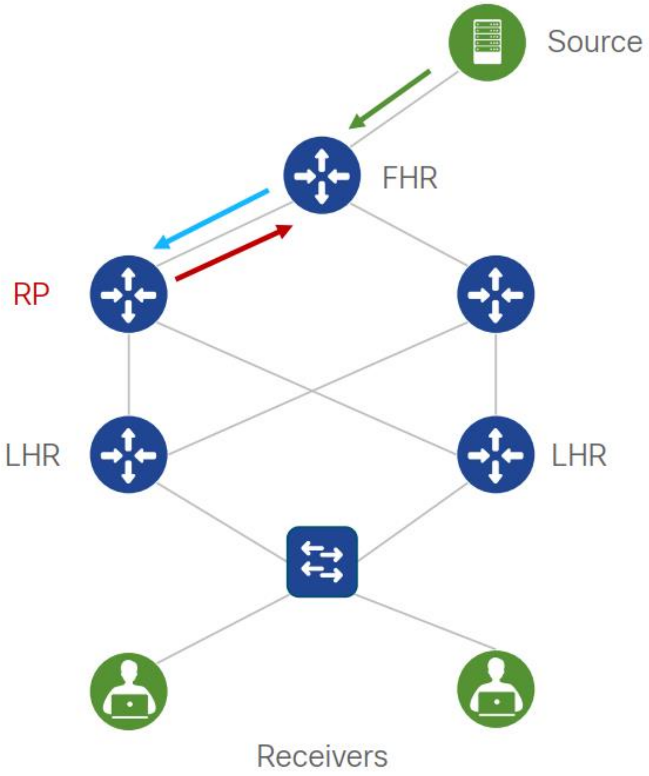
- Used in scenarios where receivers do not know the sources sending to a multicast group.
- ASM is the only option in IGMP version 1 and 2. It is also supported in IGMP version 3.
- Multicast devices must learn which sources are sending to multicast group in order to forward packets to receivers.
- In ASM we need a Rendezvous Point(s)!



ASM basic workflow

Source starts sending multicast stream

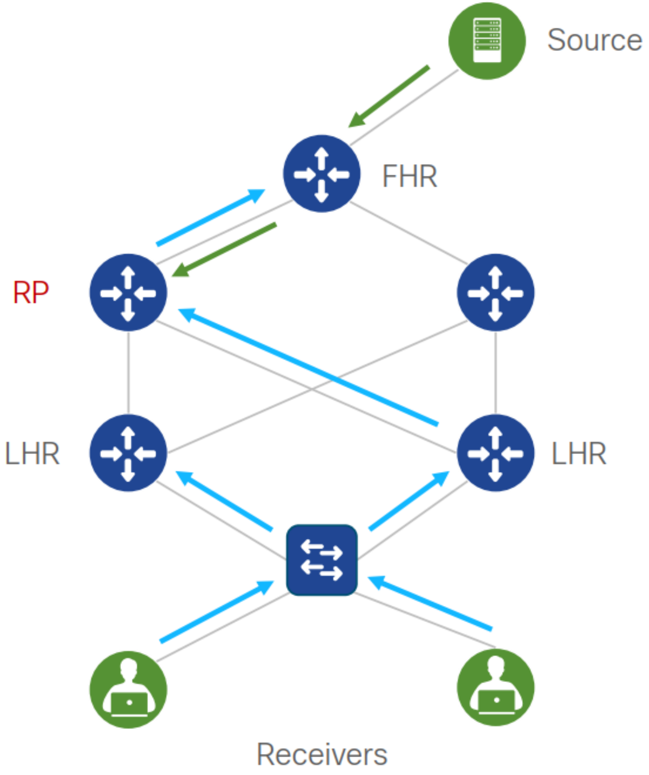
- Source starts sending traffic to a multicast group. It reaches FHR first.
- FHR sends a PIM Register unicast packet encapsulated in PIM Tunnel to RP.
- At this point the multicast traffic is being sent in unicast tunneling to RP.
- What happens next depends if receivers requested a multicast stream. If there are no receivers yet, RP sends PIM Register Stop message up to FHR and waits.



ASM basic workflow

Receivers signal interest in multicast group

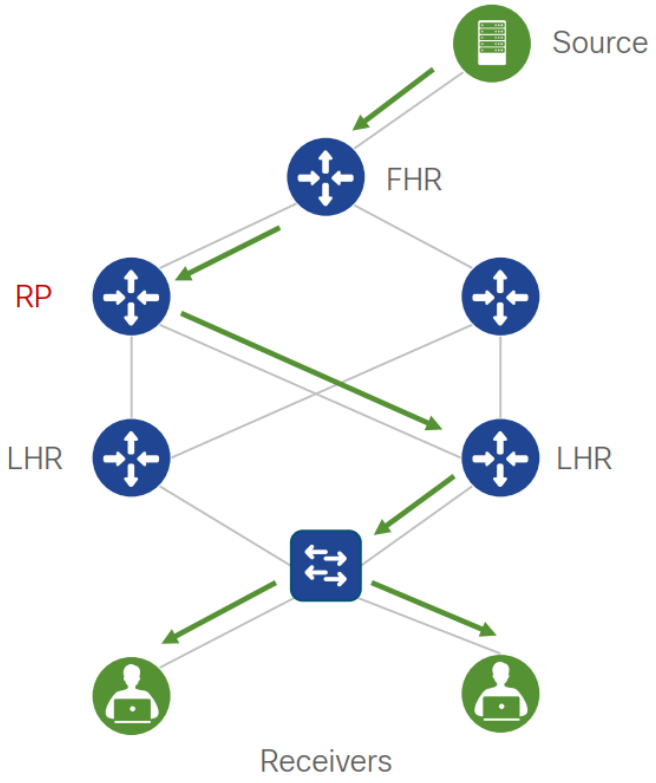
- Receivers request multicast stream by sending IGMP Join messages to the segment
- Designated multicast router for this segment (DR) sends PIM Join (*,G) to RP.
- RP sends a PIM Join message to FHR to request a stream. FHR adds to OIL interface facing RP and forwards traffic.
- Shared Tree (RPT) is now ready, so multicast stream can be forwarded down to receivers.



ASM basic workflow

Multicast traffic forwarded through RPT

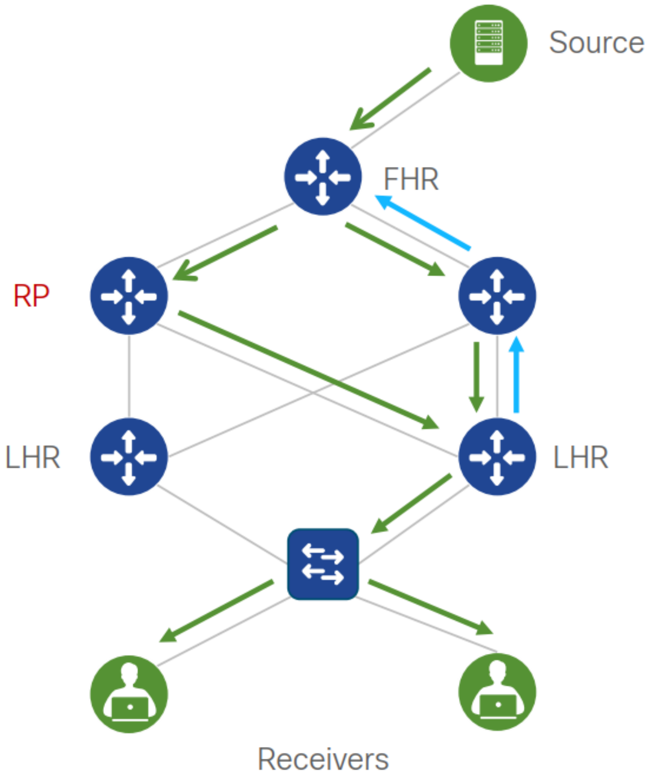
- Multicast traffic flows down through RPT following OIL on all multicast devices.
- Once multicast stream hits LHR, it learns about multicast source!
- While traffic flows to receivers, LHR now starts building a separate PIM Join (S,G) directly to the source.



ASM basic workflow

Building Shortest Path Tree (SPT)

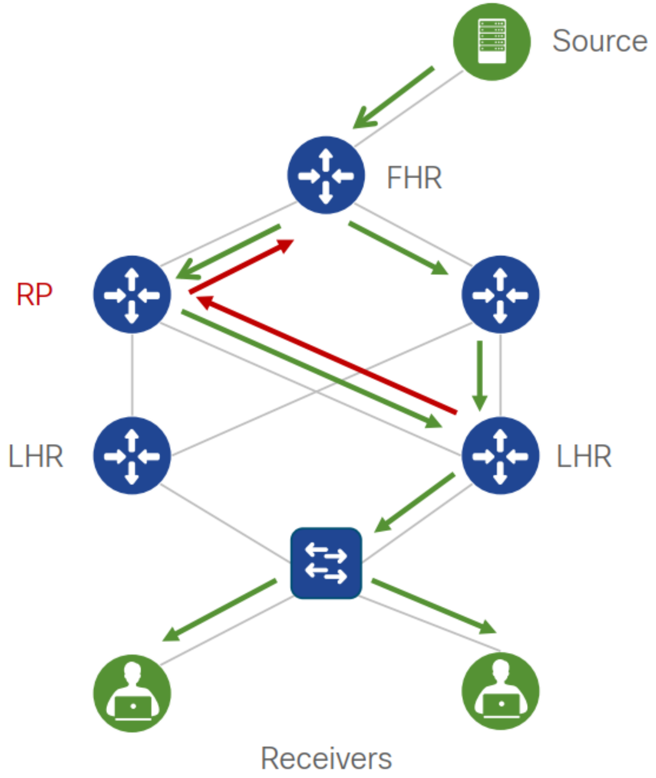
- LHR sends new PIM Join towards multicast source.
- FHR adds interface towards LHR to OIL and traffic starts flowing down OIL to LHR.
- LHR now has two multicast streams…



ASM basic workflow

Switching to Shortest Path Tree (SPT) !

- LHR sends a PIM Prune message to the RP for the (*,G) entry.
- RP removes the interface facing LHR from OIL and stops delivering traffic.
- If there are no other OIL built for that (S,G) then the RP will prune itself.
- We've got only SPT left.



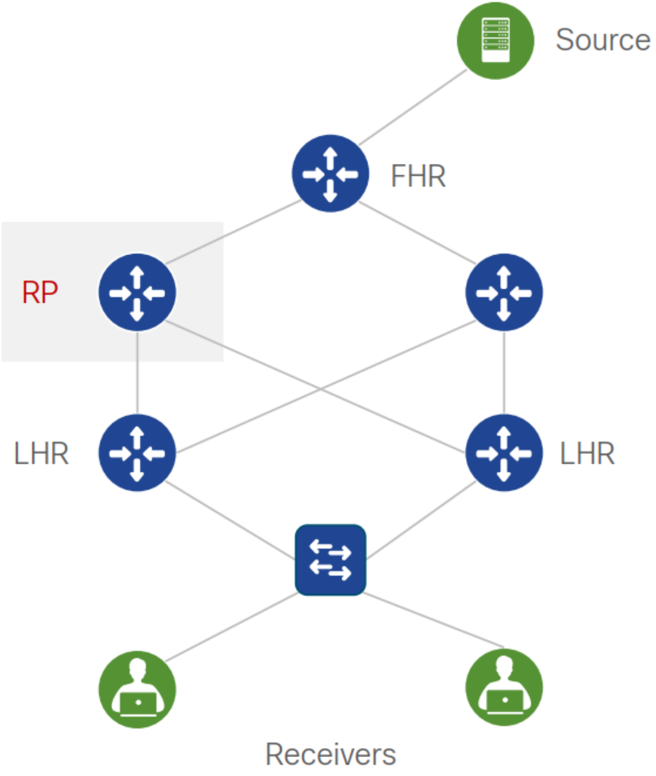
A closer look on the RP

Purpose:

- Helps to build SPT between a Source and Receivers.

Problems:

- How do all multicast devices agree on which one is the RP?
- If the RP fails in ASM, multicast traffic will fail unless already on SPT. How can we provide redundancy?



A closer look on the RP

Three ways to solve both problems

AutoRP (kind of old way)

- uses concept of Mapping Agent and Candidate RPs
- two dedicated multicast group used (224.0.1.39, 224.0.1.40)

BSR (better way)

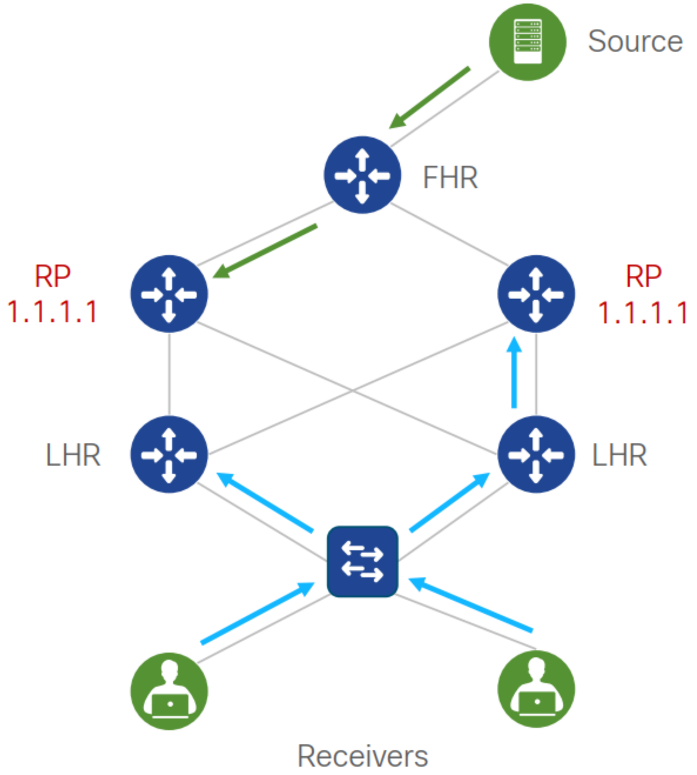
- uses concept of Candidate BSR and Candidate RP
- uses All PIM Routers multicast group (224.0.0.13)

Anycast RP (smart approach)

- advertise same RP IP address from multiple devices
- all multicast routers knows RP via any method (Static, BSR, AutoRP)

ASM with Anycast RP

- Source starts sending multicast. FHR sends a PIM Register unicast message encapsulated in PIM tunnel to one of RPs.
- Receivers request multicast stream by sending IGMP Join Message to the segment.
- DR sends PIM Join (*,G) to RP based on routing table / load-balancing algorithm.
- What if RP node which received PIM Join (*,G) doesn't have a knowledge about the source !?



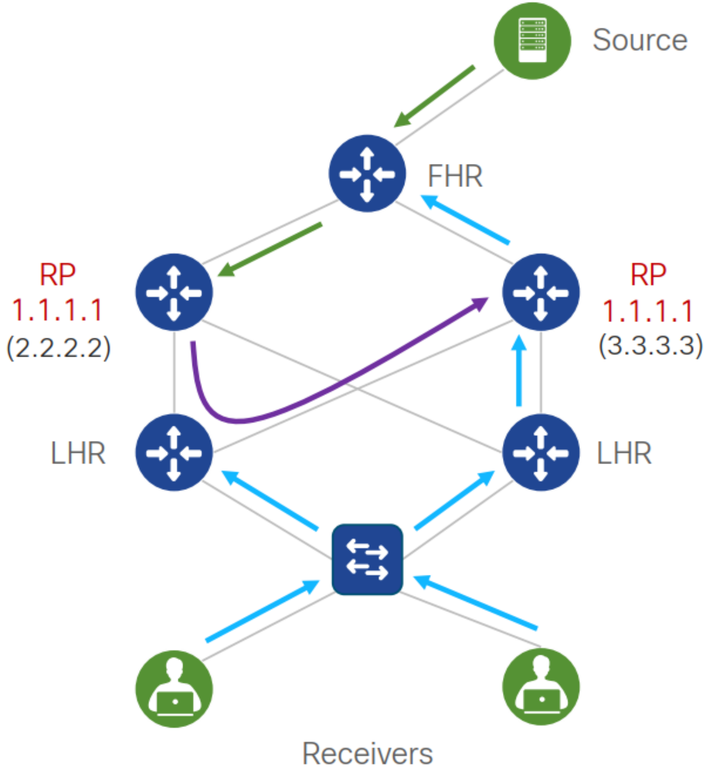
ASM with Anycast RP

Introducing Multicast Source Discovery Protocol (MSDP)

- Uses unique interfaces to exchange messages between Anycast RPs.

- When any RP receives PIM Register, sends MSDP SA message to the peer.

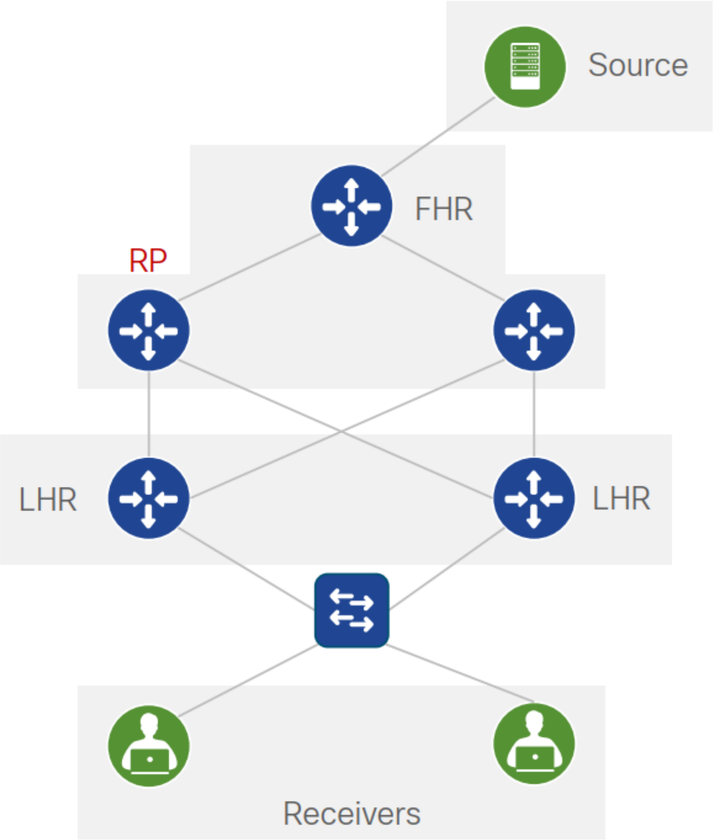
- MSDP Source Active message contains the IP of source and group address, if another RP has active PIM Joins and OIL for this group, it triggers that RP to build PIM Join to source.



BiDirectional PIM

Many-to-Many Multicast Solution

- Multicast could require immense state tracking – for each source there is tracked multicast (S,G) pair
- BiDir PIM solves this by eliminating source rivers altogether – this means RP is always in the data plane
- The RPF Check is eliminated. Instead each segment determines who will forward traffic by electing Designated Forwarder – similar to Spanning Tree



Agenda

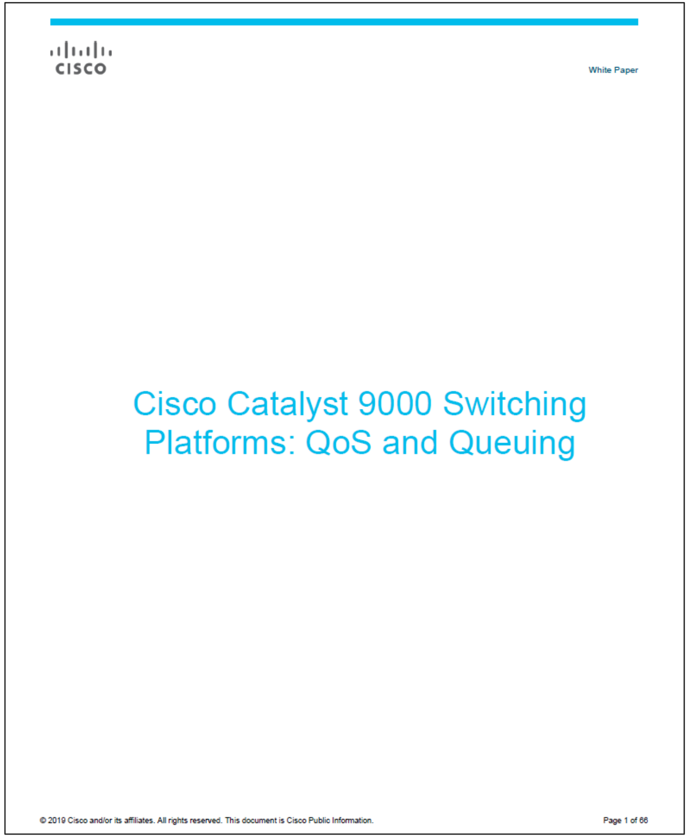
- Where to Begin?
- Campus LAN QoS Design Considerations and Best Practices
    - Cisco Catalyst 2960-X / 3560-X / 3750-X QoS Design
    - Cisco Catalyst 9000 / 3850 / 3650 Series QoS Design
- MLS to MQC Migration
- Multicast for modern tasks
- Summary and References

Summary and References

Recommended Reading

Cisco Catalyst 9000 Switching Platforms: QoS and Queuing

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



White Paper

Cisco Catalyst 9000 Switching Platforms: QoS and Queuing

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

Page 1 of 66

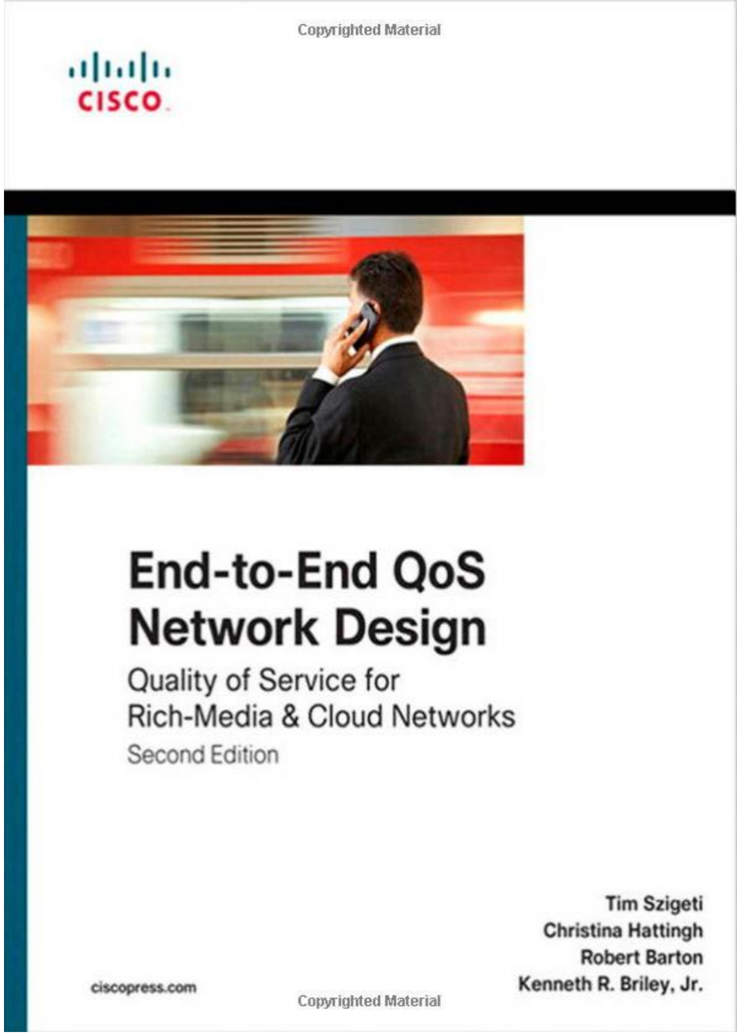
Campus QoS Design 4.0–In-Depth

Comprehensive Design Chapters

- Enterprise Quality of Service Design 4.0
  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html
- Campus QoS Design 4.0
  http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html
- Multicast useful links
  https://www.cisco.com/c/en/us/tech/ip/ip-multicast/index.html

Recommended Reading
End-to-End QoS (v2)

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



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

Thank you