QoS on Converged Access Controllers and Lightweight Access Points

This document describes how to configure Quality of Service (QoS) on a Cisco converged access controllers (CACs) with Lightweight Access Points (LAPs) and a Cisco Catalyst 3850 Series Switch.

Prerequisites

- We recommend that you have basic knowledge on the following:
  - Configure LAPs and Cisco converged access controllers.
  - Configure basic routing and QoS in a wired network.
- Ensure the Wireless Controller Module (WCM) function of the Cisco Catalyst 3850 Series Switch for basic operation is configured.
- Ensure the LAPs are registered to the WCM.

Supported Platforms and Releases

The information in this document is based on the following software and hardware versions:

- Cisco Catalyst 3850 Series Switch running on Cisco IOS XE Software Release Denali-16.1.1
- Cisco 3600 Series LAPs

Note The information in this document refers to the devices in a customized lab environment. The devices have default configuration. If you are on a live network, you must understand the potential impact of all the commands.

Information about QoS

Cisco QoS refers to the ability of the network to provide better or special service to a set of users or applications to the adverse of other users or applications.

Cisco QoS provides enhanced and reliable network with the following services:

- Supports dedicated bandwidth for critical users and applications.
- Controls the jitter and latency that is required by real-time traffic.
- Manages and minimizes network congestion.
- Shapes network traffic in order to smooth the flow of traffic.
- Sets network traffic priorities.

In the past, WLANs were mainly used to transport data application traffic with low bandwidth requirements. The WLANs got expanded into vertical such as, retail, finance, education, and enterprise environments. WLANs are now used to transport high-bandwidth data applications in conjunction with time-sensitive and multimedia applications. The use of WLANs to transport high-bandwidth, time-sensitive, and multimedia applications led to the necessity for wireless QoS.

The IEEE 802.11e working group within the IEEE 802.11 standards committee has completed the standard definition and the Wi-Fi Alliance has created the Wi-Fi Multimedia (WMM) certification. However, the adoption of the 802.11e standard is still limited. Even though most devices are WMM-certified, because WMM certification is needed for 802.11n and 802.11ac certification, many wireless devices do not assign different QoS levels to packets sent to the Data Link Layer. Hence, most of the wireless devices send their traffic with no QoS marking and no relative prioritization. However, most 802.11 Voice over Wireless LAN (VoWLAN) IP phones do mark and prioritize their voice traffic.

This document focuses on QoS configuration for VoWLAN IP phones and on video-capable wi-fi devices that mark their voice traffic.

Note Cisco QoS configuration for devices that do not perform internal marking is outside the scope of this document.

The 802.11e amendment defines eight user priority (UP) levels, grouped two by two into four QoS levels (access categories):

- Platinum and Voice (UP 7 and 6) - Ensures a high quality of service for voice over wireless.
- Gold and Video (UP 5 and 4) - Supports high-quality video applications.
- Silver and Best Effort (UP 3 and 0) - Supports normal bandwidth for clients. This is the default setting.
- Bronze and background (UP 2 and 1) - Provides the lowest bandwidth for guest services.

Platinum is commonly used for VoIP clients and Gold is for video clients.

This document provides a configuration example that illustrates how to configure QoS on controllers and communicate with a wired network that is configured with QoS for VoWLAN and video clients.

Configuring Wireless Network for QoS with MQC

The converged access solution uses the Modular QoS (MQC) command-line interface (CLI). Refer to the QoS Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3850 Switches) for additional information on the use of MQC in QoS configuration on the Cisco Catalyst 3850 Series Switch.

Configuration of QoS with MQC on converged access controllers depends on four elements:

- **Class-maps**. Class-maps are used in order to recognize traffic of interest. Class-maps use various techniques (such as existing QoS marking, access-lists, or VLANs) to identify traffic of interest.
- **Policy-maps**. Policy-maps are used in order to determine what QoS settings should be applied to the traffic of interest. Policy-maps call class-maps and apply various QoS settings (such as specific marking, priority levels, bandwidth allocation, and so on) to each class.
- **Service-policies**. Service-policies are used to apply policy-maps to strategic points of your network. In the converged access solution, service-policies can be applied to users, Service Set Identifiers (SSIDs), AP radios, and ports. Port, SSID, and client policies can be configured by the user. Radio policies are controlled by WCM. Wireless QoS policies for port, SSID, client, and radio are applied in the downstream direction when traffic is flowing from the switch or controller to wireless clients.
- **Table-maps**. Table-maps are used in order to examine incoming QoS marking and to decide outgoing QoS markings. Table-maps are positioned in policy-maps applied to SSIDs. Table-maps can be used to keep (copy) or change the marking. Table-maps can also be used to create a mapping between wired and wireless marking. Wired marking uses DSCP (L3 QoS) or 802.1p (L2 QoS). Wireless marking uses UP. Table-maps are commonly used to determine what DSCP marking should be used for each UP of interest and what UP should be used for each DSCP value of interest. Table-maps are fundamental to converged access QoS because there is no direct translation between DSCP and UP values. However, DSCP to UP table-maps also allow the *copy* instruction. In this case, the converged access solution uses the Cisco Architecture for Voice, Video, and Integrated Data (AVVID) mapping table in order to determine the DSCP to UP or UP to DSCP translation.

Label Index	Key Field	Incoming Value	Outer DSCP	CoS	UP
0	N.A.	Not checked	0	0	0
1-10	DSCP	0-7	0-7	0	0
11-18	DSCP	8-15	8-15	1	2
19-26	DSCP	16-23	16-23	2	3
27-34	DSCP	24-31	24-31	3	4
35-46	DSCP	32-39	32-39	4	5
47-48	DSCP	40-47	40-47	5	6
49-63	DSCP	48-55	48-55	6	7
64	DSCP	56-63	56-63	7	7
65	CoS	0	0	0	0
66	CoS	1	8	1	2
67	CoS	2	16	2	3
68	CoS	3	24	3	4
69	CoS	4	32	4	5
70	CoS	5	40	5	6
71	CoS	6	48	6	7
72	CoS	7	56	7	7
73	UP	0	0	0	0
74	UP	1	8	1	1
75	UP	2	16	1	2
76	UP	3	24	2	3
77	UP	4	34	3	4
78	UP	5	34	4	5
79	UP	6	46	5	6
80	UP	7	46	7	7

Default Hardcoded Policies for QoS

Converged access controllers embark hardcoded QoS policy profiles that can be applied to WLANs. The QoS policy profiles apply the metal policies (platinum, gold, and so on) that are familiar to administrators of Cisco Unified Wireless Networks (CUWN) controllers.

If your objective is not to create policies that assign specific bandwidth to voice traffic but to ensure that voice traffic receives the proper QoS marking, you can use the hardcoded policies. The hardcoded policies can be applied to the WLAN and can be different in the upstream and the downstream directions.

Platinum

The hardcoded policy for voice is known as platinum. The name cannot be changed.

The following commands describe the downstream policy of the platinum QoS level:

```
Policy-map platinum
Class class-default
 set dscp dscp table plat-dscp2dscp
 set wlan user-priority dscp table plat-dscp2up
Table-map plat-dscp2dscp
    from 45 to 45
    from 46 to 46
    from 47 to 47
    default copy
Table-map plat-dscp2up
    from 34 to 4
    from 46 to 6
    default copy
```

The following commands describe the upstream policy of the Platinum QoS level:

```
Policy-map platinum-up
    Class class-default
      set dscp wlan user-priority table plat-up2dscp

Table-map plat-up2dscp
    from 4 to 34
    from 5 to 34
    from 6 to 46
    from 7 to 8
    default copy
```

Gold

The hardcoded policy for video is known as gold. The name cannot be changed.

The following commands describe the downstream policy of the gold QoS level:

```
Policy Map gold
    Class class-default
      set dscp dscp table gold-dscp2dscp
      set wlan user-priority dscp table gold-dscp2u

Table Map gold-dscp2dscp
    from 45 to 34
    from 46 to 34
    from 47 to 34
    default copy

Table Map gold-dscp2up
    from 45 to 4
    from 46 to 4
    from 47 to 4
    default copy
```

The following commands describe the upstream policy of the gold QoS level:

```
Policy Map gold-up
    Class class-default
      set dscp wlan user-priority table gold-up2dscp

Table Map gold-up2dscp
    from 6 to 34
```

```
    from 7 to 34
    default copy
```

Silver

The hardcoded policy for best effort is known as silver. The name cannot be changed.

The following commands describe the downstream policy of the silver QoS level:

```
Policy Map silver
    Class class-default
      set dscp dscp table silver-dscp2dscp
      set wlan user-priority dscp table silver-dscp2up

Table Map silver-dscp2dscp
    from 34 to 0
    from 45 to 0
    from 46 to 0
    from 47 to 0
    default copy

Table Map silver-dscp2up
    from 34 to 0
    from 45 to 0
    from 46 to 0
    from 47 to 0
    default copy
```

The following commands describe the upstream policy of the silver QoS level:

```
Policy Map silver-up
    Class class-default
      set dscp wlan user-priority table silver-up2dscp
Table Map silver-up2dscp
    from 4 to 0
    from 5 to 0
    from 6 to 0
    from 7 to 0
    default copy
```

Bronze

The hardcoded policy for background traffic is known as bronze. The name cannot be changed.

The following commands describe the downstream policy of the bronze QoS level:

```
Policy Map bronze
    Class class-default
      set dscp dscp table bronze-dscp2dscp
 set wlan user-priority dscp table bronze-dscp2up

Table Map bronze-dscp2dscp
    from 0 to 8
    from 34 to 8
    from 45 to 8
    from 46 to 8
    from 47 to 8
    default copy

Table Map bronze-dscp2up
    from 0 to 1
    from 34 to 1
    from 45 to 1
    from 46 to 1
    from 47 to 1
    default copy
```

The following commands describe the upstream policy of the bronze QoS level:

```
Policy Map bronze-up
    Class class-default
      set dscp wlan user-priority table bronze-up2dscp
```

```
Table Map bronze-up2dscp
    from 0 to 8
    from 1 to 8
    from 4 to 8
    from 5 to 8
    from 6 to 8
    from 7 to 8
    default copy
```

Note Once you have decided which table-map best matches the target traffic for a given SSID, you can apply the matching policy to your WLAN.

In the following example, one policy is applied in the downstream direction (output, from the AP to the wireless client), and one policy is applied on the upstream direction (input, from the wireless client, through the AP, to the controller):

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z
Device(config)# wlan test1
Device(config-wlan)# service-policy output platinum
Device(config-wlan)# service-policy input platinum-up
Device(config-wlan)# end
```

To check the WLAN configuration, use the following commands. The commands also verify the policy applied to your WLAN.

```
Device# show wlan name test1
WLAN Profile Name     : test1
================================================
Identifier                                      : 1
Network Name (SSID)                             : test1
Status                                          : Disabled
Broadcast SSID                                  : Enabled
Maximum number of Associated Clients            : 0
AAA Policy Override                             : Disabled
Network Admission Control
  NAC-State                                     : Disabled
Number of Active Clients                        : 0
Exclusion list Timeout                          : 60
Session Timeout                                 : 1800 seconds
CHD per WLAN                                    : Enabled
Webauth DHCP exclusion                          : Disabled
Interface                                       : default
Interface Status                                : Up
Multicast Interface                             : Unconfigured
WLAN IPv4 ACL                                   : Unconfigured
WLAN IPv6 ACL                                   : Unconfigured
DHCP Server                                     : Default
DHCP Address Assignment Required                : Disabled
DHCP Option 82                                  : Disabled
DHCP Option 82 Format                           : AP-Mac
DHCP Option 82 ASCII Mode                      : Disabled
DHCP Option 82 Rid Mode                         : Disabled
QoS Service Policy - Input
  Policy Name                        : platinum-up
  Policy State                      : Validation Pending
QoS Service Policy - Output
  Policy Name                        : platinum
  Policy State                      : Validation Pending
QoS Client Service Policy
  Input  Policy Name                            : unknown
  Output Policy Name                            : unknown
WMM                                             : Allowed
Channel Scan Defer Priority:
  Priority (default)                            : 4
```

```
  Priority (default)                           : 5
  Priority (default)                           : 6
Scan Defer Time (msecs)                        : 100
Media Stream Multicast-direct                  : Disabled
CCX - AironetIe Support                        : Enabled
CCX - Gratuitous Probe Response (GPR)          : Disabled
CCX - Diagnostics Channel Capability           : Disabled
Dot11-Phone Mode (7920)                        : Invalid
Wired Protocol                                 : None
Peer-to-Peer Blocking Action                   : Disabled
Radio Policy                                   : All
DTIM period for 802.11a radio                  : 1
DTIM period for 802.11b radio                  : 1
Local EAP Authentication                       : Disabled
Mac Filter Authorization list name             : Disabled
Accounting list name                           : Disabled
802.1x authentication list name                : Disabled
Security
    802.11 Authentication                      : Open System
    Static WEP Keys                            : Disabled
    802.1X                                     : Disabled
    Wi-Fi Protected Access (WPA/WPA2)          : Enabled
        WPA (SSN IE)                           : Disabled
        WPA2 (RSN IE)                          : Enabled
            TKIP Cipher                        : Disabled
            AES Cipher                         : Enabled
        Auth Key Management
            802.1x                             : Enabled
            PSK                                : Disabled
            CCKM                               : Disabled
    CKIP                                       : Disabled
    IP Security                                : Disabled
    IP Security Passthru                       : Disabled
    L2TP                                       : Disabled
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Auto Anchor                                : Disabled
    Sticky Anchoring                           : Enabled
    Cranite Passthru                           : Disabled
    Fortress Passthru                          : Disabled
    PPTP                                       : Disabled
    Infrastructure MFP protection              : Enabled
    Client MFP                                 : Optional
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Parameter Map                      : Disabled
    Tkip MIC Countermeasure Hold-down Timer    : 60
Call Snooping                                  : Disabled
Passive Client                                 : Disabled
Non Cisco WGB                                  : Disabled
Band Select                                    : Disabled
Load Balancing                                 : Disabled
IP Source Guard                                : Disabled
```

Configuring QoS Manually

The hardcoded policies apply default QoS marking but do not apply bandwidth allocation. The hardcoded policies also assume that your traffic is already marked.

Perform the following steps to use a combination of policies to identify and mark voice and video traffic appropriately, to set bandwidth allocation in the downstream and upstream directions, and to use call admission control in order to limit the number of calls initiated from the wireless cell in a complex environment:

Identifying and Marking of Voice Traffic

The first step is to recognize voice and video traffic. Voice traffic can be classified into the following categories:

- Voice flow, which carries the audio part of the communication.
- Voice signaling, which carries the statistical information exchanged between voice endpoints.

The voice flow uses Real-time Transport Protocol (RTP) and User Datagram Protocol (UDP) destination ports in the range of 16384 - 32767. This is a projected range and the actual ports are usually narrower and depends on the implementation.

There are several voice signaling protocols. The configuration example that is described uses Jabber. Jabber uses the following TCP ports for connection and directory:

- TCP 80 (HTTP)
- 143 (Internet Message Access Protocol [IMAP])
- 443 (HTTPS)
- 993 (IMAP) for services such as Cisco Unified MeetingPlace or Cisco WebEx for meetings and Cisco Unity or Cisco Unity Connection for voicemail features.
- TCP 389 or 636 (Lightweight Directory Access Protocol [LDAP] server for contact searches.)
- FTP (1080)
- TFTP (UDP 69) for file transfer (such as configuration files) from peers or from server.

These services may not need a specific prioritization. Jabber uses the Session Initiation Protocol (SIP) (UDP or TCP 5060 and 5061) for voice signaling.

Video traffic uses different ports and protocols depending on your implementation.

The configuration example described uses a Tandberg PrecisionHD 720p camera for video conferences.

The Tandberg PrecisionHD 720p camera can use several codecs. The bandwidth consumed depends on the codec selected:

- C20, C40, and C60 codecs use H.323 or SIP and can consume up to 6 Mbps in point-to-point connections.
- The C90 codec uses these same protocols and can consume up to 10 Mbps in multi-site communications.

Tandberg implementation of H.323 uses UDP 970 for streaming video, UDP 971 for video signaling, UDP 972 for streaming audio, and UDP 973 for audio signaling. Tandberg cameras also use other ports, such as:

- UDP 161
- UDP 962 (Simple Network Management Protocol [SNMP])
- TCP 963 (netlog), TCP 964 (FTP)
- TCP 965 (virtual network computing [VNC])
- UDP 974 (Session Announcement Protocol [SAP])

Note The additional ports may not need a specific prioritization.

A common way to identify traffic is to create class-maps that target the traffic of interest. Each class-map can point to an access-list that targets any traffic that uses the voice and the video ports. To create class-maps, use the following commands:

```
ip access-list extended JabberVOIP
permit udp any any range 16384 32767
ip access-list extended JabberSIGNALING
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended H323Videostream
permit udp any any eq 970
ip access-list extended H323Audiostream
permit udp any any eq 972
ip access-list extended H323VideoSignaling
permit udp any any eq 971
ip access-list extended H323AudioSignaling
permit udp any any eq 973
```

You can then create one class-map for each type of traffic. Each class-map points to the relevant access-list. To create one class-map for each type of traffic, use the following commands:

```
class-map RTPaudio
match access-group name JabberVOIP
match access-group name H323Audiostream
class-map H323realtimevideo
match access-group name H323Videostream
class-map signaling
match access-group name JabberSIGNALING
match access-group name H323VideoSignaling
match access-group name H323AudioSignaling
```

When voice traffic and video traffic have been identified through class-maps, ensure that the traffic is marked properly. The marking can be done at the WLAN level through the table-maps and also through client policy-maps.

Table-maps examine the QoS marking of incoming traffic and determine what the outgoing QoS marking should be. Thus, Table-maps are useful when incoming traffic already has QoS marking. Table-maps are used exclusively at the SSID level.

By contrast, policy-maps can target traffic identified by class-maps and are better adapted to untagged traffic of interest. The configuration example assumes that traffic from the wired side has already been marked properly before it enters the Cisco Catalyst 3850 Series Switch. If this is not the case, you can use a policy-map and apply it at the SSID level as a client policy. Because traffic from wireless clients may not have been marked, you need to mark voice and video traffic properly by ensuring the following:

- Real time voice should be marked with DSCP 46 (Expedited Forwarding [EF]).
- Video should be marked DSCP 34 (Assured Forwarding Class 41 [AF41]).
- Signaling for voice and video should be marked DSCP 24 (Class Selector Service value 3 [CS3]).

To apply these markings, create a policy-map that calls each of these classes and that marks the equivalent traffic. To create a policy-map, use the following commands:

```
policy-map taggingPolicy
 class RTPaudio
 set dscp ef

 class H323realtimevideo
 set dscp af41
```

```
class signaling
set dscp cs3
```

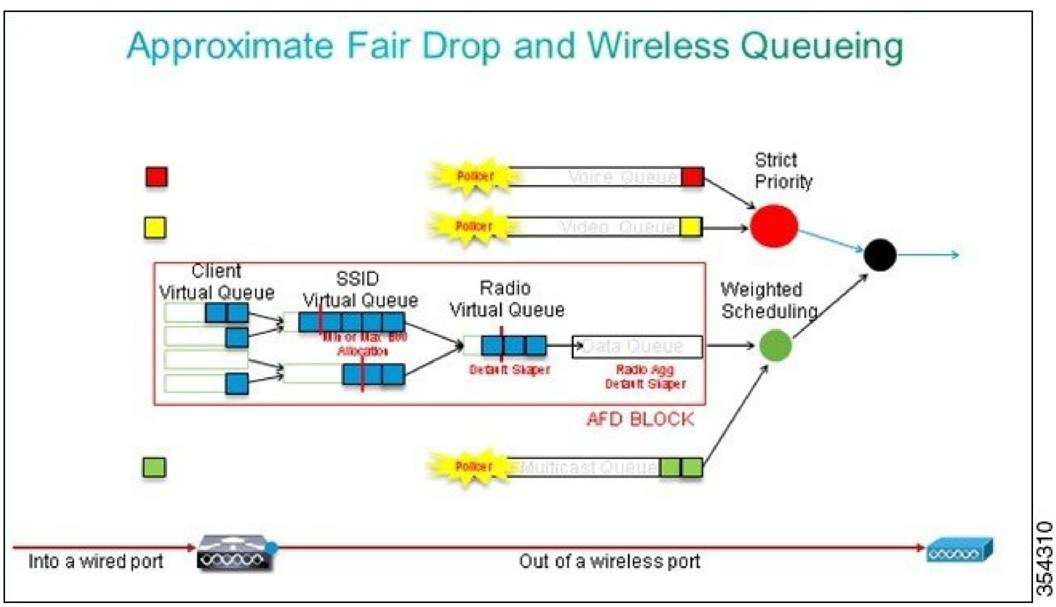
Bandwidth and Priority Management at Port Level

The next step is to determine a QoS policy for ports that come and go to APs. This step primarily applies to Cisco Catalyst 3850 Series Switches.

Cisco Catalyst 3850 Series Switches ports carry voice and video traffic that goes to or comes from wireless clients and APs. QoS configuration in this context matches the following requirements:

1. **Allocate bandwidth.** You may want to decide how much bandwidth is allocated for each type of traffic. The bandwidth allocation can also be done at the SSID level. Set the port bandwidth allocation to define how much bandwidth can be received by each AP that serves the target SSID. The bandwidth has to be set for all SSIDs on the target AP. For a simplified configuration which has only one SSID and one AP, the port bandwidth allocation for voice and video is the same as the global bandwidth allocation for voice and video at the SSID level. Each traffic type is allocated 6 Mbps and is policed so that the allocated bandwidth is not exceeded.
2. **Prioritize traffic.** The port has four queues. The first two queues are prioritized and reserved for real time traffic - typically voice and video, respectively. The fourth queue is reserved for non-real-time multicast traffic, and the third queue contains all other traffic. With converged access queuing logic, traffic for each client is assigned to a virtual queue, where QoS can be configured. The result of the client QoS policy is injected into the SSID virtual queue, where QoS can also be configured. Since several SSIDs can exist on a given AP radio, the result of each SSID that is present on an AP radio is injected into the AP radio virtual queue, where traffic is shaped based on the radio capacity. Traffic can be delayed or dropped at any of these stages by use of a QoS mechanism called Approximate Fair Drop (AFD). The result of this policy is then sent to the AP port (called the wireless port), where priority is given to the first two queues (up to a configurable amount of bandwidth), and then to the third and fourth queues.

Figure 1: Appropriate Fair Drop and Wireless Queuing



Note You cannot use class-maps that target traffic based on access control lists (ACLs). Policies applied at the port level can target traffic based on class-maps, but these class-maps should target traffic identified by its QoS value. Once you have identified traffic based on ACLs and marked this traffic properly at the client SSID level, it would be redundant to perform a second inspection of that same traffic at the port level. When traffic reaches the port that goes to the AP, it is already marked properly.

In the following example, the general class-maps created for the SSID policy is re-used and voice RTP traffic and video real time traffic are directly targeted:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
match dscp cs3
```

Once you have identified the traffic of interest, you can decide which policy to apply. To apply the policy, use the following commands. The default policy (called parent_port) is applied automatically at each port when an AP is detected.

The following example displays the default policy.

```
policy-map parent_port
class class-default
shape average 1000000000
service-policy port_child_policy
```

Note It is not recommended to change the default policy.

Because the default parent_port policy calls the port_child_policy, one option is to edit the port_child_policy (it is not recommended to change the name). The child policy determines what traffic should go in each queue and how much bandwidth should be allocated. The first queue has the highest priority, the second queue has the second highest priority, and so on. The first two queues are reserved for real time traffic. The fourth queue is used for non-real-time multicast traffic. The third queue contains all other traffic.

In the following example, voice traffic is allocated to the first queue and video traffic to second queue and the bandwidth is allocated to each queue and to all other traffic:

In the policy mapped defined below, the priority statement associated to the voice and the 'videoandsignaling' classes allows you to assign the traffic to the relevant priority queue. However, the police rate percent statements apply only to multicast and not unicast traffic.

You need not apply the port_child_policy policy at the port level because it is applied automatically as soon as an AP is detected.

```
Policy-map port_child_policy
Class allvoice
 Priority level 1
 police rate percent 10
 conform-action transmit
 exceed-action drop
class videoandsignaling
 priority level 2
 police rate percent 20
 conform-action transmit
 exceed-action drop
class non-client-nrt-class
 bandwidth remaining ratio 7
class class-default
 bandwidth remaining ratio 63
```

Bandwidth and Priority Management at SSID Level

The next step is to verify the QoS policy at the SSID level. The configuration assumes that voice and video traffic are identified through the use of class-map and access-lists and is tagged properly. However, some incoming traffic that is not targeted by the access-list may not display its QoS marking. In such a case, you can decide if this traffic should be marked with a default value or left untagged. The same logic goes for traffic already marked but not targeted by the class-maps. Use the **default copy** command in a table-map to ensure that unmarked traffic is left unmarked and the tagged traffic keeps the tag and it is not remarked.

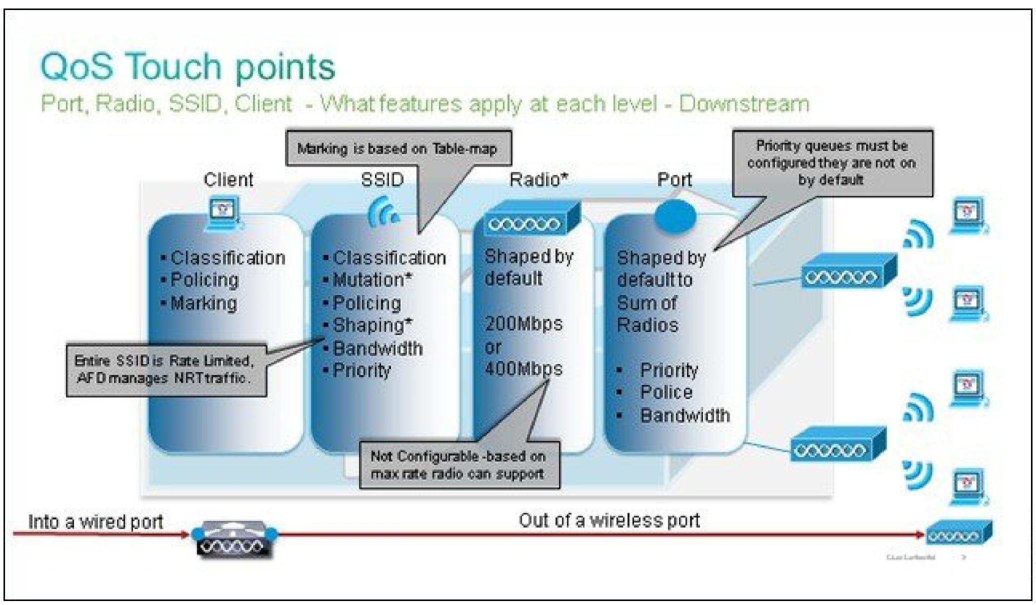
Table-maps decide the outgoing DSCP value but are also used to create an 802.11 frame to decide the frame UP value.

In the following example, incoming traffic that displays voice QoS level (DSCP 46) maintains its DSCP value and the value is mapped to the equivalent 802.11 marking (UP 6). Incoming traffic that displays video QoS level (DSCP 34) maintains its DSCP value and the value is mapped to the equivalent 802.11 marking (UP 5). Similarly, traffic marked DSCP 24 may be voice signaling and the DSCP value should be maintained and translated into the 802.11 UP 3:

```
Table-map dscp2dscp
Default copy
Table-map dscp2up
Map from 46 to 6
Map from 24 to 3
Map from 34 to 5
Default copy
```

Marking could also be done at the incoming wired port level. The following figure shows what QoS actions can be taken as traffic transits from wired to wireless:

Figure 2: QoS Touch Points



The configuration example described focuses on the wireless aspect of QoS configuration and marks traffic at wireless client level. Once the marking portion has been completed, you need to allocate bandwidth. Here, 6 Mbps of bandwidth is allocated to voice traffic flows. (While this is the overall bandwidth allocation for voice, each call would consume less - for example, 128 kbps.) The 6 Mbps bandwidth is allocated with the **police** command to reserve the bandwidth and to drop traffic in excess.

The video traffic is also allocated 6 Mbps and it is policed.

Note The configuration assumes that there is only one video flow.

The signaling part of the video and voice traffic also needs to be allocated bandwidth. There are two possible strategies:

- Use the shape average command, which allows traffic in excess to be buffered and sent later. This logic is not efficient for the voice or video flow because the voice and video flows require consistent delay and jitter; however, it can be efficient for signaling because signaling can be slightly delayed without an effect on call quality. In the converged access solution, **shape** commands do not accept buckets configurations, which determine how much traffic in excess of the allocated bandwidth can be buffered. Therefore, a second command, queue-buffers ratio 0, must be added in order to specify that the bucket size is 0. If you include signaling in the rest of the traffic and use **shape** commands, signaling traffic might be dropped in times of high congestion. This might, in turn, cause the call to be dropped, because both the ends determine that communication is no longer occurring.
- To avoid the risk of dropped calls, you can include signaling in one of the priority queues. The configuration example previously defined the priority queues as voice and video and now adds signaling to the video queue.

  The policy uses call admission control (CAC) for the voice flow. CAC targets wireless traffic and matches a specific UP (in this configuration example, UP 6 and 7). CAC then determines the maximum amount of bandwidth this traffic should use. In a configuration where you police voice traffic, CAC should be allocated a subset of the overall amount of bandwidth allocated for voice. For example, if voice is policed to 6 Mbps, CAC cannot exceed 6 Mbps. CAC is configured in a policy-map (called a child policy) that is integrated into the main downstream policy-map (called the parent policy). CAC is introduced with the admit **cac wmm-tspec**command, followed by the target UPs and the bandwidth allocated to the targeted traffic.

Each call does not consume all the bandwidth allocated to voice. For example, each call may consume 64 kbps each way, which results in 128 kbps of effective bi-directional bandwidth consumption. The rate instruction determines each call bandwidth consumption, while the police statement determines the overall bandwidth allocated to voice traffic. If all calls that occur within the cell use close to the maximum allowed bandwidth, any new call that is initiated from within the cell and that causes the consumed bandwidth to exceed the maximum bandwidth allowed for voice will be denied. You can fine tune this process through configuration of CAC at the band level, as explained in Call Limitation with CAC.

Therefore, you need to configure a child policy that contains the CAC instructions and that is integrated into the main downstream policy. CAC is not configured in the upstream policy-map. CAC does apply to voice calls initiated from the cell, but, because it is a response to those calls, CAC is set only into the downstream policy-map. The upstream policy-map will be different. You cannot use the class-maps created previously because these class-maps target traffic based on an ACL. Traffic injected into the SSID policy has gone through the client policy, so you should not perform inspection on the packets a second time. Instead, target traffic with a QoS marking that results from the client policy.

If you decide not to leave signaling in the default class, you will also need to prioritize signaling.

In the following example, signaling and video are in the same class and more bandwidth is allocated to that class to accommodate the signaling part. 6 Mbps is allocated for video traffic (one Tandberg camera point-to-point flow) and 1 Mbps is allocated to signaling for all voice calls and the video flow:

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
Match dscp cs3
```

The following describes the downstream child policy:

```
Policy-map SSIDout_child_policy
class allvoice
priority level 1
police 6000000
admit cac wmm-tspec
rate 128
wlan-up 6 7
class videoandsignaling
priority level 2
police 1000000
```

The following describes the downstream parent policy:

```
policy-map SSIDout
class class-default
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
shape average 30000000
queue-buffers ratio 0
service-policy SSIDout_child_policy
```

Upstream traffic comes from wireless clients and is sent to the WCM before the traffic is sent out of a wired port or to another SSID. In both cases, you can configure policy-maps that define the bandwidth allocated to each type of traffic. The policy will probably differ based on whether the traffic is sent out of a wired port or to another SSID.

In the upstream direction, the primary concern is to decide the priority and not the bandwidth. In other words, the upstream policy-map does not allocate bandwidth to each type of traffic. Because the traffic is already at the AP and has already crossed the bottle-neck formed by the half-duplex wireless space, your goal is to bring this traffic to the controller function of the Cisco Catalyst 3850 Series Switch for further processing. When traffic is collected at the AP level, you can decide if you should trust potential existing QoS marking in order to prioritize traffic flows sent to the controller. In the following example, existing DSCP values can be trusted:

```
Policy-map SSIDin
Class class-default
set dscp dscp table dscp2dscp
```

As you create your policies, apply the policy-maps to the WLAN.

In the following example, any device connecting to the WLAN is expected to support WMM, so WMM is required:

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
```

Call Limitation with CAC

The last step is to customize CAC as per your requirements. In the CAC configuration explained in the Bandwidth and Policy Management at SSID Level, the AP drops any voice packet that exceeds the allocated bandwidth.

In order to avoid the bandwidth maximum, you need to configure the WCM in order to recognize calls that are placed and calls that will cause the bandwidth to exceed. Some phones support WMM Traffic Specification (TSPEC) and inform the wireless infrastructure of the bandwidth that the projected call is expected to consume. The WCM can then refuse the call before it is placed.

Some SIP phones do not support TSPEC, but the WCM and the AP can be set to recognize call initiation packets sent to SIP ports and can use this information in order to establish that a SIP call is about to be placed. Because the SIP phone does not specify the bandwidth that is to be consumed by the call, the administrator must determine the expected bandwidth based on the codec, the sampling time, and so on.

CAC calculates the consumed bandwidth at each AP level. CAC can be set to use only the client bandwidth consumption in its calculations (static CAC) or to also consider neighboring APs and devices on the same channel (load-based CAC). We recommend that you use static CAC for SIP phones and load-based CAC for TSPEC phones.

Finally, CAC is activated on a per band basis.

In the following example, phones use SIP rather than TSPEC for their session initiation. Each call uses 64 kbps for each stream direction, load-based CAC is disabled when static CAC is enabled, and 75% of each AP bandwidth max is allocated to voice traffic:

```
ap dot11 5ghz shutdown
ap dot11 5ghz cac voice acm
no ap dot11 5ghz cac voice load-based
ap dot11 5ghz cac voice max-bandwidth 75
ap dot11 5ghz cac voice sip bandwidth 64
no ap dot11 5ghz shutdown
```

You can repeat the same configuration for the 2.4 GHz band as shown in the following example:

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

Once CAC is applied for each band, you also need to apply SIP CAC at the WLAN level. This process enables the AP to examine Layer 4 (L4) information of the wireless client traffic for identifying queries sent to UDP 5060 indicating SIP call attempts. TSPEC operates at the 802.11 level and is natively detected by APs. SIP phones do not use TSPEC and AP must perform packet inspection to identify SIP traffic. To avoid AP to perform this inspection on all SSIDs, you need to determine which SSIDs expect SIP traffic. You can enable call snooping on those SSIDs to perform specific voice calls. You can also determine what action to perform if a SIP call needs to be rejected - disassociate the SIP client or send a SIP busy message.

In the following example, call snooping is enabled and a busy message is sent, if the SIP call needs to be rejected. With the addition of the QoS policy (Refer to Step 3), Bandwidth and Priority Management at SSID Level, this is the SSID configuration for the example WLAN:

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
call-snoop
sip-cac platinum
```

Verifying Configuration for QoS

To verify the configuration, use the following commands:

show class-map

The following is an example of the class-maps configured on the platform:

```
Device# show class-map
 Class Map match-any H323realtimeaudio (id 6)
   Match access-group name H323Audiostream
Class Map match-any H323realtimevideo (id 7)
   Match access-group name H323Videostream
Class Map match-any allvideo (id 10)
   Match   dscp af41 (34)
Class Map match-any jabberaudiosignaling (id 11)
   Match access-group name JabberSIGNALING
Class Map match-any allvoice (id 12)
   Match   dscp ef (46)
Class Map match-any RTPaudio (id 19)
   Match access-group name JabberVOIP
   Match access-group name H323Audiostream
Class Map match-any class-default (id 0)
   Match any
Class Map match-any jabberRTPaudio (id 14)
   Match access-group name JabberVOIP
Class Map match-any non-client-nrt-class (id 1)
   Match non-client-nrt
Class Map match-any H323audiosignaling (id 17)
   Match access-group name H323AudioSignaling
Class Map match-any H323videosignaling (id 18)
   Match access-group name H323VideoSignaling
Class Map match-any signaling (id 20)
   Match access-group name JabberSIGNALING
   Match access-group name H323VideoSignaling
   Match access-group name H323AudioSignaling
```

show policy-map

The following is an example of the policy-maps configured on the platform:

```
Device# show policy-map
show policy-map
  Policy Map port_child_policy
    Class non-client-nrt-class
      bandwidth remaining ratio 7
    Class allvoice
      priority level 1
     police rate percent 10
       conform-action transmit
       exceed-action drop
    Class allvideo
      priority level 2
     police rate percent 20
       conform-action transmit
       exceed-action drop
    Class class-default
      bandwidth remaining ratio 63
  Policy Map SSIDin
    Class class-default
      set dscp dscp table dscp2dscp
  Policy Map SSIDout_child_policy
    Class allvoice
      priority level 1
     police cir 6000000 bc 187500
       conform-action transmit
       exceed-action drop
      admit cac wmm-tspec
        rate 6000 (kbps)
```

```
        wlan-up 6
    Class allvideo
      priority level 2
     police cir 6000000 bc 187500
       conform-action transmit
       exceed-action drop
      admit cac wmm-tspec
        rate 6000 (kbps)
        wlan-up 4 5
  Policy Map taggingPolicy
    Class RTPaudio
      set dscp ef
    Class H323realtimevideo
      set dscp af41
    Class signaling
      set dscp cs3
  Policy Map SSIDout
    Class class-default
      set dscp dscp table dscp2dscp
      set wlan user-priority dscp table dscp2up
      shape average 30000000 (bits/sec)
      queue-buffers ratio 0
      service-policy SSIDout_child_policy
  Policy Map parent_port
    Class class-default
      shape average 1000000000 (bits/sec) op
```

show wlan

The following is an example of the WLAN configuration and service-policy parameters:

```
Device# show wlan name test1 | include Policy
AAA Policy Override                               : Disabled
QoS Service Policy - Input
  Policy Name                                     : SSIDin
  Policy State                                    : Validated
QoS Service Policy - Output
  Policy Name                                     : SSIDout
  Policy State                                    : Validated
QoS Client Service Policy
  Input  Policy Name                              : taggingPolicy
  Output Policy Name                              : taggingPolicy
Radio Policy                                      : All
```

show policy-map interface

The following is an example of the policy-map installed for a specific interface:

```
Device# show policy-map interface wireless ssid name test1
Remote SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00C2EB000000001F
  Service-policy input: SSIDin
    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp dscp table dscp2dscp

Remote SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00D0D08000000021

  Service-policy input: SSIDin

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
```

```
        30 second rate 0 bps
      QoS Set
        dscp dscp table dscp2dscp

SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E

  Service-policy input: SSIDin

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp dscp table dscp2dscp

  Service-policy output: SSIDout

    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp dscp table dscp2dscp
        wlan user-priority dscp table dscp2up
      shape (average) cir 30000000, bc 120000, be 120000
      target shape rate 30000000
      queue-buffers ratio 0

      Service-policy : SSIDout_child_policy

        Class-map: allvoice (match-any)
          Match:  dscp ef (46)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 1
          police:
              cir 6000000 bps, bc 187500 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps
          cac wmm-tspec rate 6000 kbps

        Class-map: allvideo (match-any)
          Match:  dscp af41 (34)
            0 packets, 0 bytes
            30 second rate 0 bps
          Priority: Strict,

          Priority Level: 2
          police:
              cir 6000000 bps, bc 187500 bytes
            conformed 0 bytes; actions:
              transmit
            exceeded 0 bytes; actions:
              drop
            conformed 0000 bps, exceed 0000 bps
          cac wmm-tspec rate 6000 kbps

        Class-map: class-default (match-any)
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps

SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00DB568000000020

  Service-policy input: SSIDin

    Class-map: class-default (match-any)
      Match: any
```

```
          0 packets, 0 bytes
          30 second rate 0 bps
        QoS Set
          dscp dscp table dscp2dscp

    Service-policy output: SSIDout

      Class-map: class-default (match-any)
        Match: any
          0 packets, 0 bytes
          30 second rate 0 bps
        QoS Set
          dscp dscp table dscp2dscp
          wlan user-priority dscp table dscp2up
        shape (average) cir 30000000, bc 120000, be 120000
        target shape rate 30000000
        queue-buffers ratio 0

        Service-policy : SSIDout_child_policy

          Class-map: allvoice (match-any)
            Match:  dscp ef (46)
              0 packets, 0 bytes
              30 second rate 0 bps
            Priority: Strict,

            Priority Level: 1
            police:
                cir 6000000 bps, bc 187500 bytes
              conformed 0 bytes; actions:
                transmit
              exceeded 0 bytes; actions:
                drop
              conformed 0000 bps, exceed 0000 bps
            cac wmm-tspec rate 6000 kbps

          Class-map: allvideo (match-any)
            Match:  dscp af41 (34)
              0 packets, 0 bytes
              30 second rate 0 bps
            Priority: Strict,

            Priority Level: 2
            police:
                cir 6000000 bps, bc 187500 bytes
              conformed 0 bytes; actions:
                transmit
              exceeded 0 bytes; actions:
                drop
              conformed 0000 bps, exceed 0000 bps
            cac wmm-tspec rate 6000 kbps

          Class-map: class-default (match-any)
            Match: any
              0 packets, 0 bytes
              30 second rate 0 bps

  Device(config)# show policy-map interface wireless client
  Client 8853.2EDC.68EC iifid:
  0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E.0x00E0D04000000022

    Service-policy input: taggingPolicy

      Class-map: RTPaudio (match-any)
        Match: access-group name JabberVOIP
          0 packets, 0 bytes
          30 second rate 0 bps
        Match: access-group name H323Audiostream
          0 packets, 0 bytes
          30 second rate 0 bps
        QoS Set
          dscp ef
```

```
    Class-map: H323realtimevideo (match-any)
      Match: access-group name H323Videostream
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp af41

    Class-map: signaling (match-any)
      Match: access-group name JabberSIGNALING
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name H323VideoSignaling
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name H323AudioSignaling
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp cs3
    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps

  Service-policy output: taggingPolicy

    Class-map: RTPaudio (match-any)
      Match: access-group name JabberVOIP
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name H323Audiostream
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp ef

    Class-map: H323realtimevideo (match-any)
      Match: access-group name H323Videostream
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp af41

    Class-map: signaling (match-any)
      Match: access-group name JabberSIGNALING
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name H323VideoSignaling
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: access-group name H323AudioSignaling
        0 packets, 0 bytes
        30 second rate 0 bps
      QoS Set
        dscp cs3
    Class-map: class-default (match-any)
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
```

show platform qos policies

The following is an example of the QoS policies installed for ports, AP radios, SSIDs, and clients.

Note: You can only verify, but cannot change the radio policies.

```
Device# show platform qos policies PORT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ----------------  ---------------
L:0 Gi1/0/20           0x01023f4000000033 OUT defportangn       INSTALLED IN HW
L:0 Gi1/0/20           0x01023f4000000033 OUT port_child_policy INSTALLED IN HW

Device(config)# show platform qos policies RADIO
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- --------------------------------
L:0 R56356842871193604 0x00c8384000000004 OUT def-11an         INSTALLED IN HW
L:0 R68373680329064451 0x00f2e98000000003 OUT def-11gn         INSTALLED IN HW

Device(config)# show platform qos policies SSID
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- --------------------------------
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout_child_policy INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout_child_policy INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout           INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout           INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b IN  SSIDin            INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 IN  SSIDin            INSTALLED IN HW

Device(config)# show platform qos policies CLIENT
Loc Interface          IIF-ID             Dir Policy           State
--- ------------------ ------------------ --- ---------------- ---------------
L:0 8853.2edc.68ec     0x00e0d04000000022 IN  taggingPolicy    NOT INSTALLED IN HW
L:0 8853.2edc.68ec     0x00e0d04000000022 OUT taggingPolicy    NOT INSTALLED IN HW
```

show wireless client mac-address <mac> service-policy

The following is an example of the policy-maps applied at client level:

```
Device# show wireless client mac-address 8853.2EDC.68EC service-policy output
Wireless Client QoS Service Policy
Policy Name  : taggingPolicy
Policy State : Installed
Device# show wireless client mac-address 8853.2EDC.68EC service-policy in
Device# show wireless client mac-address 8853.2EDC.68EC service-policy input
Wireless Client QoS Service Policy
Policy Name  : taggingPolicy
Policy State : Installed
```

Troubleshooting QoS Configuration Issues

Currently, there is no specific troubleshooting information available for this configuration.