



Implementing Quality of Service in a Wireless LAN

This module describes how to implement quality of service (QoS) features on a Cisco 800, 1800, 2800, or 3800 series integrated services router, hereafter referred to as an access point or AP.

QoS enables you to use congestion management and avoidance tools, which prevent traffic from slowing down on your wireless LAN (WLAN).

In a wired network, routers or switches primarily enforce QoS. In a WLAN, however, the access point manages QoS duties for traffic to wireless clients.

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.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [“Feature Information for Implementing Quality of Service in a Wireless LAN”](#) section on page 13.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Implementing QoS in a Wireless LAN, page 2](#)
- [Information About Implementing QoS in a Wireless LAN, page 2](#)
- [Configuration Examples for Implementing QoS on a Wireless LAN, page 11](#)
- [Additional References, page 12](#)
- [Feature Information for Implementing Quality of Service in a Wireless LAN, page 13](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Implementing QoS in a Wireless LAN

The following prerequisites apply to implementing QoS in a wireless LAN:

- If you use VLANs on your wireless LAN, make sure the necessary VLANs are configured on your access point before configuring QoS.
- Be familiar with the traffic on your wireless LAN. If you know the applications used by wireless client devices, the sensitivity of applications to delay, and the amount of traffic associated with the applications, configuring QoS improves performance.
- QoS does not create additional bandwidth on a wireless LAN; it helps control the allocation of bandwidth. If there is enough bandwidth on your wireless LAN, it might not be necessary to configure QoS.

Information About Implementing QoS in a Wireless LAN

Before you configure QoS on an access point, you should understand the following concepts:

- [QoS for Wireless LANs, page 2](#)
- [QoS Configuration Guidelines for Wireless LANs, page 4](#)
- [Access Control Lists, page 6](#)
- [Wi-Fi Multimedia Mode, page 7](#)

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 Compared to QoS on Wired LANs

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

- They do not classify packets; they prioritize packets based on the Dynamic Host Configuration Protocol (DSCP) value, client type (such as a wireless phone), or the priority value in the 802.1q or 802.1p tag.
- They do not match packets using access control lists (ACL); they use only Modular QoS CLI (MQC) class maps for matching clauses.
- They do not construct internal DSCP values; they support mapping only by assigning IP DSCP, Precedence, or Protocol values to Layer 2 Class of Service (CoS) values.

- They carry out Enhanced Distributed Coordination Function (EDCF) like queueing on the radio egress port only.
- They do only First In First Out (FIFO) queueing on the Ethernet egress port.
- They support only 802.1q/p tagged packets. Access points do not support Inter-Switch Link (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.

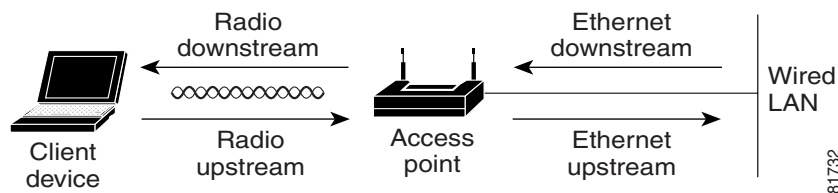
Impact of QoS on a Wireless LAN

Wireless LAN QoS features are a subset of the 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 10](#) shows the upstream and downstream traffic flow.

Figure 10 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 CoS value for each packet. If a packet matches one of the filter types based on its current precedence, the packet is classified based on the matching filter and no other filters are applied.

There are three levels of precedence for QoS filters.

- 0—Dynamically created VoIP client filter. Traffic from voice clients takes priority over other traffic regardless of other policy settings. This setting takes precedence over all other policies, second only to previously assigned packet classifications.
- 1—User configured class-map match clause (except match any). QoS policies configured for and that 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.
- 2—User configured class-map match any clause (match VLAN). If a default classification for all packets on a VLAN is set, that policy is fourth in the precedence list.

Precedence number zero is the highest.

QoS Configuration Guidelines for Wireless LANs

An access point is essentially a Layer 2 transparent bridge between wired and wireless networks. Typically, bandwidth on the wireless side constrains the wired side. For example, 802.11b offers 6 Mbps half duplex and 100BASE-T offers 100 Mbps full duplex.

A Cisco access point uses ACLs for forwarding or blocking packets on selective basis, as designated by the user for the purpose of:

- Providing QoS for Voice-over-IP (VoIP) phones.
- Mapping IP precedence values into 802.1p/q CoS values for downlink traffic.
- Providing Layer 2 and Layer 3 ACL features to the bridging path and access point host receive path.

802.11 VoIP Phone Support

The Symbol element is advertised by the access point. This helps a Symbol phone to make an association decision if there are multiple access points serving the area. The current packet rate is the calculation of average means of number of packets transmitted per second for the past 8 seconds.

After the normal 802.11 association process, a Symbol phone sends a proprietary Symbol 802.11 phone registration message (WNMP) to the access point to complete the association.

The Symbol phone does not associate to an access point if the advertised packet rate is above the threshold of the access point. The Symbol phone uses its Symbol element as optional information. Basic operation does not require an access point to send Symbol elements.

Cisco Wireless IP Phone 7920 Support

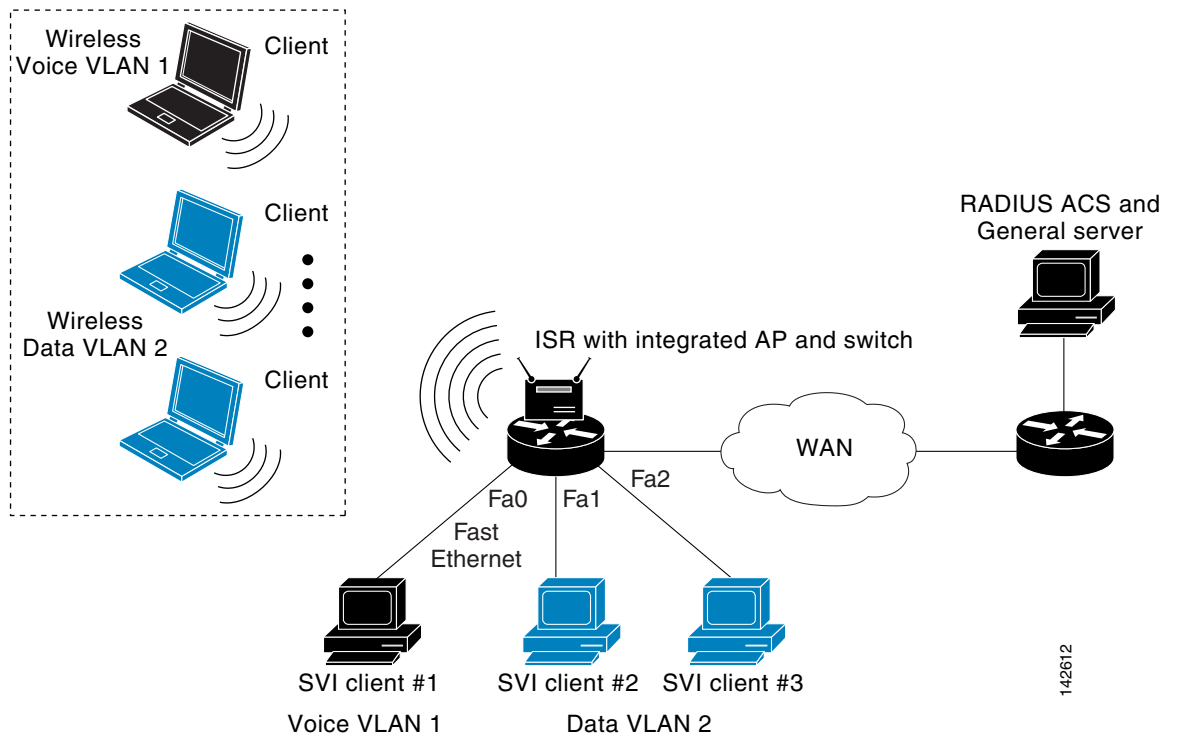
The wireless IP Phone 7920 uses Cisco Discovery Protocol (CDP) messages with Appliance VLAN-ID TLV to inform the access point of its presence. The access point intercepts the CDP messages sent from the client, and if it contains the Appliance VLAN-ID Type-Length-Value (TLV), it should flag the client as VoIP phone client.

If a VLAN is enabled, we recommend that all phone clients be associated to a single voice VLAN and that all data clients be associated to a separate data VLAN. If a VLAN is not enabled, we recommend that all the VoIP packets be classified by using the same user_priority value (6).

The access point always uses DIFS with minimum contention window (CW) value derived from the CWmax and CWmin range parameters to prioritize voice traffic.

Figure 11 shows the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 11 LAN and VLAN Segmentation with Wireless Devices



142612

Radio Interface Transmit Queues

The access point radio maintains four priority queues, one for each traffic category, and 802.11e EDCF to provide differentiated Distributed Coordination Function (DCF) access to the wireless medium. An EDCF-aware access point is assigned distinct pairs of CWmin and CWmax parameters for each traffic category. The CWmin and CWmax parameters can be modified through the CLI.

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 minimum and maximum 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 the standard.

We recommend that you use the default settings. Changing these values can lead to unexpected blockages of traffic on your wireless LAN, and the blockages might be difficult to diagnose.

Ethernet Interface Transmit Queue

Because the Ethernet interface always has a larger bandwidth than radio interface, there is no need to maintain priority queues for Ethernet interface. There will be only one transmit queue per Ethernet interface.

802.1Q Untagged Voice Packets

If a VLAN is enabled, Cisco IOS bridging code adds 802.1q tags into the untagged voice packets. The CoS value should be part of the VLAN configuration. For a voice VLAN, the CoS should be (6).

If a VLAN is not enabled, the access point relies on the DSCP-to-CoS filter configured by the user to assign CoS value to the packet.

CoS Values on a VLAN

The default CoS value for all the VLANs is zero (best effort). This ensures that the access point provides differentiated services based on VLAN IDs. Packets sent to these clients are queued into the appropriate priority queue based on their VLAN CoS value.

If a VLAN is enabled, and packets from a wireless client must be forwarded to the wired network, a 802.1q tag is added by the forwarding module.

Access Control Lists

ACLs are applied on either outbound or inbound interfaces. For standard inbound access lists, after receiving a packet, the Cisco IOS software checks the source address of the packet against the access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an Internet Control Message Protocol (ICMP) host unreachable message.

For extended access lists, the router also checks the destination access list. If the access list permits the address, the software continues to process the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

For standard outbound access lists, after receiving and routing a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists, the router also checks the destination access list. If the access list permits the address, the software sends the packet. If the access list rejects the address, the software discards the packet and returns an ICMP host unreachable message.

If the specified access list does not exist, all packets are passed.

When you enable outbound access lists, you automatically disable autonomous switching for that interface. When you enable input access lists on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception—a Storage Services Enabler (SSE) configured with simple access lists can still switch packets, on output only).

When you apply an access list that has not yet been defined to an interface, the software will act as if the access list has not been applied to the interface and will accept all packets. Remember this behavior if you use undefined access lists as a means of security in your network.

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.
- 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.

To disable WMM, use the **no dot11 qos mode wmm** command in interface configuration mode.

How to Implement QoS on a Wireless LAN

This section contains the following task:

- [Implementing QoS on a Wireless LAN, page 7](#) (optional)

Implementing QoS on a Wireless LAN

Perform this task to implement QoS features on a wireless LAN.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **dot11 phone**
4. **interface dot11Radio** *interface*
5. **ip access-group** {*access-list-number* | *access-list-name*} {**in** | **out**}
6. **bridge-group** *bridge-group* **input-address-list** *access-list-number*
7. **l2-filter bridge-group-acl**
8. **traffic-class** {**best-effort** | **background** | **video** | **voice**} [**cw-min** *min-value* | **cw-max** *max-value* | **fixed-slot** *backoff-interval*]
9. **end**
10. copy running-config startup-config

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	dot11 phone Example: Router(config)# dot11 phone	Enables 802.11 compliance phone support.

	Command or Action	Purpose
Step 4	interface dot11Radio <i>interface</i> Example: Router(config)# interface dot11Radio 0	(Optional) Enters interface configuration mode for the radio interface.
Step 5	ip access-group { <i>access-list-number</i> <i>access-list-name</i> } { in out } Example: Router(config-if)# ip access-group 101 out	(Optional) Controls access to an interface. <ul style="list-style-type: none"> The example shows how to apply access list 101 on packets outbound from an interface.
Step 6	bridge-group <i>bridge-group</i> input-address-list <i>access-list-number</i> Example: Router(config-if)# bridge-group 1 input-address-list 700	(Optional) Assigns an access list to a particular interface. <ul style="list-style-type: none"> This access list is used to filter packets received on that interface based on their MAC source addresses.
Step 7	l2-filter bridge-group-acl Example: Router(config-if)# l2-filter bridge-group-acl	(Optional) Applies a Layer 2 ACL filter to bridge group incoming and outgoing packets between the access point and the host (upper layer). <ul style="list-style-type: none"> If this command is enabled, and any Layer 2 ACLs are installed in ingress or egress, the same ACLs are applied to packets received or sent by the access point host stack.
Step 8	traffic-class { best-effort background video voice } [cw-min <i>min-value</i> cw-max <i>max-value</i> fixed-slot <i>backoff-interval</i>] Example: Router(config-if)# traffic-class best-effort cw-min 4 cw-max 10 fixed-slot 2	(Optional) Configures the radio interface QoS traffic class parameters for each of the four traffic types. <ul style="list-style-type: none"> Backoff parameters control how the radio accesses the airwaves. The cw-min and cw-max keywords specify the collision window as a power of 2. For example, if the value is set to 3, the contention window is 0 to 7 backoff slots (2 to the power 3 minus 1). The fixed-slot keyword specifies the number of backoff slots that are counted before the random backoff counter starts to count down.
Step 9	end Example: Router(config-if)# end	Returns to privileged EXEC mode.
Step 10	copy running-config startup-config Example: Router# copy running-config startup-config	Saves configuration changes to NVRAM so that they are not lost if there is a system reload or power outage.

Configuration Examples for Implementing QoS on a Wireless LAN

This section contains the following examples:

- [Configuring QoS on a Wireless LAN: Example, page 11](#)
- [Configuring QoS for a Voice VLAN on an Access Point in Routing Mode: Example, page 12](#)

Configuring QoS on a Wireless LAN: Example

The following example shows how to:

- Enable 802.11 compliance phone support.
- Configure the best effort traffic class for contention windows and fixed-slot backoff values.

Each time the backoff for best effort is started, the backoff logic waits a minimum of the 802.11 Short Inter-Frame Space (SIFS) time plus two backoff slots. It then begins counting down the 0 to 15 backoff slots in the contention window.

- Save your entries in the configuration file.

```
configure terminal
dot11 phone
interface dot11Radio 0/3/0
traffic-class best-effort cw-min 4 cw-max 10 fixed-slot 2
end
copy running-config startup-config
```

Configuring QoS for a Voice VLAN on an Access Point in Routing Mode: Example

Using [Figure 11](#) as a reference, this example shows how to create a VLAN for voice traffic on an access point in routing mode and apply QoS parameters to that voice VLAN:

```
configure terminal
class-map match-any voice_vlan
match vlan 2
policy-map voice
class voice_vlan
set cos 6
exit
exit
interface Dot11Radio 0/3/0
no ip address
ssid serialvoicevlan
vlan 2
authentication open
exit
exit
interface Dot11Radio 0/3/0.2
encapsulation dot1Q 2
ip address 10.2.1.1 255.255.255.0
service-policy output voice
end
copy running-config startup-config
```

Additional References

The following sections provide references related to implementing QoS on a wireless LAN.

Related Documents

Related Topic	Document Title
Cisco IOS bridging commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Bridging Command Reference</i>
Cisco IOS wireless LAN commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS Wireless LAN Command Reference</i>

Standards

Standard	Title
No new or modified standards are supported, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified.	—

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Implementing Quality of Service in a

Wireless LAN

Table 8 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Release 12.4T or later appear in the table.

For information on a feature in this technology that is not documented here, see the “Cisco IOS Wireless LAN Features Roadmap” module.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.



Note

Table 8 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 8 Feature Information for Implementing Quality of Service in a Wireless LAN

Feature Name	Releases	Feature Information
Wi-Fi Multimedia (WMM) Required Elements	12.4(15)T	WMM provides enhancements over basic QoS mode. The following section provides information about this feature: <ul style="list-style-type: none"> • Wi-Fi Multimedia Mode

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.