Product Bulletin No. 3209

Cisco Unified Wireless Network Software Release 3.2

Cisco Systems® announces the availability of Cisco® Unified Wireless Network Software Release 3.2. This release contains new features, as well as support for the features delivered in Cisco Centralized Wireless LAN Software Release 3.1. This software release provides support for the following new features:

- Cisco Catalyst® 6500 Series Wireless Services Module (WiSM)
- Cisco Wireless LAN Controller Module (WLCM) for integrated services routers
- Wireless mesh enhancements to Cisco Wireless Control System (WCS)
- Cisco 2700 Series Wireless Location Appliance enhancements
- Multicast performance enhancements
- Link aggregation for the Cisco 4400 Series and the Cisco WiSM
- Layer 3 QoS packet-marking enhancements
- Guest tunnel origination for Cisco 2000 Series wireless LAN controllers
- Cisco WCS serviceability improvements
- Static and dynamic Wired Equivalent Privacy (WEP) on the same WLAN
- Configurable DHCP Proxy
- VPN Termination Module for the 4400 Series wireless LAN controller
- Regulatory domain updates

NEW FEATURES

The following new features are included in Cisco Unified Wireless Network Software Release 3.2. These features are supported by Cisco Aironet® lightweight access points, Cisco wireless LAN controllers, Cisco 2700 Series wireless location appliances, and the Cisco Wireless Control System (WCS).

Cisco Catalyst 6500 Wireless Services Module (WiSM)

Cisco Unified Wireless Network Software Release 3.2 provides support for the new Cisco Wireless Services Module (WiSM) for the Cisco Catalyst 6500 Series. For more information, visit: http://www.cisco.com/en/US/products/ps6526/index.html

Wireless LAN Controllers Supported: Cisco WiSM

Access Points Supported: Cisco Aironet 1000, 1130, 1230, 1240, and 1500 series lightweight access points

Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

Cisco Wireless LAN Controller Module (WLCM) for Integrated Services Routers

Cisco Unified Wireless Network Software Release 3.2 provides support for the new Cisco Wireless LAN Controller Module (WLCM) for integrated services routers. For more information, visit: http://www.cisco.com/en/US/products/ps6730/index.html

Wireless LAN Controllers Supported: Cisco WLCM for integrated services routers

Access Points Supported: Cisco Aironet 1000, 1130, 1230, 1240, and 1500 series lightweight access points

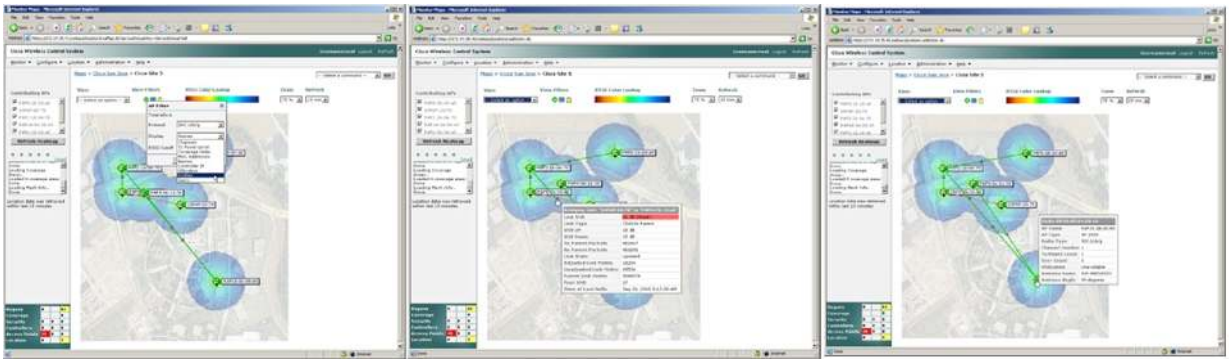
Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

Wireless Mesh Enhancements to Cisco WCS

With the addition of wireless mesh access points to the Cisco Aironet product portfolio, Cisco WCS now includes tools to help manage and troubleshoot wireless mesh deployments. Examples of these enhancements are shown in Figures 1–4.

- Mesh topology maps that graphically depict mesh access point location, access point status, and mesh link type and state

Figure 1. Mesh Topology Maps



- Mesh statistics, including parent, child, and neighbor relationships

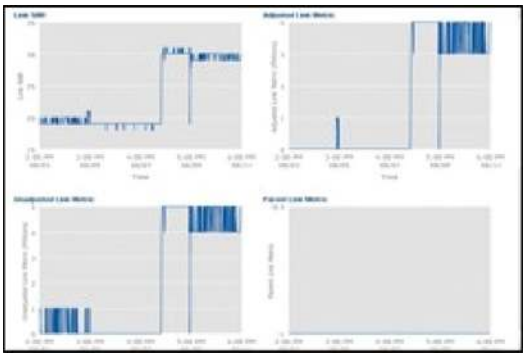
Figure 2. Mesh Statistics

- Mesh link details, including historical information on uplink signal-to-noise ratio (SNR), downlink SNR, combined link SNR, and transmitted and received packet counts

Figure 3. Mesh Link Details

- Historical mesh routing information, including unadjusted and adjusted metrics

Figure 4. Historical Mesh Routing Information



Benefits of Wireless Mesh Enhancements to Cisco WCS

- Eases management and troubleshooting of wireless mesh deployments

Wireless LAN Controllers Supported: Not applicable

Access Points Supported: Cisco Aironet 1500 Series lightweight access points

Management Interfaces Supported: Cisco WCS

Cisco 2700 Series Wireless Location Appliance Enhancements

Cisco Unified Wireless Network Software Release 3.2 provides significant enhancements to the Cisco 2700 Series Wireless Location Appliance:

- **Location-Based Alerts**

This feature provides the ability to proactively send event notifications from Cisco 2700 Series wireless location appliances when one of the following events occurs:

  - Zone detection—An endpoint enters or exits a specified area
  - Absence detection—An endpoint becomes undetectable by the 802.11 network after a specified time interval
  - Movement detection—An endpoint moves beyond a specified landmark on the floor

- **Automatic Synchronization of the Cisco 2700 Series Wireless Location Appliance with Cisco WCS**

This feature gives the system the ability to automatically synchronize any configuration changes made on the Cisco WCS to the Cisco 2700 Series Wireless Location Appliance, and vice-versa. Until now, the WCS and the wireless location appliance needed to be synchronized manually via the user interface. If the two are not synchronized, issues can result, including elements not being tracked or the wrong location information being calculated. With this feature, customers can make modifications to the maps and access point positions without having to remember to synchronize the configuration. Synchronization will occur when:

- Elements have been modified in Cisco WCS (push)
- Elements have been modified in the Cisco 2700 Series Wireless Location Appliance (pull)
- Elements exist in the Cisco 2700 Series Wireless Location Appliance but not yet in Cisco WCS (the auto-sync policy will pull these)

Additionally, alarms will be generated in Cisco WCS for elements that are out of sync with a Cisco 2700 Series Wireless Location Appliance.

- **Ease of Image Installation**

This feature provides customers with the ability to install a complete system from a single ISO file that contains both the operating system and the Cisco 2700 Series Wireless Location Appliance image.

Benefits of Wireless Location Appliance Enhancements

- Location-based alerts enable proactive enforcement of business policies correlated with location coordinates and time
- Improvements in the way configuration changes are tracked and synchronized between the Cisco WCS and the Cisco 2700 Series Wireless Location Appliance
- Ease of installation and maintenance of the Cisco 2700 Series Wireless Location Appliance

Wireless LAN Controllers Supported: Not applicable

Access Points Supported: Not applicable

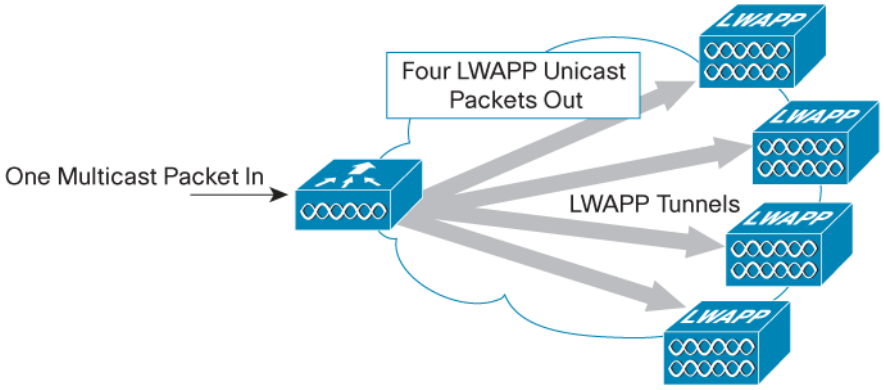
Management Interfaces Supported: Cisco WCS

Multicast Performance Enhancements

In Release 3.2, the multicast performance of the Cisco Unified Wireless Network has been significantly optimized. This enables high-bandwidth multicast applications, such as Cisco IP/TV®, to work over wireless networks.

Prior to this release, each multicast frame received by the controller was unicast over the Lightweight Access Point Protocol (LWAPP) tunnel to each of the access points connected to it, as shown below in Figure 5.

Figure 5. Original Multicast Forwarding Mechanism

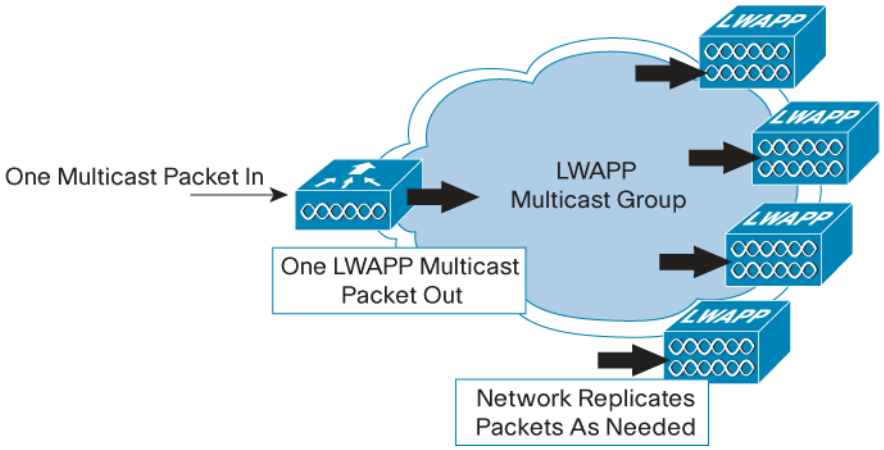


Therefore, depending on the platform, the controller would need to generate up to 300 copies of each multicast packet. This mechanism is inefficient, placing a large processing burden on the controller and flooding the network with a large number of packets.

Release 3.2 introduces a more efficient way of delivering multicast traffic from the controller to the access points. Instead of unicasting each multicast packet over the LWAPP tunnel to each access point, an LWAPP multicast group is used to deliver the multicast packet to each access point. This works as follows:

1. When an access point boots up, it issues an Internet Group Management Protocol (IGMP) join request to join the LWAPP multicast group
2. When the controller receives a multicast packet, it transmits the packet to the LWAPP multicast group via the management interface
3. The network delivers the multicast packet to each of the access points that have joined the LWAPP multicast group, replicating the packet along the way as needed (Figure 6)

Figure 6. Enhanced Multicast Forwarding Mechanism



In order for this to work, the network between the controller and the access points must be multicast-enabled. To accommodate networks that do not support multicast, the controller will continue to support the original multicast forwarding mechanism. The system administrator, through a configuration option, will be able to choose between the two mechanisms.

Notes on Multicast Performance

- To use the multicast performance enhancements, the wireless LAN controller must operate in Layer 3 LWAPP Mode.
- If the network between the controller and access points consists of multiple Layer 3 subnets, a multicast routing protocol such as Protocol-Independent Multicast (PIM) must be enabled.
- The multicast address used for the LWAPP multicast group is configurable on the system. The controller downloads the LWAPP multicast group address to the LWAPP access points during the join process. If the administrator changes the multicast group, the access points are informed of the change, and will leave the old group address and join the new group address.
- All controllers in the same cluster (mobility group) must use the same multicast address for the LWAPP multicast group.
- All multicast packets are sent out at the lowest QoS level.
- Multicast traffic on a WLAN is transmitted by every access point, even if that access point has no clients associated with it that have requested the multicast traffic (i.e. no IGMP snooping).
- The access points use IGMPv1 to join the LWAPP multicast group.
- In a mobility event (a client moves from an access point on their anchor controller to an access point on a foreign controller), the client can only receive multicast packets if one of the following happens:

  - The foreign controller has connectivity to the same VLAN that the client is on. In this case, the foreign controller will become the anchor controller for the client, and the client will continue to receive the multicast stream.
  - Another client on the foreign controller that is on the same WLAN as the roaming client is already receiving the same multicast stream.
- All controllers attached to the same VLAN will forward the same multicast packet to the LWAPP multicast group. This will result in multiple copies of the multicast packet being sent to the LWAPP multicast group. However, access points will only pick up the multicast packet that was sourced from the controller they are currently joined to; the other copies are discarded. Therefore, only one copy of the multicast packet will be transmitted over the air to wireless clients.
- The multicast performance enhancements are not available on Cisco 4100 Series wireless LAN controllers, Airespace 4000 Series wireless switches, and Airespace 4100 Series wireless LAN appliances.

Benefits of Multicast Performance Improvements

- Improved multicast performance enables high-bandwidth multicast applications, such as Cisco IP/TV, to work over wireless networks
- Multicast packet replication occurs only at points in the network where it is required, saving wired network bandwidth

Wireless LAN Controllers Supported: Cisco 2000 and 4400 series wireless LAN controllers; Cisco WiSM; Cisco WLCM for integrated services routers

Access Points Supported: Cisco Aironet 1000, 1130, 1230, 1240, and 1500 series lightweight access points

Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

Link Aggregation for the Cisco 4400 Series and the Cisco WiSM

Link aggregation is an effective way to create a high-speed connection between Cisco 4400 Series wireless LAN controllers and the network infrastructure. Link aggregation allows load sharing of traffic among the links in the channel, as well as redundancy if one or more links in the channel fails. Configuration and design is also simplified—only a single AP-Manager interface is required, backup interfaces are not required, and the total bandwidth of the link aggregation bundle is available to all interfaces.

Link aggregation uses Cisco EtherChannel® to combine all four physical Ethernet ports on a Cisco 4404 Wireless LAN Controller (or two on a 4402) into one logical channel, called a link aggregation bundle. See Figures 7 and 8 below.

Figure 7. Link Aggregation on the Cisco 4402

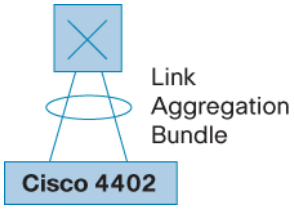
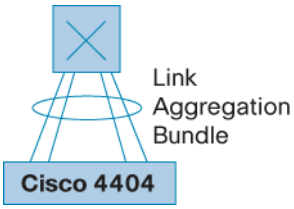
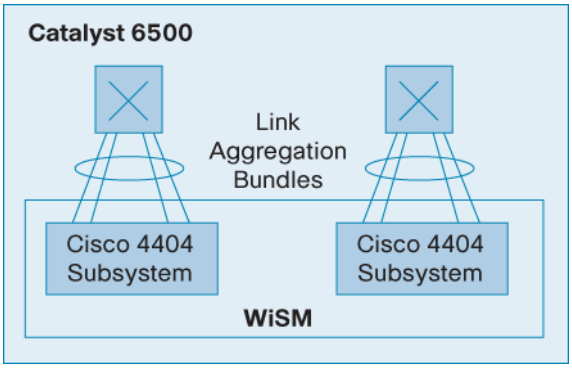


Figure 8. Link Aggregation on the Cisco 4404



Link aggregation is also used on the Cisco Catalyst 6500 Series WiSM. The WiSM consists of two Cisco 4404 Wireless LAN Controller subsystems; the four gigabit links for each of the 4404 subsystems are aggregated, as shown in the Figure 9.

Figure 9. Link Aggregation on the Cisco WiSM



Note that link aggregation is enabled by default on the Cisco WiSM and cannot be disabled.

Notes on Link Aggregation

- Any change to the link aggregation configuration will require the system to be rebooted.
- When link aggregation is enabled, existing interfaces are modified as follows:
  - The management interface is moved to the link aggregation port.
  - The static AP-Manager interface is moved to the link aggregation port. All dynamic AP-Manager interfaces are removed from the system.
  - All VLAN-tagged dynamic interfaces are moved to the link aggregation port. Any untagged interfaces are removed from the system.
- When link aggregation is disabled, existing interfaces are modified as follows:
  - The management interface is moved to Port 1
  - The static AP-Manager interface is moved to Port 1
  - All dynamic interfaces are moved to Port 1
- The mechanism used to load-balance traffic across the links is determined by the Ethernet switch the controller connects to. The controller simply sends a packet out on the same port that it received the packet on. For example, if an LWAPP packet from an access point enters the controller on physical Port 1, the controller will remove the LWAPP wrapper, process the packet, and forward it back to the network on physical Port 1.
- Link aggregation is enabled by default on the Cisco WiSM and cannot be disabled.

Benefits of Link Aggregation

- **Link Redundancy**—Any single link in the bundle can go down and traffic will automatically migrate to the other links. As long as at least one of the physical links is functioning, the system remains functional; access points remain connected to the switch and data service for users continues uninterrupted.
- **Eliminates the Complexity of Configuring Primary and Backup Ports for the Management and Dynamic Interfaces**—Link failure protection is an inherent part of the link aggregation bundle and does not need to be configured by the network manager.
- **Simplified Configuration**—Eliminates the need for multiple AP-Manager interfaces; only a single AP-Manager interface needs to be defined for the system.
- **Simplified Network Design**—No traffic engineering is needed to ensure distribution of traffic across the multiple physical interfaces; the aggregate bandwidth of the link aggregation bundle is available to all logical interfaces on the controller.

Wireless LAN Controllers Supported: Cisco 4400 Series wireless LAN controllers; Cisco WiSM

Access Points Supported: Not applicable

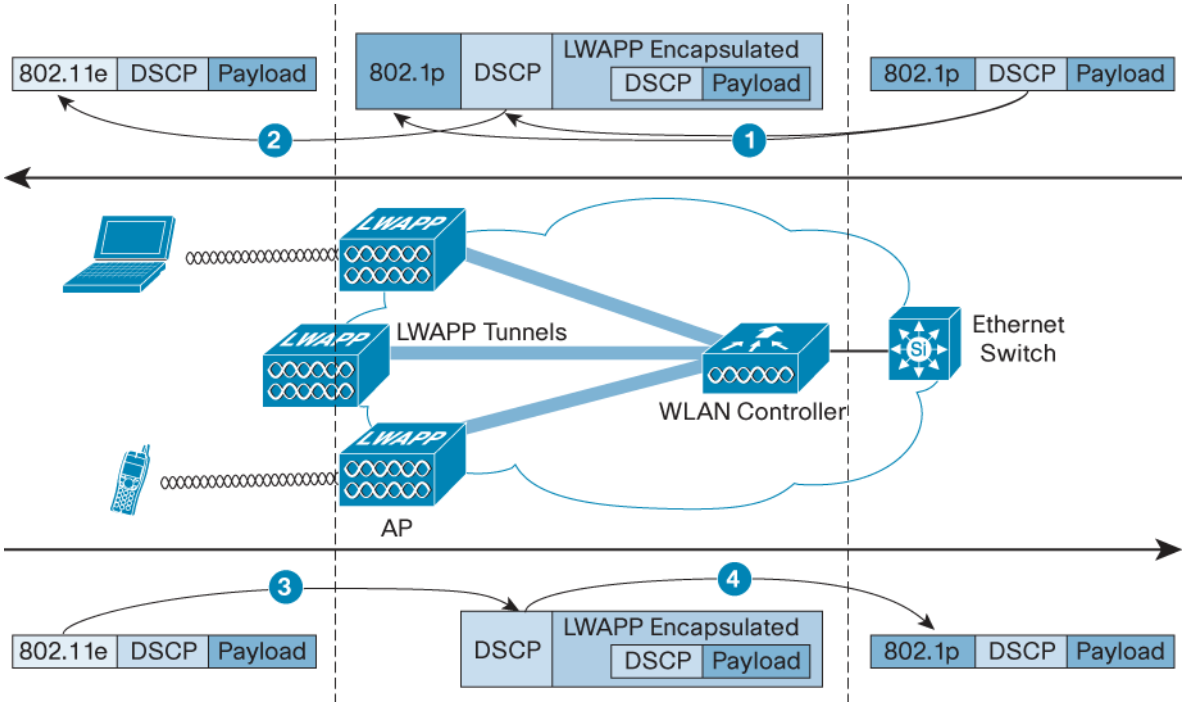
Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

Layer 3 QoS Packet Marking Enhancements

This feature adds support for Layer 3 IP Differentiated Services Code Point (DSCP) marking of packets sent by wireless LAN controllers and lightweight access points. It also enhances how access points use this Layer 3 information to ensure that packets receive the correct over-the-air prioritization from the access point to the wireless client.

In the centralized wireless LAN architecture, wireless LAN data is tunneled between the access point and the wireless LAN controller via 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. See Figure 10.

Figure 10. Mapping of QoS Packet Markings



For example, when 802.11e traffic is sent by a WLAN client, it will have a User Priority (UP) classification in its frame. The access point needs to map this 802.11e classification into a DSCP value for the LWAPP packet carrying the frame to ensure that the packet is given the appropriate priority on its way to the wireless LAN controller. A similar process needs to occur on the wireless LAN controller for LWAPP packets going to the access point. Also needed is a mechanism to classify traffic on both the access point and the wireless LAN controller for non-802.11e clients, so that their LWAPP packets can also be given the appropriate priority.

Table 1 details the various mappings that occur for packets. Any translations that occur are defined in Table 2.

Table 1. QoS Packet Marking Mappings

#	From	To	UP (802.1p/802.11e)	IP DSCP
1	Controller	Access Point	Translate the DSCP value of the incoming packet to the AVVID 802.1p UP value.	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 802.11 Tx queue for the WLAN QoS policy assigned to that client.	N/A (original DSCP value is preserved)
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 packet to the 802.1p UP value.	N/A (original DSCP value is preserved)

Table 2 provides the translations that occur between 802.11e/802.1p UP values and IP DSCP values. Because Cisco AVVID (Architecture for Voice, Video and Integrated Data) 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.

Table 2. QoS Packet Marking Translations

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
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.

Notes on Layer 3 QoS Packet Marking Enhancements

- Layer 3 QoS is not supported when using Layer 2 LWAPP. 802.1p tagging must be used for QoS marking to ensure that packets receive the proper level of QoS.
- The Layer 3 QoS packet marking translations are not configurable.

Benefits of Layer 3 QoS Packet-Marking Enhancements

- Ensures that packets receive the proper QoS handling from end to end.
- Policing of 802.11e UP / 802.1p and IP DSCP values ensures that wireless endpoints conform to network QoS policies.

Wireless LAN Controllers Supported: Cisco 2000, 4100, and 4400 Series wireless LAN controllers; Cisco WiSM; Cisco WLCM for integrated services routers; Airespace 3500, 4000, and 4100 Series wireless LAN controllers

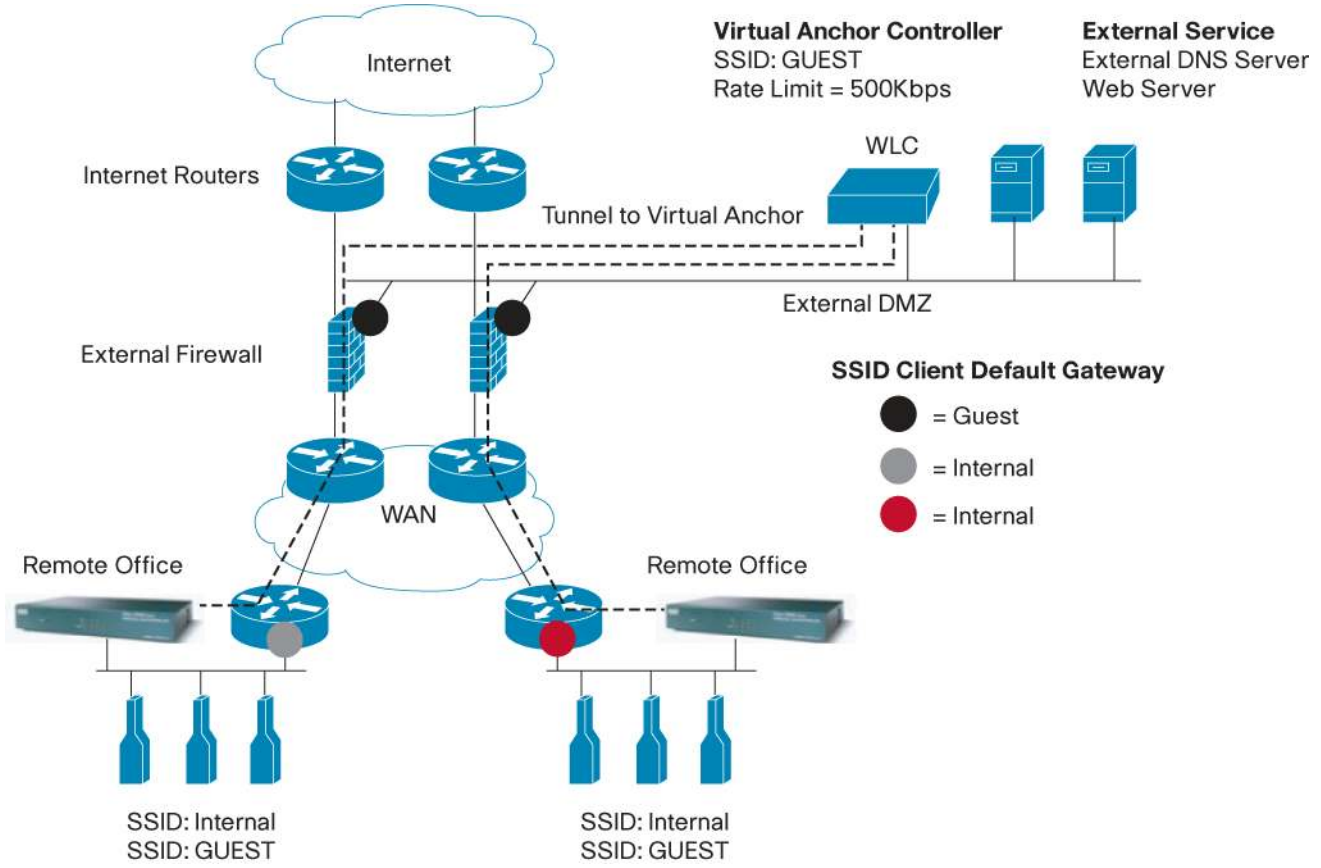
Access Points Supported: Cisco Aironet 1000, 1130, 1230, 1240, and 1500 series lightweight access points

Management Interfaces Supported: Not applicable

Guest Tunnel Origination for Cisco 2000 Series Wireless LAN Controllers

The Guest Tunneling feature was first introduced in Cisco Unified Wireless Network Software Release 3.0 and provides additional security for guest-user access to the corporate wireless network. For a complete description of the Guest Tunneling feature, refer to the Cisco Unified Wireless Network Software Release 3.0 Product Bulletin (http://www.cisco.com/en/US/products/ps6366/prod_bulletin0900aecd802d2742.html). In Release 3.0, this feature was not available on Cisco 2000 Series wireless LAN controllers. Release 3.2 adds support for the Cisco 2000 Series to originate guest tunnels. This capability is also available on the Cisco WLCM for integrated services routers. As these platforms are typically deployed in remote offices, the ability to originate guest tunnels from these controllers to a guest controller in the DMZ provides a flexible and secure way to provide guest access in remote offices.

Figure 11. Guest Tunneling for Cisco 2000 Series Wireless LAN Controller



Notes on Guest Tunnel Origination for the Cisco 2000 Series

- The guest user's IP address is administered from the DMZ.
- All user traffic is transported over an Ethernet over IP (EoIP) tunnel between the regular wireless LAN controller and the virtual anchor wireless LAN controller, which acts as an anchor as the client moves around the network.
- Mobility is supported as a client device roams between wireless LAN controllers.
- Each virtual anchor controller can support 40 tunnels from various "inside" controllers. These tunnels are established from each controller for each SSID using a virtual anchor, meaning that many wireless clients can ride the tunnel.
- Cisco 2000 Series wireless LAN controllers and WLCMs cannot terminate guest tunnels and therefore can not be virtual anchor controllers; these controllers can only originate guest tunnels.

Benefits of the Cisco 2000 Series Guest Tunnel Origination Feature

- For customers with remote sites using Cisco 2000 Series wireless LAN controllers or Cisco WLCMs for integrated services routers, it is now possible to use the Guest Tunneling feature to provide additional security for guest-user access to the corporate wireless network.

Wireless LAN Controllers Supported: Cisco 2000 Series wireless LAN controllers; Cisco WLCM for integrated services routers; Airespace 3500 Series wireless LAN controllers (already supported on Cisco 4100 and 4400 Series; Cisco WiSM; and Airespace 4000 and 4100 Series)

Access Points Supported: Not applicable.

Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

Cisco WCS Serviceability Improvements

The following serviceability improvements have been made to Cisco WCS:

- Enable the user to schedule automatic backups
- Backups can be run while the server is running and clients are logged in
- Run a backup or restore operation via both the GUI and the command line interface
- Cisco WCS backup file is now a single, compressed file
- The Linux version of Cisco WCS can now be installed as a service

Benefits of Cisco WCS Serviceability Improvements

- Ability for network administrators to automatically run backups during off-peak hours
- Backups can be run without affecting any users that may be actively using Cisco WCS
- Ability to have a single compressed backup file, reducing file transfer time, saving disk space, and making it easier to manage backup files
- Easier installation on Linux systems

Wireless LAN Controllers Supported: Not applicable

Access Points Supported: Not applicable

Management Interfaces Supported: Cisco WCS

Static and Dynamic WEP on the Same WLAN

In previous releases of Cisco Unified Wireless Network Software, static and dynamic WEP could not be used on the same WLAN. Separate WLANs had to be configured, one for static WEP and one for dynamic WEP. In Release 3.2, static and dynamic WEP can be used on the same WLAN.

Benefits of Static and Dynamic WEP on the Same WLAN

- More flexible options for deploying secure WLANs

Wireless LAN Controllers Supported: Cisco 2000, 4100, and 4400 Series wireless LAN controllers; Cisco WiSM; Cisco WLCM for integrated services routers; Airespace 3500, 4000, and 4100 Series wireless LAN controllers

Access Points Supported: Cisco Aironet 1000, 1130, 1230, 1240, and 1500 series lightweight access points

Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

Configurable DHCP Proxy

The DHCP Proxy function on the WLAN controller can now be configured to work like a standard DHCP relay. The standard DHCP Proxy function modifies certain fields, such as the DHCP Server Identifier, which caused some client to not work properly. By configuring the DHCP Proxy to work as a standard DHCP relay, these clients will now work properly.

Benefits of Configurable DHCP Proxy

- Clients depending on standard DHCP relay will now work properly with the WLAN controller.

Wireless LAN Controllers Supported: Cisco 2000, 4100, and 4400 Series wireless LAN controllers; Cisco WiSM; Cisco WLCM for integrated services routers; Airespace 3500, 4000, and 4100 Series wireless LAN controllers

Access Points Supported: Not applicable

Management Interfaces Supported: command line interface

VPN Termination Module for the 4400 Series Wireless LAN Controller

A VPN termination hardware module (AIR-VPN-4400-K9=) is being released for the 4400 Series wireless LAN controllers. As with the VPN termination module available today for the 4100 Series wireless LAN controllers, this module enables the 4400 Series wireless LAN controller to terminate VPN client sessions directly on the controller. The module features the following capabilities:

- Support for one VPN termination module on the 4402, and support for one or two VPN termination modules on the 4404
  - If two modules are installed, clients are automatically load balanced across the two modules (applicable to the 4404 only).
- Support for up to 1000 client VPN sessions per module (maximum of 2000 client VPN sessions for a 4404 with two modules)
- Up to 1 Gbps of encryption / decryption per module (maximum of 2 Gbps for a 4404 with two modules)
- Support for the following IPsec clients: Cisco VPN Client, NetScreen Remote, SSH Sentinel, Movian, and Openswan

Notes

- The 4400 VPN termination module (AS-VPN-4400-K9=) is a different physical form factor than the 4400 VPN termination module (AS-VPN-4100-K9=) – the two modules are not interchangeable.
- L2TP is not supported on the 4400 VPN termination module. L2TP is supported on the 4100 VPN termination module

Benefits of VPN Termination Module for the 4400 Series wireless LAN controller:

- Termination of VPN sessions directly on the controller enables client traffic to enter the corporate network as close the edge as possible
- Support for a second VPN termination module on the 4404 enables scaling of VPN termination traffic
- Support for a variety of IPsec clients provides flexible deployment options

Wireless LAN Controllers Supported: Cisco 4400 Series wireless LAN controllers

Access Points Supported: Not applicable

Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

Regulatory Domain Updates

International regulatory requirements are constantly changing. To stay up-to-date on these changes, the following regulatory domain updates are included in Cisco Unified Wireless Network Software Release 3.2:

- Addition of the –P regulatory domain to support the new 802.11a channel and power settings for Japan. The following combinations of access points are permitted:
  - All new –P access points; country code JP2—The system will fully support both the UNII 1 and the UNII 2 changes in the new frequency plan, as well as the normal 2.4-GHz channels.
  - Mix of older “blank” and –J access points; country code JP—All access points work using the legacy frequency plan for 5 GHz, as well as the normal 2.4-GHz channels.
  - Mix of older “blank”, –J, and –P access points; country code JP—All access points to be operational for 2.4-GHz channels, but only the “blank” and –J access points are operational for 5 GHz providing, support for the unshifted UNII 1 channels only. The –P access points will not be operational in the 5-GHz band in this operating mode.
  - Mix of older “blank”, –J, and –P access points; country code JP2—All access points to be operational for 2.4-GHz channels, but only the –P access points operational for 5 GHz, providing support for the shifted UNII 1 channels as well as the new UNII 2 channels.
- Addition of the –K regulatory domain, which adds support for 802.11a in Korea
- Modification of the –I regulatory domain to add support for 802.11a
- Modification of the country Malaysia to permit 802.11a

- Addition of Argentina to the list of configurable country codes on the wireless LAN controller
- Addition of Brazil to the list of configurable country codes on the wireless LAN controller

Benefits of these regulatory domain updates include:

- Ability to use the new 802.11a frequencies that are now available in Japan
- Ability to use 802.11a in South Korea, Israel, and Malaysia
- Ability to use Cisco WLANs using lightweight access points in Argentina and Brazil

Wireless LAN Controllers Supported: Cisco 2000, 4100, and 4400 Series wireless LAN controllers; Cisco WiSM; Cisco WLCM for integrated services routers; Airespace 3500, 4000, and 4100 Series wireless LAN controllers

Access Points Supported: Cisco Aironet 1000, 1130, 1230, 1240, and 1500 Series lightweight access points

Management Interfaces Supported: Cisco WCS, controller web user interface, command line interface

DOWNLOAD THE NEW SOFTWARE FOR THIS RELEASE

Download Cisco Unified Wireless Network Software Release 3.2 from the Cisco Wireless Software Display Tables.

RELATED INFORMATION

For more information about Cisco wireless LAN products, visit: http://www.cisco.com/go/securewireless

For more information about the Cisco Unified Wireless Network, visit: http://www.cisco.com/go/integratedwireless

For more information about wireless security, visit: http://www.cisco.com/go/aironet/security

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C25-338180-00 03/06