# Strategic QoS Design

At-A-Glance

## The Quality of Service Challenge

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

## Step 1: Articulate Business Intent and Application Relevance

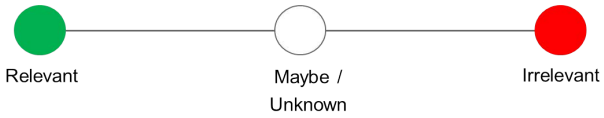
The first step may seem obvious and superfluous, but in actuality it is crucial: clearly define the business objectives that your QoS policies are to enable. These may include any/all of the following:

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

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

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

**Figure 1 Determining Application Business Relevance**




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

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

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

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

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

**Figure 2 Cisco (RFC 4594-Based) QoS Recommendations**

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

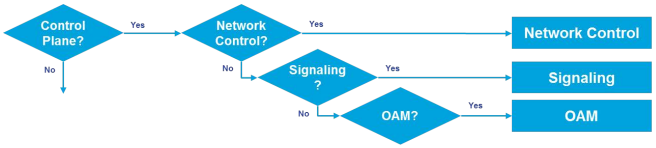
RFC 4594 also provides some application classification rules to help network architects to assign applications to the optimal traffic classes; these are summarized in the following sections:

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

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

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

**Figure 3 Control Plane Traffic Classes**




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

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

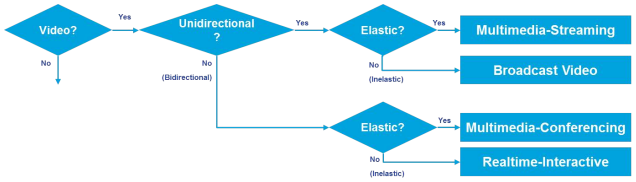
- **Operations/Administration/Management (OAM)**—This traffic class is intended for network operations, administration, and management traffic. This class is critical to the ongoing maintenance and support of the network. Traffic in this class should be marked CS2 and provisioned with a (moderate, but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

Provisioning for voice is relatively straightforward:

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

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

**Figure 4 Video Traffic Classes**




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

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

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

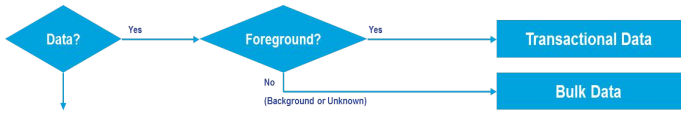
• **Broadcast Video**—This traffic class is intended for broadcast TV, live events, video surveillance flows, and similar "inelastic" streaming video flows Traffic in this class should be marked Class Selector 5 (CS5) and may be provisioned with an EF PHB; as such, admission to this class should be controlled.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

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

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

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

**Figure 5 Data Traffic Classes**




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

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

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

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

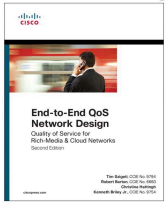
• **Bulk Data**—This traffic class is intended for non-interactive "background" data applications Traffic in this class should be marked AF Class 1 (AF11) and should be provisioned with a dedicated bandwidth queue with DSCP-WRED enabled. This traffic class may be subject to policing and re-marking. Example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

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

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

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

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



# Tactical QoS Design

At-A-Glance

## Translating QoS Strategy into Tactical Designs

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

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

- hardware constraints
- software constraints
- media capability constraints
- bandwidth constraints
- service provider constraints

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

Additional recommendations to keep in mind during the tactical design phase are to:

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

## QoS Design Recommendations:

### 1) Hardware vs. Software Best Practices

Some Cisco routers (such as Cisco ISRs) perform QoS in software, which places incremental loads on the CPU. The actual incremental load will depend on the numerous factors, including: the complexity and functionality of the policy, the volume and composition of the traffic, the speed of the interface, the speed of the CPU, the memory of the router, etc.

On the other hand, other devices (such as Cisco Catalyst switches) perform QoS in dedicated hardware Application Specific Integrated Circuits (ASICs). As such, these switches can perform even the most complex QoS policy on maximum traffic loads at line rates on GE/10GE/40GE/100GE interfaces—all without any marginal CPU tax.

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

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

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

### 2) Classification and Marking Best Practices

When classifying and marking traffic, a recommended design best practice is to classify and mark applications as close to their sources as technically and administratively feasible. This principle promotes end-to-end Differentiated Services and Per-Hop Behaviors.

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

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

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

### 3) Policing and Remarking Best Practices

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

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

### 4) Queuing and Dropping Best Practices

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

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

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

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

Cisco offers design recommendations for each of these types of queues. These queuing best practices are illustrated in Figure 1.

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

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

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

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

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

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

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

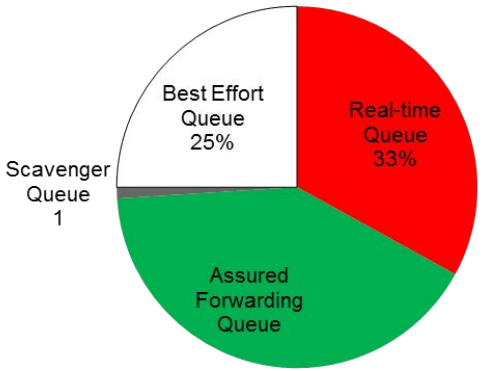
The **Best Effort Queue** is the default treatment for all traffic that has not been explicitly assigned to another queue. Only if an application has been selected for preferential/deferential treatment is it removed from the default class. Because most enterprises have several thousand applications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

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

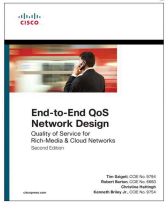
Whenever the **Scavenger Queue** is enabled, it should be assigned a ***minimal amount of bandwidth, such as 1%*** (or whatever the minimal bandwidth allocation that the platform supports).

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

**Figure 1 Queuing Best Practices**




For more details, see:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSIntro_40.html
And the Cisco Press Book: **End-to-End QoS Network Design** (Second Edition)-Chapter 11



# Cisco NBAR2 QoS 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.

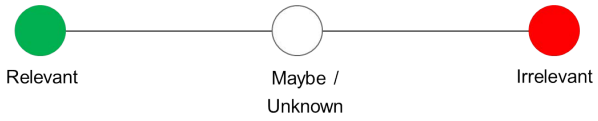
To assist in policy-definition and in browsing the application library, applications are grouped into categories and sub-categories. For example, NBAR application categories include:

- browsing
- business-and-productivity-tools
- email
- file-sharing
- gaming
- industrial-protocols
- instant-messaging
- internet-privacy
- layer3-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-relevancy setting to align with their objectives.

A **business-irrelevant** application is intended for a RFC 3662 “Scavenger” treatment. An application with a business-relevancy 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 |
| real-time-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 straighforward and user-intuitive syntax, as is shown on the reverse.

**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
```

**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 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
```

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

```
service-policy input MARKING
```

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

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

At-A-Glance

## The Role of DNS-AS

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

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

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

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

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

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

Consider two main DNS-AS use-cases:

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

### Identifying Internal Applications

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

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

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

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

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

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

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

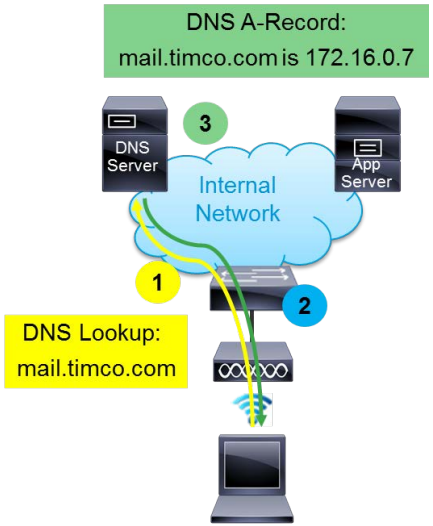
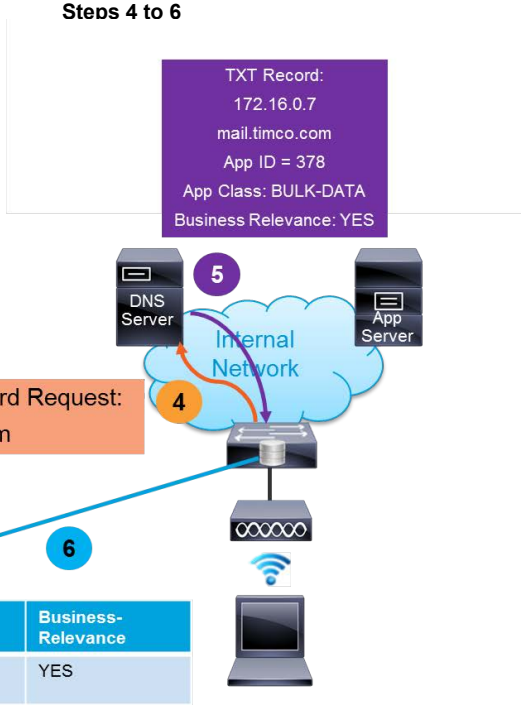



**Figure 2 DNS-AS Identification of Internal Applications-Steps 4 to 6**




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

### Identifying External Applications

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

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

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

**A) On the first flow:**

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

**B) On subsequent flows:**

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

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

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

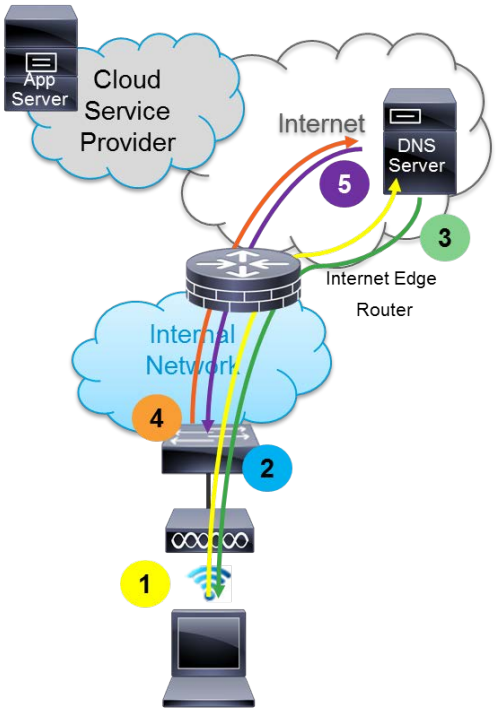



**Figure 4 DNS-AS Identification of External Applications- Steps 6 and 7**

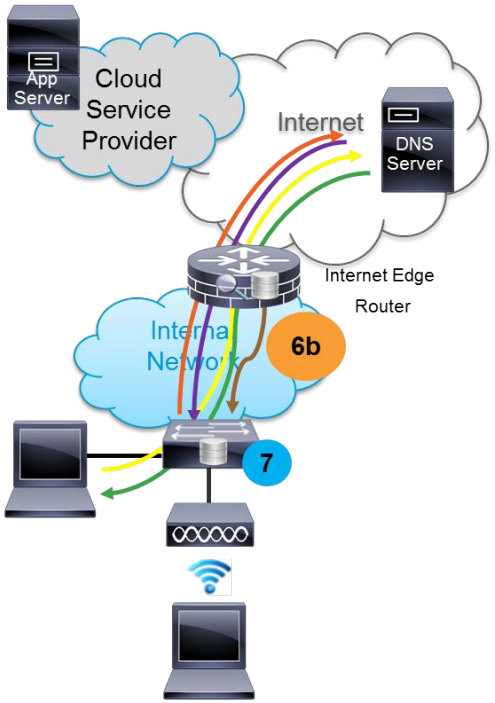
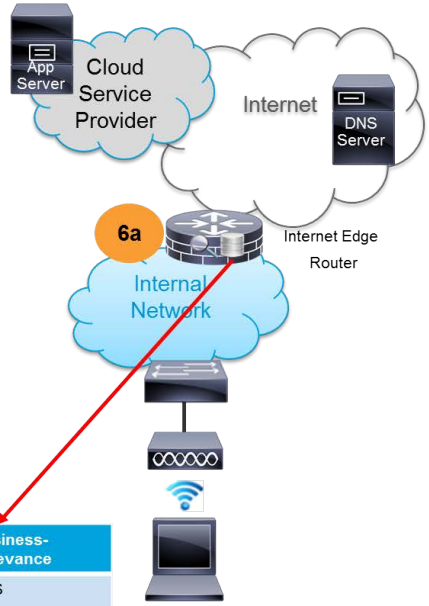



**Figure 4 DNS-AS Identification of External Applications- Step 6a**




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

# Cisco APIC-EM QoS



## The Roles of APIC-EM QoS

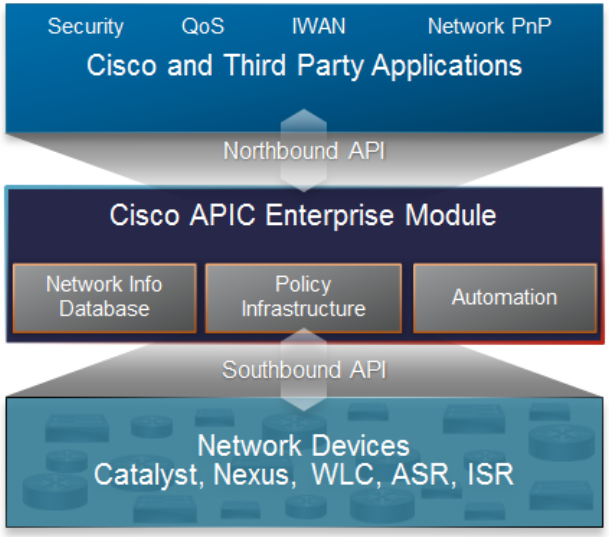
QoS is one of the most widely-deployed technologies in the enterprise and needs to be deployed in a holistic, integrated, end-to-end manner to ensure maximum effectiveness. As such, it is a prime candidate technology to showcase the value-add of Software Defined Networking (SDN), which allows for:

- 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 a end-to-end strategy that is to be deployed across ***all*** network devices in a consistent manner.

### Abstracting Platform-Specific Implementation Details

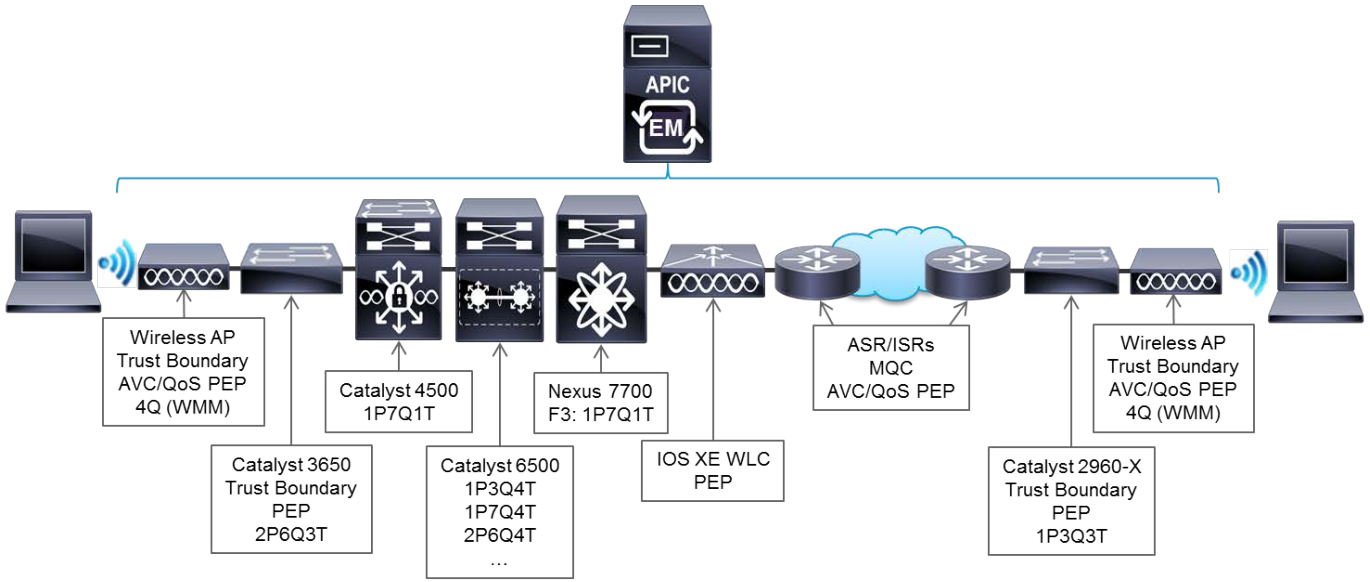
With a central QoS strategy defined, the controller can then apply Cisco Validated Design (CVD) best-practices to translate the policy to device-specific configurations, which it then pushes down to all network devices via (Southbound) APIs, as shown in Figure 2.

In this manner, device-specific details are completely abstracted from the network operator, who can thus focus on business objectives and results.

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***.

**Figure 2 APIC-EM Adaption of Business Intent QoS Policies to Platform-Specific Capabilities and Constraints**



### 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 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)**

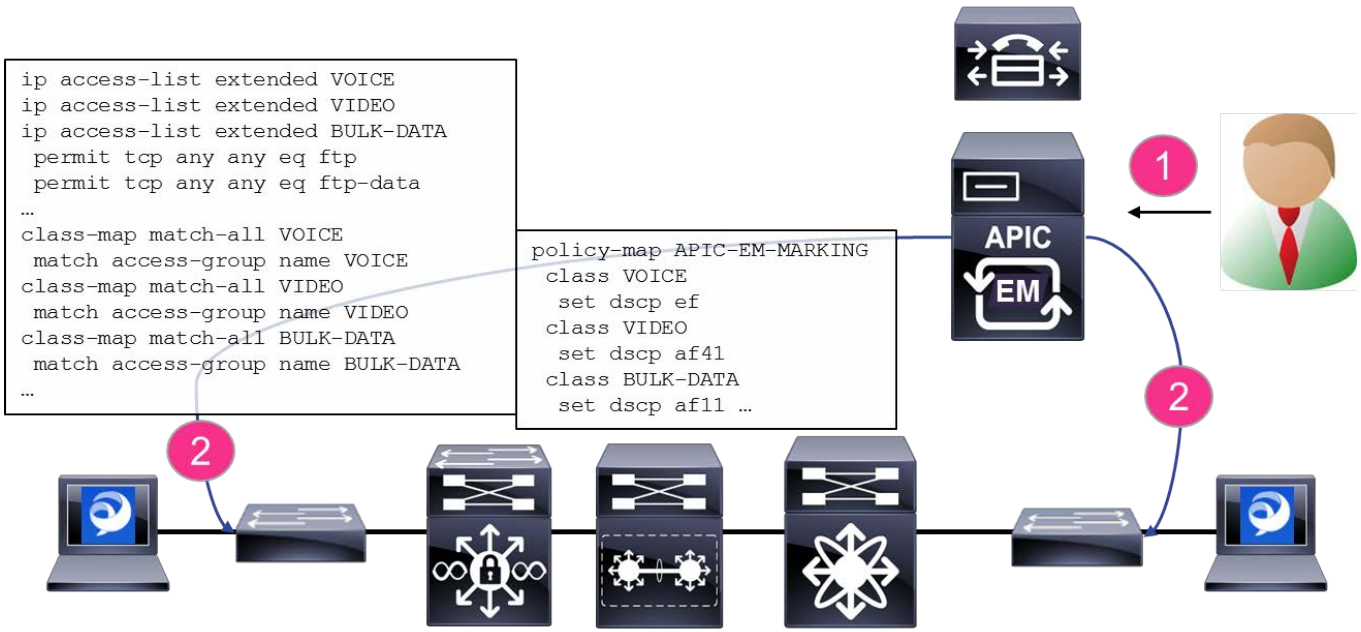
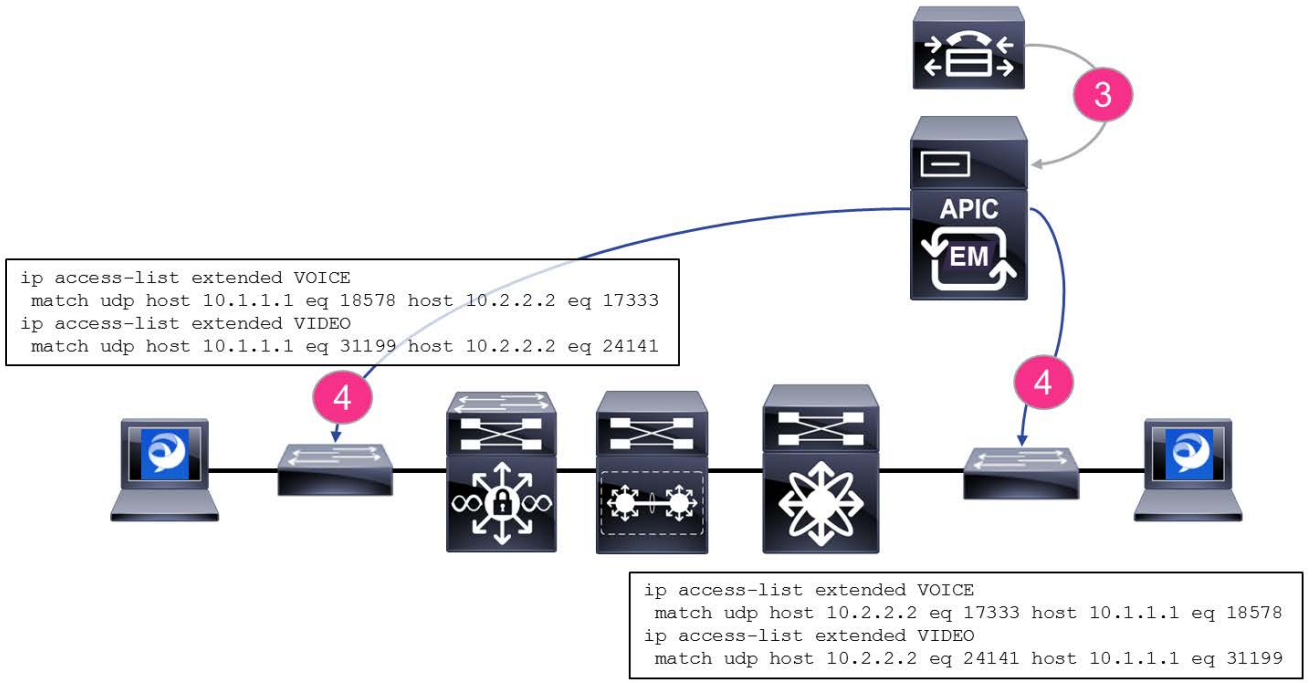



**Figure 4 APIC-EM Dynamic QoS Policies - Steps 3 (APIC-EM is Informed of a Proceeding Call) and 4 (Dynamic ACEs are Pushed)**



# Intelligent WAN QoS Design



## Deploying Cisco IWAN QoS

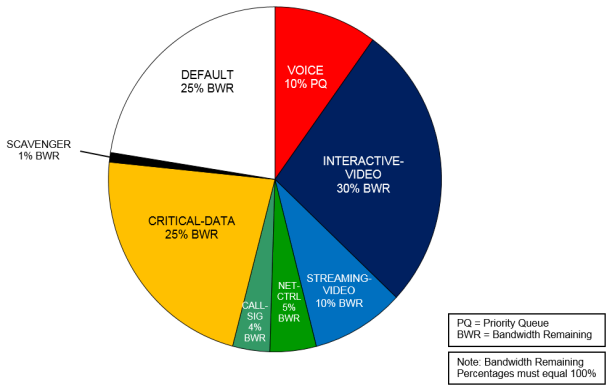
Quality of Service (QoS) has already proven itself as the enabling technology for the convergence of voice, video, and data networks. As business needs evolve, so do demands on QoS technologies. The need to protect voice, video, and critical data with QoS mechanisms is extremely important on the WAN 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 of the traffic is put into class-based weighted fair queues. The bandwidth remaining percentages must equal 100%.

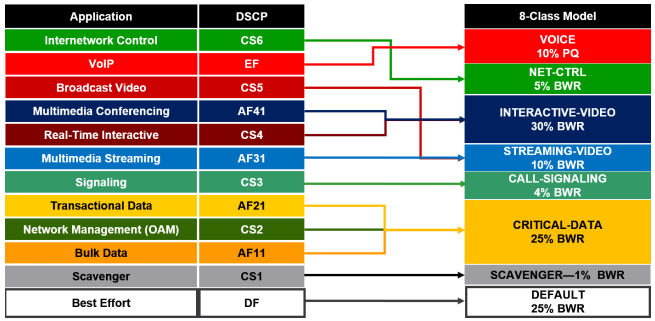
The values used below are a good starting point, but the final numbers should be based on an analysis of your traffic patterns over a period of time.

**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. Combining 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**

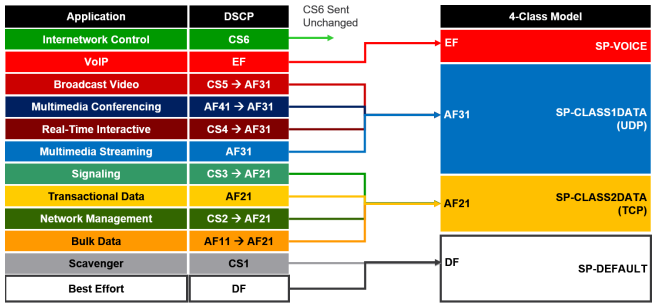



The 12-class view should always be preserved across the Enterprise even though we treat it differently at the egress of the router and send it to different channels in the service provider network.

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**

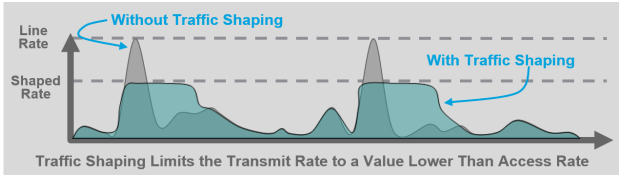



When the access rate of an interface is different from the service rate, traffic shapers are used to limit the transmit rate. A shaper will guarantee that traffic will not exceed the contracted rate. A nested queuing policy will force queuing to engage at the contracted sub-line rate to prioritize packets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

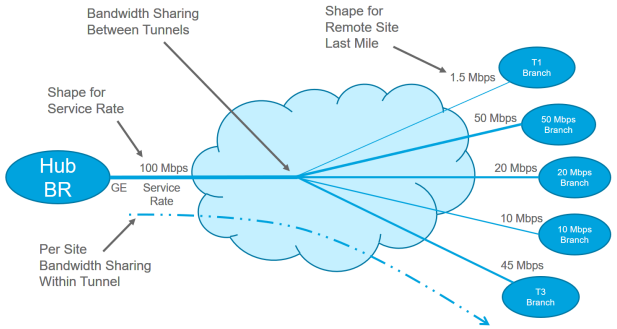
**Figure 4 Traffic Shaping**




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**



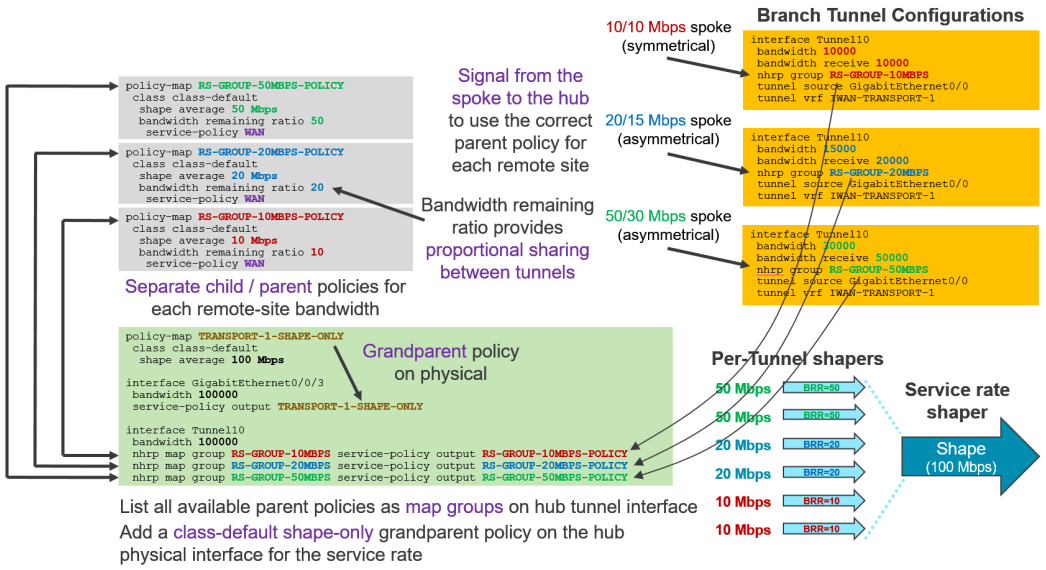
### Implementing 8-class Egress Queuing and 4-class SP Mapping

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

**Class-map for 8-class QoS Model**

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

### Implementing DMVPN Per Tunnel QoS




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

```
policy-map WAN
 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
  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
```

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

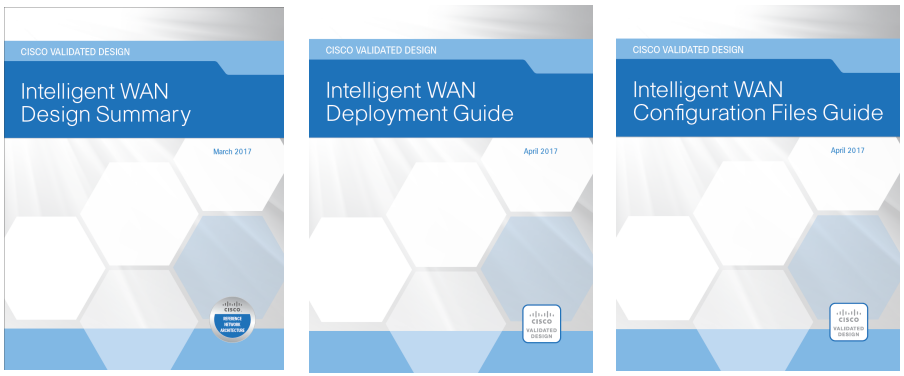
```
policy-map WAN
 class INTERACTIVE-VIDEO
  bandwidth remaining percent 30
  random-detect dscp-based
  set dscp af31
 class STREAMING-VIDEO
  bandwidth remaining percent 10
  random-detect dscp-based
  set dscp af31
 class NET-CTRL
  bandwidth remaining percent 5
  set dscp cs6
 class CALL-SIGNALING
  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 tunnel default
```

1. On the hub border router, create the child and parent shaper policies for each remote site bandwidth type using the policy-map for the service provider.
2. List the available policies as nhrp map groups on the hub tunnel interfaces.
3. Create a "shape only" grandparent policy and apply it on the hub outbound physical interface.
4. On the remote site router, signal from the spoke to the hub using the nhrp 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 Deployment 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 and Internet Edge: http://www.cisco.com/go/cvd/wan



# Campus QoS Design



## The Case for QoS in Campus Networks

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

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

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

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

## Campus QoS Design Considerations

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

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

### Global Default QoS Setting

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

### Trust States

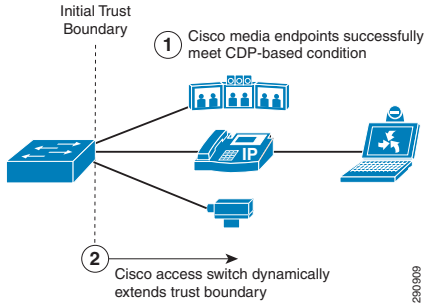
A switch port that is set to trust will accept and preserve either Layer 2 or Layer 3 packet markings. There are four static trust states with which a switch port may be configured:

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

### Conditional Trust

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

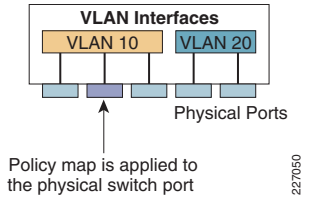
**Figure 1 Conditional Trust Operation**




### Per-Port QoS

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

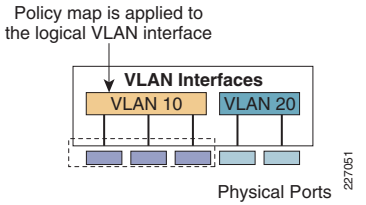
**Figure 2 Port-Based QoS**




### Per-VLAN QoS

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

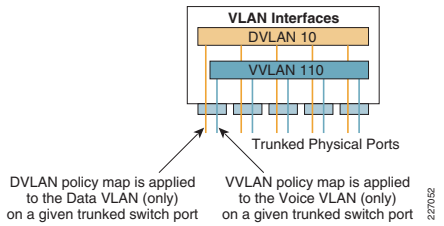
**Figure 3 VLAN-Based QoS**




### Per-Port/Per-VLAN QoS

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

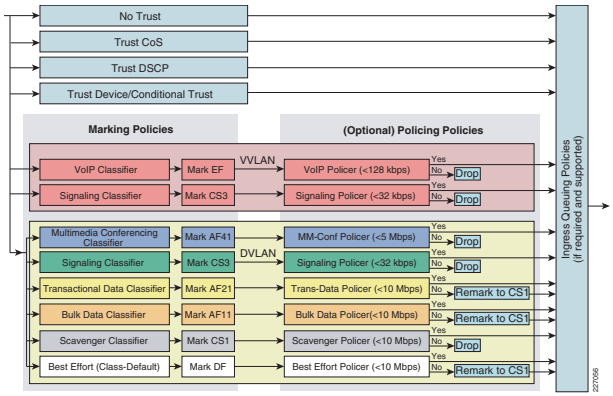
**Figure 4 Per-Port-Per-VLAN-Based QoS**




### Ingress QoS Models

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

**Figure 5 Ingress QoS Models**




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

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

Combinations of these may be used at the same time

## Egress QoS Models

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

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

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

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

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

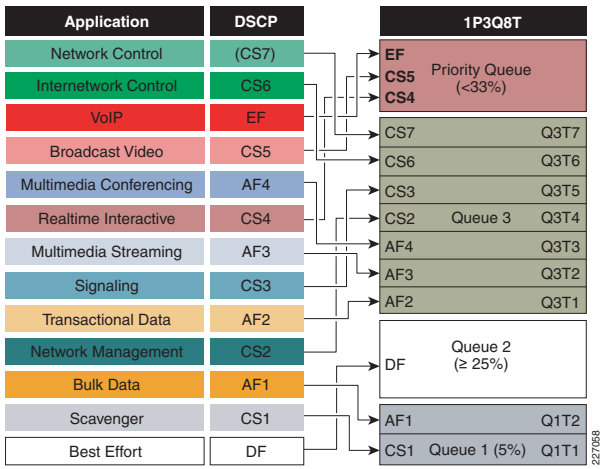
- Realtime queue should not exceed 33% BW
- Default queue should be at least 25% BW
- Bulk/scavenger queue should not exceed 5% BW

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

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

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

**Figure 6 An Egress Queuing Example Model**




## EtherChannel QoS

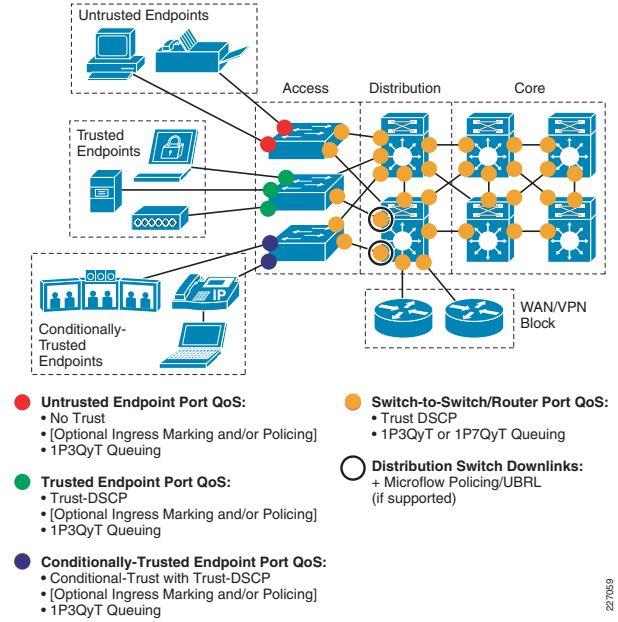
On some platforms ingress QoS policies (such as DSCP trust) are applied on the logical Port-Channel interface; however, on all platforms egress QoS policies (such as queuing policies) are always applied to the physical port-member interfaces.

## QoS Roles in a Campus

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

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

**Figure 7 Campus Port QoS Roles**

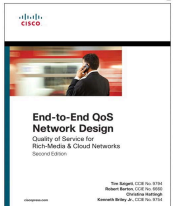



## AutoQoS

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

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

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



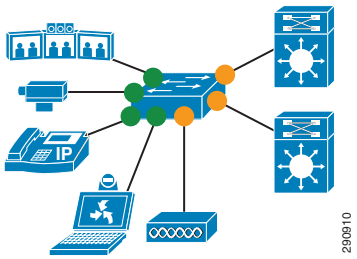
# Cisco Catalyst 2960-X QoS Design

At-A-Glance

## Role in Campus Network

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

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




## QoS Design Steps

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

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

### Step 1: Globally Enable QoS

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

### Step 2: Configure Ingress QoS Model(s)

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

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

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

*Trust DSCP Model*

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

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

*Conditional Trust Model*

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

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

*Service Policy Models*

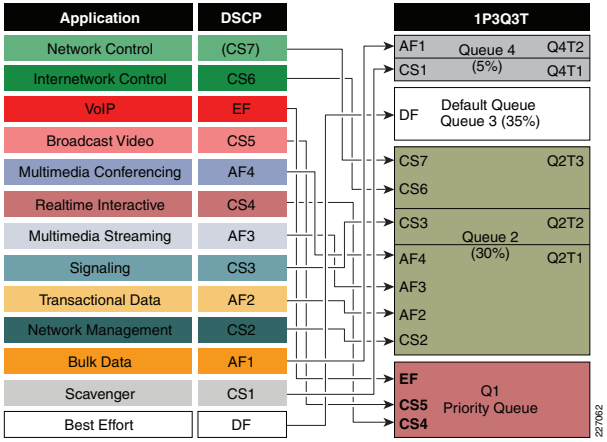
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

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

### Step 3: Configure Egress Queuing

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

**Figure 2 Catalyst 2960-X Egress Queuing Model**




## EtherChannel QoS

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

## Cisco Validated Design

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

**Step 1: Enable QoS:**

```
mls qos
```

**Step 2: Configure Ingress QoS Model :**

**Trust DSCP Model :**

```
mls qos trust dscp
```

**Conditional Trust Model :**

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

**Service Policy Models :**

```
[class-maps omitted for brevity]

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

service-policy input MARKING-POLICY
```

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

**Step 3 : Configure Egress Queuing**

```
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 100 100 400
```

Egress Queue and Threshold Tuning

```
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
```

Egress CoS-to-Queue Mapping

```
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
```

Egress DSCP-to-Queue Mapping

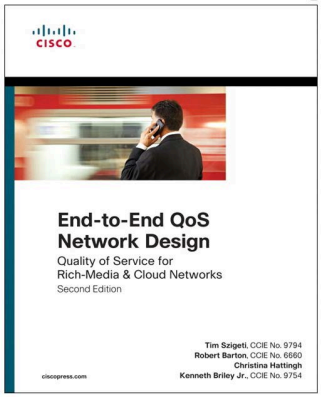
```
queue-set 1
srr-queue bandwidth share 1 30 35 5
priority-queue out
```

Egress Queuing Interface-Specific Commands

290911

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

For more details, see Campus QoS Design 4.0:
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html
And the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 14



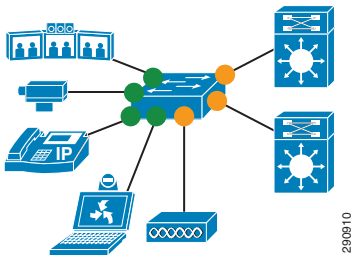
# Cisco Catalyst 3560-X/3750-X QoS Design

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 Ingress Queuing
4. Configure Egress Queuing

### Step 1: Globally Enable QoS

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

### Step 2: Configure Ingress QoS Model(s)

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

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

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

*Trust DSCP Model*

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

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

*Conditional Trust Model*

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

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

*Service Policy Models*

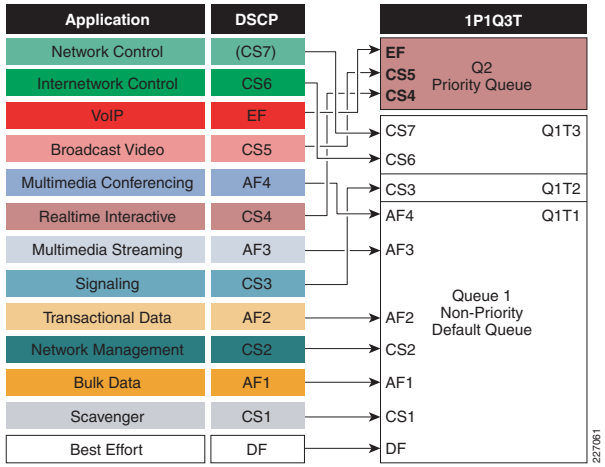
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC-based policies to implement classification, marking, and/or policing policies. These policies are constructed with:

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

### Step 3: Configure Ingress Queuing

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

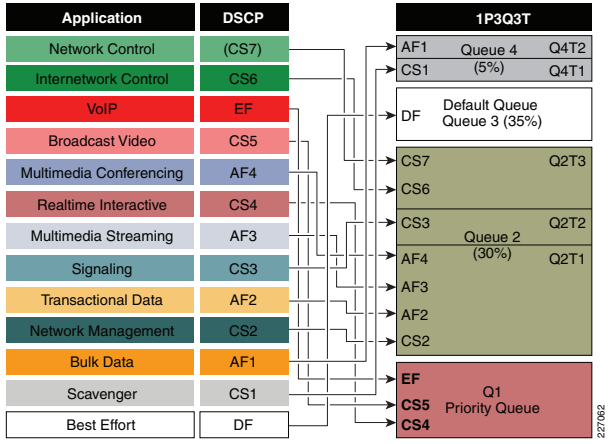
**Figure 2 Catalyst 3560-X/3750-X Ingress Queuing Model**




### Step 4: Configure Egress Queuing

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

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



## EtherChannel QoS

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

## Cisco Validated Design

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

**Step 1: Enable QoS:**

```
mls qos
```

**Step 2: Configure Ingress QoS Model :**

**Trust DSCP Model :**

```
mls qos trust dscp
```

**Conditional Trust Model :**

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

**Service Policy Models :**

```
[class-maps omitted for brevity]

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

service-policy input MARKING-POLICY
```

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

**Step 3 :Configure Ingress Queuing**

```
mls qos srr-queue input priority-queue 2 bandwidth 30
mls qos srr-queue input bandwidth 70 30
mls qos srr-queue input buffers 90 10
mls qos srr-queue input threshold 1 80 90
```

Ingress Queue and Threshold Tuning

```
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
```

Ingress CoS-to-Queue Mapping

```
mls qos srr-queue input dscp-map queue 1 threshold 1 0 8 10 12 14
mls qos srr-queue input dscp-map queue 1 threshold 1 16 18 20 22
mls qos srr-queue input dscp-map queue 1 threshold 1 26 28 30 34 36 38
mls qos srr-queue input dscp-map queue 1 threshold 2 24
mls qos srr-queue input dscp-map queue 1 threshold 3 48 56
mls qos srr-queue input dscp-map queue 2 threshold 3 32 40 46
```

Ingress DSCP-to-Queue Mapping

**Step 4 : Configure Egress Queuing**

```
mls qos queue-set output 1 buffers 15 30 35 20
mls qos queue-set output 1 threshold 1 100 100 100 100
mls qos queue-set output 1 threshold 2 80 90 100 400
mls qos queue-set output 1 threshold 3 100 100 100 400
mls qos queue-set output 1 threshold 4 60 100 100 400
```

Egress Queue and Threshold Tuning

```
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
```

Egress CoS-to-Queue Mapping

```
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
```

Egress DSCP-to-Queue Mapping

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

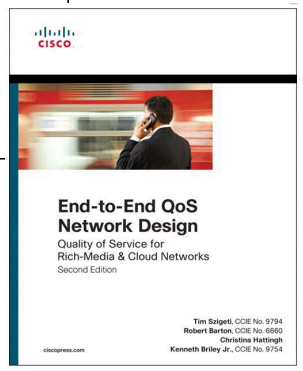
Egress Queuing Interface-Specific Commands

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

For more details, see Campus QoS Design 4.0:

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

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



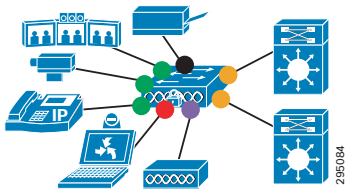
# Cisco Catalyst 3650/3850 QoS Design

At-A-Glance

## Role in Campus Network

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

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




## QoS Design Steps

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

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

### Step 1: Configure Ingress QoS Model(s)

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

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

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

*Trust DSCP Model*

Wired ports on the Catalyst 3650/3850 default to a trusted state (shown as orange circles in Figure 1). 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:

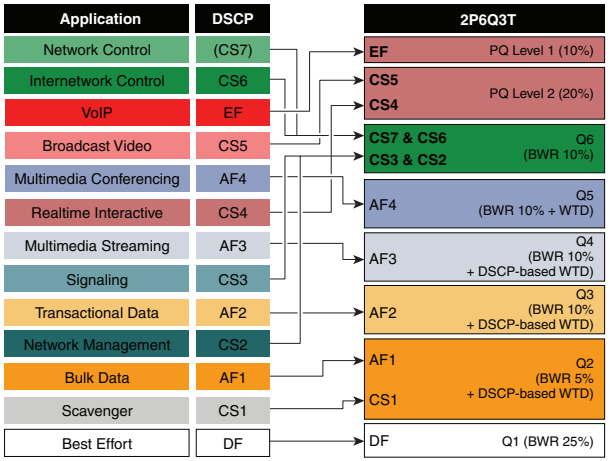
- **class-maps** which identify the flows using packet markings or by access-lists or other criteria. As of IOS XE 16.3 NBAR2 classification on wired ports is also supported.
- **policy-maps** which specify policy actions to be taken on a class-by-class basis
- **service-policy** statements which apply 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 1P7Q3T or 2P6Q3T egress queuing model. The only difference between the models is the number of priority queues configured via the **priority level 1** or **priority level 2** policy-map action commands.

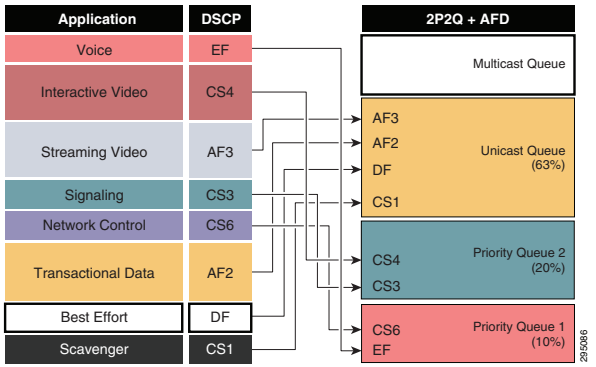
**Figure 2 Catalyst 3650/3850 2P6Q3T (Wired Port) Egress Queuing Model**




### Step 2b: Configure Egress Queuing for Wireless Ports

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

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



## 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 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
```

**Wired Port Application:**

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

**Wireless SSID Application:**

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

**Per-Wireless-Client Application:**

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

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

```
policy-map 2P6Q3T
 class VOICE-PQ1
  priority level 1
  police rate percent 10
class VIDEO-PQ2
  priority level 2
  police rate percent 20
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
  queue-limit dscp af43 percent 80
  queue-limit dscp af42 percent 90
  queue-limit dscp af41 percent 100
class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 10
queue-buffers ratio 10
  queue-limit dscp af33 percent 80
  queue-limit dscp af32 percent 90
  queue-limit dscp af31 percent 100
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 10
  queue-buffers ratio 10
  queue-limit dscp af23 percent 80
  queue-limit dscp af22 percent 90
  queue-limit dscp af21 percent 100
class SCAVENGER-BULK-DATA-QUEUE
  bandwidth remaining percent 5
  queue-buffers ratio 10
  queue-limit dscp values af13 cs1 percent 80
  queue-limit dscp values af12 percent 90
  queue-limit dscp values af11 percent 100
 class class-default
  bandwidth remaining percent 25
  queue-buffers ratio 25
```

**Wired Port Application:**

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

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

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

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

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

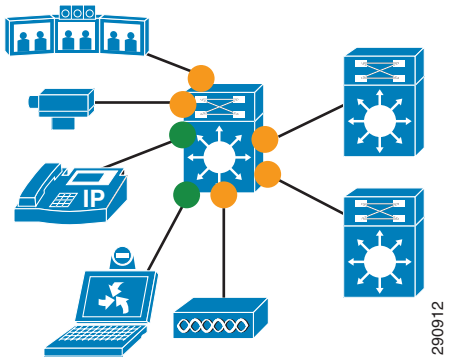
# Cisco Catalyst 4500 (Supervisor 6-E / 7-E / 8-E) QoS Design

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

*Conditional Trust Model*

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

This model is suitable for switch ports connecting to:

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

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

*Service Policy Models*

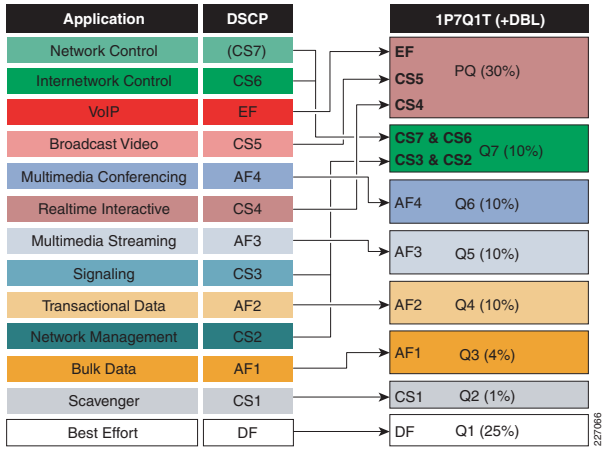
There may be cases where administrators require more detailed or granular policies on their ingress edges and as such they may construct MQC policies to implement classification, marking, and/or policing policies. These policies are constructed with:

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

### Step 2: Configure Egress Queuing

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

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




## EtherChannel QoS

Ingress QoS policies (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 simply 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
```

**Step 2 : Egress Queuing Configuration**

```
class-map match-any PRIORITY-QUEUE
 match dscp ef
 match dscp cs5
 match dscp cs4
```
Assigns VoIP (EF), Broadcast Video (CS5) and Realtime Interactive (CS4) to the PRIORITY-QUEUE

```
class-map match-any CONTROL-MGMT-QUEUE
 match dscp cs7
 match dscp cs6
 match dscp cs3
 match dscp cs2
```
Assigns Network Control (CS7), Internetwork Control (CS6), Signaling (CS3) and Management (CS2) to the CONTROL-MGMT-QUEUE

```
class-map match-all MULTIMEDIA-CONFERENCING-QUEUE
 match dscp af41 af42 af43
```
Assigns AF4 to the MULTIMEDIA-CONFERENCING-QUEUE

```
class-map match-all MULTIMEDIA-STREAMING-QUEUE
 match dscp af31 af32 af33
```
Assigns AF3 to the MULTIMEDIA-STREAMING-QUEUE

```
class-map match-all TRANSACTIONAL-DATA-QUEUE
 match dscp af21 af22 af23
```
Assigns AF2 to the TRANSACTIONAL-DATA-QUEUE

```
class-map match-all BULK-DATA-QUEUE
 match dscp af11 af12 af13
```
Assigns AF1 to the BULK-DATA-QUEUE

```
class-map match-all SCAVENGER-QUEUE
 match dscp cs1
```
Assigns CS1 to the SCAVENGER-QUEUE

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

```
 class CONTROL-MGMT-QUEUE
  bandwidth remaining percent 10
```
CONTROL-MGMT-QUEUE gets 10% of remaining bandwidth

```
 class MULTIMEDIA-CONFERENCING-QUEUE
  bandwidth remaining percent 10
```
MM-CONF-QUEUE gets 10% of remaining bandwidth

```
 class MULTIMEDIA-STREAMING-QUEUE
  bandwidth remaining percent 10
```
MM-STREAMING-QUEUE gets 10% of remaining bandwidth

```
 class TRANSACTIONAL-DATA-QUEUE
  bandwidth remaining percent 10
  dbl
```
TRANS-DATA-QUEUE gets 10% of remaining bandwidth and Dynamic Buffer Limiting

```
 class BULK-DATA-QUEUE
  bandwidth remaining percent 4
  dbl
```
BULK-DATA-QUEUE gets 4% of remaining bandwidth and Dynamic Buffer Limiting

```
 class SCAVENGER-QUEUE
  bandwidth remaining percent 1
```
SCAVENGER-QUEUE is limited to 1% of remaining bandwidth

```
 class class-default
  bandwidth remaining percent 25
  dbl
```
Default (Best-Effort) queue 25% of remaining bandwidth and Dynamic Buffer Limiting

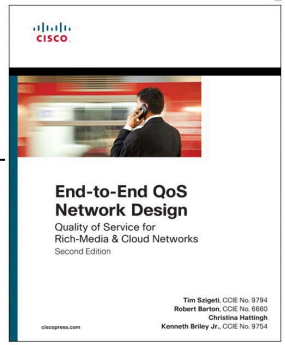
```
service-policy output EGRESS-QUEUING
```
Applies EGRESS-QUEUEING policy to interface

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

For more details, see Campus QoS Design 4.0:

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

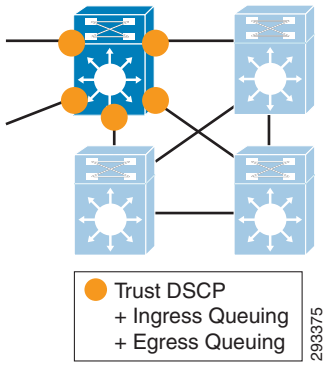
And the Cisco Press Book: **End-to-End QoS Network Design** (Second Edition)-Chapter 15



## 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

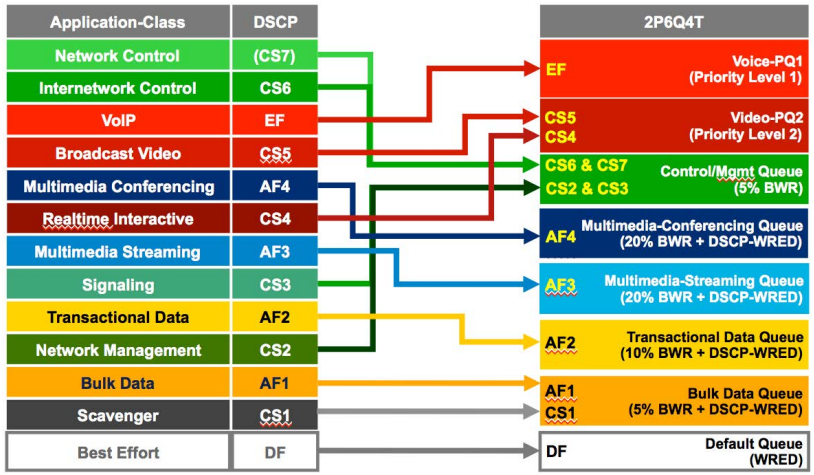
There are two main steps to configure QoS on Cisco Catalyst 6500 series switches with Supervisor 2T:

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& 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
```

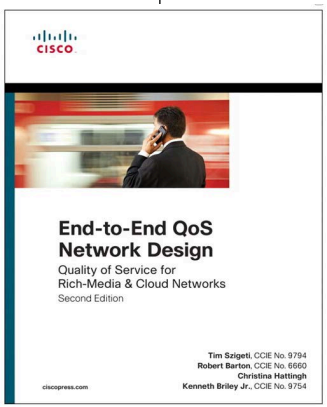
**Step 2 Configure 2P6Q4T Ingress & Egress Queuing Policy-Map and apply to Interface(s)**

```
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/QoSCampus_40.html



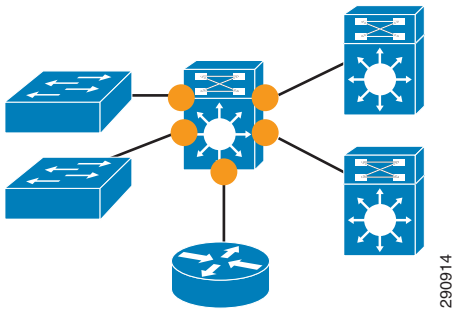
# Cisco Catalyst 6500 (Supervisor 720 / Supervisor 32) QoS Design At-A-Glance

## Role in Campus Network

The Cisco Catalyst 6500 series switches 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.

To simplify design, this document assumes the use of WS-X6716-10GE linecards.

**Figure 1 Cisco Catalyst 6500 Switches in a Campus Network**




## QoS Design Steps

There are four main steps to configure QoS on Cisco Catalyst 6500 series switches:

1. Enable QoS
2. Configure DSCP-Trust
3. Configure Ingress Queuing
4. Configure Egress Queuing

### Step 1: Globally Enable QoS

QoS is globally enabled on the Cisco Catalyst 6500 with the **mls qos** command.

### Step 2: Configure DSCP-Trust

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

Switch ports that can be set to trust DSCP are shown as yellow circles in Figure 1.

### Step 3: Configure Ingress Queuing

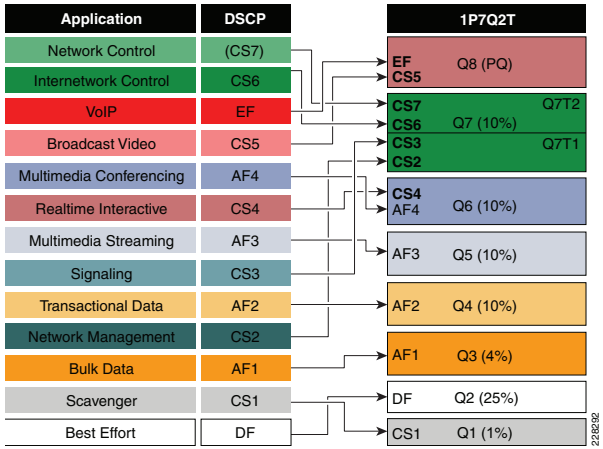
Three considerations need to be taken into account when determining if ingress queuing configuration is required on the Cisco Catalyst 6500 linecard:

- Is the linecard oversubscribed?
- Is the linecard operating in the distribution or core layers of the campus network?
- Does the linecard support DSCP-to-Queue mapping?

Ingress queuing is only recommended when the answer to all three questions is Yes.

The ingress queuing model for the Cisco Catalyst 6500 (with 6716 linecards) is shown in Figure 2.

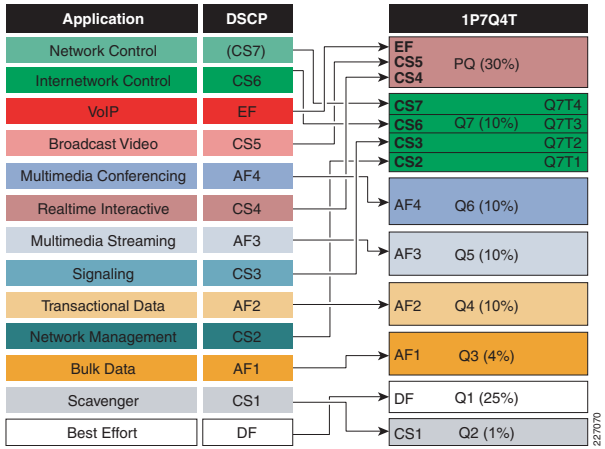
**Figure 2 Catalyst 6500 (6716) Ingress Queuing Model**




### Step 4: Configure Egress Queuing

The egress queuing model for the Cisco Catalyst 6500 (with 6708 or 6716 linecards) is shown in Figure 3.

**Figure 3 Catalyst 6500 (6716) Egress Queuing Model**




## EtherChannel QoS

Ingress QoS policies on the Cisco Catalyst 6500 are configured on the logical Port-Channel interface (typically these are simply to enable DSCP trust), while egress 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 WS-X6716-10GE linecards in the role of a distribution- or core-layer switch in a campus network is presented on the reverse.

**Step 1: Enable QoS**

```
mls qos
```

**Step 2: Configure DSCP-Trust**

```
mls qos trust dscp
```

**Step 3: Configure Ingress Queuing**

```
mls qos queue-mode mode-dscp
```
Enables DSCP-based Queue/Threshold Mapping

```
rcv-queue bandwidth 1 25 4 10 10 10 10
rcv-queue queue-limit 10 25 10 10 10 10 10
```
Ingress Queue Tuning

```
rcv-queue threshold 1 100 100
rcv-queue threshold 2 100 100
rcv-queue threshold 3 80 100
rcv-queue threshold 4 80 100
rcv-queue threshold 5 80 100
rcv-queue threshold 6 80 100
rcv-queue threshold 7 80 100
```
Ingress Threshold Tuning

```
rcv-queue dscp-map 1 2 8
rcv-queue dscp-map 2 2 0
rcv-queue dscp-map 3 1 12 14
rcv-queue dscp-map 3 2 10
rcv-queue dscp-map 4 1 20 22
rcv-queue dscp-map 4 2 18
rcv-queue dscp-map 5 1 28 30
rcv-queue dscp-map 5 2 26
rcv-queue dscp-map 6 1 36 38
rcv-queue dscp-map 6 2 32 34
rcv-queue dscp-map 7 1 16 24
rcv-queue dscp-map 7 2 48 56
```
Ingress DSCP-to-Queue/Threshold Mapping

**Step 4: Configure Egress Queuing**

```
wrr-queue queue-limit 10 25 10 10 10 10 10
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
```
Egress Queue Tuning

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

**Step 4: Configure Egress Queuing (continued)**

```
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
```
Enables WRED on Egress Queues 1-7

```
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
```
Tunes WRED on Egress Queues 1-7

```
wrr-queue dscp-map 1 1 8
wrr-queue dscp-map 2 1 0
wrr-queue dscp-map 3 1 14
wrr-queue dscp-map 3 2 12
wrr-queue dscp-map 3 3 10
wrr-queue dscp-map 4 1 22
wrr-queue dscp-map 4 2 20
wrr-queue dscp-map 4 3 18
wrr-queue dscp-map 5 1 30
wrr-queue dscp-map 5 2 28
wrr-queue dscp-map 5 3 26
wrr-queue dscp-map 6 1 38
wrr-queue dscp-map 6 2 36
wrr-queue dscp-map 6 3 34
wrr-queue dscp-map 7 1 16
wrr-queue dscp-map 7 2 24
wrr-queue dscp-map 7 3 48
wrr-queue dscp-map 7 4 56
priority-queue dscp-map 1 32 40 46
```
Egress DSCP-to-Queue/Threshold Mapping

290915

For more details, see Campus QoS Design 4.0:

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

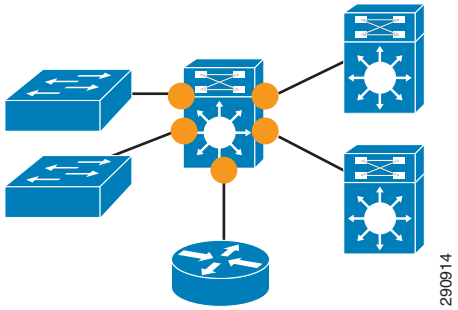
# Cisco Catalyst 6500 (Supervisor 720-10GE) QoS Design At-A-Glance

## Role in Campus Network

The Cisco Catalyst 6500 Series switches with Sup720s 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.

To simplify design, this document assumes the use of WS-X6716-10GE linecards.

**Figure 1 Cisco Catalyst 6500 Switches in a Campus Network**




## QoS Design Steps

There are four main steps to configure QoS on Cisco Catalyst 6500 series switches:

1. Enable QoS
2. Configure DSCP-Trust
3. Configure Ingress Queuing
4. Configure Egress Queuing

### Step 1: Globally Enable QoS

QoS is globally enabled on the Cisco Catalyst 6500 with the mls qos command.

### Step 2: Configure DSCP-Trust

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

Switch ports that can be set to trust DSCP are shown as yellow circles in Figure 1.

### Step 3: Configure Ingress Queuing

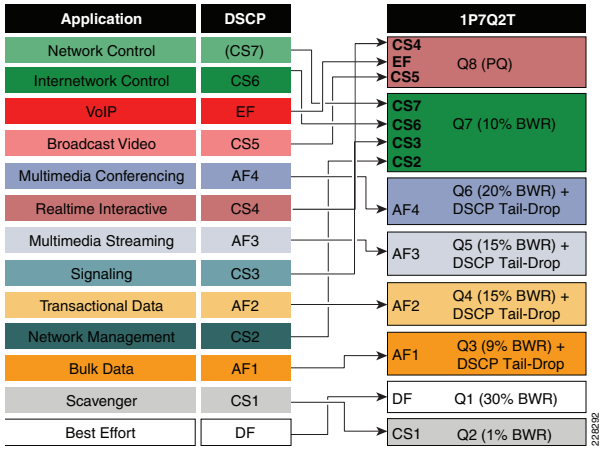
Three considerations need to be taken into account when determining if ingress queuing configuration is required on the Cisco Catalyst 6500 linecard:

- Is the linecard oversubscribed?
- Is the linecard operating in the distribution or core layers of the campus network?
- Does the linecard support DSCP-to-Queue mapping?

Ingress queuing is only recommended when the answer to all three questions is Yes.

The ingress queuing model for the Cisco Catalyst 6500 (with 6716 linecards) in oversubscription mode is shown in Figure 2.

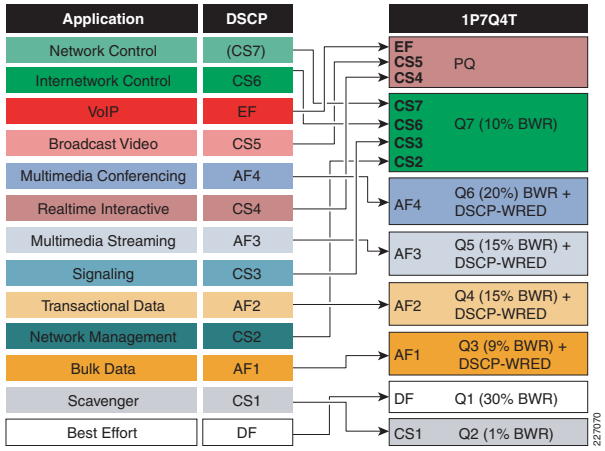
**Figure 2 Catalyst 6500 (6716) Ingress Queuing Model**




### Step 4: Configure Egress Queuing

The egress queuing model for the Cisco Catalyst 6500 (with 6708 or 6716 linecards) is shown in Figure 3.

**Figure 3 Catalyst 6500 (6716) Egress Queuing Model**




## EtherChannel QoS

Ingress classification & marking QoS policies on the Cisco Catalyst 6500 are configured on the logical Port-Channel interface (typically these are simply to enable DSCP trust). 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 WS-X6716-10GE linecards in the role of a distribution- or core-layer switch in a campus network is presented on the reverse.

**Step 1: Enable QoS**

```
mls qos
```

**Step 2: Configure DSCP-Trust**

```
mls qos trust dscp
```

**Step 3: Configure Ingress Queuing**

```
mls qos queue-mode mode-dscp
```
Enables DSCP-based Queue/Threshold Mapping

```
rcv-queue bandwidth 30 1 9 15 15 20 10
rcv-queue queue-limit 25 10 10 15 15 15 10
```
Ingress Queue Tuning

```
rcv-queue threshold 1 100 100
rcv-queue threshold 2 100 100
rcv-queue threshold 3 80 100
rcv-queue threshold 4 80 100
rcv-queue threshold 5 80 100
rcv-queue threshold 6 80 100
rcv-queue threshold 7 100 100
```
Ingress Threshold Tuning

```
rcv-queue dscp-map 1 2 0
rcv-queue dscp-map 2 2 8
rcv-queue dscp-map 3 1 12 14
rcv-queue dscp-map 3 2 10
rcv-queue dscp-map 4 1 20 22
rcv-queue dscp-map 4 2 18
rcv-queue dscp-map 5 1 28 30
rcv-queue dscp-map 5 2 26
rcv-queue dscp-map 6 1 36 38
rcv-queue dscp-map 6 2 34
rcv-queue dscp-map 7 1 16 24 48 56
rcv-queue dscp-map 7 2 48 56
priority-queue dscp-map 1 32 40 46
priority-queue queue-limit 15
```
Ingress DSCP-to-Queue/Threshold Mapping

**Step 4: Configure Egress Queuing**

```
wrr-queue queue-limit 25 10 10 10 10 10 10
wrr-queue bandwidth 30 1 9 15 15 20 10
priority-queue queue-limit 15
```
Egress Queue Tuning

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

**Step 4: Configure Egress Queuing (continued)**

```
wrr-queue random-detect 1
no wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
no wrr-queue random-detect 7
```
Enables WRED on Egress Queues 1 and 3-6

```
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 3 100 100 100 100
wrr-queue random-detect min-threshold 3 60 70 80 100
wrr-queue random-detect min-threshold 4 100 100 100 100
wrr-queue random-detect max-threshold 4 60 70 80 100
wrr-queue random-detect min-threshold 5 100 100 100 100
wrr-queue random-detect max-threshold 5 60 70 80 100
wrr-queue random-detect min-threshold 6 100 100 100 100
wrr-queue random-detect max-threshold 6 60 70 80 100
```
Tunes WRED on Egress Queues

```
wrr-queue dscp-map 1 1 0
wrr-queue dscp-map 2 1 8
wrr-queue dscp-map 3 1 14
wrr-queue dscp-map 3 2 12
wrr-queue dscp-map 3 3 10
wrr-queue dscp-map 4 1 22
wrr-queue dscp-map 4 2 20
wrr-queue dscp-map 4 3 18
wrr-queue dscp-map 5 1 30
wrr-queue dscp-map 5 2 28
wrr-queue dscp-map 5 3 26
wrr-queue dscp-map 6 1 38
wrr-queue dscp-map 6 2 36
wrr-queue dscp-map 6 3 34
wrr-queue dscp-map 7 1 16 24 48 56
priority-queue dscp-map 1 32 40 46
```
Egress DSCP-to-Queue/Threshold Mapping

290915

For more details, see Campus QoS Design 4.0:

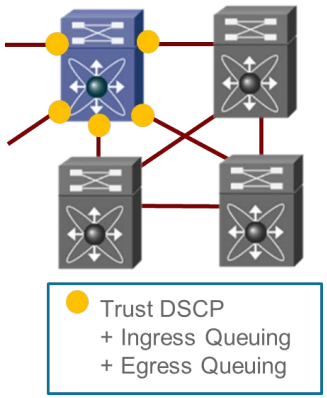
http://www.cisco.com/en/US/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND_40/QoSCampus_40.html.

# Cisco Nexus 7700 (F3 Module) Campus QoS Design

## Role in Campus Network

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

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




## QoS Design Steps

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

1. Configure Ingress Queuing
2. Configure Egress Queuing

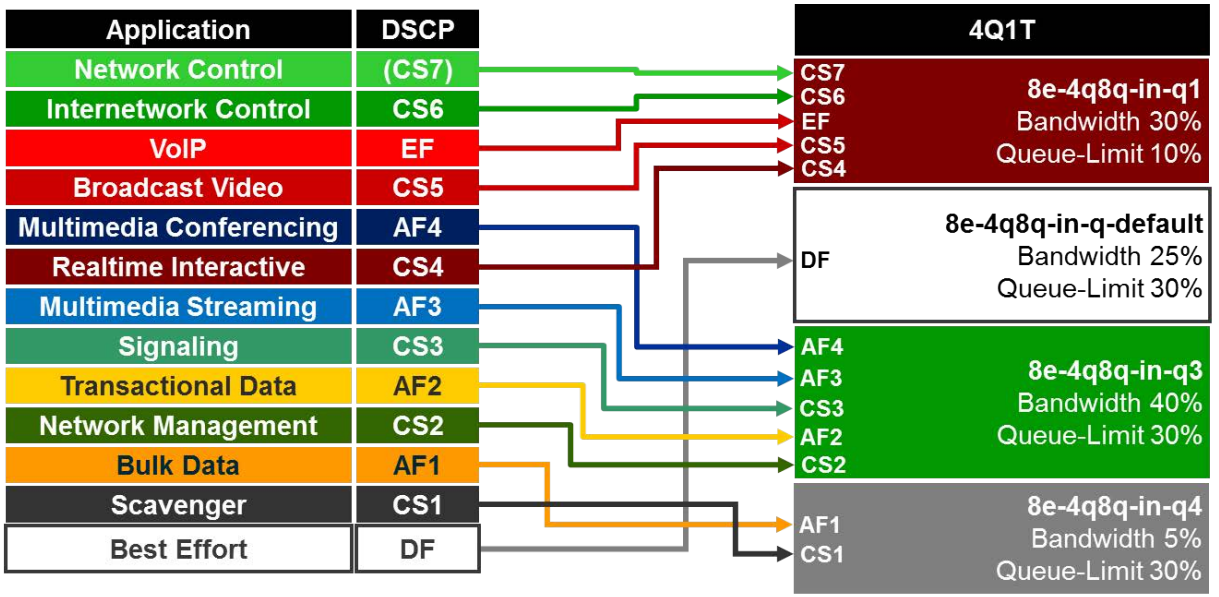
### Step 1: Configure Ingress Queuing

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

## Cisco Validated Design (CVD)

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

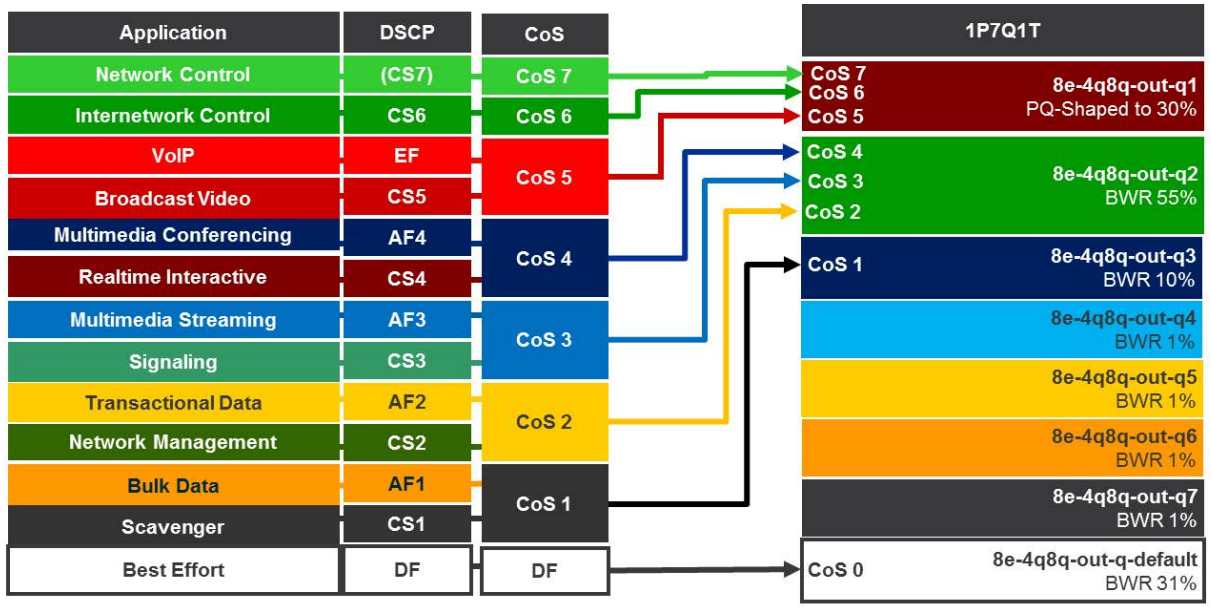
**Figure 2 Nexus 7700 F3 (4Q1T) Ingress Queuing Model**




### Step 2: Configure Egress Queuing

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

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



### Step 1: Configure 4Q1T Ingress Queuing Policies

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

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

service-policy type queuing input CAMPUS-F3-4Q1T-INGRESS
```

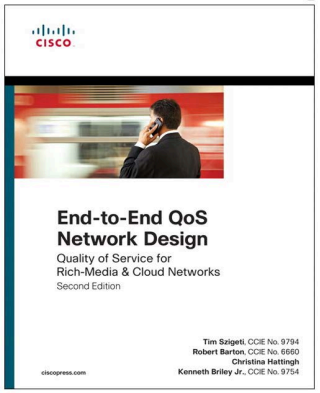
Note: Highlighted commands are interface specific; otherwise these are global.

### Step 2 Configure (CoS-Based) 1P7Q1T Egress Queuing Policies

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


policy-map type queuing 1P7Q1T-OUT

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

service-policy type queuing output 1P7Q1T-OUT
```

293378

For more details on Cisco Nexus 7000 QoS design,
see the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapter 25



# WLAN QoS Design

At-A-Glance

## The Case for QoS in the Wireless LAN

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

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

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

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

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

## WLAN QoS Design Best Practices

Four QoS design principles that apply to WLAN deployments include:

- Classify and mark applications as close to their sources as technically and administratively possible
- Police unwanted traffic flows as close to their sources as possible
- Enable queuing policies at every node where the potential for congestion exists

## WLAN QoS Design Considerations

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

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

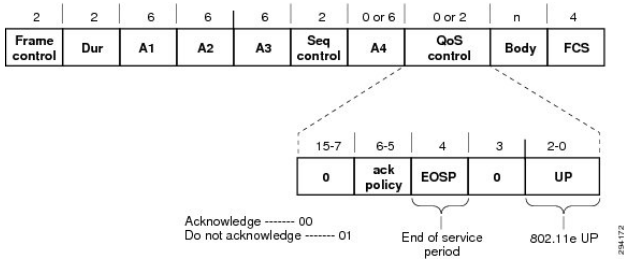
### *IEEE 802.11e EDCF*

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

*User Priorities (UP)*

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

**Figure 1 IEEE 802.11e User Priority Field**




*Access Categories (AC)*

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

**Figure 2 IEEE 802.11e Access Categories**

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

*Arbitration Interframe Spaces (AIFS)*

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

**Figure 3 IEEE 802.11e AIFS by Access Category**

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

*Contention Windows*

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

**Figure 4 IEEE 802.11e Contention Windows by AC**

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

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

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**

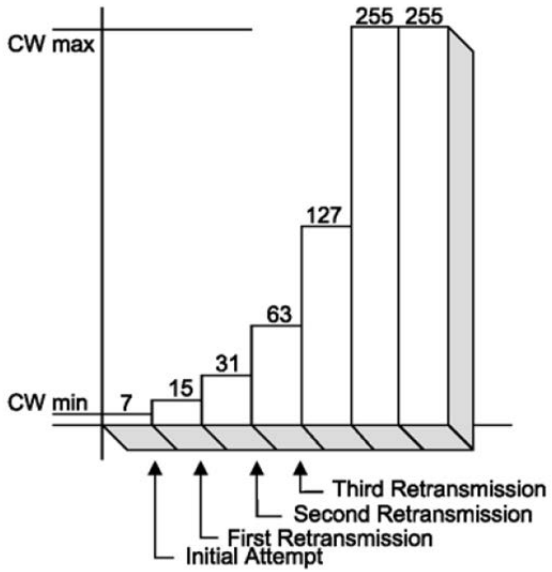
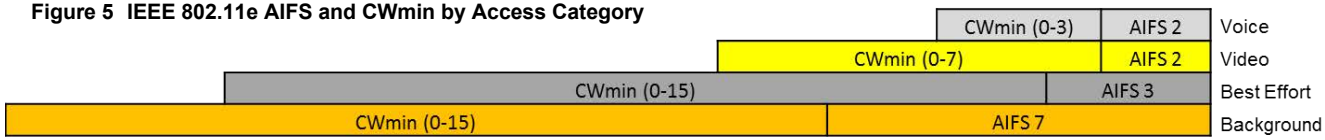



**Figure 5 IEEE 802.11e AIFS and CWmin by Access Category**




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

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

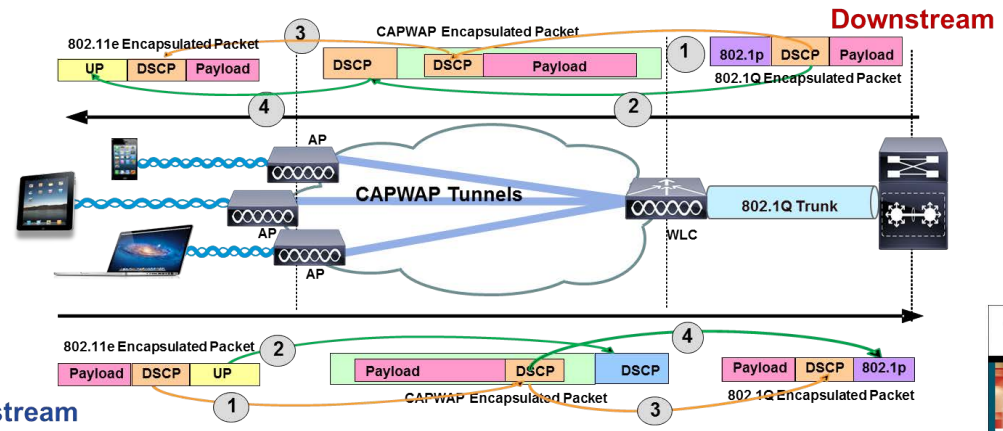
***DSCP-to-UP and UP-to-DSCP Mapping***
Upstream and downstream DSCP<>UP mapping is shown in Figure 7. By default, 6-bit DSCP values are mapped to 3-bit 802.11e UP values by taking the three Most-Significant Bits (MSB) of the DSCP and copying these as UP values. For example, DSCP EF/46 (binary **101**110)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

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

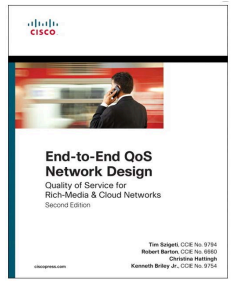
As can be seen in the above pair of examples, because information is being truncated from 6-bits to 3-bits, marking details can get lost in translation. In this example, the original voice packet was sent with DSCP EF, but was received as DSCP CS5 (based solely on default Layer 2-to-Layer 3 mapping).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

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

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




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



## Role in Wireless Campus Network

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

## QoS Design Steps

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

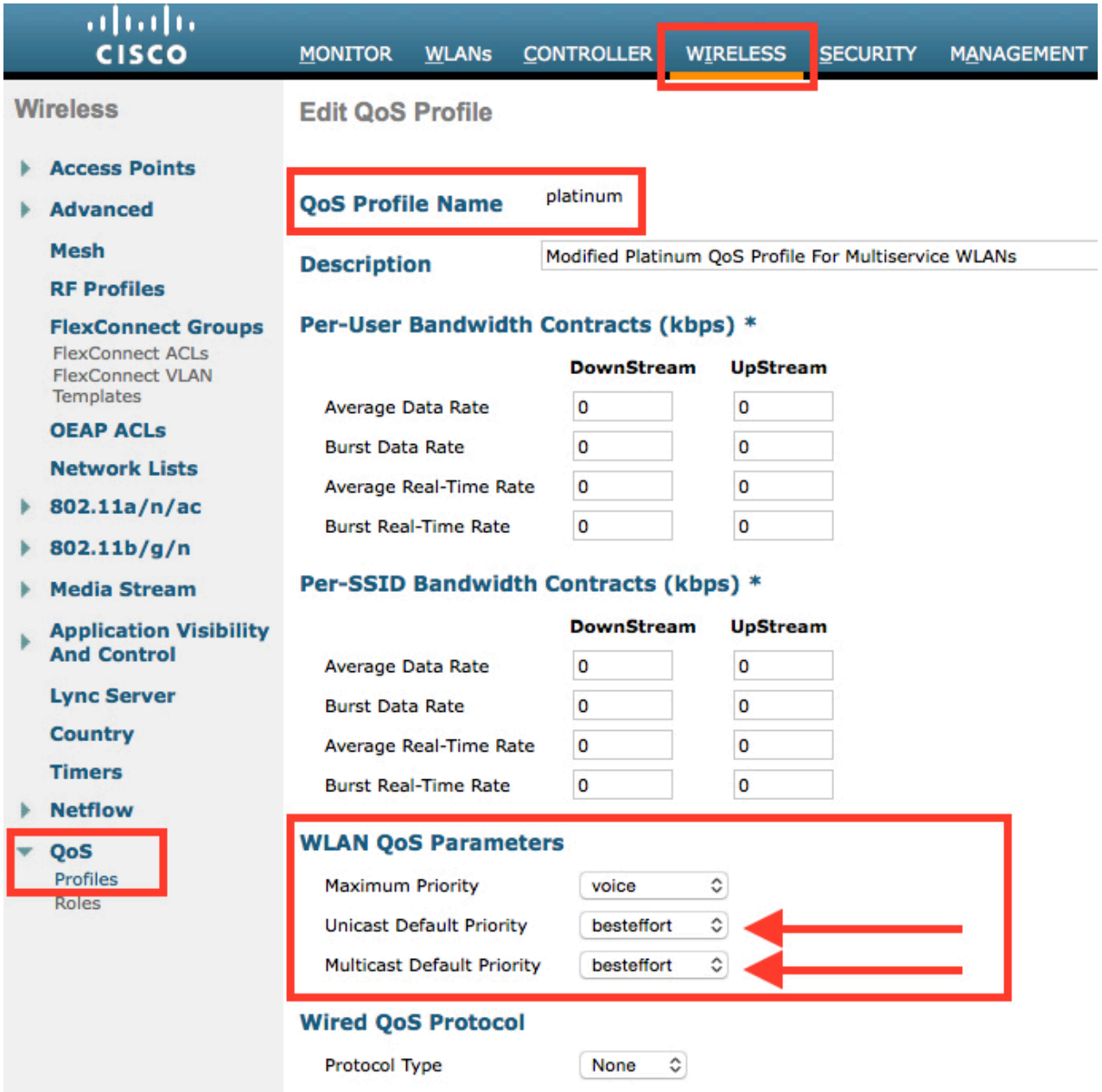
1. Select and tune the desired QoS Profile
2. Configure an AVC Profile
3. Apply the QoS and AVC Profiles on the WLAN and enable Application Visibility

### Step 1: Selecting and Tuning the QoS Profile

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

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

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



**Step 2: Configure an AVC Profile**
AVC Profiles are applied to both upstream and downstream flows on WLC ingress. While this may simplify the QoS policy configuration on the WLC, it has design implications in upstream/downstream mapping.

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

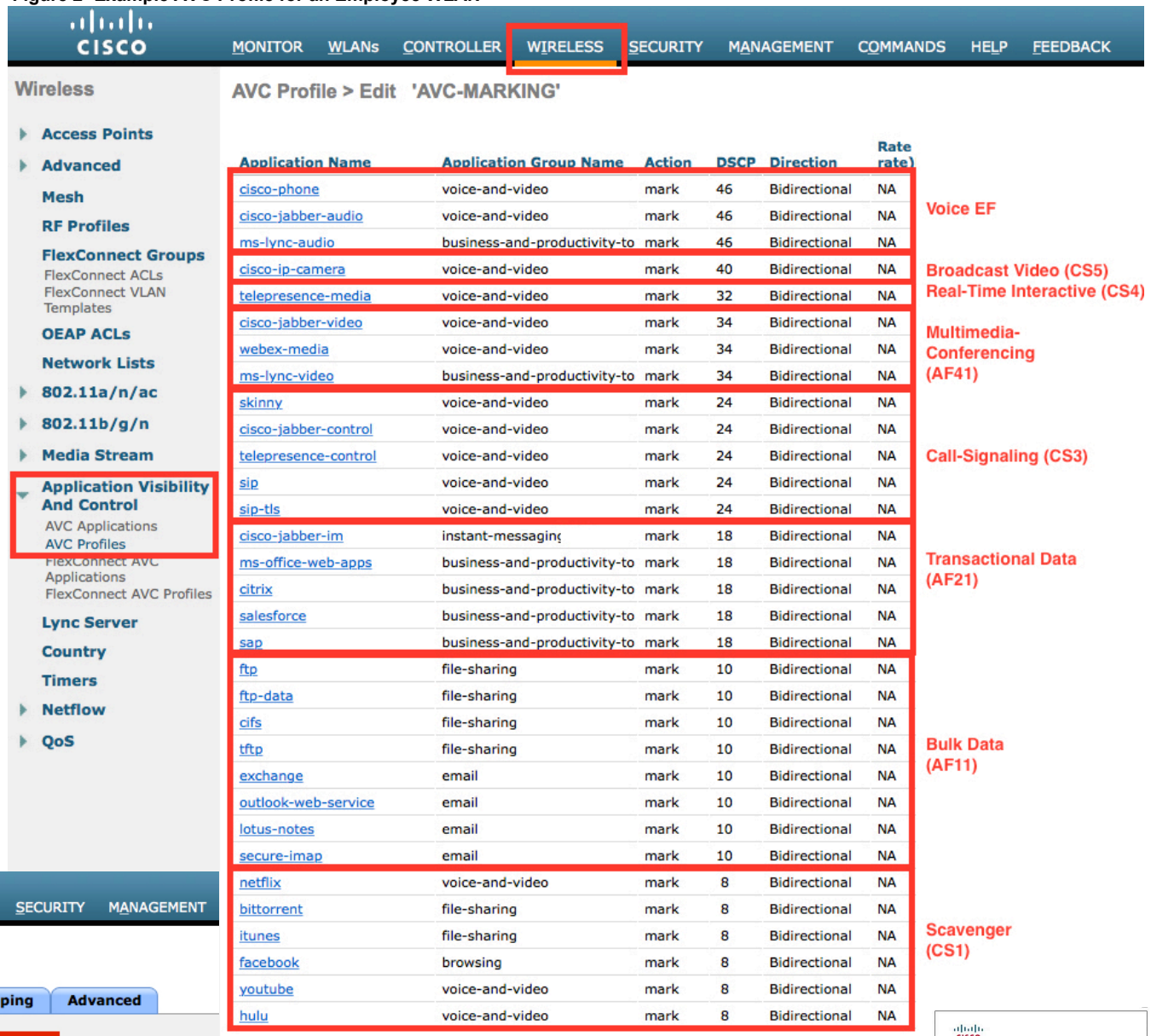
As has been previously discussed, it also is important to note that each WLAN can have both a QoS Profile and an AVC Profile attached to it. The AVC Profile is applied when the packet *enters* the WLC and the QoS policy is applied when packet *exits* the WLC. QoS Profiles may define a Maximum Priority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

An example AVC Profile is shown in Figure 2.

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

**Figure 3 Example AVC Profile for an Employee WLAN**

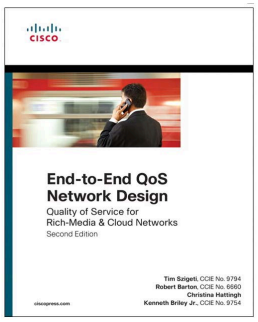

**Figure 2 Example AVC Profile for an Employee WLAN**




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

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

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



# WLAN QoS Mapping for AireOS Wireless LAN Controllers

At-A-Glance

## The Case for QoS Mapping in the Wireless LAN

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

Three are three general options for wired/wireless QoS mapping:

- (Downstream) DSCP-to-UP Mapping
- (Upstream) UP-to-DSCP Mapping
- (Upstream) DSCP-Trust

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

### DSCP-to-UP Mapping

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

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

### Upstream DSCP-to-UP Mapping

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

### Upstream DSCP Trust

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

**Figure 1: Default Downstream DSCP-to-UP Mapping**

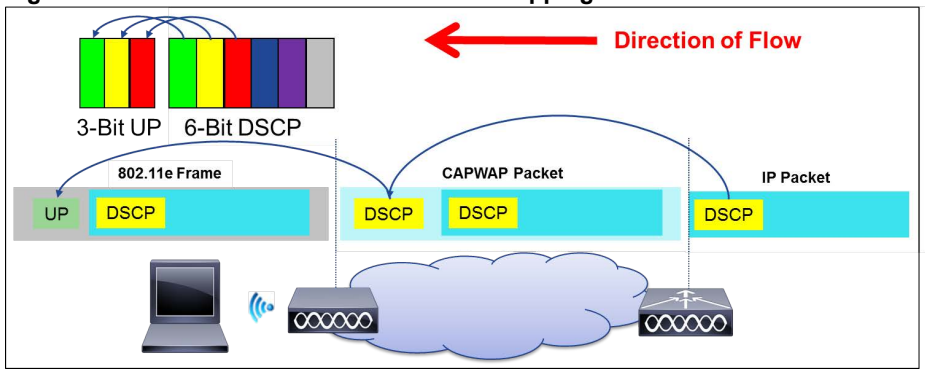



**Figure 2: Default Upstream UP-to-DSCP Mapping**

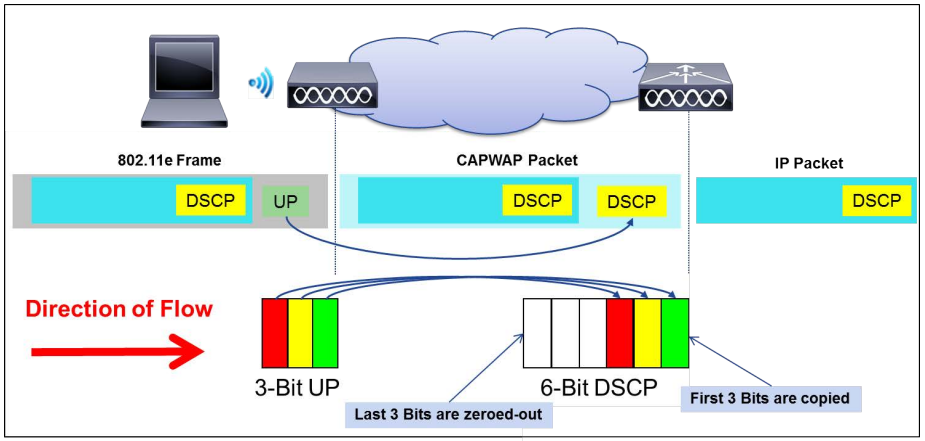
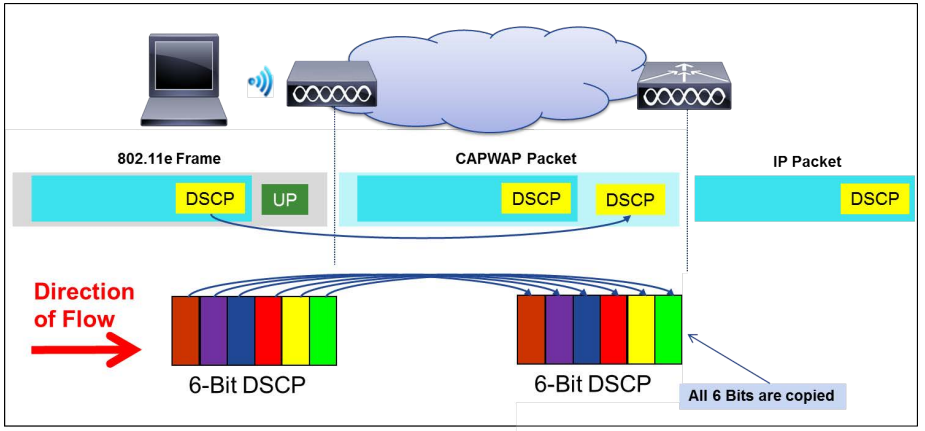


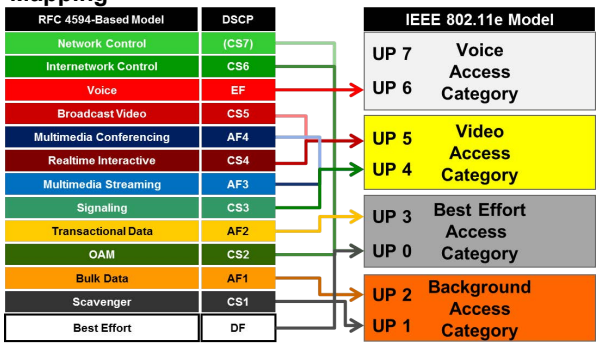

**Figure 3: Upstream DSCP Trust**



### Cisco DSCP<>UP QoS Mapping Recommendations

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

**Figure 4: Cisco Recommended DSCP-to-UP Mapping**




Note: The details behind Cisco's recommendations for IETF/IEEE QoS Mapping are documented in the Internet Draft: https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-03

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

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

## AireOS Recommended QoS Mapping Configuration

**Note: This requires AireOS 8.1MR+**

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

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

### Step 2: Configure the UP-to-DSCP Maps

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

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

### Step 3: Configure DSCP-to-UP Mapping Exceptions

Only the exceptions noted in Figure 4 will be explicitly mapped to various UP values; all remaining (unused) DSCPs will continue to be mapped to UP 0.

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

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

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

# IOS XE Wireless LAN Controller AVC/QoS Design

At-A-Glance

## Role in Wireless Campus Network

Cisco IOS XE wireless LAN controllers may be deployed in a centralized controller model or in a converged access model. In either deployment model, IOS XE controllers centrally manage QoS policies which - in turn - are enforced on wireless LAN access points, including:

- Application Visibility and Control (AVC)
- classification
- marking
- policing
- dropping
- DSCP-to-UP and UP-to-DSCP mapping

## Enabling Application Visibility

There are four steps to enabling application visibility on IOS XE wireless LAN controllers:

1. Create a Flow Record
2. (Optional) Create a Flow Exporter
3. Create a Flow Monitor
4. Apply the Flow Monitor to the WLAN

**Step 1: Create a Flow Record**
The first step in enabling application visibility for IOS XE wireless controllers is to configure a flow record. A flow record specifies the details of a given flow that is to be tracked by matching one or more of the following parameters:

- IPv4 Source Address
- IPv4 Destination Address
- Transport Protocol Source-Port
- Transport Protocol Destination Port
- Flow Direction
- Application Name
- WLAN SSID

Once the match details are specified so as to identify a discrete flow, then the flow record also specifies the type of statistics and information that is to collected by the flow record, including:

- Bytes
- Packets
- Access Point (BSSID) MAC address
- Client MAC address

**Step 2: (Optional) Create a Flow Exporter**
An optional second step is to configure a flow exporter. The flow exporter defines the destination and transport parameters of the management station that the flow details are to be exported to via Flexible NetFlow (FNF). Application flow information is gathered by the NBAR2 engine on the access point and sent to the management station using NetFlow version 9 format.

**Step 3: Create a Flow Monitor**
The next step is to configure a flow monitor. A flow monitor associates a flow record with an optional flow exporter and can be applied to a WLAN.

**Step 4: Apply the Flow Monitor to the WLAN**
Once the flow monitor has been defined, then it can be applied to a given WLAN(s) and the direction of application can be specified.

## Configuring AVC/QoS Policies

Application Visibility - by itself- only reports traffic statistics; however, the same deep packet inspection engine can be coupled with QoS policies to control these applications, via marking, policing or even outright dropping.

The steps to configure AVC/QoS policies on IOS XE wireless LAN controllers are:

1. Configure AVC-based class-maps
2. Configure a policy map to mark, police or drop applications
3. Apply the policy-map to the WLAN

**Step 1: Configure AVC-based Class-Maps**
The key command to enabling AVC within a standard Modular QoS Command-Line-Interface (MQC) class-map is **match protocol**. This command can be configured to match on:

- Individual applications:
  **match protocol** *application_name*
- Categories of applications:
  **match protocol attribute category** *category_name*
- Sub-categories of applications:
  **match protocol attribute sub-category** *sub_cat_name*
- Groups of applications:
  **match protocol attribute application-group** *app_group_name*

**Step 2: Configure a Policy-Map**
The policy map will specify the action to be performed on a given class of traffic. These actions may include:

- Marking via the **set** command
- Policing via the **police** command
- Dropping via the **drop** command

  Note: Only upstream dropping is supported

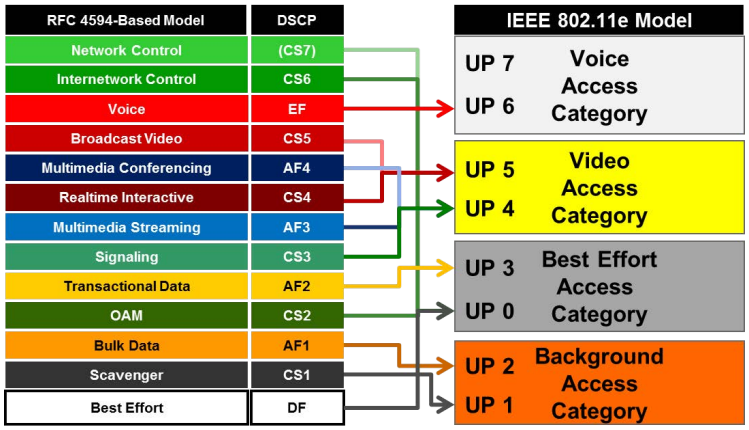
**Step 3: Attach the Policy-Map to the WLAN**
The policy map is attached to the desired WLAN(s) via a **service-policy** statement, which also specifies direction of application.

## Configuring DSCP-to-UP Table Maps

There may be times when the default mappings between L2 User Priority and L3 DSCP may be sub-optimal for QoS. This can sometimes be the case because of marking recommendation discrepancies between the IEEE and IETF standards bodies.

The Cisco-recommended DSCP-to-UP mappings to reconcile IETF and IEEE markings are shown in Figure 1.

**Figure 1 Cisco Recommended DSCP-to-UP Mappings**




In the upstream direction, Cisco recommends trusting DSCP.

Note: The details behind Cisco's recommendations for IETF/IEEE QoS Mapping are documented in the Internet Draft:
https://tools.ietf.org/html/draft-szigeti-tsvwg-ieee-802-11e-00

## Enabling Application Visibility

### Step 1: Create a Flow Record

```
flow record AVC-FLOW-RECORD
 description BASIC-AVC-FLOW-RECORD
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 match flow direction
 match application name
 match wireless ssid
 collect counter bytes long
 collect counter packets long
 collect wireless ap mac address
 collect wireless client mac address
```

### Step 2: Create a Flow Exporter

```
flow exporter AVC-FLOW-EXPORTER
 destination 10.10.10.10
 transport udp 2055
 destination 10.20.20.20
 transport udp 9991
```

Note: Lancope collects Netflow on port 2055 and Cisco Prime Infrastructure collects Netflow on port 9991

### Step 3: Create a Flow Monitor

```
flow monitor AVC-FLOW-MONITOR
 record AVC-FLOW-RECORD
 exporter AVC-FLOW-EXPORTER
```

### Step 4: Apply the Flow Monitor to the WLAN

```
wlan EMPLOYEE-WLAN
 ip flow monitor AVC-FLOW-MONITOR input
 ip flow monitor AVC-FLOW-MONITOR output
```

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

## Configuring AVC/QoS Policies

### Step 1: Configure AVC-based Class-Maps

```
class-map match-any VOICE
 match protocol cisco-phone
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
```

### Step 2: Configure a Policy-Map

```
policy-map AVC-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
```

### Step 3: Attach the Policy-Map to the WLAN

```
wlan EMPLOYEE-WLAN
service-policy client input AVC-MARKING
```

## Configuring Downstream DSCP-to-UP Table Map (Upstream DSCP-Trust is enabled by default)

### Step 1: Configure Cisco-Recommended Downstream DSCP-to-UP Table Map

```
table-map DSCP-to-UP
 map from 46 to 6
 map from 40 to 5
 map from 38 to 4
 map from 36 to 4
 map from 34 to 4
 map from 32 to 5
 map from 30 to 4
 map from 28 to 4
 map from 26 to 4
 map from 24 to 4
 map from 22 to 3
 map from 20 to 3
 map from 18 to 3
 map from 16 to 0
 map from 14 to 2
 map from 12 to 2
 map from 10 to 2
 map from 8 to 1
 default 0
```

### Step 2: Reference this Table-Map within a Policy-Map

```
policy-map DSCP-TO-UP-POLICY
 class class-default
  set wlan user-priority
      dscp table DSCP-to-UP
```

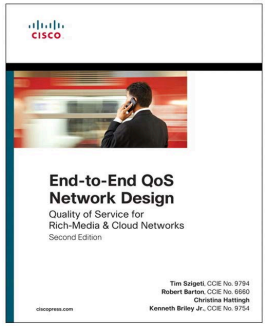
### Step 3: Attach the Policy-Map to WLAN

```
wlan EMPLOYEE-WLAN
 service-policy output
  DSCP-TO-UP-POLICY
```

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

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

And the Cisco Press book: **End-to-End QoS Network Design** (Second Edition)-Chapters 20 & 21



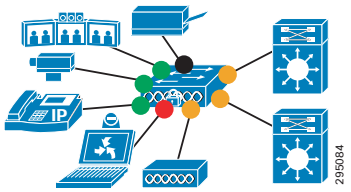
# Cisco Catalyst 9000 Series QoS Design



## Roles in Campus Network

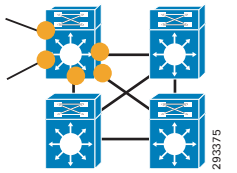
The Catalyst 9300 & 9400 Series switches are engineered to serve as access-layer switches in campus networks. As such, these switches may connect directly to a variety of endpoints and aggregation-layer switches, as shown in Figure 1.

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




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

**Figure 2 Cisco Catalyst 9500 Series Switches in a Campus Network**




● Trust DSCP
+ Egress Queuing

## QoS Design Steps

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

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

### Step 1: Configure Ingress QoS Model(s)

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

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

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

*Trust DSCP Model*

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

*Conditional Trust Model*

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

This model is suitable for switch ports connecting to:

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

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

*Service Policy Models*

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

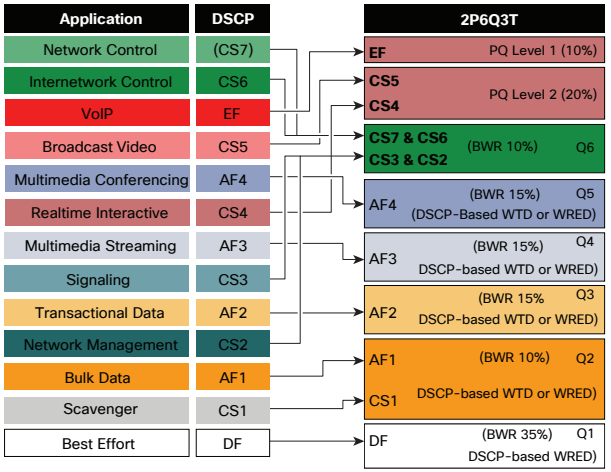
- **class-maps** which identify the flows using packet markings, access-lists, NBAR2 classification, or other criteria
- **policy-maps** which specify policy actions to be taken on a class-by-class basis
- **service-policy** statements which apply a specific policy-map to an interface(s) and specify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

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

### Step 2: Configure Egress Queuing for Switch Ports

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

**Figure 3 Cisco Catalyst 9000 Series 2P6Q3T Egress Queuing Model**




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

## IOS XE 16.8.1 AVC / NBAR2 Policy Example

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

**Step 1: Configure Ingress QoS Model :**

**Trust DSCP Model:**
**Switch Ports :** <default>

**Conditional Trust Model:**

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

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

**Service Policy Models:**

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

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

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

**Switch Port Application:**

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

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

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

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

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

**Switch Port Application:**

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

# Cisco DNA Application Experience

## Intent-Based Networking for Applications in the Enterprise

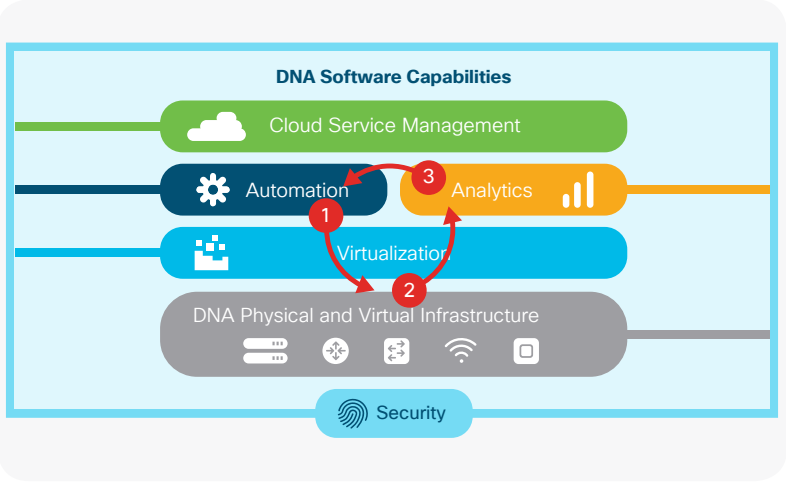
### Requirements of intent-based networks

The primary functions of intent-based networks are:

- **Translation and validation of intent:** Business-level intent is expressed by an operator and is translated into validated platform-specific configurations.
- **Automation:** Network device configurations are deployed at scale by a controller.
- **Analytics:** The network operational state is continually monitored via telemetry.
- **Assurance:** The system validates that the expressed intent is being delivered via quantitative metrics OR recognizes that the intent is not being met and then guides or automates remediation actions.

The Cisco® Digital Network Architecture (Cisco DNA™), illustrated in **Figure 1**, meets all of these requirements for intent-based application networking in the enterprise.

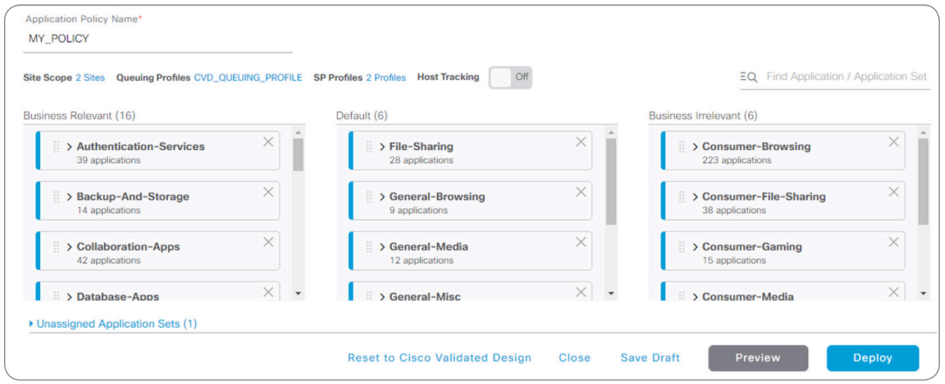
Figure 1. Cisco Digital Network Architecture




Cisco DNA delivers intent-based networking for applications via the following three main components:

- **Cisco DNA Application Policy** (item 1 in Figure 1) is an application within Cisco DNA Center™ that solicits business intent, **translates and validates** this **intent**, and **automates** the deployment of Cisco Validated Design configurations to network devices.
- **Cisco Programmable Infrastructure** (item 2 in Figure 1): Programmable hardware enables powerful infrastructure software solutions to **recognize** and **prioritize** application traffic, as well as **report** on application treatment across the enterprise routing, switching, and wireless network; this capability includes advanced application recognition for hundreds of encrypted applications, without compromising privacy or confidentiality.
- **Cisco DNA Application Assurance** (item 3 in Figure 1) is an application within DNA Center that ingests telemetry data from the network and adjacent data sources and performs contextual correlation and **analytics** to determine the network state in the context of the expressed intent. This application provides **assurance** either by confirming that the intent is being met (and supplying quantitative metrics to support such a validation) or by identifying that the intent is not being met and then initiating guided remediation workflows.

Figure 2. Creating an intent-based Cisco DNA Application Policy




# Cisco DNA Application Policy

Network operators can deploy application policies across their routed, switched, and wireless enterprise infrastructure with just three easy steps:

1. Name their policy.
2. Select a site scope (to which their policy will apply).
3. Assign business relevance to their applications.

Note: Operators can also perform optional steps, such as tuning bandwidth allocations and/or service provider profiles, as well as previewing and testing the policy prior to deployment.

Operators can assign applications to one of three levels of business relevance, as shown in **Figure 2**.

- **Business relevant:** These applications are **known to contribute to the business objectives** of the organization.
- **Default:** These applications may or may not contribute to business objectives, or there is no business reason to justify explicit policy treatment.
- **Business irrelevant:** These applications are known to have no contribution to business-objectives.

# Cisco DNA Programmable Infrastructure

The next set of requirements for enforcing application policy across the infrastructure is:

- Identifying the applications on the network, even though the majority of these are encrypted
- Grouping these applications into traffic classes
- Expressing the operator-selected business relevance of the applications
- Marking the traffic from end to end across the network
- Applying consistent congestion management and congestion avoidance to the traffic from end to end across the network

DNA Center abstracts heterogeneous platform-specific tools and features needed to implement these requirements across the network and deploys a consistent, cohesive, and comprehensive policy to express the intent from end to end, as shown in **Figure 3**.

A key technology used by Cisco DNA infrastructure is Next-Generation Network-Based Application Recognition (NBAR2). NBAR2 recognizes over 1400 applications, including more than 150 encrypted applications (without compromising confidentiality or privacy). NBAR2 is now supported not only on routing and wireless platforms, but also on switching platforms, such as the Cisco Catalyst® 9300 Series, because of its advanced Cisco Unified Access® Data Plane (UADP) 2.0 Application-Specific Integrated Circuit (ASIC).

Figure 3. Cisco DNA infrastructure enabling and enforcing Cisco DNA Application Policy

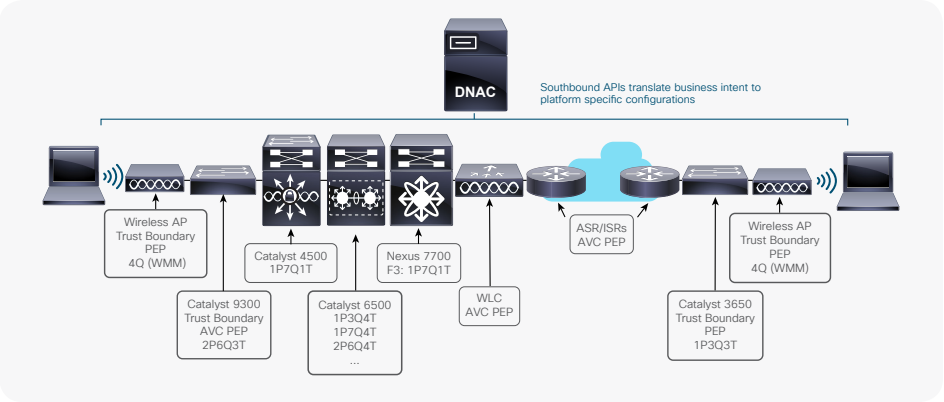
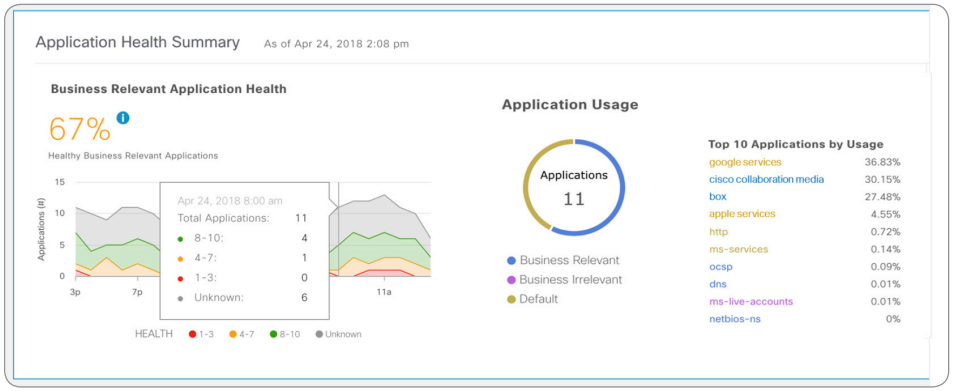



Figure 4. Cisco DNA Application Assurance—Application Health Summary




# Cisco DNA Application Assurance

Cisco DNA Application Assurance closes the intent-based application experience loop illustrated in **Figure 1**.

Cisco DNA Application Assurance ingests telemetry data from the network, as well as from relevant non-network sources (such as application servers, peer-analytics systems, client devices, etc.) and performs contextual correlation and analysis of all such data to determine the operational state of applications on the enterprise network.

To do this, Cisco DNA Application Assurance monitors multiple application Key Performance Indicators (KPIs) and—by applying standards-based guidance—interprets these for the network operator. In such a manner, raw network data (such as latency, jitter, and packet-loss values) can be transformed into more meaningful information, such as the overall health score of an application, as shown in **Figure 4**.

Additionally, Cisco DNA Application Assurance flags issues with underperforming applications and presents actionable insights and guided remediation to the network operator.