QoS on Wireless LAN Controllers and Lightweight APs Configuration Example

Document ID: 81831

Introduction

This document provides a configuration example that shows how to configure Quality of Service (QoS) in Cisco Unified Wireless network using Cisco Wireless LAN Controllers (WLCs) and Lightweight Access Points (LAPs).

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Basic knowledge of the configuration of LAPs and Cisco WLCs
- Knowledge of how to configure basic routing and QoS in a wired network

Components Used

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

- Cisco 2006 WLC that runs firmware release 4.0
- Cisco 1000 Series LAPs
- Cisco 802.11a/b/g Wireless Client Adapter that runs firmware release 2.6
- Cisco 3725 Router that runs Cisco IOS® Software Release 12.3(4)T1
- Cisco 3640 Router that runs Cisco IOS Software Release 12.2(26)
- Two Cisco 3500 XL Series Switches that run Cisco IOS Software Release 12.0(5)WC3b

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

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

With QoS, bandwidth can be managed more efficiently across LANs, which includes WLANs and WANs. This is how QoS provides enhanced and reliable network service:

- Supports dedicated bandwidth for critical users and applications
- Controls jitter and latency (required by real–time traffic)
- Manages and minimizes network congestion
- Shapes network traffic to smoothen the traffic flow
- Sets network traffic priorities

In the past, WLANs were mainly used to transport low–bandwidth, data–application traffic. Currently, with the expansion of WLANs into vertical (such as retail, finance, and education) and enterprise environments, WLANs are used to transport high–bandwidth data applications in conjunction with time–sensitive, multimedia applications. This requirement led to the necessity for wireless QoS.

The IEEE 802.11e working group within the IEEE 802.11 standards committee has completed the standard definition. However, the adoption of the 802.11e standard is in its early stages, and as with many standards there are many optional components. Just as what occurred with 802.11 security in 802.11i, industry groups such as the Wi–Fi Alliance, and industry leaders such as Cisco are defining the key requirements in WLAN QoS through their Wi–Fi MultiMedia (WMM) and Cisco Compatible Extensions (CCX) programs. This ensures the delivery of key features and interoperation through their certification programs.

Cisco Unified Wireless Products support WMM, a QoS system based on the IEEE 802.11e draft that has been published by the Wi–Fi Alliance.

The controller supports four QoS levels:

- Platinum/Voice Ensures a high quality of service for voice over wireless.
- Gold/Video Supports high–quality video applications.
- Silver/Best Effort Supports normal bandwidth for clients. This is the default setting.
- Bronze/Background Provides the lowest bandwidth for guest services.

Voice over IP (VoIP) clients should be set to Platinum, Gold, or Silver while low–bandwidth clients can be set to Bronze.

You can configure the bandwidth of each QoS level using QoS profiles and then apply the profiles to WLANs. The profile settings are pushed to the clients associated to that WLAN. In addition, you can create QoS roles to specify different bandwidth levels for regular and guest users.

For information on how to configure QoS profiles using the GUI, refer to Using the GUI to Configure QoS Profiles.

For information on how to configure QoS profiles using the CLI, refer to Using the CLI to Configure QoS Profiles.

Refer to the *Cisco Unified Wireless QoS* section of Enterprise Mobility Design Guide for more information on how QoS works in the Cisco Unified Wireless network.

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

Layer 3 QoS Packet Marking Enhancements

Cisco Unified Wireless network supports Layer 3 IP Differentiated Services Code Point (DSCP) marking of packets sent by WLCs and LAPs. This feature enhances how access points (APs) use this Layer 3 information in order to ensure that packets receive the correct over–the–air prioritization from the AP to the wireless client.

In a centralized WLAN architecture, WLAN data is tunneled between the AP and the WLC via Lightweight Access Point Protocol (LWAPP). In order to maintain the original QoS classification across this tunnel, the QoS settings of the encapsulated data packet must be appropriately mapped to the Layer 2 (802.1p) and Layer 3 (IP DSCP) fields of the outer tunnel packet.

It is not possible to DSCP–tag packets between the controller and LAP if there is no DSCP or 802.1P value in the original packet itself.

The controller does not apply its own QoS. The QoS support on the WLC gives the WLC the ability to apply the same priority that is set on the wire (or application).

Therefore, the only action a WLC or AP will do is copy the value of the original packet to the outer header of the LWAPP packet. The whole purpose of the gold, silver, and bronze QoS options on the WLC is to perform proper QoS translations between 802.11e/802.1p UP values and IP DSCP values, which depend on the application or standard that is used. Once again, QoS on the WLC ensures that packets receive the proper QoS handling from end to end. The controller does not perform its own QoS behavior. The support is there for the controller to follow suit if QoS already exists and priority needs to be applied to wireless packets.You cannot have QoS only exist on the controller.

The controller does not support Class of Service (CoS) marking values based on WLAN configuration in Layer 2 LWAPP mode. It is recommended to use Layer 3 LWAPP in order to implement CoS QoS.

This is an example of how QoS works with WLCs. The application, for example CallManager, might set a QoS value of **High**. Therefore, the orginal data packet from the application will be encapsulated by an IP header that has the DCSP value set to **High**. Now, the packet reaches the controller. Next, the packet goes through the SSID **Test**. However, if you have a SSID **Test** on your controller configured for QoS profile **Bronze**, the IP header of the packet that encapsulates the LWAPP packet form controller to AP, will have the value **Bronze** (although the IP header around the original packet from the application will have High priority). This document assumes that the DCSP set by the application and the QoS profile for that SSID on the controller are the same. This is not always the case.
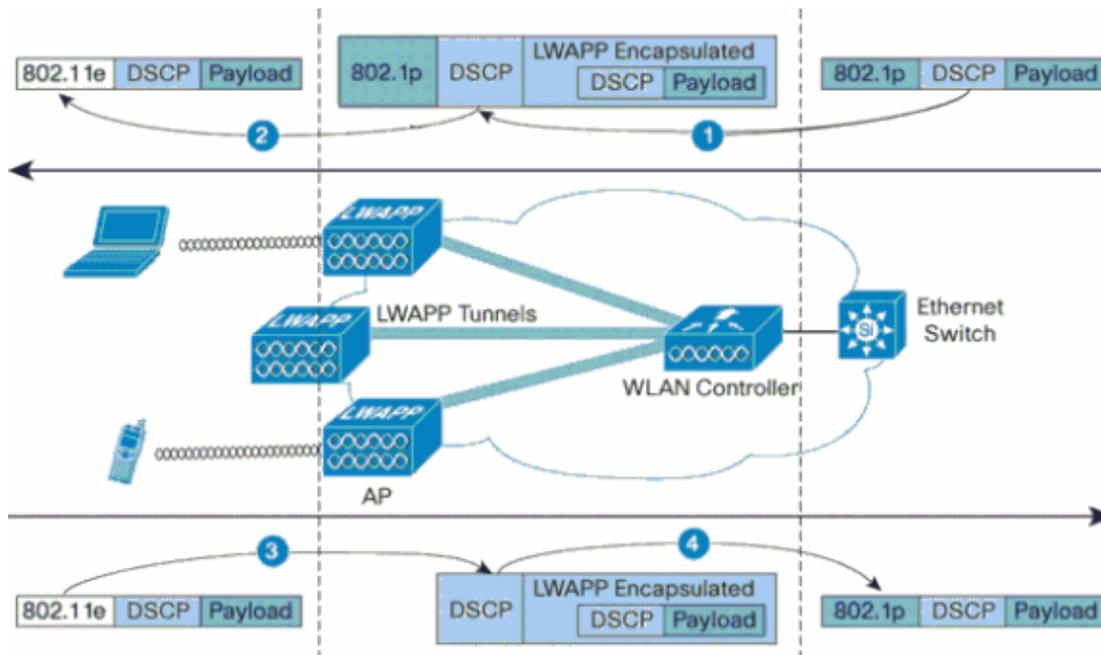
For example, when 802.11e traffic is sent by a WLAN client, it has a User Priority (UP) classification in its frame. The AP needs to map this 802.11e classification into a DSCP value for the LWAPP packet that carries the frame. This ensures that the packet is given the appropriate priority on its way to the WLC. A similar process needs to occur on the WLC for LWAPP packets going to the AP. Also, a mechanism is needed to classify traffic on both the AP and the WLC for non−802.11e clients, so that their LWAPP packets can also be given the appropriate priority. This table illustrates how packets are handled at each device:

#	From	To	UP (802.1p/802.11e)	IP DSCP
1	Controller	Access Point	It does NOT translate the DSCP value of the incoming packet to the AVVID 802.1p UP value. The DSCP value, if present in the packet, goes transparently in the packet.	Copy the DSCP value from the incoming packet.
2	Access Point	Wireless Client	WMM Client: Translate the DSCP value of the incoming LWAPP packet to the 802.11e UP value. Police the value to ensure it does not exceed the maximum value allowed for the WLAN QoS policy assigned to that client. Place packet in the 802.11 Tx queue appropriate for the UP value. Regular client: Place packet in the default	N/A (original DSCP value is preserved)

		802.11 Tx queue for the WLAN QoS policy assigned to that client.		
3	Access Point	Controller	N/A (access points do not support 802.1Q/802.1p tags)	WMM Client: Police the 802.11e UP value to ensure it does not exceed the maximum value allowed for the QoS policy assigned to that client; translate the value to the DSCP value. Regular client: Use the 802.11e UP value for the QoS policy assigned to that client; translate the value to the DSCP value.
4	Controller	Ethernet Switch	Translate the DSCP value of the incoming LWAPP packets to the 802.1p UP value.	N/A (original DSCP value is preserved)

This next table provides the translations that occur between 802.11e/802.1p UP values and IP DSCP values. Because Cisco Architecture for Voice, Video and Integrated Data (AVVID) defines the translation from 802.1 UP to IP DSCP, and the IEEE defines the translation from IP DSCP to 802.11e UP, two different sets of translations must be used.

Cisco AVVID 802.1p UP–Based Traffic Type	Cisco AVVID IP DSCP	Cisco AVVID 802.1p UP	IEEE 802.11e UP	Notes
Network Control	–	7	–	Reserved for network control only
Inter–Network Control	48	6	7 (AC_VO)	LWAPP control
Voice	46 (EF)	5	6 (AC_VO)	Controller: Platinum QoS profile
Video	34 (AF41)	4	5 (AC_VI)	Controller: Gold QoS profile

| Traffic type	DSCP	802.1p	AC	Controller
Voice Control	26 (AF31)	3	4 (AC_VI)	–
Best Effort	0 (BE)	0	3 (AC_BE) 0 (AC_BE)	Controller: Silver QoS profile –
Background (Cisco AVVID Gold Background)	18 (AF21)	2	2 (AC_BK)	–
Background (Cisco AVVID Silver Background)	10 (AF11)	1	1 (AC_BK)	Controller: Bronze QoS profile

Network Setup

This document uses this network setup:

- The wired network comprises of the two routers, Router1 and Router2, that run OSPF between them. The wired hosts comprise of a FTP server (F1), a Voice client (V1) and a Video Client (Vi1). The wired hosts connect to the network through a Layer 2 Switch which is connected to the Fast Ethernet of Router R1.
- The wireless network connects to the network through Router2 as shown in the diagram. The wireless hosts comprise of a FTP client (non–WMM enabled), a Voice client V1 (7920 Phones) and a Video Client Vi1 (WMM enabled).
- Voice packets should be given the highest priority followed by Video packets. FTP packets must be given the least priority.
- On the wired network, Weighted Random Early Detection (WRED) is used in order to implement QoS. The different traffic types are classified and prioritized based on the DSCP values. WRED is implemented on prioritized packets.
- On the wireless network, three WLANs must be created for each traffic type, and to enable appropriate QoS profiles.

  - WLAN 1 **FTP Clients:** Bronze QoS Profile
  - WLAN 2 **Video Clients:** Gold QoS Profile
  - WLAN 3 **Voice Clients:** Platinum QoS Profile

The devices for basic IP connectivity and enable QoS both need to be configured on the wired network and wireless network.

Voice,Video and FTP packets classified and marked at F3/0

WRED Implemented on S2/0 and S0/0
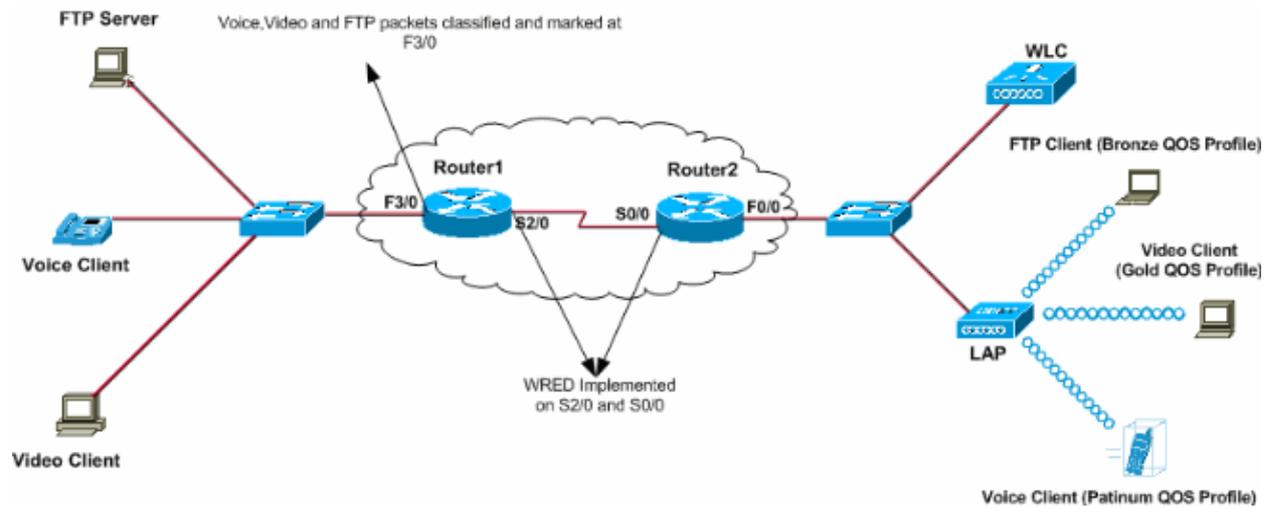
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to find more information on the commands used in this document.

In order to configure the devices for this setup, these need to be performed:

- Configure the Wireless Network for QoS
- Configure the Wired Network for QoS

Configure the Wireless Network for QoS

Before you configure QoS on WLCs, you must configure the WLC for basic operation and register the LAPs to the WLC. This document assumes that the WLC is configured for basic operation and that the LAPs are registered to the WLC. If you are a new user trying to set up the WLC for basic operation with LAPs, refer to Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC).

Once the LAPs are registered to the WLC, complete these tasks in order to configure the LAPs and WLC for this setup:
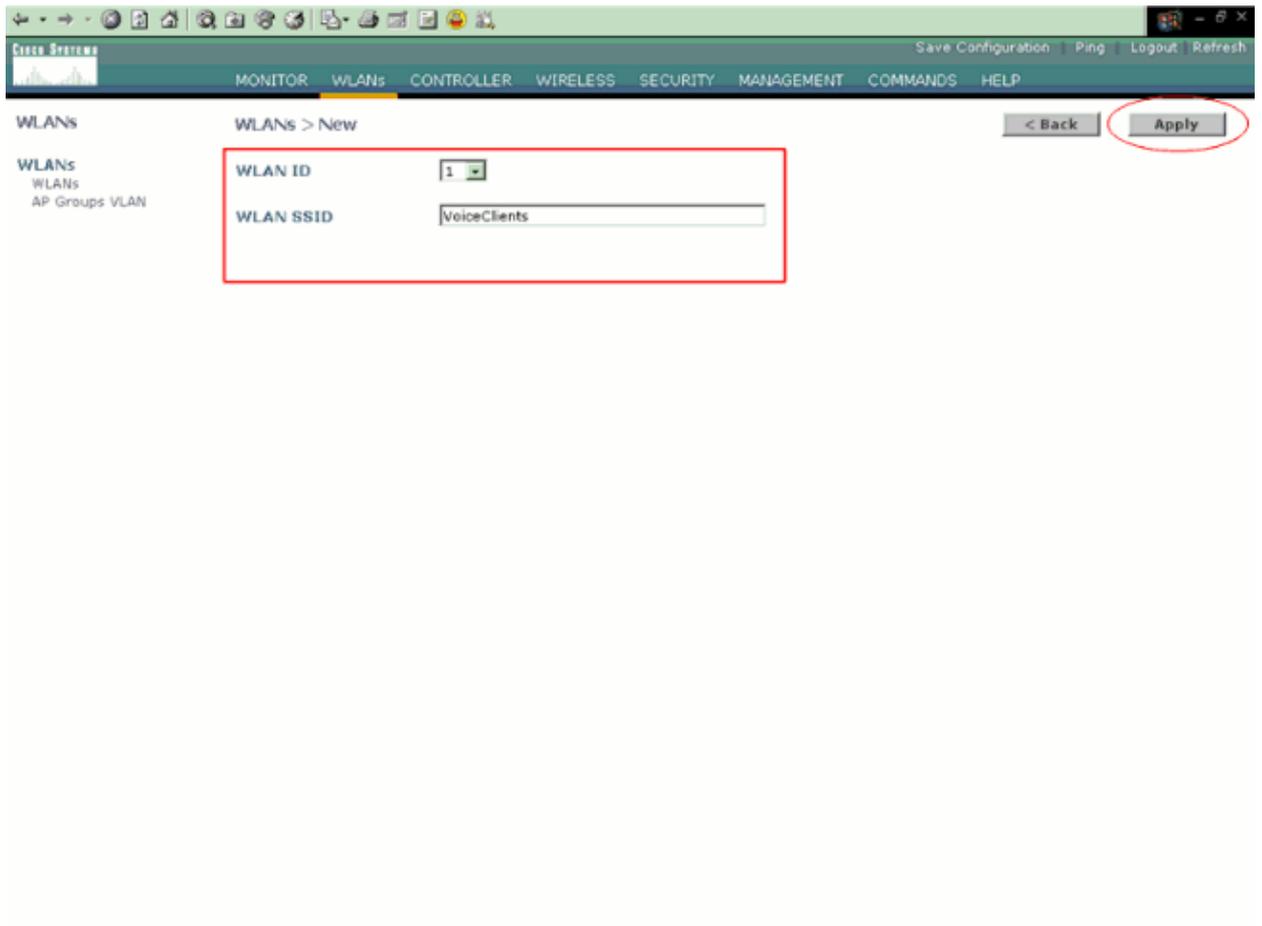
1. Configure WLANs for the different traffic classes
2. Enable QoS profiles for the WLANs

Complete these steps in order to create a WLAN on the WLC for the Voice clients:

1. Click **WLANs** from the controller GUI in order to create a WLAN.
2. Click **New** in order to configure a new WLAN.

   In this example, the WLAN is named VoiceClients and the WLAN ID is 1.
3. Click **Apply**.

4. In the **WLAN > Edit** window, define the parameters specific to the WLAN **VoiceClients**.

     a. For the WLAN, choose the appropriate interface from the Interface Name field.

       This example maps the interface **Voice** to the WLAN **VoiceClients**.

     b. From the Quality of Service (QoS) pull down menu, choose the appropriate QoS profile for the WLAN.

       In this example, the **Platinum** QoS profile is selected. This gives the highest priority to the Voice WLAN.
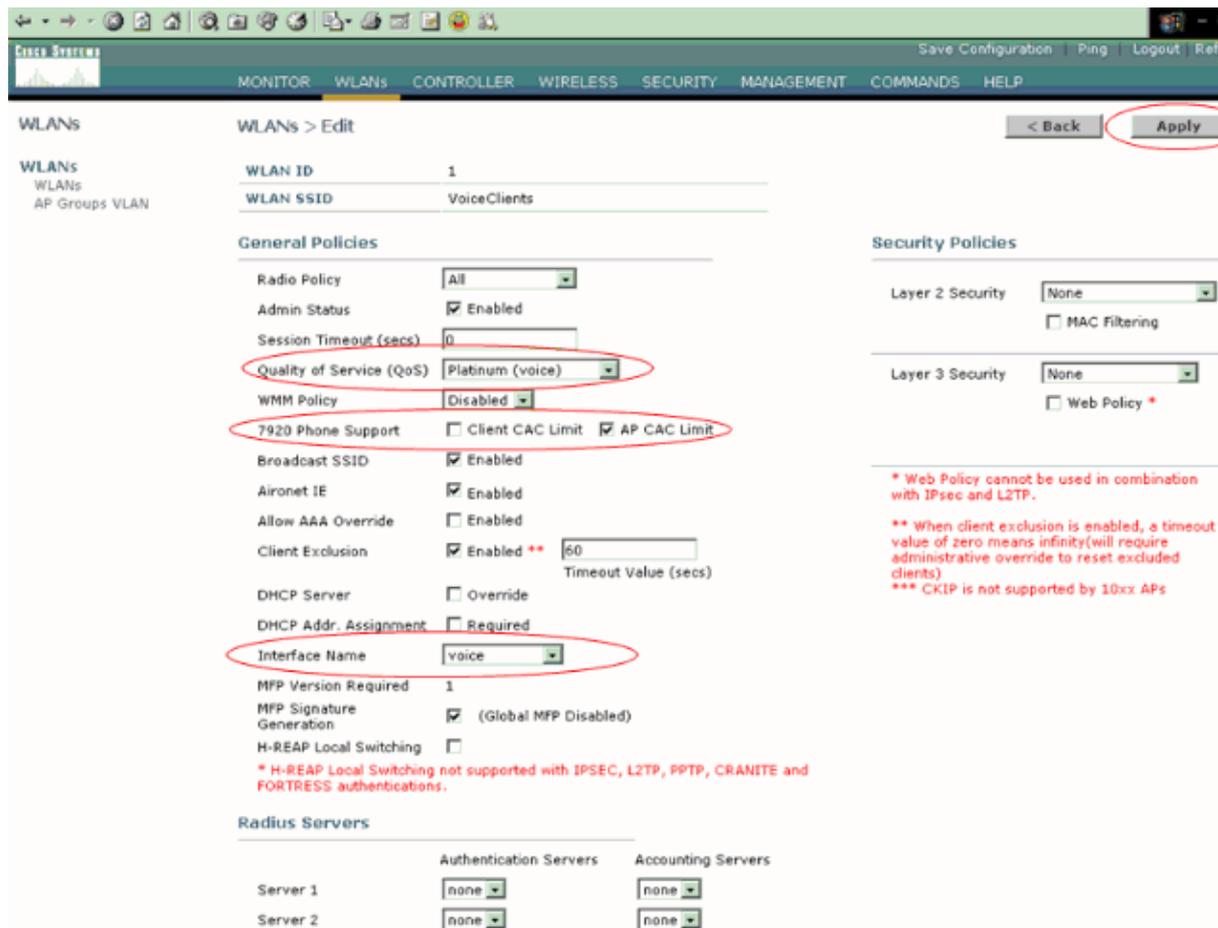
     c. For the 7920 Phone Support parameter, choose the type of call admission control (CAC).

       This example uses **AP CAC Limit**.

     d. Select the other parameters, which depend on the design requirements.

       The default values are used in this example.
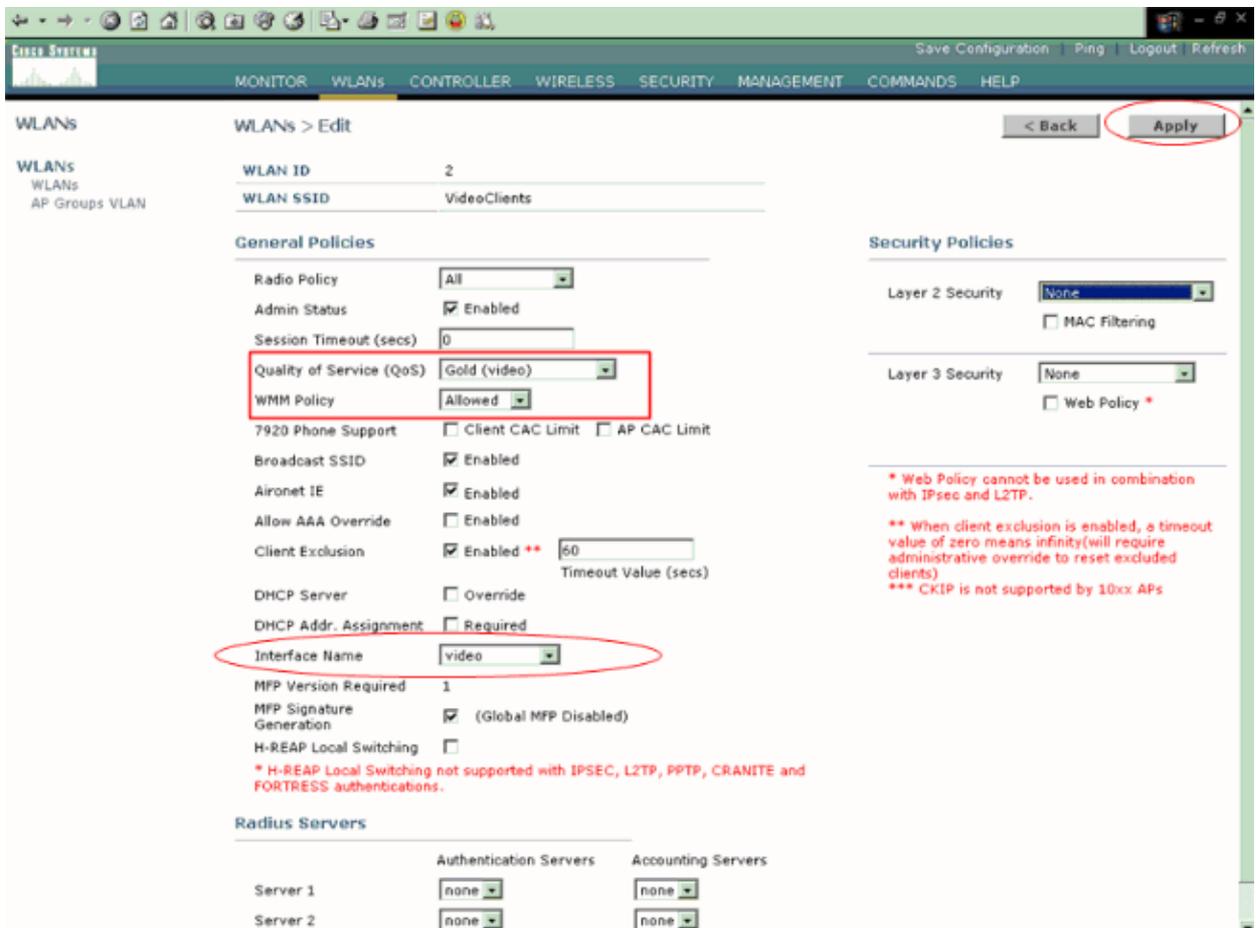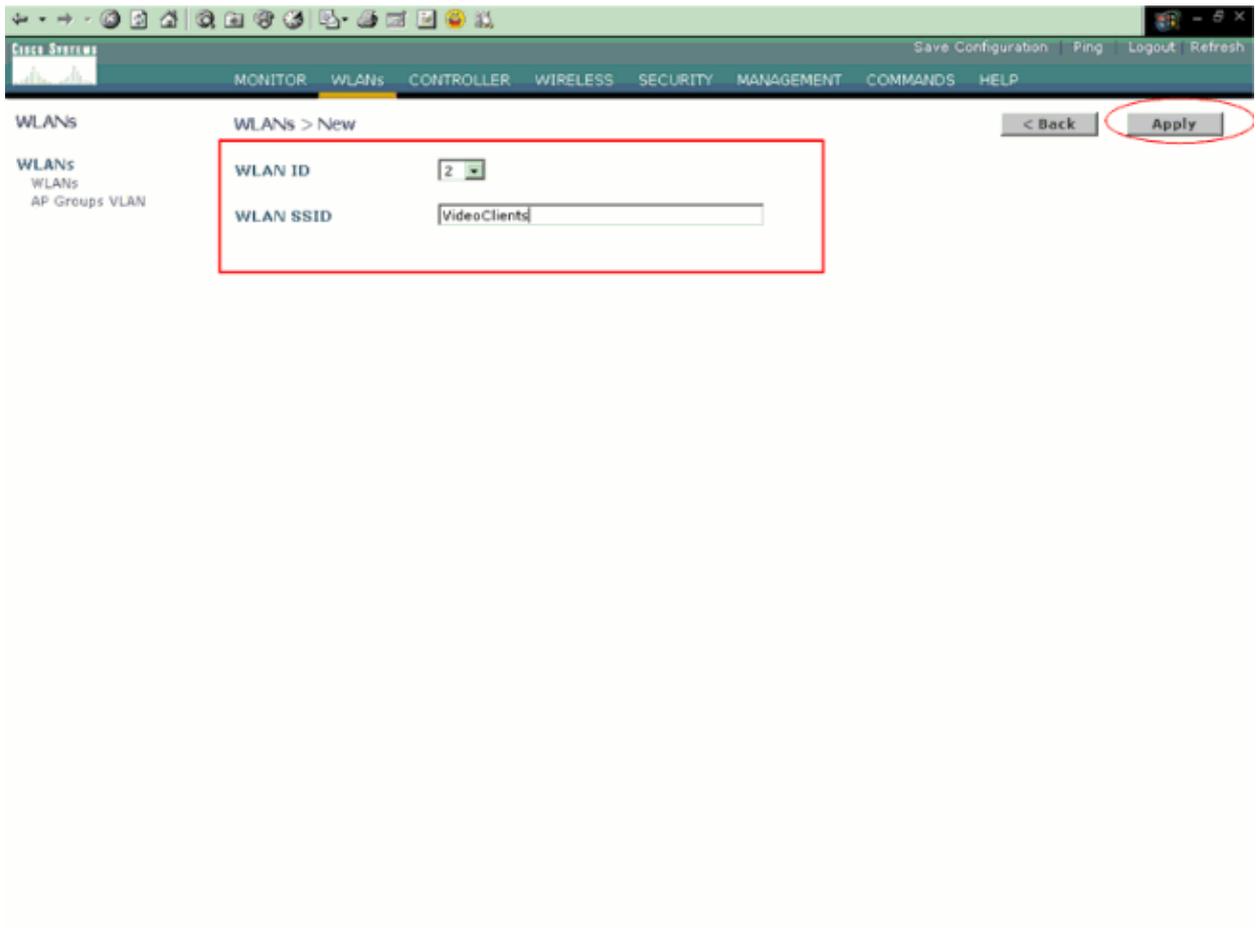
     e. Click **Apply**.

Note: Do not enable WMM mode if Cisco 7920 phones are used on your network. You cannot enable both WMM mode and client–controlled CAC mode on the same WLAN. When an AP–controlled CAC is enabled, the AP sends out a Cisco proprietary CAC Information Element (IE) and does not send out the standard QBSS IE.

The deployment of voice over WLAN infrastructure involves more than simply providing QoS on WLAN. A voice WLAN needs to consider site survey coverage requirements, user behavior, roaming requirements and admission control. This is covered in the Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide.

Similarly, create the WLANs for the Video clients and the FTP clients. Video clients are mapped to the dynamic interface Video and FTP clients are mapped to the dynamic interface FTP. These are the screenshots:

Note: This document does not explain how to create VLANs on WLCs. Refer to VLANs on Wireless LAN Controllers Configuration Example for information on how to configure dynamic interfaces on WLCs.

WLANs

WLANs
  WLANs
  AP Groups VLAN

WLANs > New   < Back   Apply

WLAN ID   2

WLAN SSID   VideoClients

WLANs

WLANs
  WLANs
  AP Groups VLAN

WLANs > Edit   < Back   Apply

WLAN ID   2
WLAN SSID   VideoClients

General Policies

Radio Policy	All
Admin Status	☑ Enabled
Session Timeout (secs)	0
Quality of Service (QoS)	Gold (video)
WMM Policy	Allowed
7920 Phone Support	☐ Client CAC Limit ☐ AP CAC Limit
Broadcast SSID	☑ Enabled
Aironet IE	☑ Enabled
Allow AAA Override	☐ Enabled
Client Exclusion	☑ Enabled ** 60
	Timeout Value (secs)
DHCP Server	☐ Override
DHCP Addr. Assignment	☐ Required
Interface Name	video
MFP Version Required	1
MFP Signature Generation	☑ (Global MFP Disabled)
H-REAP Local Switching	☐

* H-REAP Local Switching not supported with IPSEC, L2TP, PPTP, CRANITE and FORTRESS authentications.

Security Policies

Layer 2 Security   None
                    ☐ MAC Filtering

Layer 3 Security   None
                    ☐ Web Policy *

* Web Policy cannot be used in combination with IPsec and L2TP.

** When client exclusion is enabled, a timeout value of zero means infinity(will require administrative override to reset excluded clients)

*** CKIP is not supported by 10xx APs

Radius Servers

	Authentication Servers	Accounting Servers
Server 1	none	none
Server 2	none	none

Note: WLAN client support for WMM does not mean that the client traffic automatically benefits from WMM. The applications that look for the benefits of WMM assign an appropriate priority classification to their traffic, and the operating system needs to pass that classification to the WLAN interface. In purpose–built devices, such as VoWLAN handsets, this is done as part of the design. However, if you implement on a general purpose platform, such as a PC, application traffic classification and OS support must be implemented before the WMM features can be used to good effect.

For Video clients, QoS profile Gold is selected and WMM is enabled. For FTP clients, Bronze is selected as the QoS profile and WMM is disabled because in this example the FTP clients do not support WMM.
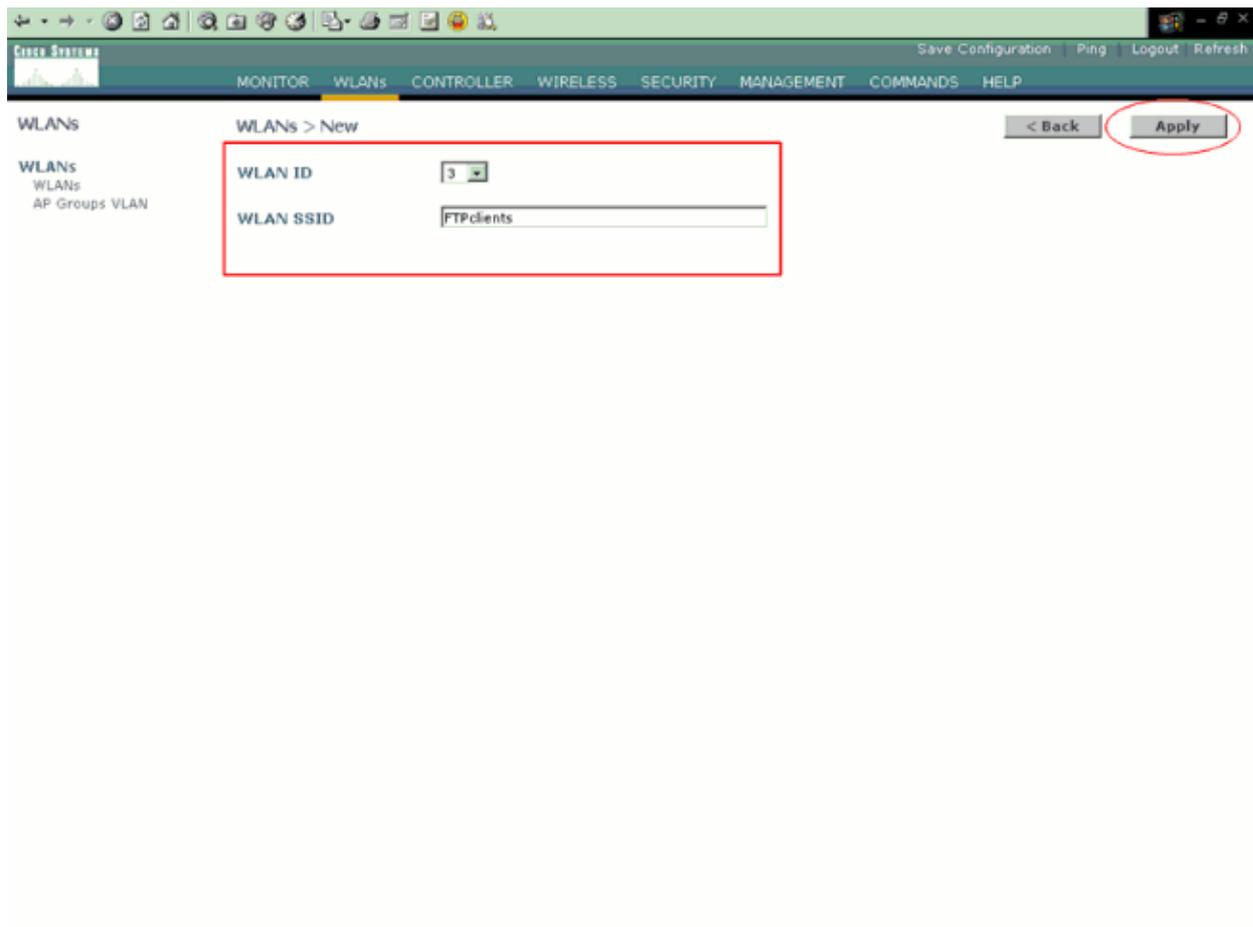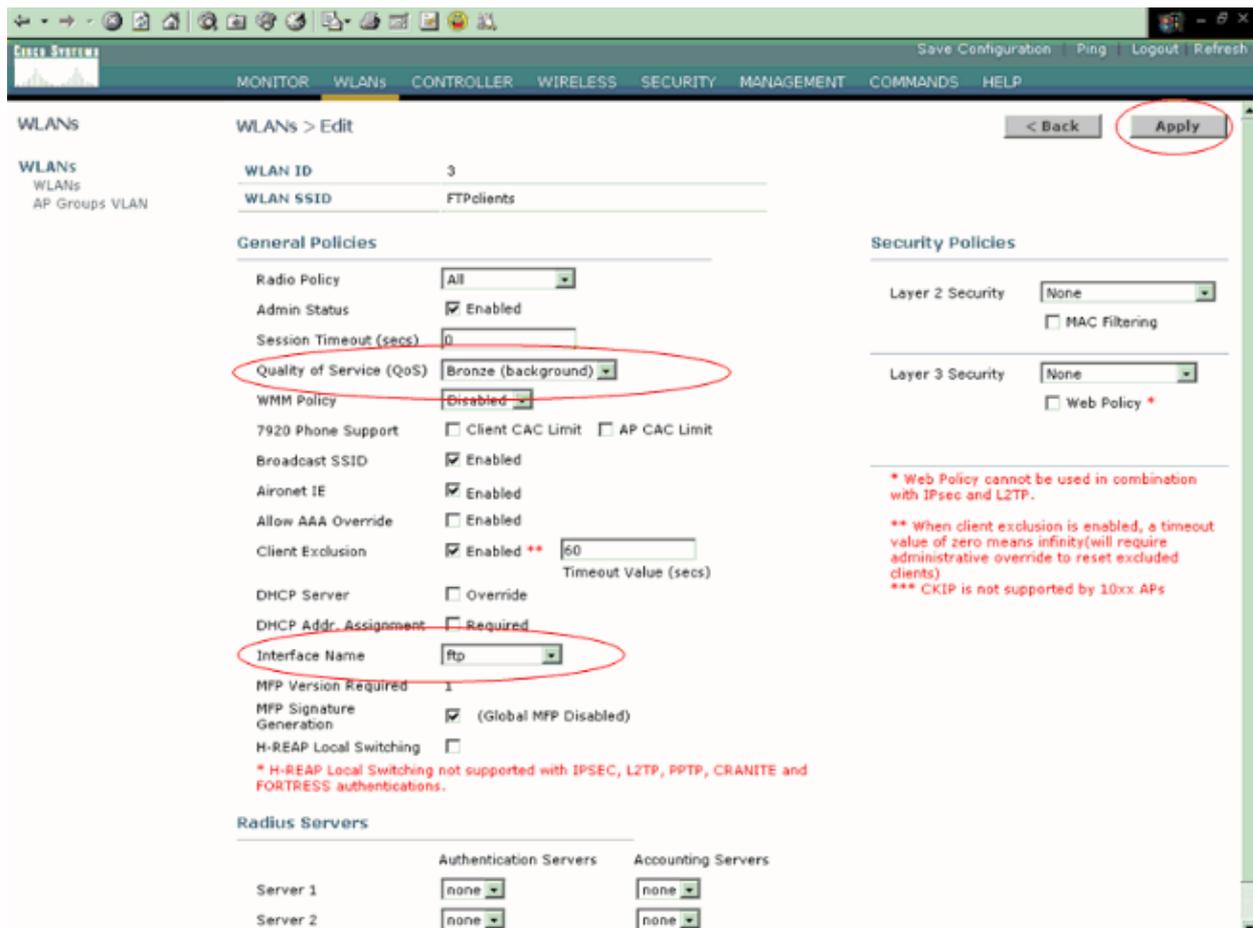
Note: When the controller is in Layer 2 mode and WMM is enabled, you must put the APs on a trunk port in order to allow them to join the controller.

Issue these commands in order to configure the WLANs and QoS on WLC using the CLI:

- Issue the **config wlan create** *<wlan−id> <wlan−name>* command in order to create a new WLAN. For wlan−id, enter an ID from 1 to 16. For wlan−name, enter an SSID up to 31 alphanumeric characters.
- Issue the **config wlan enable** *<wlan−id>* command in order to enable a WLAN.
- Issue the **config wlan qos** *wlan−id* **{bronze | silver | gold | platinum}** command in order to assign a QoS level to a WLAN.
- Issue the **config wlan wmm {disabled | allowed | required}** *wlan−id* command in order to enable WMM mode.
- Issue the **config wlan 7920−support client−cac−limit {enabled | disabled}** *wlan−id* command for phones that require client−controlled CA.
- Issue the **config wlan 7920−support ap−cac−limit {enabled | disabled}** *wlan−id* command for phones that require AP−controlled CAC.

Configure the Wired Network for QoS

In order to configure the wired network for this setup, you need to configure the routers for basic connectivity and enable QoS in the wired network. OSPF is used as the unicast routing protocol.

The WRED feature is used to implement QoS in the wired network. The DiffServ Compliant WRED feature enables WRED to use the DSCP value when it calculates the drop probability for a packet.

These are the configurations for Routers R1 and R2:

Router1

```
Router1#show run
Building configuration...

Current configuration : 2321 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router1
!
!
ip subnet-zero
!
!
!
call rsvp-sync
!


!
class-map match-all FTP

!--- Classifies FTP Packets based on Access List 103.

  match access-group 103
class-map match-all Video

!--- Classifies Video Packets based on Access List 102.

  match access-group 102
class-map match-all Voice

!--- Classifies Voice Packets based on Access List 101.

  match access-group 101
!
!
policy-map Marking-For-FTP

!--- Sets DSCP value af11 for FTP packets.

  class FTP
    set ip dscp af11
policy-map Marking-For-Voice

!--- Sets DSCP value ef for Voice packets.

  class Voice
    set ip dscp ef
policy-map Marking-For-Video

!--- Sets DSCP value af41 for Video packets.

  class Video
    set ip dscp af41
!
!
!
interface Serial2/0
 description Connected to Router2
 ip address 10.2.3.2 255.255.255.0
```

```
 random-detect dscp-based
```

```
 random-detect dscp 10 30 40
```

```
 random-detect dscp 34 40 50
```

```
 random-detect dscp 46 50 60
```

```
 clockrate 56000
!
interface Serial2/1
 no ip address
 shutdown
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
interface Serial2/4
 no ip address
 shutdown
!
interface Serial2/5
 no ip address
 shutdown
!
interface Serial2/6
 no ip address
 shutdown
!
interface Serial2/7
 no ip address
 shutdown
!
interface FastEthernet3/0
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3/0.1
 description Connected to Voice Clients
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.0.0
 service-policy output Marking-For-Voice
```

```
!
interface FastEthernet3/0.2
 description Connected to Video Clients
 encapsulation dot1Q 20
```

```
 ip address 172.16.0.1 255.255.0.0
 service-policy output Marking-For-Video
```

```
!
interface FastEthernet3/0.3
 description Connected to FTP Server
 encapsulation dot1Q 30
 ip address 30.0.0.1 255.0.0.0
 service-policy output Marking-For-FTP
```

```
!
interface FastEthernet3/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 1
```

```
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 30.0.0.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.255.255 area 0
 network 192.168.0.0 0.0.255.255 area 0
!
ip classless
ip http server
!
access-list 101 permit ip 192.168.0.0 0.0.255.255 any
```

```
access-list 102 permit ip 172.16.0.0 0.0.255.255 any
```

```
access-list 103 permit ip 30.0.0.0 0.0.0.255 any
```

```
!
voice-port 1/0/0
!
voice-port 1/0/1
!
voice-port 1/1/0
!
voice-port 1/1/1
!
dial-peer cor custom
!
!
!
dial-peer voice 1 pots
 destination-pattern 4085551234
 port 1/0/0
!
!
line con 0
line aux 0
```

```
line vty 0 4
!
end
```

Router2

```
Router2#show run
Building configuration...

Current configuration : 1551 bytes
!
version 12.3
service config
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!


!
interface FastEthernet0/0
 ip address dhcp
 duplex auto
 speed auto
!
interface FastEthernet0/0.1
 description Connected to Voice Clients
 encapsulation dot1Q 40
 ip address 20.0.0.1 255.0.0.0
!
interface FastEthernet0/0.2
 description Connected to Video Clients
 encapsulation dot1Q 50
 ip address 40.0.0.1 255.0.0.0
!
interface FastEthernet0/0.3
 description Connected to FTP Clients
 encapsulation dot1Q 60
 ip address 50.0.0.1 255.0.0.0
!
interface Serial0/0
 description Connected to Router1
 ip address 10.2.3.1 255.255.255.0
 random-detect dscp-based

!--- Enables WRED based on DSCP Value of the packet.

 random-detect dscp 10 30 40

!--- Sets the Minimum and Maximum Threshold of Packets
!--- to 30 and 40 packets for the DSCP value 10.

 random-detect dscp 34 40 50

!--- Sets the Minimum and Maximum Threshold of Packets
!--- to 40 and 50 packets for the DSCP value 34.
```

```
   random-detect dscp 46 50 60

!--- Sets the Minimum and Maximum Threshold of Packets
!--- to 50 and 60 packets for the DSCP value 46.

!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Service-Engine2/0
 no ip address
 shutdown
 hold-queue 60 out
!
router ospf 1

!--- Configures OSPF as the routing protocol.

 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
 network 20.0.0.0 0.255.255.255 area 0
 network 40.0.0.0 0.255.255.255 area 0
 network 50.0.0.0 0.255.255.255 area 0
!
ip http server
ip classless
!
!
control-plane
!
!
voice-port 1/0/0
!
voice-port 1/0/1
!
gatekeeper
 shutdown
!
!
line con 0
line 65
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output all
line aux 0
line vty 0 4
!
!
end
```

Verify and Troubleshoot

Once the wireless and wired network are configured for basic connectivity and QoS is implemented, the packets are classified, marked and sent based on the policies configured for each traffic type.

The application of QoS features might not be easily detected on a lightly loaded network. QoS features start to impact application performance as the load on the network increases. QoS works to keep latency, jitter, and loss for selected traffic types within acceptable boundaries.

For a WMM enabled Video client:

When a Video client on the wired side sends data to the video client on the wireless side, this sequence of events occurs:

1. At the FastEthernet interface on Router1, the **Marking−For−Video** policy is applied to the video packets and the packets are marked with a DSCP value of **AF41**.
2. The marked video packets pass through the serial interfaces S3/0 on Router1 and S0/0 on Router2. This is where the drop probability of the packet is checked against the threshold configured for WRED. When the average queue length reaches the minimum threshold (40 packets in this case for Video packets), WRED randomly drops some packets with the DSCP value AF41. Similarly, when the average queue length exceeds the maximum threshold (50 packets in this case for Video packedts), WRED drops all packets with the DSCP value AF41.
3. Once the Video packets reach the WLC through the fastethernet on Router2, the WLC translates the DSCP value of the incoming packet to the AVVID 802.1p UP value and copies the DSCP value from the incoming packet to the LWAPP packet as shown here. In this example, the DSCP value AF41 is translated to the corresponding 802.1p value 4.
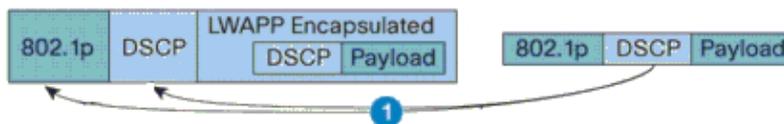
DSCP Value for Voice Packets af41 translated to Cisco AVVID 802.1p UP value 4 and original DSCP Value af41 copied

4. When the packet reaches the LAP, the LAP translates the DSCP value of the incoming LWAPP packet to the 802.11e UP value and polices the value in order to ensure it does not exceed the maximum value allowed for the WLAN QoS policy assigned to that client. The LAP then places the packet in the 802.11 Tx queue appropriate for the UP value. In this example, the DSCP value AF41 is translated to the corresponding 802.11e UP value 5.
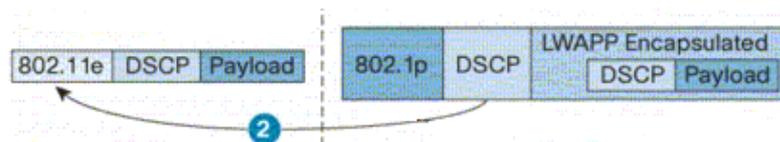
DSCP value of the incoming LWAPP packet af41 translated to the 802.11e UP value 5 for a WMM enabled client

When a Video client on the wireless side sends data to the wired side, this sequence of events occurs:

1. When a WMM enabled client sends a packet to the LAP, the LAP polices the 802.11e UP value in order to ensure it does not exceed the maximum value allowed for the QoS policy assigned to that client. Then, it translates the value to the DSCP value. In this example, the Video WLAN has been configured with the QoS profile Gold, which has a 802.11e UP value of 4. This value is translated to the corresponding DSCP value AF41 and is sent to the controller.

802.11e UP value translated to DSCP value af41 and sent to Controller

2. The controller translates the DSCP value of the incoming LWAPP packet to the 802.1p UP value as shown and the original DSCP value is also sent unaltered.

DSCP value af41 of the incoming LWAPP packet transalted to 802.1p UP value 5 and original DSCP value af41 is sent unaltered

3. The packets with DSCP value af41 at the fastethernet on Router2 pass through the serial interfaces on Router2 and Router1, and reach the video clients on the wired side. When the packet traverses the serial interfaces, the drop probability of the packet is checked against the threshold configured for WRED.

For a WMM disabled FTP client:

When the FTP server on the wired side sends data to the FTP client on the wireless side, this sequence of events occurs:

1. At the FastEthernet interface on Router1, the **Marking−For−FTP** policy is applied to the FTP packets and the packets are marked with a DSCP value of AF11.
2. The marked FTP packets pass through the serial interfaces s3/0 on Router1 and S0/0 on Router2. This is where the drop probability of the packet are checked against the threshold configured for WRED. When the average queue length reaches the minimum threshold (30 packets in this case for FTP packets), WRED randomly drops some packets with the DSCP value AF11. Similarly, when the average queue length exceeds the maximum threshold (40 packets in this case for FTP packets), WRED drops all packets with the DSCP value AF11.
3. Once the FTP packets reach the WLC through the fastethernet on Router2, the WLC translates the DSCP value of the incoming packet to the AVVID 802.1p UP value and copies the DSCP value from the incoming packet to the LWAPP packet as shown here. In this example, the DSCP value AF11 is translated to the corresponding 802.1p value 1.
4. When the packet reaches the LAP, the LAP places the packet in the default 802.11 Tx queue for the WLAN QoS policy assigned to that client. In this example, the packet is placed in the queue for the Bronze QoS profile.
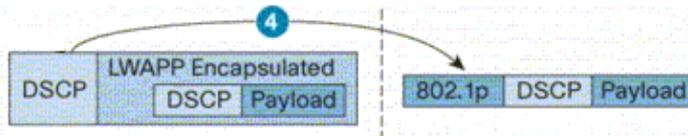
When a FTP client on the wireless side sends data to the wired side, this sequence of events occurs:

1. When a FTP client on the wireless network sends a packet to the LAP, the LAP uses the 802.11e UP value for the QoS policy assigned to that client. Then, the LAP translates the value to the DSCP value and sends the packet to the controller. Because the FTP client belongs to QoS profile bronze IEEE 802.11e UP value 1 is translated to the DSCP value AF11.
2. The controller translates the DSCP value of the incoming LWAPP packet to the 802.1p UP value as shown and the original DSCP value is also sent unaltered. The packet is then forwarded to Router2 through the Layer 2 switch.

3. The packets with DSCP value AF11 at the fastethernet on Router2 pass through the serial interfaces on Router2 and Router1, and reach the Video clients on the wired side. When the packet traverses the serial interfaces, the drop probability of the packet is checked against the threshold configured for WRED.

A similar procedure occurs when voice packet traverse from the wired to wireless network and vice versa.

Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

You can issue these Cisco IOS commands on the routers in order to troubleshoot and verify your QoS configuration:

- **show queue** {*interface−name interface−number*} Lists information about the packets that are waiting in a queue on the interface.
- **show queueing random−detect interface** {*interface−name interface−number*} Lists configuration and statistical information about the queuing tool on an interface.
- **show policy−map interface** {*interface−name interface−number*} Displays the statistics and the configurations of the input and output policies that are attached to an interface. Make sure to use this command in the appropriate EXEC mode.

```
Router1#show policy-map interface F3/0.1
 FastEthernet3/0.1

  Service-policy output: Marking-For-Voice

    Class-map: Voice (match-all)
      18 packets, 1224 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      QoS Set
        dscp ef
          Packets marked 18

    Class-map: class-default (match-any)
      2 packets, 128 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

- **debug qos set** Displays information on QoS packet marking.

On the WLC, issue this command in order to view the QoS profile settings:

- **show qos** {*bronze/silver/gold/platinum*} Provides information on the QoS profile configured for the WLANs.

  Here is a sample output of the **show qos** command:

```
(Cisco Controller) >show qos Platinum

Description.................................... For Voice Applications
Average Data Rate.............................   0
Burst Data Rate...............................   0
Average Realtime Data Rate....................   0
Realtime Burst Data Rate......................   0
```

```
       Maximum RF usage per AP (%)...................... 100
       Queue Length.................................... 100
       protocol........................................ none


       (Cisco Controller) >show qos Gold


       Description..................................... For Video Applications
       Average Data Rate...............................   0
       Burst Data Rate.................................   0
       Average Realtime Data Rate......................   0
       Realtime Burst Data Rate........................   0
       Maximum RF usage per AP (%)...................... 100
       Queue Length....................................  75
       protocol........................................ none


       (Cisco Controller) >show qos Bronze


       Description..................................... For Background
       Average Data Rate...............................   0
       Burst Data Rate.................................   0
       Average Realtime Data Rate......................   0
       Realtime Burst Data Rate........................   0
       Maximum RF usage per AP (%)...................... 100
       Queue Length....................................  25
       protocol........................................ none
```
- **show wlan** <*WLAN−ID*> Displays information about the WLAN. Here is a sample output:

```
       (Cisco Controller) >show wlan 1


       WLAN Identifier................................. 1
       Network Name (SSID)............................. VoiceClients
       Status.......................................... Enabled
       MAC Filtering................................... Disabled
       Broadcast SSID.................................. Enabled
       AAA Policy Override............................. Disabled
       Number of Active Clients........................ 0
       Exclusionlist Timeout........................... 60 seconds
       Session Timeout................................. 1800 seconds
       Interface....................................... management
       WLAN ACL........................................ unconfigured
       DHCP Server..................................... Default
       DHCP Address Assignment Required................ Disabled
       Quality of Service.............................. Platinum (voice)
       WMM............................................. Disabled
       CCX - AironetIe Support......................... Enabled
       CCX - Gratuitous ProbeResponse (GPR)............ Disabled
       Dot11-Phone Mode (7920)......................... Disabled
       Wired Protocol.................................. None
       IPv6 Support.................................... Disabled
       Radio Policy.................................... All
       Security

          802.11 Authentication:....................... Open System
          Static WEP Keys.............................. Disabled
          802.1X....................................... Enabled
          Encryption:.................................. 104-bit WEP
          Wi-Fi Protected Access (WPA/WPA2)............ Disabled
          CKIP ........................................ Disabled
          IP Security Passthru......................... Disabled
          Web Based Authentication..................... Disabled
          Web-Passthrough.............................. Disabled
          Auto Anchor.................................. Disabled
          H-REAP Local Switching....................... Disabled
          Management Frame Protection.................. Enabled (Global MFP Disabled)
```

Related Information

- **Lightweight AP (LAP) Registration to a Wireless LAN Controller (WLC)**
- **VLANs on Wireless LAN Controllers Configuration Example**
- **Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4**
- **Wireless Product Support**
- **Technical Support & Documentation – Cisco Systems**

Updated: Jun 27, 2008   Document ID: 81831