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.

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.

Note When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. See the "Using Wi-Fi Multimedia Mode" section on page 15-4 for information on WMM.

QoS for Wireless LANs Versus QoS on Wired LANs

The QoS implementation for wireless autonomous access points differs from QoS implementations on wired devices:

- 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 WMM type of queuing on the radio egress ports.
- They do only FIFO queuing 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 VoWLAN IP 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

Impact of QoS on a Wireless LAN

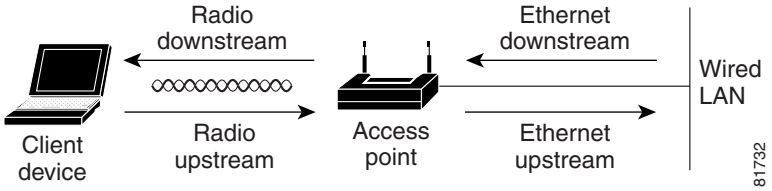
Wireless LAN QoS features are an implementation of the Wi-FI Alliance WMM certification, based on the IEEE 802.11e amendment. Any wireless client certified WMM can implement Wireless LAN QOS in the upstream direction (from the wireless client to the AP). Any client certified 802.11n or 802.11ac is also certified WMM.

Regardless of the client support (or lack of support) for WMM, Cisco access points support WMM and can be configured to provide wireless QoS in the downstream direction (from the AP toward the wireless clients), and in the upstream direction when forwarding wireless frames to the wired interface.

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 15-1 shows the upstream and downstream traffic flow.

Figure 15-1 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. Each client independently determines what prioritization mechanisms should be used for this traffic. The AP cannot force a prioritization mechanism for the client uplink traffic. However, the AP configuration determines if uplink prioritization is allowed (when WMM is enabled on the AP SSID) or disallowed (when WMM is disabled on the AP SSID).
- 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. However, the AP maintains the traffic QoS marking.

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 and uses the matching 802.11e user priority queue to send the packet over the air. You can use the Streams page to configure the rate at which each queue should be sent and the number of retries for unicast packets.

2. *QoS Element for Wireless Phones* setting—If you enable the *QoS Element for Wireless Phones* setting, dynamic voice classifiers are created for are created for RTP-based traffic, which allows the wireless phone traffic to be a higher priority than other clients' traffic. Additionally, the QoS Basic Service Set (QBSS) is enabled to advertise channel load information in the beacon and probe response frames. Some IP phones use QBSS elements to determine which access point to associate to, based on the traffic load.
   You can use the Cisco IOS command dot11 phone dot11e command to enable 802.11e/WMM QBSS Load IE. The 7920 phones with 1.05 firmware, and older, do not support the 802.11e QBSS IE. If your network wireless clients are primarily 7920 phones with firmware 1.05 or older, enable dot11 phone.
   If your network wireless clients are primarily 7920 with firmware 1.09 or later, or WMM compatible VoWLAN phones, enable the IEEE 802.11e compatible QBSS IE with the command dot11 phone dot11e.

   This example shows how to enable IEEE 802.11 phone support with the legacy QBSS Load element:

   ```
   AP(config)# dot11 phone
   ```

   This example shows how to enable IEEE 802.11 phone support with the standard IEEE 802.11e QBSS Load element:

   ```
   AP(config)# dot11 phone dot11e
   ```

   This example shows how to stop or disable the IEEE 802.11 phone support:

   ```
   AP(config)# no dot11 phone
   ```

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.

Using Wi-Fi Multimedia Mode

When you enable QoS, the access point uses Wi-Fi Multimedia (WMM) mode by default. WMM provides these enhancements over basic QoS mode:

- The access point adds each packet's class of service to the packet's 802.11 header to be passed to the receiving station.
- Each access class has its own 802.11 sequence number. The sequence number allows a high-priority packet to interrupt the retries of a lower-priority packet without overflowing the duplicate checking buffer on the receiving side.
- WPA/WPA2 replay detection is done per access class on the receiver. Like 802.11 sequence numbering, WPA/WPA2 replay detection allows high-priority packets to interrupt lower priority retries without signaling a replay on the receiving station.
- For access classes that are configured to allow it, transmitters that are qualified to transmit through the normal backoff procedure are allowed to send a set of pending packets during the configured transmit opportunity (a specific number of microseconds). Sending a set of pending packets improves throughput because each packet does not have to wait for a backoff to gain access; instead, the packets can be transmitted immediately one after the other.
- U-APSD Power Save is enabled.

The access point uses WMM enhancements in packets sent to client devices that support WMM. The access point applies basic QoS policies to packets sent to clients that do not support WMM.

Use the **no dot11 qos mode wmm** configuration interface command to disable WMM using the CLI. To disable WMM using the web-browser interface, unselect the check boxes for the radio interfaces on the QoS Advanced page. Figure 15-3 shows the QoS Advanced page.

Using Band Select

Band Select allows you to move dual-band capable wireless clients joining the cell, to the less congested 5 GHz radio, if your SSID is available on both radios. This feature improves the overall performance of the network.

When the Band Select feature is enabled, the access point delays the probe responses on the 2.4 GHz radio to all new clients, for all SSIDs that are Band Select-enabled. At the same time, the access point does not delay the probe responses on the 5 GHz radio. This mechanism allows dual-band clients to discover the SSID on the 5 GHz radio first, thus pushing these clients to associate to the SSID on the AP 5 GHz radio instead of the 2.4 Ghz radio. Only those clients that are 2.4 GHz-only will stay on the 2.4 GHz radio.

To enable Band Select, follow these steps:

Step 1 Choose **Security > SSID Manager.**

Step 2 Click **NEW** to create a new SSID.

or

Choose the required SSID from the **Current SSID.**

Step 3 Click the **Band Select** radio button.

Step 4 Click **Apply**.

Note The band select feature is useful only if the SSID is assigned to both radios.

When a client actively discovers a network, that client sends probe requests on one or several channels. A typical behavior is to send a burst of probe requests on a given channel, collect the replies from the responding APs, and then move to the next channel. For this reason, two consecutive probe requests received on a given channel does not necessarily indicate two attempts to discover APs on a channel, but may be part of the same scan cycle through a burst.

You can fine tune the Band Select behavior to determine information such as:

- How long a scan cycle is expected to last
- The number of cycles during which an AP will not respond to probe request from a client on a 2.4 GHz channel, along with client RSSI
- Timeout for the Band Select mechanism to be triggered.

To assign the parameters for Band Select, follow these steps:

Step 1 Choose **Services > Band Select.**

Step 2 Check the **Band Select** check box.

Step 3 Enter the values for the following:

- Client-Rssi—Minimum Receive Signal Strength Indicator (RSSI) required for the client to be eligible for band select. The range is from 20 to 90.
- Cycle-Count—Number of probe requests on the 2.4 GHz band that the access point ignores.
- Cycle-Threshold (ms)—Time in milliseconds that the access point can expect each probe request burst cycle from the client. The range is from 1 to 1000.
- Expire-Dual-Band (secs)—Time after which dual-band clients will be declared as new and may have their probe request frames delayed or ignored again. The range is from 10 to 300.
- Expire-Suppression (secs)—Time after which 2.4 GHz-only clients will be declared as new and may have their probe frames delayed or ignored again. The range is from 10 to 200.

Step 4 Click **Apply**.

Beginning in privileged EXEC mode, use these commands to configure BandSelect using the access point CLI:

- ap(config)# **dot11 band-select parameters**
- ap(config-bs-profile)# **cycle-count?**
- ap(config-bs-profile)# **cycle-threshold?**
- ap(config-bs-profile)# **expire-suppression?**
- ap(config-bs-profile)# **expire-dual-band?**
- ap(config-bs-profile)# **client-rssi?**
- ap (config)# **dot11 ssid abcd**
- ap(config-ssid)# **band-select**

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

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.
- The **ampdu** command is available for the 802.11n radio interfaces. Aggregate MAC protocol data unit (AMPDU) is a structure containing multiple MPDUs transported as a single PSDU by the physical layer. For additional information about this command, see the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges.*

Configuring QoS Using the Web-Browser Interface

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

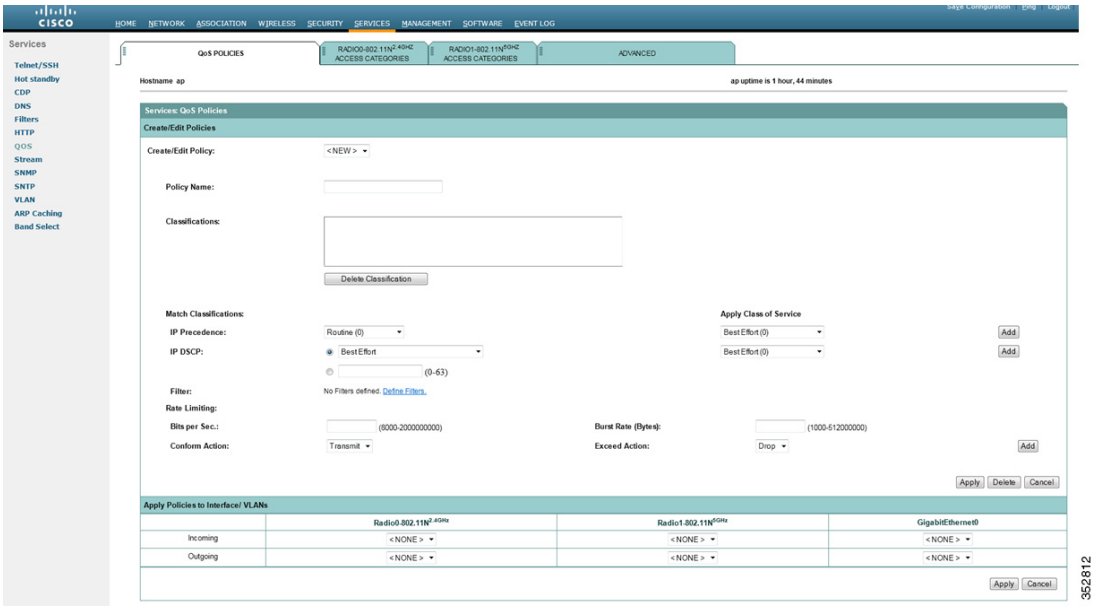
For a list of Cisco IOS commands for configuring QoS using the CLI, consult the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*.

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 general menu bar at the top of any page in the web-browser interface. When the list of Services appears, click **QoS**. The QoS Policies page appears. Figure 15-2 shows the QoS Policies page.

Figure 15-2 QoS Policies Page



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.

Note You can also select two preconfigured QoS policies: WMM and Spectralink. When you select either of these, a set of default classifications are automatically populated in the Classification field.

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 list. 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 To select the 802.11e User Priority value that the access point will apply to the frames that will be sent to wireless clients, for packets of type that you selected from the IP Precedence menu. The access point matches your IP Precedence selection with your 802.11 user priority (class of service) selection. The Apply Class of Service (representing the 802.11e user priority value to apply) drop-down list contains:

- 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 instead of IP precedence information in the IP header ToS field, select an IP DSCP classification from the IP DSCP drop-down list. 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 list to select the class of service (that is, the 802.11e user priority value) 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 list 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 list 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 list.) 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 only affects the prioritization of the target packets, not the AP (security) forwarding decisions.

Step 13 Use the Apply Class of Service drop-down list 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 When you finish adding classifications to the policy, click the **Apply** button under the Apply Class of Service drop-down lists. To cancel the policy and reset all fields to defaults, click the **Cancel** button under the Apply Class of Service drop-down lists. To delete the entire policy, click the **Delete** button under the Apply Class of Service drop-down lists.

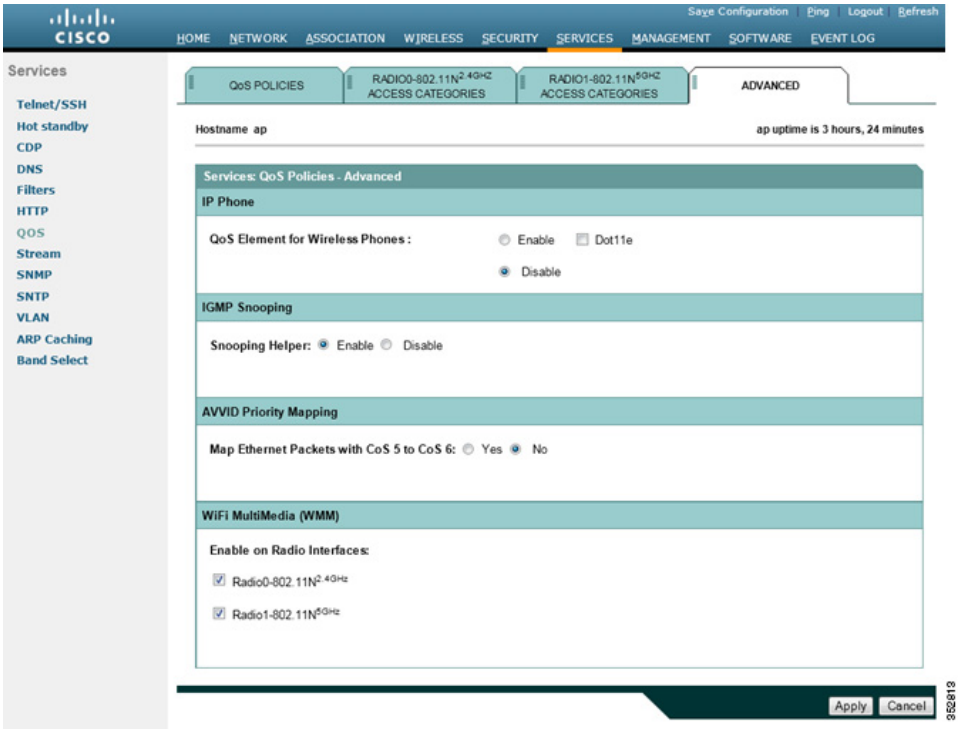
Step 16 Use the Apply Policies to Interface/VLANs drop-down lists to apply policies to the access point Ethernet and radio ports. If VLANs are configured on the access point, drop-down lists for each VLANs' virtual ports appear in this section. If VLANs are not configured on the access point, drop-down lists for each interface appear.

Step 17 Click the **Apply** button at the bottom of the page to apply the policies to the access point ports.

The QoS Policies Advanced Page

The QoS Policies Advanced page (Figure 15-3)

Figure 15-3 QoS Policies - Advanced Page



Select **Enable the QoS Element for Wireless Phones** option and click Select Enable the QoS Element for Wireless Phones option and click Apply to give top priority to all voice packets.

QoS Element for Wireless Phones

When you enable the 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.

Select **dot11e** to use the WMM / 802.11e version of QBSS Load IE. If you leave this selection blank, the CCX pre-802.11e version of the QBSS Load IE is used. Use the pre-802.11e version if your wireless clients are primarily 7920 phones with firmware 1.05 or older. Use the 802.11e version if your clients are primarily WMM compatible clients.

IGMP Snooping

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch, the switch forwards multicast traffic only to those ports where the switch registers that multicast traffic as needed. As a consequence, when a wireless client roams from one access point to another access point connected to the same switch, the switch initially does not know whether or not the multicast traffic is needed on the port to the second access point. The result is that the clients' multicast session is interrupted. IGMP snooping on the access point helps mitigating this issue.

When the access points' IGMP snooping helper is enabled, and a client joins the access point cell, the access point immediately sends a general IGMP query to the wireless LAN, prompting the client to send in an IGMP membership report. The membership report is forwarded to the wired interface. When the network infrastructure receives the host's IGMP membership report, it ensures delivery of that host's multicast data stream to the access point port. The traffic is then relayed to the wireless interface. This way, the wireless client multicast flow is not interrupted while roaming.

When Internet Group Membership Protocol (IGMP) snooping is enabled on a switch and a client roams from one access point to another, the clients' multicast session is dropped. When the access points' IGMP snooping helper is enabled, the access point sends a general query to the wireless LAN, prompting the client to send in an IGMP membership report. When the network infrastructure receives the host's IGMP membership report, it ensures delivery of that host's multicast data stream.

The IGMP snooping helper is enabled by default. To disable it, browse to the QoS Policies - Advanced page, select **Disable**, and click **Apply**.

Note If there is no multicast router for processing IGMP query and response from the host, it is mandatory that **no igmp snooping** be configured on the access point. when IGMP snooping is enabled, all multicast group traffic must send IGMP query and response packets. If IGMP query or response packets are not detected, all multicast traffic for the group is dropped.

AVVID Priority Mapping

The 802.11e protocol assigns to voice packets a User Priority value of 6. Cisco wired networks follow the IETF recommendation to assign to voice packets a class of service value of 5. Enabling AVVID priority mapping maps the Ethernet packets tagged as class of service 5, to class of service 6 when these packets are exchanged between the wireless and the wired sides of the access point. 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**.

WiFi Multimedia (WMM)

Using the Admission Control check boxes, you can enable or disable WMM support on the access point's radio interfaces. Default is enabled. When WMM is enabled, both WMM and non-WMM clients are allowed to join the access point radio.

Note When you enable admission control (in RADIO1-802.11N2.4GHZ ACCESS CATEGORIES or RADIO1-802.11N5GHZ ACCESS CATEGORIES), clients associated to the access point must complete the WMM admission control procedure before they can use that access category.

Rate Limiting

Rate limiting provides control over the data traffic transmitted or received on an interface.The Class-Based Policing feature performs the following functions:

- Limits the input or output transmission rate of a class of traffic based on user-defined criteria.
- Marks packets by setting the IP precedence value, IP differentiated services code point (DSCP) value and Quality of Service (QoS) group.

This is used to rate-limit the upstream traffic originating from each of the non-roots to root bridge incase of P2MP setup. To do rate-limiting on downstream traffic , class-maps are applied at the root-side router/switch.

Note Rate-limiting can be applied to ethernet ingress only

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 802.11 amendment. For detailed information on these values, see the IEEE 802.11e amendment, 7.3.2.27 or 802.11-2012 standard, 8.4.2.31 (EDCA Parameter Set element).

Cisco strongly recommends 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 15-1.

The values listed in Table 15-1 are to the power of 2. The access point computes Contention Window values with this equation:

CW = 2 ** X minus 1

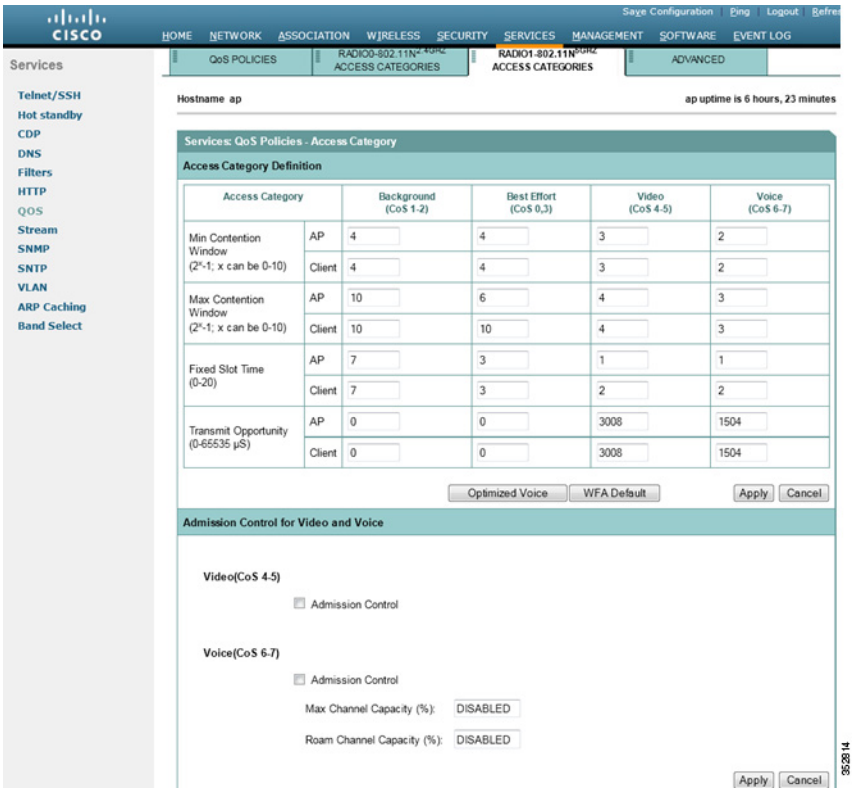
where X is the value from Table 15-1.

Table 15-1 Default QoS Radio Access Categories

Class of Service	Min Contention Window		Max Contention Window		Fixed Slot Time		Transmit Opportunity		Admission Control	
	Local	Cell	Local	Cell	Local	Cell	Local	Cell	Local	Cell
Background	4		10		6		0			
Best Effort	4		10		2		0			
Video <100ms Latency	3		2		1		3008			
Voice <100ms Latency	2		3		1		1504			

Figure 15-4 shows the Radio Access Categories page. Dual-radio access points have a Radio Access Categories page for each radio.

Figure 15-4 Radio Access Categories Page



Wireless clients using TCLAS and TSPEC can request a class of service through an ADDTS (add Traffic Stream Request) sent to the access point before the client initiates the traffic stream. The ADDTS describes the intended traffic, along with the expected nominal rates for that traffic.

Configuring Nominal Rates

When an access point receives an ADDTS (add traffic stream) request from a WMM client, it checks the nominal rate or minimum PHY rate in the ADDTS request against the nominal rates defined by the CLI command **traffic-stream**. If they do not match, the access point rejects the ADDTS request.

If you choose Optimized Voice Settings (see Figure 15-4), the following nominal rates are configured:

- 5.5Mbps, 6.0Mbps, 11.0Mbps, 12.0Mbps, and 24.0Mbps

Information about the **traffic-stream** command can be found in the *Command Reference for Cisco Aironet Access Points and Bridges*, which is available at cisco.com at the following URL:

http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr12410b-chap2.html#wp3257080

Note The above rates work fine for Cisco phones and most WMM VoWLAN IP phones. However, some third party wireless phones.... Third parties wireless phones may have a different nominal rate or minimum PHY rate. You may need to enable additional nominal rates for these phones.

Optimized Voice Settings

Using the Admission Control check boxes, you can control client use of the access categories. When you enable admission control for an access category, clients associated to the access point must complete the WMM admission control procedure before they can use that access category. However, access points do not support the admission control procedure in this release, so clients cannot use the access category when you enable Admission Control.

Configuring Call Admission Control

Configuring Call Admission Control (CAC) on an access point involves the following:

1. Configuring the radio.
2. Enabling admission control on an SSID.

Configuring the Radio

This section describes how to configure admission control on an access point's radio.

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

Follow these steps to configure admission control on a radio:

Step 1 Click the Access Categories page of the radio you want to configure.

Figure 15-4 shows an example of an Access Categories page.

Step 2 Select the **Admission Control** check box under **Voice(CoS 6-7)**.

Step 3 Enter the maximum percentage of the channel to be used for voice in the **Max Channel Capacity (%)** field.

Step 4 Enter the maximum percentage of the channel to use for roaming calls in the **Roam Channel Capacity (%)** field.

The percentage of the channel used by roaming calls up to the value specified in this field is deducted from the value you specified in the **Max Channel Capacity (%)** field.

For example, suppose you have entered 75% in the **Max Channel Capacity (%)** field and 6% in the **Roam Channel Capacity (%)**. If roaming calls are using 5% of the channel, a maximum of 70% of the channel can be used for voice calls (new calls initiated by clients in the cell).

Step 5 To enable call admission control for real time video traffic (AC_VO), check the **Admission Control** check box under **Video (CoS 5-6)**.

Note The admission control settings you have configured in this section will not take effect until you enable admission control on an SSID.

Enabling Admission Control on the SSID

This section describes how to enable admission control on an SSID.

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

Follow these steps to enable admission control on an SSID:

Step 1 Open the SSID Manager page.

Step 2 Select an SSID.

Step 3 Under **General Settings**, select **Enable** in the **Call Admission Control** field.

Troubleshooting Admission Control

You can use two CLI commands to display information to help you troubleshoot admission control problems:

- To display current admission control settings on radio 0, enter the following command:

  ```
  # show dot11 cac int dot11Radio 0
  ```

- To display current admission control settings on radio 1, enter the following command:

  ```
  # show dot11 cac int dot11Radio 1
  ```

- To display information about admitted streams with admission control and MT, enter the following command:

  ```
  # show dot11 traffic-streams
  ```

Configuring Streams

QoS policies mark or remark packets that go through the access point. When defining a QoS policy, you can also decide on limiting the rate of certain traffic.

QoS Elements for Wireless phones allows you to prioritize any voice packet regardless of any other consideration. This applies a low latency configuration to voice packets, without any upper limit.

Configuring streams is the third way of applying prioritization techniques to time-sensitive traffic, by determining which traffic should be sent with higher priority (low latency queue), and limit the amount of retries for these time-sensitive packets. Streams can be used in combination with other QoS configurations.

To configure these features, go to **Services > Streams** page (see Figure 15-5).

Step 1 From the Packet Handling per User Priority section, select the User Priorities queues that should be served with a low latency queuing logic.

- If **Reliable** is selected, unicasts packets are resent, if they are not acknowledged, as long as the destination is still reachable (wireless client associated or wireless bridge connected). The maximum amount of retries for a unicast packet that has not be acknowledged is determined at the radio level, with the Max data retries value configured in the Settings tab of each radio configuration section.

- If **Low Latency** is selected, you can configure the amount of retries that the AP should use before discarding the current packet and sending the next one. For low latency traffic, skipping a packet is usually preferable to interrupting the flow of traffic. In the Max Retries for Packet Discard, enter the max number of retries that the Ap should use for the matching User Priority set to Low Latency.

Step 2 Click **Apply** to validate.

Step 3 At the bottom of the page, in the Low Latency Packet Rates section, you can also configure the rate at which the frames set for the Low Latency queues should be sent.

- Nominal—The AP will try to use this rate to send the Low Latency Packets (using the faster rate first, and depending on the client signal level).
- Non-nominal—The AP will try not to use that rate, but will revert to it if no nominal rate is possible.
- Disabled—The AP will not try to use that rate.

Step 4 Click **Apply** to validate.

To configure streams using the CLI, see Chapter 6, "Configuring Radio Settings."

Figure 15-5 Streams Page