



## Configuring QoS

---

This chapter describes how to configure quality of service (QoS) on your access point. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the access point offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.



**Note**

---

For complete syntax and usage information for the commands used in this chapter, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release.

---

This chapter consists of these sections:

- [Understanding QoS for Wireless LANs, page 14-2](#)
- [Configuring QoS, page 14-4](#)
- [QoS Configuration Examples, page 14-10](#)

# Understanding QoS for Wireless LANs

Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

When you configure QoS on the access point, you can select specific network traffic, prioritize it, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. Implementing QoS in your wireless LAN makes network performance more predictable and bandwidth utilization more effective.

When you configure QoS, you create QoS policies and apply the policies to the VLANs configured on your access point. If you do not use VLANs on your network, you can apply your QoS policies to the access point's Ethernet and radio ports.

## QoS for Wireless LANs Versus QoS on Wired LANs

The QoS implementation for wireless LANs differs from QoS implementations on other Cisco devices. With QoS enabled, access points perform the following:

- They do not classify packets; they prioritize packets based on DSCP value, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag.
- They do not construct internal DSCP values; they only support mapping by assigning IP DSCP, Precedence, or Protocol values to Layer 2 COS values.
- They carry out EDCF like queuing on the radio egress port only.
- They do only FIFO queueing on the Ethernet egress port.
- They support only 802.1Q/P tagged packets. Access points do not support ISL.
- They support only MQC policy-map **set cos** action.
- They prioritize the traffic from voice clients (such as Symbol phones) over traffic from other clients when the QoS Element for Wireless Phones feature is enabled.
- They support Spectralink phones using the class-map IP protocol clause with the protocol value set to 119.

To contrast the wireless LAN QoS implementation with the QoS implementation on other Cisco network devices, see the *Cisco IOS Quality of Service Solutions Configuration Guide* at this URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_c/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_c/index.htm)

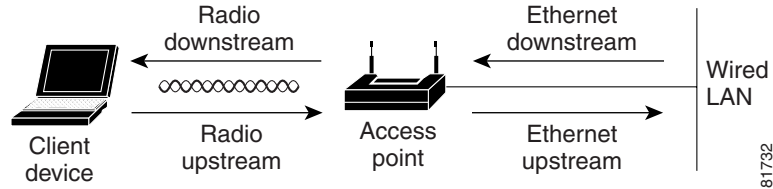
## Impact of QoS on a Wireless LAN

Wireless LAN QoS features are a subset of the proposed 802.11e draft. QoS on wireless LANs provides prioritization of traffic from the access point over the WLAN based on traffic classification.

Just as in other media, you might not notice the effects of QoS on a lightly loaded wireless LAN. The benefits of QoS become more obvious as the load on the wireless LAN increases, keeping the latency, jitter, and loss for selected traffic types within an acceptable range.

QoS on the wireless LAN focuses on downstream prioritization from the access point. [Figure 14-1](#) shows the upstream and downstream traffic flow.

Figure 14-1 Upstream and Downstream Traffic Flow



- The radio downstream flow is traffic transmitted out the access point radio to a wireless client device. This traffic is the main focus for QoS on a wireless LAN.
- The radio upstream flow is traffic transmitted out the wireless client device to the access point. QoS for wireless LANs does not affect this traffic.
- The Ethernet downstream flow is traffic sent from a switch or a router to the Ethernet port on the access point. If QoS is enabled on the switch or router, the switch or router might prioritize and rate-limit traffic to the access point.
- The Ethernet upstream flow is traffic sent from the access point Ethernet port to a switch or router on the wired LAN. The access point does not prioritize traffic that it sends to the wired LAN based on traffic classification.

## Precedence of QoS Settings

When you enable QoS, the access point queues packets based on the Layer 2 class of service value for each packet. The access point applies QoS policies in this order:

1. Packets already classified—When the access point receives packets from a QoS-enabled switch or router that has already classified the packets with non-zero 802.1Q/P user\_priority values, the access point uses that classification and does not apply other QoS policy rules to the packets. An existing classification takes precedence over all other policies on the access point.



**Note** Even if you have not configured a QoS policy, the access point always honors tagged 802.1P packets that it receives over the radio interface.

2. *QoS Element for Wireless Phones* setting—If you enable the *QoS Element for Wireless Phones* setting, traffic from voice clients takes priority over other traffic regardless of other policy settings. The *QoS Element for Wireless Phones* setting takes precedence over other policies, second only to previously assigned packet classifications.
3. Policies you create on the access point—QoS Policies that you create and apply to VLANs or to the access point interfaces are third in precedence after previously classified packets and the *QoS Element for Wireless Phones* setting.
4. Default classification for all packets on VLAN—If you set a default classification for all packets on a VLAN, that policy is fourth in the precedence list.

# Configuring QoS

QoS is disabled by default (however, the radio interface always honors tagged 802.1P packets even when you have not configured a QoS policy). This section describes how to configure QoS on your access point. It contains this configuration information:

- [Configuration Guidelines, page 14-4](#)
- [Configuring QoS Using the Web-Browser Interface, page 14-4](#)
- [Adjusting Radio Access Categories, page 14-8](#)
- [Disabling AVVID Priority Mapping, page 14-10](#)

## Configuration Guidelines

Before configuring QoS on your access point, you should be aware of this information:

- The most important guideline in QoS deployment is to be familiar with the traffic on your wireless LAN. If you know the applications used by wireless client devices, the applications' sensitivity to delay, and the amount of traffic associated with the applications, you can configure QoS to improve performance.
- QoS does not create additional bandwidth for your wireless LAN; it helps control the allocation of bandwidth. If you have plenty of bandwidth on your wireless LAN, you might not need to configure QoS.

## Configuring QoS Using the Web-Browser Interface

This section describes configuring QoS using the web-browser interface.

For a list of Cisco IOS commands for configuring QoS using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

Follow these steps to configure QoS:

- 
- Step 1** If you use VLANs on your wireless LAN, make sure the necessary VLANs are configured on your access point before configuring QoS.
- Step 2** Click **Services** in the task menu on the left side of any page in the web-browser interface. When the list of Services expands, click **QoS**. The QoS Policies page appears. [Figure 14-2](#) shows the QoS Policies page.

Figure 14-2 QoS Policies Page

QoS POLICIES    RADIO0-802.11B ACCESS CATEGORIES    RADIO1-802.11A ACCESS CATEGORIES    ADVANCED

Hostname UD\_AP1230    UD\_AP1230 uptime is 2 days, 17 hours, 27 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: <NEW>

Policy Name:

Classifications:

Delete Classification

Match Classifications:    Apply Class of Service

IP Precedence: Routine (0)    Best Effort (0) Add

IP DSCP:  Best Effort    Best Effort (0) Add  
  (0-63)

IP Protocol 119    Best Effort (0) Add

Filter: No Filters defined. [Define Filters.](#)

Apply    Delete    Cancel

Apply Policies to Interface/ VLANs

	FastEthernet	Radio0-802.11B	Radio1-802.11A
Incoming	< NONE >	< NONE >	< NONE >
Outgoing	< NONE >	< NONE >	< NONE >

Apply    Cancel

98779

**Step 3** With <NEW> selected in the Create/Edit Policy field, type a name for the QoS policy in the Policy Name entry field. The name can contain up to 25 alphanumeric characters. Do not include spaces in the policy name.

- Step 4** If the packets that you need to prioritize contain IP precedence information in the IP header TOS field, select an IP precedence classification from the IP Precedence drop-down menu. Menu selections include:
- Routine (0)
  - Priority (1)
  - Immediate (2)
  - Flash (3)
  - Flash Override (4)
  - Critic/CCP (5)
  - Internet Control (6)
  - Network Control (7)
- Step 5** Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets of the type that you selected from the IP Precedence menu. The access point matches your IP Precedence selection with your class of service selection. Settings in the Apply Class of Service menu include:
- Best Effort (0)
  - Background (1)
  - Spare (2)
  - Excellent (3)
  - Control Lead (4)
  - Video <100ms Latency (5)
  - Voice <100ms Latency (6)
  - Network Control (7)
- Step 6** Click the **Add** button beside the Class of Service menu for IP Precedence. The classification appears in the Classifications field. To delete a classification, select it and click the **Delete** button beside the Classifications field.
- Step 7** If the packets that you need to prioritize contain IP DSCP precedence information in the IP header TOS field, select an IP DSCP classification from the IP DSCP drop-down menu. Menu selections include:
- Best Effort
  - Assured Forwarding — Class 1 Low
  - Assured Forwarding — Class 1 Medium
  - Assured Forwarding — Class 1 High
  - Assured Forwarding — Class 2 Low
  - Assured Forwarding — Class 2 Medium
  - Assured Forwarding — Class 2 High
  - Assured Forwarding — Class 3 Low
  - Assured Forwarding — Class 3 Medium
  - Assured Forwarding — Class 3 High
  - Assured Forwarding — Class 4 Low
  - Assured Forwarding — Class 4 Medium
  - Assured Forwarding — Class 4 High

- Class Selector 1
- Class Selector 2
- Class Selector 3
- Class Selector 4
- Class Selector 5
- Class Selector 6
- Class Selector 7
- Expedited Forwarding

- Step 8** Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets of the type that you selected from the IP DSCP menu. The access point matches your IP DSCP selection with your class of service selection.
- Step 9** Click the **Add** button beside the Class of Service menu for IP DSCP. The classification appears in the Classifications field.
- Step 10** If you need to prioritize the packets from Spectralink phones (IP Protocol 119) on your wireless LAN, use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to Spectralink phone packets. The access point matches Spectralink phone packets with your class of service selection.
- Step 11** Click the **Add** button beside the Class of Service menu for IP Protocol 119. The classification appears in the Classifications field.
- Step 12** If you need to assign a priority to filtered packets, use the Filter drop-down menu to select a Filter to include in the policy. (If no filters are defined on the access point, a link to the Apply Filters page appears instead of the Filter drop-down menu.) For example, you could assign a high priority to a MAC address filter that includes the MAC addresses of IP phones.



---

**Note** The access list you use in QoS does not affect the access point's packet forwarding decisions.

---

- Step 13** Use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to packets that match the filter that you selected from the Filter menu. The access point matches your filter selection with your class of service selection.
- Step 14** Click the **Add** button beside the Class of Service menu for Filter. The classification appears in the Classifications field.
- Step 15** If you want to set a default classification for all packets on a VLAN, use the Apply Class of Service drop-down menu to select the class of service that the access point will apply to all packets on a VLAN. The access point matches all packets with your class of service selection.
- Step 16** Click the **Add** button beside the Class of Service menu for *Default classification for packets on the VLAN*. The classification appears in the Classifications field.
- Step 17** When you finish adding classifications to the policy, click the **Apply** button under the Apply Class of Service drop-down menus. To cancel the policy and reset all fields to defaults, click the **Cancel** button under the Apply Class of Service drop-down menu. To delete the entire policy, click the **Delete** button under the Apply Class of Service drop-down menu.
- Step 18** Use the Apply Policies to Interface/VLANs drop-down menus to apply policies to the access point Ethernet and radio ports. If VLANs are configured on the access point, drop-down menus for each VLAN's virtual ports appear in this section. If VLANs are not configured on the access point, drop-down menus for each interface appear.

- Step 19** Click the **Apply** button at the bottom of the page to apply the policies to the access point ports.
- Step 20** If you want the access point to give priority to all voice packets regardless of VLAN, click the **Advanced** tab. [Figure 14-3](#) shows the QoS Policies - Advanced page.

**Figure 14-3 QoS Policies - Advanced Page**

HOME EXPRESS SET-UP NETWORK MAP + ASSOCIATION NETWORK INTERFACES + SECURITY + SERVICES Telnet/SSH Hot Standby CDP DNS Filters HTTP Proxy Mobile IP QoS SNMP NTP VLAN ARP Caching WIRELESS SERVICES + SYSTEM SOFTWARE + EVENT LOG +

QoS POLICIES RADIO0-802.11B ACCESS CATEGORIES RADIO1-802.11A ACCESS CATEGORIES **ADVANCED**

Hostname UD\_AP1230 UD\_AP1230 uptime is 2 days, 17 hours, 40 minutes

Services: QoS Policies - Advanced

IP Phone

QoS Element for Wireless Phones :  Enable  Disable

IGMP Snooping

Snooping Helper:  Enable  Disable

AVVID Priority Mapping

Map Ethernet Packets with CoS 5 to CoS 6:  Yes  No

Apply Cancel 98778

Select **Enable** and click **Apply** to give top priority to all voice packets.



**Note** When you enable QoS Element for Wireless Phones, the access point gives top priority to voice packets even if you do not enable QoS. This setting operates independently from the QoS policies that you configure.

## Adjusting Radio Access Categories

The access point uses the radio access categories to calculate backoff times for each packet. As a rule, high-priority packets have short backoff times.

The default values in the Min and Max Contention Window fields and in the Slot Time fields are based on settings recommended in IEEE Draft Standard 802.11e. For detailed information on these values, consult that standard.

We strongly recommend that you use the default settings on the Radio Access Categories page. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose. If you change these values and find that you need to reset them to defaults, use the default settings listed in [Table 14-1](#).

The values listed in Table 14-1 are to the power of 2. The access point computes Contention Window values with this equation:

$$CW = 2^{**} X \text{ minus } 1$$

where X is the value from Table 14-1.

Table 14-1 Default QoS Radio Access Categories

Class of Service	Min Contention Window	Max Contention Window	Fixed Slot Time
Background	5	10	6
Best Effort	3	10	2
Video <100ms Latency	4	5	1
Voice <100ms Latency	3	4	1

Figure 14-4 shows the Radio Access Categories page. Dual-radio access points have a Radio Access Categories page for each radio.

Figure 14-4 Radio Access Categories Page

HOME  
EXPRESS SET-UP  
NETWORK MAP +  
ASSOCIATION  
NETWORK INTERFACES +  
SECURITY +  
**SERVICES**  
Telnet/SSH  
Hot Standby  
CDP  
DNS  
Filters  
HTTP  
Proxy Mobile IP  
**QoS**  
SNMP  
NTP  
VLAN  
ARP Caching  
WIRELESS SERVICES +  
SYSTEM SOFTWARE +  
EVENT LOG +

QoS POLICIES    **RADIO0-802.11B ACCESS CATEGORIES**    RADIO1-802.11A ACCESS CATEGORIES    ADVANCED

Hostname UD\_AP1230    UD\_AP1230 uptime is 2 days, 18 hours, 41 minutes

Services: QoS Policies - Access Category Definition

Access Category	Min Contention Window (2 <sup>x</sup> -1; x can be 0-10)	Max Contention Window (2 <sup>x</sup> -1; x can be 0-10)	Fixed Slot Time (0-20)
Background (CoS 1-2)	5	10	6
Best Effort (CoS 0)	5	10	2
Video (CoS 3-5)	4	5	1
Voice (CoS 6-7)	3	4	1

Apply    Cancel

98780

## Disabling IGMP Snooping Helper

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch and a client roams from one access point to another, the client's multicast session is dropped. When the access point's IGMP snooping helper is enabled, the access point sends a general IGMP query to the network infrastructure on behalf of the client every time the client associates or reassociates to the access point. By doing so, the multicast stream is maintained for the client as it roams.

The IGMP snooping helper is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **Disable**, and click **Apply**. [Figure 14-3](#) shows the QoS Policies - Advanced page.

## Disabling AVVID Priority Mapping

AVVID priority mapping maps Ethernet packets tagged as class of service 5 to class of service 6. This feature enables the access point to apply the correct priority to voice packets for compatibility with Cisco AVVID networks.

AVVID priority mapping is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **No** for Map Ethernet Packets with CoS 5 to CoS 6, and click **Apply**. [Figure 14-3](#) shows the QoS Policies - Advanced page.

## QoS Configuration Examples

These sections describe two common uses for QoS:

- [Giving Priority to Voice Traffic, page 14-10](#)
- [Giving Priority to Video Traffic, page 14-12](#)

## Giving Priority to Voice Traffic

This section demonstrates how you can apply a QoS policy to your wireless network's voice VLAN to give priority to wireless phone traffic.

In this example, the network administrator creates a policy named *voice\_policy* that applies voice class of service to traffic from Spectralink phones (protocol 119 packets). The user applies the *voice\_policy* to the incoming and outgoing radio ports and to the outgoing Ethernet port for VLAN 77. [Figure 14-5](#) shows the administrator's QoS Policies page.

Figure 14-5 QoS Policies Page for Voice Example

QoS POLICIES    RADIO0-802.11B ACCESS CATEGORIES    RADIO1-802.11A ACCESS CATEGORIES    ADVANCED

Hostname UD\_AP1230    UD\_AP1230 uptime is 2 days, 18 hours, 36 minutes

Services: QoS Policies

Create/Edit Policies

Create/Edit Policy: voice\_policy

Policy Name: voice\_policy

Classifications: IP Protocol 119 - COS Voice < 10ms Latency (6)

Delete Classification

Match Classifications:

IP Precedence: Routine (0)    Best Effort (0)    Add

IP DSCP:  Best Effort    Best Effort (0)    Add  
 (0-63)

IP Protocol 119: Best Effort (0)    Add

Filter: A795    Best Effort (0)    Add

Default Classification for Packets on the VLAN: Best Effort (0)    Add

Apply    Delete    Cancel

Apply Policies to Interface/ VLANs

VLAN 13	FastEthernet	Radio0-802.11B	Radio1-802.11A
Incoming	< NONE >	voice_policy	
Outgoing	voice_policy	voice_policy	
VLAN 14	FastEthernet	Radio0-802.11B	Radio1-802.11A
Incoming	< NONE >		< NONE >
Outgoing	< NONE >		< NONE >

Apply    Cancel

The network administrator also enables the *QoS element for wireless phones* setting on the QoS Policies - Advanced page. This setting gives priority to all voice traffic regardless of VLAN.

98782

## Giving Priority to Video Traffic

This section demonstrates how you could apply a QoS policy to a VLAN on your network dedicated to video traffic.

In this example, the network administrator creates a policy named *video\_policy* that applies video class of service to video traffic. The user applies the *video\_policy* to the incoming and outgoing radio ports and to the outgoing Ethernet port for VLAN 87. Figure 14-6 shows the administrator's QoS Policies page.

Figure 14-6 QoS Policies Page for Video Example

The screenshot displays the Cisco IOS QoS Policies configuration page. The left sidebar shows navigation options, with 'QoS' selected. The main content area is titled 'QoS POLICIES' and shows the configuration for a policy named 'video\_policy'.

**Hostname:** UD\_AP1230  
**UD\_AP1230 uptime:** is 2 days, 18 hours, 36 minutes

**Services:** QoS Policies

**Create/Edit Policies**

**Create/Edit Policy:** video\_policy

**Policy Name:** video\_policy

**Classifications:**  
 Precedence Priority - COS Video < 100ms Latency (5)  
 DSCP Class Selector 7 - COS Video < 100ms Latency (5)

**Match Classifications:**

**IP Precedence:** Routine (0) | **Apply Class of Service:** Best Effort (0) [Add]

**IP DSCP:** Best Effort | Best Effort (0) [Add]

**IP Protocol 119:** | Best Effort (0) [Add]

**Filter:** A795 | Best Effort (0) [Add]

**Default Classification for Packets on the VLAN:** Best Effort (0) [Add]

[Apply] [Delete] [Cancel]

**Apply Policies to Interface/ VLANs**

VLAN 13	FastEthernet	Radio0-802.11B	Radio1-802.11A
Incoming	< NONE >	< NONE >	
Outgoing	< NONE >	< NONE >	
<b>VLAN 14</b>	<b>FastEthernet</b>	<b>Radio0-802.11B</b>	<b>Radio1-802.11A</b>
Incoming	< NONE >		video_policy
Outgoing	video_policy		video_policy

[Apply] [Cancel]

98781