

Configuring QoS

This chapter describes how to configure quality of service (QoS) on your access point/bridge. With this feature, you can provide preferential treatment to certain traffic at the expense of others. Without QoS, the access point/bridge 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 14-5
- QoS Configuration Examples, page 14-12

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/bridge, 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 VLAN configured on your access point/bridge. If you do not use VLANs on your network, you can apply your QoS policies to the access point/bridge'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 14-4 for information on WMM.

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/en/US/docs/ios/12_2/qos/configuration/guide/fqos_c.html

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/bridge 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



QoS on the wireless LAN focuses on downstream prioritization from the access point/bridge. These are the effects of QoS on access point/bridge traffic:

- The radio downstream flow is traffic transmitted out the access point/bridge 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/bridge. 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/bridge. 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/bridge Ethernet port to a switch or router on the wired LAN. The access point/bridge 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/bridge queues packets based on the Layer 2 class of service value for each packet. The access point/bridge applies QoS policies in this order:

1. Packets already classified—When the access point/bridge 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/bridge 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/bridge.



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, dynamic voice classifiers are created for some of the wireless phone vendor clients, 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 the future upgrade of the 7920 Wireless Phone firmware to support the standard QBSS Load IE. The new 7920 Wireless Phone firmware will be announced at a later date.



This release continues to support existing 7920 wireless phone firmware. Do not attempt to use the new standard (IEEE 802.11e draft 13) QBSS Load IE with the 7920 Wireless Phone until new phone firmware is available for you to upgrade your phones.

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 draft 13) QBSS Load element:

AP(config) # no 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/bridge—QoS Policies that you create and apply to VLANs or to the access point/bridge interfaces are second in precedence after previously classified packets.
- **4.** Default classification for all packets on VLAN—If you set a default classification for all packets on a VLAN, that policy is third 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 replay detection is done per access class on the receiver. Like 802.11 sequence numbering, WPA replay detection allows high-priority packets to interrupt lower priority retries without signalling 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.

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 14-4 shows the QoS Advanced page.

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 14-5
- Configuring QoS Using the Web-Browser Interface, page 14-5
- Adjusting Radio Access Category Definitions, page 14-9
- "Disabling IGMP Snooping Helper" section on page 14-11
- "Disabling AVVID Priority Mapping" section on page 14-11

Configuration Guidelines

Before configuring QoS on your access point/bridge, 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 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 browse to the command reference:

1. Click this link to browse to the Cisco Support and Documentation home page:

http://www.cisco.com/cisco/web/support/index.html

 Follow this path to the product, document, and chapter: Products & Solutions > Wireless > All Wireless Products > Cisco Aironet 1300 Series > Technical Documentation > Command References > Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, 12.x(xx)JA

Follow these steps to configure QoS:

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 1 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.

Ciso	co Aironet 1300 Series Wireless	Bridge
	RADIO0-802.11G ACCESS CATEGORIES	ED
Hostname repeater	·	repeater uptime is 6 days, 23 hours, 47 r
+		
Services: QoS Policies	;	
+ Create/Edit Policies		
Create/Edit Policy:	<new></new>	
Policy Name:		
Classifications:		
+		
-	Delete Classification	
Match Classification	ns:	Apply Class of Service
IP Precedence:	Routine (0)	Best Effort (0)
IP DSCP:	 Best Effort 	Best Effort (0)
	0 (0-63)	
ID D		
IP Protocol 119	No Fillers defined Define Fillers	
Filter:	No Fliters defined. <u>Define Fliters.</u>	
Default Classificat	tion for Packets on the VLAN:	Best Effort (0)
		Apply Delete Can
Apply Policies to Interf	ace/ VLANs	
VLAN 1	FastEthernet	Radio0-802.11G
Incoming		< NONE >
Outgoing	< NONE > -	< NONE > 🔽
1/1 AN 74	F 4Fab	De 31-0 000 44/0
Incoming		
Outgoing		
	< NUNE >	
		Apply Can

Figure 14-2 QoS Policies Page

Step 2 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 3** 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 4** 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 5 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 6** 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 7** 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 8** Click the Add button beside the Class of Service menu for IP DSCP. The classification appears in the Classifications field.
- Step 9 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 10** Click the **Add** button beside the Class of Service menu for IP Protocol 119. The classification appears in the Classifications field.
- **Step 11** 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.



The access list you use in QoS does not affect the access points' packet forwarding decisions.

- **Step 12** 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 13** Click the **Add** button beside the Class of Service menu for Filter. The classification appears in the Classifications field.
- Step 14 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 15** 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 16 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 menus. To delete the entire policy, click the Delete button under the Apply Class of Service drop-down menus.
- Step 17 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 VLANs' virtual ports appear in this section. If VLANs are not configured on the access point, drop-down menus for each interface appear.

Step 18 Click the **Apply** button at the bottom of the page to apply the policies to the access point ports.

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
Figure 14-3	QoS Policies - Advanced Page

IOME	QoS POLICIES		
	A00233 CA12001		
	Hostnama AD12128C		AD1242AC untimo io 1 hour. 12 minutor
	Hosmame AP1242AG		AP1242AG uptime is 1 hour, 15 minutes
SSOCIATION +			
IETWORK	Services: QoS Policies - Advanced		
TERFACES +			
ECURITY +	IP Phone		
ERVICES			
Teinet/SSH	QoS Element for Wireless Phones :	🖲 Enable 🛛 Dot11e	
Hot Standby		C. Disable	
CDP		© Disable	
DNS	ICMD Speening		
Filters	IGMP Shooping		
HTTP			
QoS	Snooping Helper: 🖲 Enable 🔘 Disable		
SNMP			
SNTP			
/LAN	AVVID Priority Mapping		
ARP Caching			
IRELESS SERVICES + YSTEM SOFTWARE + VENT LOG +	Map Ethernet Packets with CoS 5 to CoS 6:	C Yes ⊙ No	
	WiFi MultiMedia (WMM)		
	Enable on Radio Interfaces:		
	Radio0-802 11G		
	Radio1-802.11A		

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



Click **dot11e** to use the latest version of QBSS Load IE. If you do click **dot11e**, the previous version QBSS Load IE is used.

<u>Note</u>

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 Category Definitions

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.

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 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 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	Transmit Opportunity
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 14-4 shows the Radio 802.11G Access Categories page.

HOME	QoS POLICIES	RADIO0-802.11G ACCESS CATEGORIES		D		
EXPRESS SET-UP EXPRESS SECURITY NETWORK MAP +	Hostname repeater				repeater uptime	e is 1 week, 19 minute
ETWORK +	Services: QoS Policies - A	Access Category Definiti	on			
NTERFACES BECURITY + SERVICES Telnet(SSH	Access Category	Min Contention Window (2 [×] -1; x can be 0-10)	Max Contention Window (2 [×] -1; x can be 0-10)	Fixed Slot Time (0-20)	Admission Control	Transmit Opportunity (0-65535 µS)
CDP DNS	Background (CoS 1-2)	4	10	7	🗖 Enable	0
Filters HTTP	Best Effort (CoS 0,3)	4	10	3	🗖 Enable	0
QoS SNMP	- Video (CoS 4-5)	3	4	2	🗖 Enable	3008
VLAN	Voice (CoS 6-7)	2	3	2	🗆 Enable	1504

Figure 14-4 Radio 802.11G Access Categories Page

<u>Note</u>

In this release, clients are blocked from using an access category when you select **Enable** for Admission Control.

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.

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 clients' multicast session is dropped. When the access points' 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.

CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links

For best performance on your bridge links, adjust the CW-min and CW-max contention window settings according to the values listed in Table 14-2. The default settings, CW-min 3 and CW-max 10, are best for point-to-point links. However, for point-to-multipoint links, you should adjust the settings depending on the number of non-root bridges that associate to the root bridge.



If packet concatenation is enabled, you need to adjust the CW-min and CW-max settings only for traffic class 0. Concatenation is enabled by default.

Table 14-2	CW-min and CW-max Settings for Point-to-Point and Poir	nt-to-Multipoint Bridge Links
------------	--	-------------------------------

Setting	Point-to-Point Links	Point-to-Multipoint Links with up to 5 Non-Root Bridges	Point-to-Multipoint Links with up to 10 Non-Root Bridges	Point-to-Multipoint Links with up to 17 Non-Root Bridges
CW-min	3	4	5	6
CW-max	10	10	10	10

	Command	Purpose		
Step 1	configure terminal	Enter global configuration mode.		
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.		
Step 3	<pre>traffic class { cw-min number } { cw-max number } { fixed-slot number }</pre>	Assign CW-min, CW-max, and fixed-slot settings to a traffic class. Use the values in Table 14-2 to enter settings that provide the best performance for your network configuration. Note If packet concatenation is enabled, you need to adjust the CW min and CW may settings only for traffic class.		
		0. Concatenation is enabled by default.		
Step 4	end	Return to privileged EXEC mode.		
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.		

Beginning in privileged EXEC mode, follow these steps to adjust the CW-min and CW-max settings:

Use the **no** form of the command to reset the setting to defaults.

QoS Configuration Examples

These sections describe two common uses for QoS:

- Giving Priority to Voice Traffic, page 14-12
- Giving Priority to Video Traffic, page 14-13

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.

EXPRESS SECURITY totalge uptime is 1 day, 23 hours, 55 minutes NETWORK MAP • NETWORK MAP • NETWORK MAP • Security • NETWORK MAP • Security • Pointy Security • OP ONS Sinkip • NTP • VLAN • Sinkip • NP • VLAN • Sinkip • NP • VLAN • Sinkip • NP • VLAN • Sinkip • Pointy I Base • IP Procedence: • Pointy Eles Centreli •	HOME		RADIO0-802.11G ACCESS CATEGORIES	
EXPRESS SECURITY Hostname bridge bridge uptme is 1 day, 23 hours, 55 minutes Secure Call Policies Services: 005 Policies Services: 005 Policies Create Edit Policy: voice_policy Policy Name: voice_policy Policy Name: Policy Name: Policy Name: voice_policy Policy Name: Policy Name: Policy Name: Prove Mobile IP Cos Policy Name: Precedence Priority-COS Voice < 10ms Latency (6) INTP VA.N Precedence: Policy Name: Precedence Priority-COS Voice < 10ms Latency (6) IP Precedence: Policy Name: Precedence Priority-COS Voice < 10ms Latency (6) Add IP Precedence: Policy IIP Precedence: Policy IIP Add IP Precedence: Pouline (0) Best Effort (0) Add IP Precedence: Pouline (1) Best Effort (0) Add IP Precedence: Pouline Effort Best Effort (0) Add IP Precedence: No Filters defined. Define Filters. Apply Defete Cencel Apply Defete Cencel Apply Policies to Interface/ VLANs FastEthernet Radiol 802.116 Apply Cencel <t< th=""><th>EXPRESS SET-UP</th><th></th><th></th><th></th></t<>	EXPRESS SET-UP			
Services: OoS Palicies Services: OoS Palicies Create Edit Policy: Create Edit Policy: Policy Name: Voice_policy Policy Name: Voice_policy Policy Name: Voice_policy Cassifications: Precedence Priority-COS Voice < 10ms Latency (6) Delete Clossification Match Classifications: Precedence Priority-COS Voice < 10ms Latency (6) Delete Clossification Match Classifications: Precedence: Procedence: Proceden	EXPRESS SECURITY	Hostname bridge		bridge uptime is 1 day, 23 hours, 55 minutes
Services: OoS Policies Services: OoS Policies Create/Edit Policy: Policy Name: Voice_policy Policy Name: Voice_policy Policy Name: Voice_policy Policy Name: Porow Mobile IP OoS SIMP NTP VLAN STP ARP Caching Match Classifications: Precedence Priority-COS Voice < 10ms Latency (6) Delete Classification NTP VLAN STP ARP Caching Match Classifications: Precedence: Policy Name: Policy Name: Policy Name: Precedence: Policy Name: Policy Name: Policy Name: Policy Name: Policy Name: Policy Name: Pol	NETWURK MAP +			
NTERFACES TenderScis TenderScis SERVICS Create/Edit Policy: Vicate/Edit Policy: Policy Name: Voice_policy Policy Name: Vicate/Edit Policy: Vicate/Edit Policy: Policy Name: Policy:	NETWORK	Services: OoS Policies		
SECURITY • Create/Edit Policies TeineWSSH COP DNS Filters HTTP Proxy Mobile IP OOS OSS SIMP NTP VLAN STP ARP Caching Precedence: Policy Name: VENT LOO Match Classifications: Precedence: Policy Classifications: Precedence: Policy Name: VENT LOO Match Classifications: Apply Class of Service IP Precedence: Poutine (0) @ IP Precedence: Poutine (0) @ @ Protocol 119 Eest Effort (0) @ Policy S to Interface/ VLAMs Poly Delete Cancel Apply Policies to Interface/ VLAMs Policy @ Outgoing Voice_policy @ Outgoing Voice_policy @ Outgoing <	NTERFACES +			
SERVICES Tokes3814 COP DNS Filters Policy Name: Voice_policy Policy Name: Voice_policy Policy Name: Voice_policy Policy Name: Voice_policy Policy Name: Precedence Priority-COS Voice < 10ms Latency (6) Classifications: Precedence Priority-COS Voice < 10ms Latency (6) Delete Classification MRELEBS SERVICES NAPC Delete Classification MRELEBS SERVICES Hatch Classifications: Precedence: Poutine (0) Pest Etion Prove that the the the the the the the the the th	SECURITY +	Create/Edit Policies		
TeinetSSH Create/Edit Policy: voice_policy • DNS Filters Filters Policy Name: voice_policy. Prov Mobile IP OoS OoS SNMP NTP UAN STP ARP Caching MRELESS SERVICES + * YOTEM SOFTWARE + * Match Classifications: Precedence: Policy Name: Delete Classification NTP Delete Classification Match Classifications: Precedence: Portice Policy Name () IP Precedence: Policy Nam	SERVICES			
COP NS Filters Provy Mobile IP OoS SNMP NPP VLAN STP APP Caching WIRELESS SERVICES * Match Classifications: Delete Classification ************************************	Teinet/SSH	Create/Edit Policy:	voice_policy 💌	
DNS Filters HTTP Prog Mobile IP OoS SNMP NTP VLAN STP ARP Caching MRELESS SERVICES + VSTEM SOFTWARE + VENT LOO * Policy Name: voice_policy Delete Classification: Precedence Priority - COS Voice < 10ms Latency (6) Delete Classification: Precedence Priority - COS Voice < 10ms Latency (6) Delete Classification: Delete Classification: Precedence: Routine (0) Precedence: Routi	CDP			
Filters Policy Name:: Voice_policy OOS OOS Classifications: Precedence Priority - COS Voice < 10ms Latency (6) NTP VLAN Delete Classification Delete Classification STP ARP Caching Delete Classification Match Classifications: VENT LOG Match Classifications: Routine (0) Delete Classification VENT LOG Match Classifications: Routine (0) Delete Classification IP Precedence: Routine (0) Best Effort (0) Add IP DSCP: e Best Effort Best Effort (0) Add IP Protocol 119 Best Effort (0) Add Filter: No Filters defined Define Eliters. Apply Delete Cancel Apply Delete to Interface/ VLANs Apply Delete Cancel Apply Cencel	DNS			
HTTP Prov Mobile IP OoS SINMP NTP VLAN STP ARP Caching Match Classifications: Precedence Routine (0) STEM SOFTWARE YENT LOO Match Classifications: Apply Class of Service IP Precedence: Routine (0) C Good IP DSCP: © Good IP Protocol 119 Filter: No Filters defined Define Filters. Apply Delete Cancel Apply Policies to Interface/ VLANs Incoming CNONE> Outgoing Voice_policy Outgoing Voice_policy	Filters	Policy Name:	voice policy	
Prozy Mobile IP OoS OSS SNMP NTP ULAN YLAN Delete Classification ARP Caching Delete Classification MIRELESS SERVCES + Match Classifications: YETEM SOFWARE + No Filters defined Define Filters.	HTTP	-		
OoS SIMP SIMP NTP VLAN STP ARP Caching Delete Classification WRELESS SERVICES + Precedence Priority - COS Voice < 10ms Latency (6) BYSTEM SOFTWARE + Delete Classification WRELESS SERVICES + Match Classifications: Bystem SOFTWARE + Match Classifications: IP Precedence: Routine (0) IP Precedence: Routine (0) IP DSCP: © Best Effort Best Effort (0) IP Protocol 119 Best Effort (0) Filter: No Filters defined. Define Filters. Apply Policies to Interface/ VLANs Add Incoming (NONE > Voice_policy Outgoing Voice_policy Voice_policy	Proxy Mobile IP			
SNMP Indeddeler holdy God Folds	QoS	Classifications:	Precedence Priority - COS Voice < 10ms Latency (6)	
NTP VLAN STP ARP Caching NIRELESS SERVICES + SYSTEM SOFTWARE + SYSTEM SOFTWARE + NIRELESS SERVICES + SYSTEM SOFTWARE + Match Classifications: Apply Class of Service IP Precedence: Routine (0) • Best Effort (0) • Add IP DSCP: Best Effort Best Effort (0) • Add Composition IP Protocol 119 Filter: No Filters defined. Define Filters. Apply Policies to Interface/ VLANs Incoming Incoming Outgoing Voice_policy • Outgoing Voice_policy • Apply Cence	SNMP			
VLAN STP ARP Caching MRTELESS SERVICES EVENT LOO Match Classifications: Apply Class of Service IP Precedence: Routine (0) IP DSCP: e Best Effort (0) IP Protocol 119 Filter: No Filters defined. Define Filters. Apply Delete Cancel Apply Policies to Interface/ VLANs Incoming Outgoing Voice_policy Voice_policy Apply Cancel	NTP			
STP ARP Caching WIRELESS SERVICES STETEM SOFTWARE EVENT LOG Match Classifications: Apply Class of Service IP Precedence: Routine (0) • IP DSCP: © (0-63) IP Protocol 119 Filter: No Filters defined. Define Filters. Apply Delete Cancel Apply Policies to Interface/ VLANs Incoming (NONE > • Outgoing Voice_policy • Outgoing	VLAN			
APC Caching MIRELESS SERVICES ** Match Classifications: Match Classifications: P Precedence: Routine (0) @ (0-63) IP Protocol 119 Filter: No Filters defined. Define Filters. Apply Delete Cancel Apply Policies to Interface/ VLANs Incoming Inc	STP		<u> </u>	
Arr calling Match Classifications: IP Precedence: Routine (0) • IP Precedence: Routine (0) • IP DSCP: Best Effort IP Protocol 119 Filter: No Filters defined. Define Filters. Apply Delete Apply Delete Cancel Apply Olicies to Interface/VLANs Incoming Incoming Voice_policy • Voice_policy • Apply Cancel	APP Coching		Delete Classification	
Mitcle So service * Match Classifications: P Precedence: P Precedence: P DSCP: Best Effort P Protocol 119 Filter: Protocol 119 Filters Protocol 119 Filters Poscience: Apply Delete Apply Delete Apply Delete Apply Once_policy Apply Cancel Apply Cancel			Delete Classification	
Add IP Precedence: Routine (0) IP DSCP: Best Effort IP Protocol 119 Filter: No Filters defined. Define Filters. Apply Policies to Interface/ VLANs Apply Policies to Interface/ VLANs Incoming				
Match Classifications: Apply Class of Service IP Precedence: Routine (0) IP DSCP: © Best Effont © (0-63) IP Protocol 119 Best Effort (0) Filter: No Filters defined. Define Filters. Apply Policies to Interface/ VLANs Incoming NONE > Outgoing voice_policy Apply Cancel	EVENTIOG +			
IP Precedence: Routine (0) IP DSCP: e Best Effort IP Dotocol 119 Best Effort (0) IP Protocol 119 Best Effort (0) Filter: No Filters defined. Define Filters. Apply Delete Cancel Apply Policies to Interface/ VLANs Incoming (NONE) Outgoing Voice_policy Apply Cancel		Match Classification	X	Apply Class of Service
IP DSCP: © @ Best Effort @ (0-63) IP Protocol 119 Best Effort (0) ▼ Add Filter: No Filters defined. Define Filters. Apply Delete Cancel Apply Delete Cancel Incoming CNONE > ▼ Incoming <none> ▼ Outgoing voice_policy ▼ Outgoing voice_policy ▼</none>		IP Precedence:	Routine (0)	Best Effort (0) Add
IP Protocol 119 Best Effort (0) ▼ Add Filter: No Filters defined. Define Filters. Apply Policies to Interface/ VLANs Apply Policies to Interface/ VLANs Incoming (NONE > ▼ Outgoing voice_policy ▼ Apply Cencel		IP DSCP:	 Best Effort 	Best Effort (0) Add
IP Protocol 119 Best Effort (0) Add Filter: No Filters defined. Define Filters. Apply Delete Cancel Apply Policies to Interface/ VLANs FastEthernet Radio0.802.11G Incoming NONE > Outgoing voice_policy Apply Cencel			C (0-63)	
Filter: No Filters defined. Define Filters. Apply Delete Cancel Apply Policies to Interface/ VLANs Radio0 802.116 Incoming NONE > ▼ Voice_policy ▼ Outgoing voice_policy ▼ Apply Cancel		IP Protocol 119		Best Effort (0) Add
Apply Policies to Interface/ VLANs Apply Policies to Interface/ VLANs Radio0.802.11G Incoming <none> Outgoing voice_policy Voice_policy Apply Cancel</none>		Filter:	No Filters defined. Define Filters.	
Apply Policies to Interface/ VLANs Apply Policies to Interface/ VLANs Radio0-802.11G Incoming NONE > Voice_policy Outgoing voice_policy Voice_policy				
Apply Policies to Interface/ VLANs FastEthernet Radio0 802.11G Incoming <none> Outgoing voice_policy Voice_policy Apply Cancel</none>				Apply Delete Cancel
FastEthernet Radio0-802.11G Incoming NONE > • Voice_policy • Voice_policy • Apply Cancel Cancel 		Apply Policies to Interfa	ce/ VLANs	
Incoming NONE > Voice_policy Outgoing voice_policy voice_policy			FastEthernet	Radio0-802.11G
Outgoing voice_policy voice_policy Apply Cancel		Incoming	<none></none>	voice_policy
Apply Cancel		Outgoing	voice_policy 💌	voice_policy 💌
				Apply Cancel

Figure 14-5 QoS Policies Page for Voice Example

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.

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.

		RADIO0-802.11G	
OME		ACCESS CATEGORIES	
XPRESS SET-UP			
XPRESS SECURITY	Hostname bridge		bridge uptime is 2 days, 0 minute
ETWORK MAP +			
SSOCIATION +			
ETWORK +	Services: QoS Policies		
ECURITY +	Create/Edit Policies		
ERVICES			
Telnet/SSH	Create/Edit Policy:	video_policy 💌	
CDP			
DNS			
Filters	Policy Name:	video_policy	
НТТР			
Proxy Mobile IP			
QoS	Classifications:	Precedence Boutine - COS Video <100ms Latency (5)	
SNMP			
NTP			
VLAN			
STP		<u> </u>	
ARP Caching		Delete Classification	
		Delete oldssinctation	
YSTEM SOFTWARE +			
VENTLOG +	Madah Chandinan		Annha Class of Canadaa
	Match Classifications		Apply Class of Service
	IP Precedence:	Routine (0)	Video <100ms Latency (5) Add
	IP DSCP:	 Best Effort 	Best Effort (0) Add
		0 (0-63)	
	IP Protocol 119		Best Effort (II)
	Filter:	No Filters defined. Define Filters.	
			Apply Delete Cancel
	Apply Policies to Interfa	ce/ VLANs	
		FastEthernet	Radio0-802.11G
	Incoming	<none></none>	video_policy 💌
	Outgoing	video_policy 💌	video_policy 💌
			Apply Cancel

Figure 14-6	QoS Policies Pa	ige for Video Example
-------------	-----------------	-----------------------