# Cisco 440X Series Wireless LAN Controllers Deployment Guide

Cisco customers are rapidly adopting the Cisco Unified Wireless Network architecture for next generation wireless LAN performance and advanced services. This document reviews the fundamental architectural concepts and deployment considerations necessary to evaluate and deploy a basic Cisco Unified Wireless Network solution.

## Terms and Acronyms

contains important terms and acronyms used in this document:

*Table 1 Terms and Acronyms*

| Term or Acronym | Description |
|---|---|
| LWAPP | Lightweight Access Point Protocol—the control and data tunneling protocol between access points and wireless LAN controllers. |
| Wireless LAN Controller; Controller | Cisco device that centralizes and simplifies network management of a wireless LAN by collapsing large numbers of managed endpoints into a single, unified system, allowing for a unified intelligent information wireless LAN network system. |
| Access point | An intelligent translational bridge device that provides network access to wireless devices. |
| Lightweight access point | An access point that runs software that allows it to operate in the Cisco Unified Wireless Network architecture using LWAPP with a wireless LAN controller. |
| WCS | Wireless control system—the software that manages Cisco wireless LAN controllers |
| ACS | Access Control Server—Cisco AAA server that typically provides RADIUS services for Cisco wireless LANs. |

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

# Introduction

Cisco customers are rapidly adopting the Cisco Unified Wireless Network architecture for next-generation wireless LAN performance and advanced services. This document reviews the fundamental architectural concepts and deployment considerations necessary to evaluate and deploy a basic Cisco Unified Wireless Network solution.

The document starts with a brief overview of the Cisco Unified Wireless Network solution and transitions into a discussion of LWAPP. This understanding of LWAPP will set the stage for explaining implementation details and then the deployment basics. We'll bring the concepts together in a simple setup example.

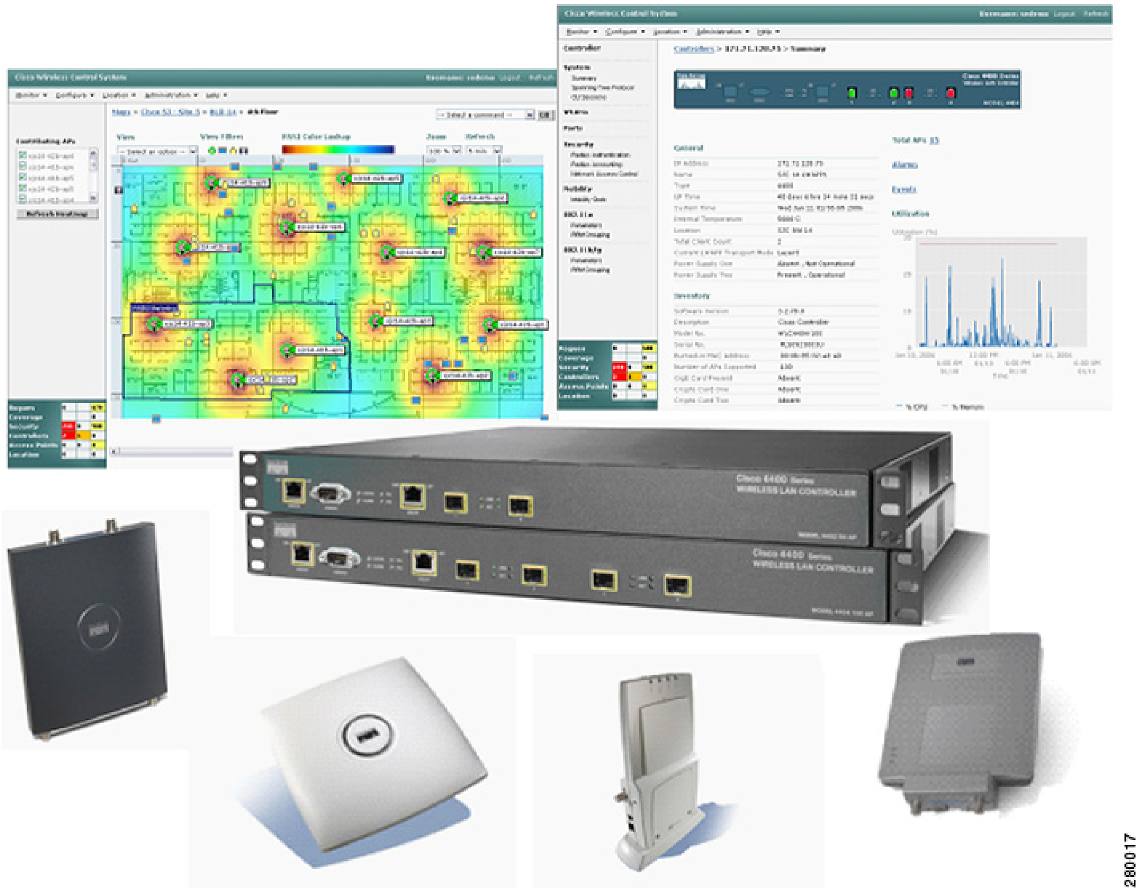
Following the setup example is a discussion of advanced deployment concepts, including support for mobility, dynamic radio management, redundancy and access point load balancing, and scaling strategies. Finally, the document reviews controller maintenance.

This document is intended for technical Cisco support personnel, partners, and customers. This deployment guide assumes that readers have an understanding of IEEE 802.11 wireless LAN concepts and basic knowledge of switching, routing, and Cisco networking concepts.

# Cisco Unified Wireless Network Archtectural Overview

The Cisco Unified Wireless Network architecture is illustrated in Figure 1:

***Figure 1 Cisco Unified Wireless Network Architecture Overview***


Cisco Wireless Control System
Cisco 4400 Series WIRELESS LAN CONTROLLER
Cisco 4400 Series WIRELESS LAN CONTROLLER
280017

The architecture centralizes wireless LAN configuration and control on the controller. This allows the wireless LAN to operate as an intelligent information network and support advanced services, unlike the traditional 802.11 wireless LAN infrastructure that is built from autonomous, discrete entities. The Cisco Unified Wireless Network architecture simplifies operational management by collapsing large numbers of managed endpoints and autonomous access points into a single managed system of wireless LAN controller(s).

In this Cisco Unified Wireless Network architecture, access points are "lightweight," meaning that they cannot act independently of a controller. The wireless LAN controller manages the access point configurations and firmware. The access points are zero-touch and no individual configuration of access points is required. The access points handle only real-time MAC functionality, leaving all the non-real-time MAC functionality to be processed by the wireless LAN controller. This is referred to as the *Split MAC* architecture.

As you can see in Figure 1, access points interact with the controller via LWAPP. LWAPP defines the following:

- Control messaging protocol and format
- Data encapsulation

Wireless LAN client data packets are encapsulated in LWAPP between the access point and the wireless LAN controller. Wireless LAN controllers forward data frames to and from wireless LAN clients after encapsulating or de-encapsulating the frames.

When a wireless LAN client sends a packet, it is received by the access point, decrypted if necessary, encapsulated with an LWAPP header and forwarded to the controller. At the controller, the LWAPP header is removed and the frame switched from the controller onto a vitrual LAN (VLAN) in the switching infrastructure. When a client on the wired network sends a packet to a wireless LAN client, the packet first goes into the wireless LAN controller where it is encapsulated with an LWAPP header and then forwarded to the appropriate access point. The access point removes the LWAPP header, encrypts the frame if necessary, and then bridges the frame onto the RF medium.

This document focuses on practical deployment scenarios of the Cisco Unified Wireless Network solution. And it reviews some LWAPP fundamentals to provide the foundation for discussions to follow in the rest of the document. A detailed discussion of the architecture itself and LWAPP is beyond the scope of this document.

# LWAPP Fundamentals

This section reviews the fundamentals of LWAPP, and provides background information for the deployment scenarios. The LWAPP protocol is defined by an IETF RFC draft document that is the basis for the IETF Control and Provisioning of Wireless Access Points (CAPWAP) working group. Today, LWAPP is the most mature protocol available for wireless network devices.

LWAPP is a generic protocol with a binding definition for the 802.11 wireless LAN protocol. LWAPPdefines how access points communicate with wireless LAN controllers. This communication can be either by means of native, Layer 2 Ethernet frames, or Layer 3 via IP packets. In the Cisco LWAPP implementation, Layer 3 LWAPP packets are carried in UDP packets.

LWAPP messages carry one of two types of payload:

- LWAPP Data Messages, which are encapsulated and forwarded data frames sent from and to wireless clients.
- LWAPP Control Messages, which are management messages exchanged between the wireless LAN controller and the access point.

The LWAPP protocol header contains a control bit (the C-Bit) which identifies data and control packets. When Layer 3 LWAPP is used, the LWAPP data and control packets are sent to separate UDP ports. Because both data and control frames can be fragmented, the payload LWAPP data or control message can be fragmented.

## Phases of LWAPP

The phases of LWAPP operation are as follows:

1. The access points send an LWAPP Discovery Request message.
2. Wireless LAN controllers receiving the LWAPP Discovery Request respond with an LWAPP Discovery Response.
3. From the LWAPP Discovery Responses received, an access point selects a wireless LAN controller to join.
4. The access point then sends an LWAPP Join Request to the selected wireless LAN controller, expecting an LWAPP Join Response.

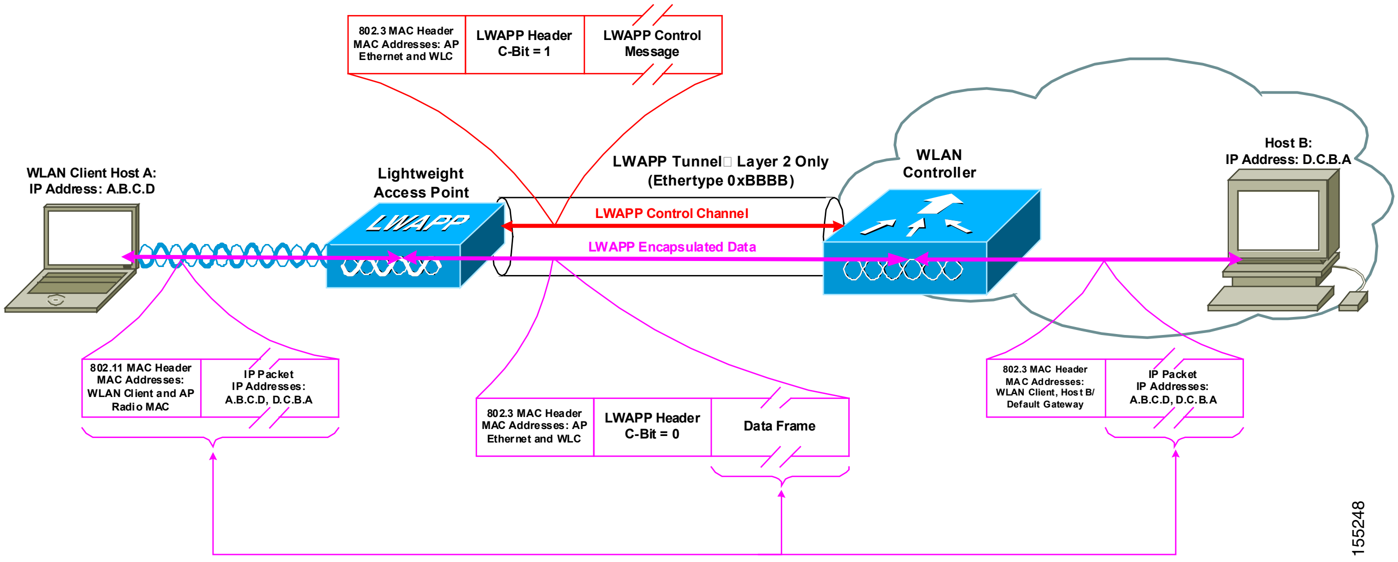
5. The wireless LAN controller receiving the LWAPP Join Request responds to the access point’s Join Request with an LWAPP Join Response. The LWAPP join process includes mutual authentication and encryption key derivation, which is used to secure the join process and future LWAPP Control messages.
6. After the access point has joined the wireless LAN controller, LWAPP messages are exchanged and the access point initiates a firmware download from the wireless LAN controller (if there is a version mismatch between the access point and wireless LAN controller). If the access point's onboard firmware is not the same as the wireless LAN controller's, the access point will download firmware to stay in sync with the wireless LAN controller. The firmware download mechanism utilizes LWAPP.
7. After the wireless LAN controller and access point match firmware revisions, the wireless LAN controller provisions the access point with the appropriate settings. These settings may include SSIDs, security parameters, 802.11 parameters like data rates and supported PHY types, radio channels and power levels.
8. After the provisioning phase is completed, the access point and wireless LAN controller enter the LWAPP runtime state and begin servicing data traffic.
9. During runtime operations, the wireless LAN controller may issue various commands to the access point through LWAPP Control messages. These commands may be provisioning commands or requests for statistical information collected and maintained by the access point.
10. During runtime operations, LWAPP keep-alive messages are exchanged between the access point and wireless LAN controller to preserve the LWAPP communication channel. When a sufficient number of keep-alive message exchanges are missed by an access point, the access point attempts to discover a new wireless LAN controller.

## LWAPP Layer 2 Transport Mode

LWAPP communication between the access point and the wireless LAN controller can be in native, Layer 2 Ethernet frames. This is known as Layer 2 LWAPP mode. Although defined in the RFC draft, Layer 2 LWAPP mode is considered deprecated in Cisco's implementation. Layer 2 LWAPP mode is described in this section for completeness, but the rest of this deployment guide assumes the controller is operating in Layer 3 LWAPP mode.

Figure 2 illustrates Layer 2 LWAPP mode:

*Figure 2 LWAPP Layer 2 Mode*



As you can see from Figure 2, the LWAPP Control and Data messages are encapsulated in Ethernet frames using Ethertype "0xBBBB". In Layer 2 LWAPP mode, although the access points may get an IP address via DHCP, all LWAPP communications between the access point and WLC are in Ethernet encapsulated frames, not IP packets. The access points must be on the same Ethernet network as the WLC. For this reason, Layer 2 LWAPP mode may not be suitable for scalability purposes in most deployments. Furthermore, Layer 2 mode is supported only by the Cisco 410x and 440x series of WLCs and the Cisco 1000 series access points. Layer 2 LWAPP is not supported by lightweight Cisco Aironet 1200, 1252, 1130AG, or 1240AG access points, or the Cisco 2006, WiSM, or WLCM series WLCs.

Figure 2 shows that the LWAPP Control Messages, including the LWAPP Header with the C-Bit set to one, and the control message elements are Ethernet encapsulated in a frame that traverses the local network. The MAC addresses in the Ethernet MAC header are the access point Ethernet MAC address and the WLC MAC address. The source and destination MAC addresses depend on the direction of the frame.  An LWAPP Control frame sent from the access point to the WLC will use the access point Ethernet MAC address as the source address and the WLC MAC address as the destination address. An LWAPP Control frame sent from the WLC to the access point will use the WLC MAC address as the source address and the access point MAC address as the destination address.

Data packets between wireless LAN clients and other hosts are typically IP packets. In Figure 2, Host A is a wireless LAN client communicating with the wired device, Host B. When Host A sends a packet to Host B, the following sequence occurs:

- An IP packet is transmitted by Host A over the 802.11 RF interface after being encapsulated in an 802.11 frame with Host A's MAC address as the source address and the access point's radio interface MAC address as the destination address.
- At the access point, the access point adds an LWAPP Header to the frame with the C-Bit set to zero and then encapsulates the LWAPP Header and 802.11 frame into an Ethernet frame. This Ethernet frame uses the access point Ethernet MAC address as the source MAC address and the WLC MAC address as the destination MAC address.
- At the WLC, the Ethernet and LWAPP headers are removed and the original 802.11 frame is processed.

- After processing the 802.11 MAC Header, the WLC extracts the payload (the IP packet), encapsulates it into an Ethernet frame, and then forwards the frame onto the appropriate wired network, typically adding an 802.1Q VLAN tag.
- The packet then travels through the wired switching and routing infrastructure to Host B.

When Host B sends an IP packet to Host A, the following sequence occurs:

- The packet is carried from Host B over the wired switching and routing network to the WLC, where an Ethernet frame arrives with Host A's MAC address as the destination MAC address. The IP packet from Host B is encapsulated inside this Ethernet frame.
- The WLC takes the entire Ethernet frame, adds the LWAPP Header with the C-Bit set to zero, and then encapsulates the combined frame inside an LWAPP Ethernet frame. This LWAPP Ethernet frame uses the WLC MAC address as the source MAC address and the access point Ethernet MAC address as the destination MAC address. This frame is sent out over the switched network to the access point.
- At the access point, the Ethernet and LWAPP headers are removed and processed.
- The payload (the IP packet) is then encapsulated in an 802.11 MAC frame and transmitted over the air by the access point to Host A.

We'll describe the LWAPP Discovery and Join process in more detail later, but for now understand that a mechanism is included to determine if the path between the access point and WLC supports jumbo frames. If jumbo frames are not supported, an MTU of 1500 bytes is assumed. Both the access point and WLC handle fragmentation and reassembly of LWAPP encapsulated packets. The architecture currently supports reassembly of a maximum of two LWAPP fragments, but it is highly unlikely that there will ever be more than two fragments with Layer 2 LWAPP.

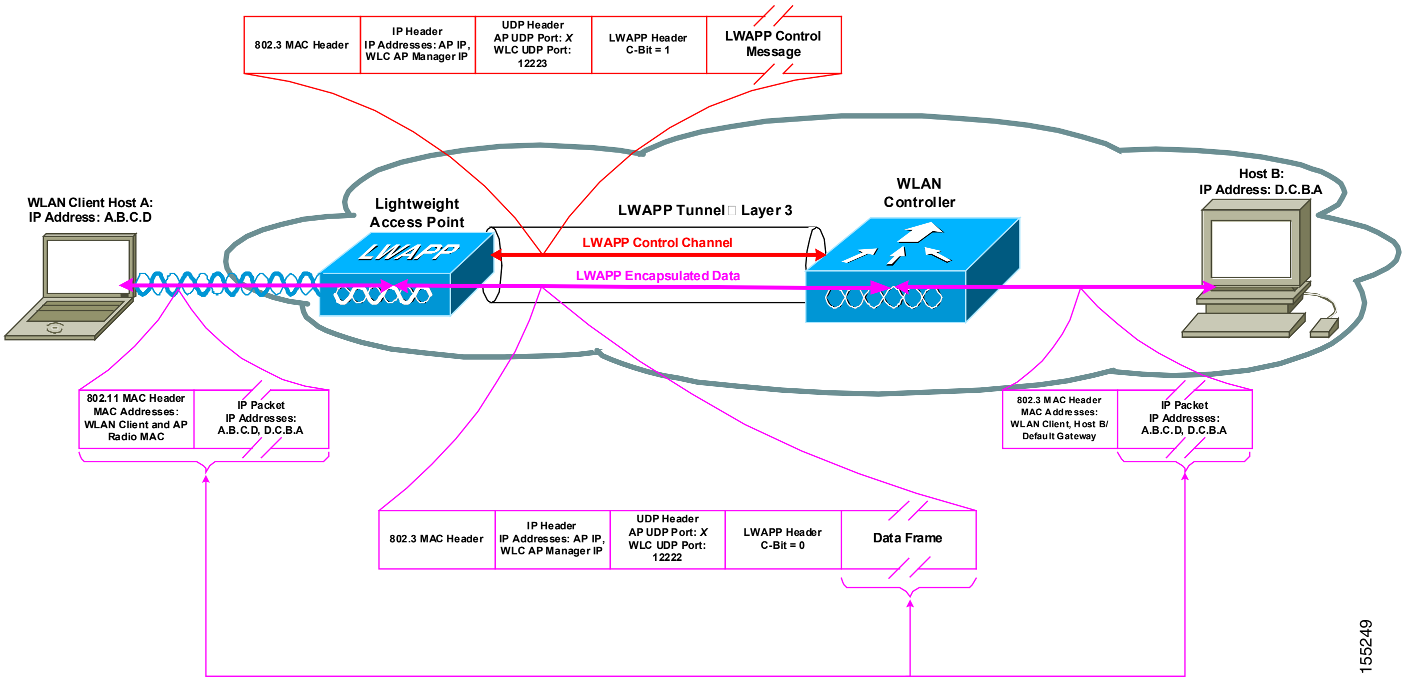
LWAPP Control Messages are encrypted using the industry standard AES-CCM encryption method. The shared encryption key is derived and exchanged when the access point joins the WLC. The payloads of encapsulated LWAPP Data Messages are not specially encrypted. A trusted Ethernet wired network is assumed and standard best practices for protecting Ethernet networks should be followed. Standards-based wireless Layer 2 encryption is handled at the access point.

Since the WLC is the point of ingress/egress for wireless LAN traffic on that IP network, the IP address of wireless LAN clients such as Host A comes from the pool of addresses on the network upstream of the WLC. This may not necessarily be the same network as the access points downstream from the WLC. For example, suppose that the packets bridged to and from the WLC are on the upstream side on network 192.168.1.0/24, and that the network between the WLC and access point is 192.168.2.0/24. Host A's IP address is on the 192.168.1.0/24 network. The address of the wireless LAN client can be either statically assigned or dynamically assigned via DHCP.

## LWAPP Layer 3 Transport Mode

Layer 3 LWAPP Control and Data messages are transported over the IP network in UDP packets. This transport architecture is inherently more flexible and scalable than Layer 2 LWAPP and is the generally preferred solution. Layer 3 LWAPP is supported on all Cisco WLC platforms and lightweight access points. Figure 3 illustrates Layer 3 LWAPP:

*Figure 3 LWAPP Layer 3 Mode*



As shown in Figure 3, the LWAPP Control and Data messages are encapsulated in UDP packets that are carried over the IP network. The only requirement is established IP connectivity between the access points and the WLC. The LWAPP tunnel uses the access point's IP address and the WLC's AP Manager interface IP address as endpoints. The AP Manager interface is explained in further detail in the implementation section. On the access point side, both LWAPP Control and Data messages use an ephemeral port that is derived from a hash of the access point MAC address as the UDP port. On the WLC side, LWAPP Data messages always use UDP port 12222. On the WLC side, LWAPP Control messages always use UDP port 12223.

The mechanics and sequencing of Layer 3 LWAPP are similar to Layer 2 LWAPP except that the packets are carried in UDP packets instead of being encapsulated in Ethernet frames. Figure 3 shows how LWAPP Control Messages, including the LWAPP Header with the C-Bit set to one, and the LWAPP Control Message elements are transported in UDP packets encapsulated in IP.

In Figure 3, Host A is a wireless LAN client communicating with the wired device, Host B. When Host A sends a data packet to Host B, the following sequence occurs:

- The packet is transmitted by Host A over the 802.11 RF interface. This packet is encapsulated in an 802.11 frame with Host A's MAC address as the source address and the access point's radio interface MAC address as the destination address.
- At the access point, the access point adds an LWAPP Header to the frame with the C-Bit set to zero and then encapsulates the LWAPP Header and 802.11 frame into a UDP packet that is transmitted over IP. The source IP address is the access point's IP address and the destination IP address is the WLC's AP Manager Address. The source UDP port is the ephemeral port based on a hash of the access point MAC address. The destination UDP port is 12222.
- The IP packet is encapsulated in Ethernet as it leaves the access point and transported by the switching and routed network to the WLC.
- At the WLC, the Ethernet, IP, UDP, and LWAPP headers are removed from the original 802.11 frame.

- After processing the 802.11 MAC header, the WLC extracts the payload (the IP packet from Host A), encapsulates it into an Ethernet frame, and then forwards the frame onto the appropriate wired network, typically adding an 802.1Q VLAN tag.
- The packet is then transmitted by the wired switching and routing infrastructure to Host B.

When Host B sends an IP packet to Host A, the process is essentially reversed:

- The packet is delivered by the wired switching and routing network to the WLC, where an Ethernet frame arrives with Host A's MAC address as the destination MAC address.
- The Ethernet header is removed by the WLC and the payload (the IP packet destined for Host A) extracted.
- The original IP packet from Host A is encapsulated with an LWAPP Header, with the C-bit set to zero, and then transported in a UDP packet to the access point over the IP network. The packet uses the WLC AP Manager IP address as the source IP address and the access point IP address as the destination address. The source UDP port is 12222 and the destination UDP port is the ephemeral port derived from the access point MAC address hash.
- This packet is carried over the switching and routing network to the access point.
- The access point removes the Ethernet, IP, UDP and LWAPP headers, and extracts the payload, which is then encapsulated in an 802.11 frame and delivered to Host A over the RF network.

Layer 3 LWAPP assumes a 1500-byte MTU. Both the access point and WLC handle fragmentation and reassembly of LWAPP-encapsulated packets based on the 1500 byte MTU assumption. The architecture currently supports reassembly of a maximum of two LWAPP fragments.

LWAPP Control Messages are encrypted using the industry standard AES-CCM encryption method. The shared encryption key is derived and exchanged when the access point joins the WLC. The payloads of encapsulated LWAPP Data Messages are not specially encrypted. A trusted wired network is assumed and standard best practices for protecting networks should be followed. Standards-based wireless Layer 2 encryption is handled at the access point.

Since the WLC is the point of ingress/egress for wireless LAN traffic on that IP network, the IP address of wireless LAN clients such as Host A comes from the pool of addresses on the network upstream of the WLC. This may not necessarily be the same network as the access points downstream from the WLC. For example, if the packets bridged to and from the WLC are on the upstream side on network 192.168.1.0/24, and the network between the WLC and access point is 192.168.2.0/24, Host A's IP address will be on the 192.168.1.0/24 network. The address of the wireless LAN client can be either statically assigned or dynamically assigned through DHCP.

## LWAPP Discovery and Join Process

Lightweight access points are "zero-touch" deployed. The steps in this process are:

- LWAPP begins with a WLC discovery and join phase. The access points send LWAPP Discovery Request messages to WLCs.
- Any WLC receiving the LWAPP Discovery Request responds with an LWAPP Discovery Response message.
- From the received discovery responses, an access point selects a WLC to join.
- The access point sends an LWAPP Join Request to the WLC, expecting an LWAPP Join Response.
- The WLC validates the access point and then sends an LWAPP Join Response to the access point. The access point validates the WLC to complete the Discovery and Join process. The validation on both the access point and WLC is a mutual authentication mechanism. An encryption key derivation process is subsequently initiated. The encryption key is used to secure future LWAPP messages.

The first problem, though, is how to determine where to send the LWAPP Discovery Request messages. The Cisco implementation defines an access point controller hunting process and discovery algorithm. A list of WLCs is built by the access point using the search and discovery process, and then the access point selects a controller to join from the list.

The search process is as follows:

1. The access point issues a DHCP Discover request to get an IP address, unless it has previously had a static IP address configured.
2. If Layer 2 LWAPP mode is supported by the access point, the access point broadcasts an LWAPP Discovery Message in a Layer 2 LWAPP frame. Any WLC connected to the network that is configured to operate in Layer 2 LWAPP mode will respond with a Layer 2 LWAPP Discovery Response. If Layer 2 LWAPP mode is not supported by the access point or the access point fails to receive an LWAPP Discovery Response to the Layer 2 LWAPP Discovery Message broadcast, the access point proceeds to **Step 3**.
3. If Step **1** fails or if the access point does not support Layer 2 LWAPP mode, attempt a Layer 3 LWAPP WLC discovery.
4. If **Step 3** fails, reset and return to Step **1**.

The controller search process repeats until at least one WLC is found and joined.

## The Layer 3 LWAPP Discovery Algorithm

Step **3** of the access point controller searching process involves running the Layer 3 LWAPP WLC discovery algorithm. The Layer 3 LWAPP WLC discovery algorithm is used to build a controller list. Once a controller list is built, the access point selects a WLC and attempts to join the WLC. The Layer 3 LWAPP discovery algorithm operates as follows:

1. The access point broadcasts a Layer 3 LWAPP Discovery Message on the local IP subnet. Any WLC configured for Layer 3 LWAPP mode that is connected to the local IP subnet will receive the Layer 3 LWAPP Discovery Message. Each of the WLCs receiving the LWAPP Discovery Message reply with a unicast LWAPP Discovery Response Message to the access point.

2. When a feature called Over-the-Air Provisioning (OTAP) is enabled on a WLC, access points that are joined to the WLC advertise their known WLCs in neighbor messages that are sent over the air.[1] New access points attempting to discover WLCs receive these messages and then unicast LWAPP Discovery Requests to each WLC. WLCs receiving the LWAPP Discovery Request messages unicast an LWAPP Discovery Response to the access point.[2]
3. The access point maintains previously learned WLC IP addresses locally in NVRAM. The access point sends a unicast LWAPP Discovery Request to each of these WLC IP addresses. Any WLC receiving the LWAPP Discovery Request responds by sending an LWAPP Discovery Response to the access point. These WLC IP addresses are learned by the access point from previously joined controllers. The stored WLC IP addresses include all of the WLCs in previously joined controller *Mobility Groups*. (The Mobility Group concept is discussed in greater detail later in this document.)
4. DHCP servers can be programmed to return WLC IP addresses in vendor specific "Option 43" in the DHCP Offer to lightweight Cisco access points. When the access point gets an IP address via DHCP, it looks for WLC IP addresses in the Option 43 field in the DHCP Offer. The access point will send a unicast LWAPP Discovery Message to each WLC listed in the DHCP option 43. WLCs receiving the LWAPP Discovery Request messages unicast an LWAPP Discovery Response to the access point.
5. The access point will attempt to resolve the DNS name. The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.
6. If, after Steps **1** through **5**, no LWAPP Discovery Response is received, the access point resets and restarts the search algorithm.

The LWAPP Layer 3 WLC discovery algorithm repeats until at least one WLC is found and joined. Note that during the LWAPP Layer 3 WLC discovery, the access point always completes Steps **1** through **5** to build a list of candidate WLCs. Once the access point has completed the LWAPP WLC Discovery steps, it selects a WLC from the candidate WLC list and sends that WLC an LWAPP Join Request.

WLCs embed important information in the LWAPP Discovery Response: the controller sysName, the controller type, the controller access point capacity and its current access point load, the "Master Controller" status, and an AP Manager IP address. The access point uses this information to make a controller selection, using the following precedence rules:

1. If the access point has previously been configured with a primary, secondary, and/or tertiary controller, the access point examines the controller sysName field (from the LWAPP Discovery Responses), attempting to find the WLC configured as "primary". If the access point finds a matching sysName for the primary controller, it sends an LWAPP Join Request to that WLC. If the access point cannot find its primary controller or the LWAPP Join fails, the access point tries to match the secondary controller sysName to the LWAPP Discovery Responses. If the access point

[1] OTAP is enabled on WLCs by default. OTAP should be enabled only during access point provisioning intervals. After access points are deployed, OTAP should be disabled as a deployment best practice.

[2] Lightweight Cisco Aironet Access Points (1130AG, 1200, and 1240AG series) ship from the factory with a minimal version of lightweight IOS called the LWAPP Recovery IOS image. The LWAPP Recovery IOS image is also what is loaded when Cisco Aironet access points are upgraded from autonomous IOS to lightweight mode. The LWAPP Recovery IOS image does not support OTAP. Cisco Aironet access points must join a WLC first to download a full LWAPP IOS image before supporting OTAP. See Appendix A for a list of Lightweight Aironet Access Point part numbers.

finds a match, it then sends an LWAPP Join to the secondary controller. If the secondary WLC cannot be found or the LWAPP Join fails, the access point repeats the process for its tertiary controller.

2. When no primary, secondary, and/or tertiary controllers have been configured for an access point, or these controllers cannot be found in the candidate list, or if the LWAPP Joins to those controllers have failed, the access point then looks at the "Master Controller" status field in the LWAPP Discovery Responses from the candidate WLCs. If a WLC is configured as a Master Controller, the access point selects that WLC and sends it an LWAPP Join Request.[1]
3. If the access point is unsuccessful at joining a WLC based on the criteria in **1.** and **2.** above, it will attempt to join the WLC with the greatest excess capacity. This has deployment implications that are discussed in a later section.

Once the access point selects a WLC, it sends an LWAPP Join Request to the WLC. In the LWAPP Join Request, the access point embeds a digitally signed X.509 certificate. When the certificate is validated, the WLC sends an LWAPP Join Response to indicate to the access point that it is successfully joined to the controller. The WLC embeds its own digitally signed X.509 certificate in the LWAPP Join Response that the access point must validate. Once the access point validates the WLC certificate, the LWAPP Join process is completed.

## Securing the LWAPP Control Plane

The LWAPP Control Plane is protected by the mutual authentication of devices during the LWAPP Join phase and by encryption of the control message payload of all LWAPP Control messages other than the LWAPP Discovery and Join messages. The LWAPP Control Message payloads are encrypted using the industry standard AES-CCM algorithm. AES-CCM is a symmetric cipher algorithm, meaning that both the access point and the WLC must have the same encryption key to encrypt and decrypt messages they exchange. The logical question then is how this key is derived and distributed securely. This document assumes the reader has a basic understanding of security and PKI concepts.

As a basis for explaining how the LWAPP Control Plane is protected, we must first verify these key facts:

- The access point and WLC have X.509 certificates burned into protected flash.
- The X.509 certificates are signed by a private key that is burned into the devices at time of manufacture. Both the access point and WLC have the appropriate public encryption keys installed.
- The access point and WLC have certificates installed that allow them to trust the issuing certificate authority (of the access point or WLC certificate).

As previously explained, when the access point sends the LWAPP Join Request to the WLC, it embeds its X.509 certificate in the LWAPP message. It also generates a random session ID that is also included in the LWAPP Join Request. When the WLC receives the LWAPP Join Request, it validates the signature of the X.509 certificate using the access point's public key and checks that the certificate was issued by a trusted certificate authority. It also looks at the starting date and time for the access point certificate's validity interval and compares that date and time to its own date and time. If the X.509 certificate is validated, the WLC generates a random AES encryption key. The WLC plumbs the AES key into its crypto engine so that it can encrypt and decrypt future LWAPP Control Messages exchanged with the access point.

The WLC next encrypts the key using the access point's public key, concatenates the resulting ciphertext with the session ID in the LWAPP Join Request, and encrypts the concatenated value using its own private key. The WLC copies the results into the LWAPP Join Response along with its own X.509 certificate.

[1] There should never be more than one WLC configured as a Master Controller.

When the access point receives the LWAPP Join Response, it validates the WLC certificate signature using the WLC's public key and checks that the certificate was issued by a trusted certificate authority. If the WLC certificate is validated, the access point extracts the encrypted key portion. It decrypts the concatenated ciphertext using the WLC's public key and validates the session ID. It then decrypts the AES key using its private key. Finally, it plumbs the AES key into its crypto engine to secure future LWAPP Control Message exchanges with the WLC.

The access point maintains a key lifetime timer. When the timer expires, the access point generates a new session ID and embeds it in an LWAPP Key Update Request message to the WLC. The WLC repeats the previously described key generation and distribution process and embeds the new ciphertext in an LWAPP Key Update Response. The key lifetime timer is 8 hours.

The X.509 certificates, certificate authority stores and public and private key pairs are burned into protected flash on both the access point and WLC at the factory by Cisco. On the access point, factory installed certificates are called manufacturing installed certificates (MIC). All Cisco access points manufactured after July 18, 2005, have MICs.

Cisco Aironet 1200, 1130, and 1240 access points manufactured prior to July 15, 2005, that have been upgraded from autonomous IOS to LWAPP IOS will generate a self-signed certificate (SSC) during the upgrade process. SSCs are not trusted by default by WLCs, so the Cisco LWAPP Upgrade Tool generates a file containing a mapping of access point MAC addresses to public keys. This file must be imported into a WLC before an access point with an SSC is allowed to join. For a discussion of managing access points with self-signed certificates, please refer to the following document:

http://www.cisco.com/en/US/products/ps6366/products_configuration_example09186a00806a426c.shtml

The rest of this document assumes that a MIC is implementated on the access point.

The access point X.509 certificates have a validity interval of 25 years that starts at the date and time the access point certificate is provisioned. Therefore, **it is extremely important that the WLC date and time are current**. When the WLC date and time are not current, the authentication of the access points might fail because the access point certificate will not be valid from the WLC's perspective. When this happens, the access point will never join the WLC. You can set the date and time on the WLC, or better yet, **use NTP if possible**.

## LWAPP Post Discovery and Join

After the LWAPP Join process is completed, the access point downloads firmware from the WLC if its running code version does not match the WLC. The access point always matches its code revision to the WLC. This means the access point downgrades its code if it joins a WLC running a lower code revision than what is currently running on the access point. This has ramifications on your controller maintenance and redundancy strategies that will be discussed later.

After syncing firmware revisions between the WLC and the access point, the WLC provisions the access point with the appropriate SSID, security, QoS, and other parameters that have been configured at the WLC. At this point, the access point is ready to serve wireless LAN clients.

The WLC periodically queries its joined access points for statistics in LWAPP Control messages. These statistics are used for dynamic radio resource management (known as RRM), alarming, reporting, and other tasks.

The access point periodically sends an LWAPP Heartbeat control message to the WLC. The WLC responds with an LWAPP Acknowledgement to the heartbeat. The heartbeat interval is 30 seconds. When a heartbeat acknowledgement from the controller is missed, the access point re-sends the heartbeat up to five times at 1- second intervals. If no acknowledgement is received after 5 retries, the access point declares the controller unreachable, releases and renews its IP address, and looks for a new controller.

# Deployment Basics

This section describes how to set up a Cisco Unified Wireless Network solution.

1. How wireless LAN controllers connect to the network.
2. How access points connect to the network.
3. Managing the wireless LAN controllers with WCS.
4. Basic setup example.

## How Wireless LAN Controllers Connect to Network

Key WLC terms and concepts to understand are:

- Port
- Interface
- Wireless LAN

A WLC port is a physical entity that connects the WLC to the neighbor switch. Cisco 2006 Series WLC devices have 4 10/100 copper Ethernet ports. Cisco 440x series controllers have either 2 or 4 fiber Gigabit Ethernet ports. Each port is, by default, an 802.1Q VLAN trunk port. The VLAN trunking characteristics of the port are not configurable. The Cisco 440x series WLC platforms also has a 10/100 copper service port. The service port is reserved for out-of-band management of the wireless LAN controller and system recovery and maintenance; use of the service port is optional.

Cisco 440x series controllers support link aggregation (LAG) with software release 3.2 and higher. LAG is based on the IEEE 802.3ad port aggregation standard. LAG allows you to aggregate all of the ports on the 440x into a single port-channel interface. The system dynamically manages traffic load balancing and port redundancy with LAG.

An *interface* is a logical entity on the WLC. An interface has multiple parameters associated with it, including IP address, default-gateway (for the IP subnet), primary physical port, secondary physical port, VLAN tag, and DHCP server. When LAG is not used, each interface is mapped to at least one primary physical port and an optional secondary port. Multiple interfaces can be mapped to a single WLC port. When LAG is used, the system dynamically maps the interfaces to the aggregated port channel.

There are multiple types of interfaces on the WLC, four of which are static types that must be present and are configured at setup time:

- "Management interface (Static and configured at setup time; mandatory)
- "AP Manager interface (When operating using L3 LWAPP, static and configured at setup time; mandatory)
- "Virtual interface (Static and configured at setup time; mandatory)
- "Service-port interface (Static and configured at setup time; optional)
- "Dynamic (User-defined)

The Management interface is the default interface for in-band management of the WLC and connectivity to enterprise services such as AAA servers. If the service port is in use, the management interface must be on a different subnet from the service port. The management interface is also used for layer 2 communications between the WLC and access points. The Management interface is the only consistently "pingable" in-band interface IP address on the WLC.

A WLC has one or more AP Manager Interfaces that are used for all Layer 3 communications between the WLC and the lightweight access points after the access point discovers the controller. The AP Manager IP address is used as the tunnel source for LWAPP packets from the WLC to the access point, and as the destination for LWAPP packets from the access point to the WLC. The AP Manager must have a unique IP address. Usually this is configured on the same subnet as the Management interface, but this is not necessarily a requirement. An AP Manager IP address is not pingable from outside the WLC. The use of multiple AP Manager Interfaces is discussed in the Advanced Deployment Concepts Section.

The Virtual Interface is used to support mobility management, DHCP relay, and embedded layer 3 security like guest web authentication and VPN termination. The Virtual Interface must be configured with an unassigned and unused gateway IP address. A typical virtual interface is "1.1.1.1". The Virtual Interface address will not be pingable and should not exist in any routing table in your network. If multiple WLCs are configured in a mobility group, the Virtual Interface IP address **must be the same on all WLC devices** to allow seamless roaming.

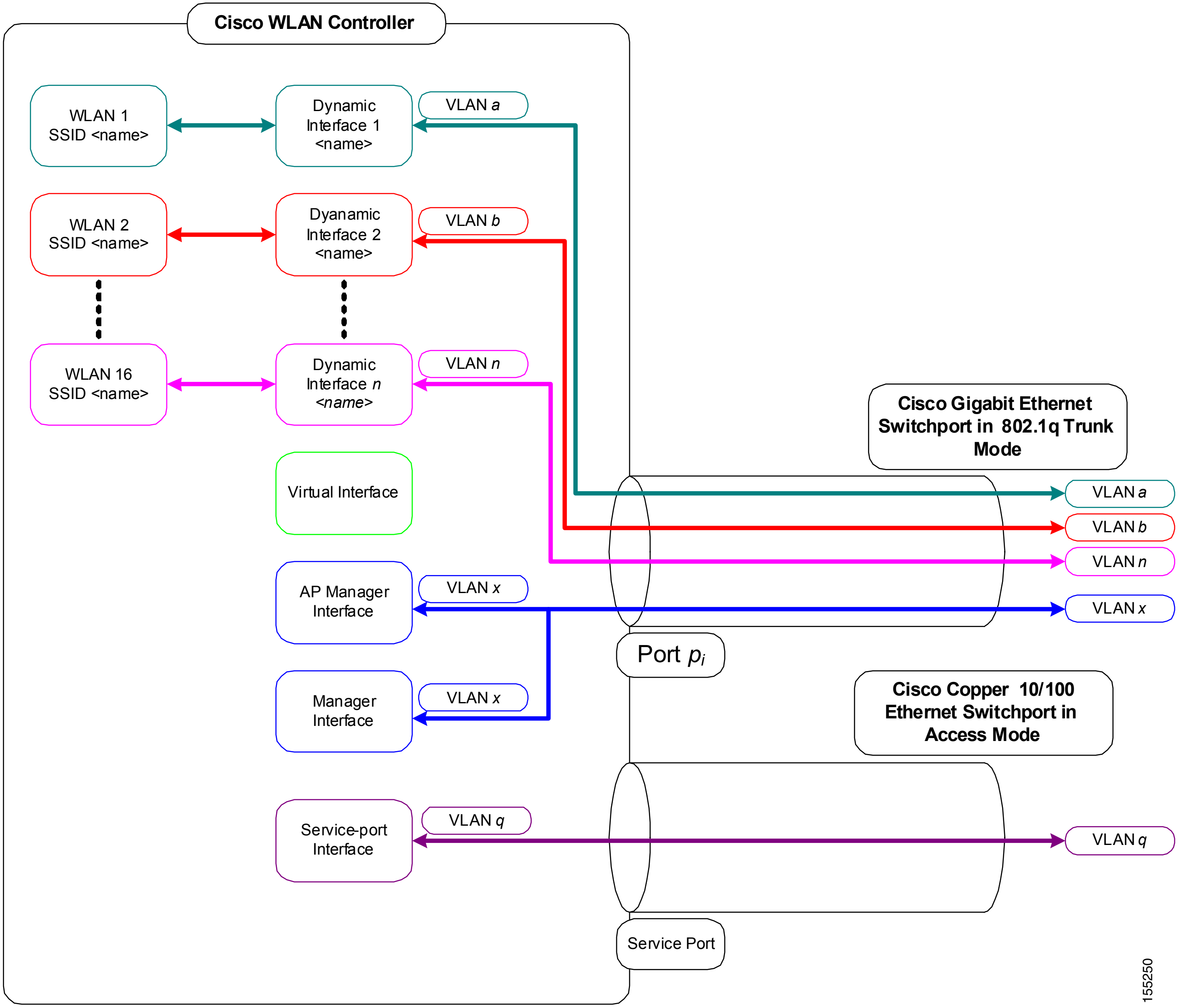
The Service-port Interface is statically mapped by the system only to the physical service port. The service port interface must have an IP address on a different subnet from the Management, AP Manager, and any dynamic interfaces. The service port can get an IP address via DHCP or it can be assigned a static IP address, but a default-gateway cannot be assigned to the Service-port interface. Static routes can be defined in the WLC for remote network access to the Service-port. The Service-port is typically reserved for out-of-band management in the event of a network failure. It is also the only port that is active when the controller is in boot mode. The physical service port is a copper 10/100 Ethernet port and is not capable of carrying 802.1Q tags so it must be connected to an access port on the neighbor switch.

Dynamic Interfaces are created by users and are designed to be analogous to VLANs for wireless LAN client device. The WLC will support up to 512 Dynamic Interface instances. Dynamic Interfaces must be configured on a unique (to the WLC) IP network and VLAN. Each Dynamic Interface acts as a DHCP relay for wireless clients associated to wireless LANs mapped to the interface.

A wireless LAN associates an SSID to an interface and is configured with security, QoS, radio policies, and other wireless network parameters. There can be up to 16 access point wireless LANs can be configured per WLC.

Figure 4 illustrates the relationship between the wireless LAN, interface, and port concepts:

*Figure 4 Wireless LAN Controller Architecture*



As can be seen in Figure 4, each controller port connection is an 802.1Q trunk and should be configured as such on the neighbor switch. On Cisco switches, the native VLAN of an 802.1Q trunk is an untagged VLAN. So if you configure an interface to use the VLAN that is configured as the native VLAN on a neighboring Cisco switch, make sure you configure the interface on the WLC to be untagged. A zero value for the VLAN Identifier (on the WLC) means the interface is untagged. The default (untagged) native VLAN on Cisco switches is VLAN 1. When WLC interfaces are configured as tagged, meaning that there is a non-zero value for the VLAN Identifier configured, then the VLAN must be allowed on the 802.1Q trunk configuration on the neighbor switch and not be the native, untagged VLAN.

Cisco recommends that as a good design practice, use only tagged VLANs on the WLC. You should also allow only relevant VLANs on the neighbor switch's 802.1Q trunk connections to WLC ports. All other VLANs should be disallowed or pruned in the switchport trunk configuration. This is extremely important for optimal performance of the WLC.

## How Access Points Connect to the Network

This section covers the material relevant only to connecting access points to the network. The key concepts to understand are:

- WLC Discovery mechanism
- Switchport configuration

Recall from the architecture review section that lightweight access points cannot operate independently from a WLC. Each lightweight access point must discover a WLC, then issue an LWAPP Join Request, and if successful, receive an LWAPP Join Response to become "joined" to a controller. As a review, the access point follows the general LWAPP WLC Discovery algorithm (assuming Layer 3 LWAPP mode) to generate a controller list from which it will select a WLC to join:

1. LWAPP Discovery Request message is broadcast on the local subnet. Any controller on the subnet will respond with an LWAPP Discovery Response.
2. If OTAP is enabled on a WLC, access points that are joined to the WLC will advertise the WLC in neighbor messages sent over the air. Access points attempting to join a WLC will hear these messages and attempt to join the WLC learned from the OTAP messages.
3. Locally stored controller IP addresses. The stored IP addresses include all of the WLCs from previously joined controller "Mobility Groups".
4. If the access point gets an IP address via DHCP, it will look for WLC IP addresses in vendor-specific Option 43 in the DHCP Offer.
5. DNS resolution of "CISCO-LWAPP-CONTROLLER.*localdomain*"—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.
6. If no controller is discovered, reboot and return to Step **1**.

Once an access point has joined a WLC, the network administrator can assign the access point to a specific WLC (primary, secondary, and tertiary controllers may be specified).

While Cisco WLCs always connect to 802.1Q trunks, Cisco lightweight access points do not understand VLAN tagging and so should be connected only to untagged, access ports on the neighbor switch. Cisco lightweight access points by default get an IP address via DHCP. This can be overridden once an access point joins a controller; by assigning a static IP addresses to the access point through the WLC GUI interface. When an access point is assigned a static IP address, the access point stores the address in NVRAM so that the static address is preserved across a reboot or power cycle. This is important to remember because an access point static IP address can only be changed through a WLC interface. If you move a statically addressed access point to a different IP network, it will not be able to forward traffic.

## Wireless LAN Controller Discovery Strategies for Access Point Deployments

When you first deploy lightweight access points in your network, you need a WLC discovery strategy in place. Normally, you will take advantage of the flexibility of the LWAPP Hunting and Discovery algorithm to allow access points to discover and join wireless LAN controllers. There are several common challenges to keep in mind:

- Access points are seldom deployed on the same subnet with the WLC, so WLC local IP subnet broadcast discovery is usually not a WLC Discovery option.
- In Greenfield deployments, OTAP is often not an option when using new Cisco Aironet access points because out-of-the-box lightweight Cisco Aironet access points running only the LWAPP Recovery IOS image don't support OTAP.
- If you are upgrading autonomous Cisco Aironet access points to LWAPP IOS, OTAP is not supported, so you will need to use another controller discovery strategy.
- When multiple controllers respond to LWAPP Discovery Responses, LWAPP will dynamically load balance access points across multiple controllers in the absence of previously configured primary, secondary, and tertiary controllers and a master controller. That has ramifications to consider.
- DHCP and DNS servers might be controlled by desktop management groups so that networking groups deploying the Cisco Unified Wireless LAN Solution cannot configure DHCP scopes and DNS options.

One strategy is to "prime" the access points prior to deploying them in their final locations. Priming the access point is accomplished by deploying the access point in a sand-box environment so that it can easily join a wireless LAN controller. Once joined, the access point will have one or more controller IP addresses stored locally. You can also assign the access point a primary, secondary, and/or tertiary WLC at this time. After the access point has been appropriately joined and provisioned, the access point can be deployed in its final location.

Here is a sample set of steps to follow for priming access points:

**Step 1** Place the WLC in a sand-box environment connected to a Cisco switch such as a Catalyst 3750.

**Step 2** Provision the WLC with its final configuration, including the Management IP address. Provision the WLC Management Interface's VLAN on the switch so that you can connect the access points to that VLAN. Ideally, you want the access points to be able to discover the WLC via LWAPP IP subnet broadcast.

**Step 3** Configure a DHCP server to provide IP addresses to the access points (you can use the Catalyst 3750 to do so).

**Step 4** Connect the access points to the switchports and power them up. The access points should find the WLC through the LWAPP IP subnet broadcast.

**Step 5** Make any access point specific configurations as desired (for example, assign the access point a primary, secondary, and/or tertiary controller).

**Step 6** Once all the access points have been provisioned, deploy the WLC in its final location.

**Step 7** Make sure there is IP connectivity between the access point's final location and the WLC in its final location.

**Step 8** Deploy the access points in their desired location.

These steps are intended as guidelines rather than rules to illustrate the priming process. There are other approaches that essentially follow similar principles.

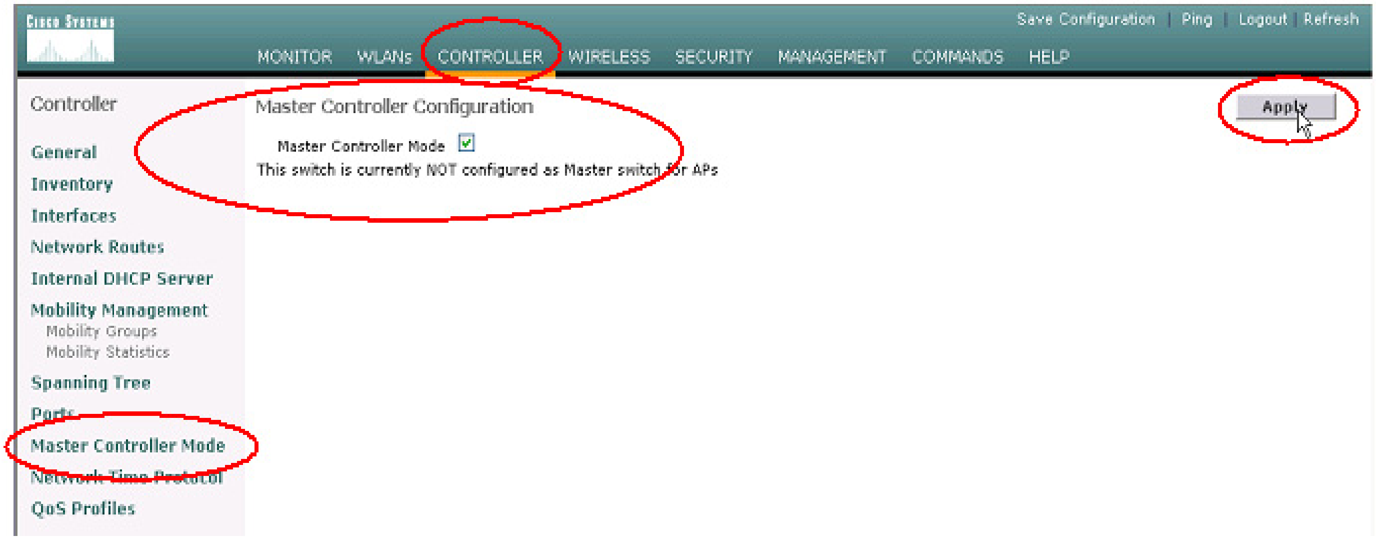
There are two other points that should be remembered when you use a priming deployment strategy:

- "The access point must learn the IP address of the desired WLC when it is primed. When an access point joins a WLC, it learns the IP addresses of all other WLCs in the joined WLC's mobility group.
- "When you configure a primary, secondary, and/or tertiary controller, you enter the sysName of the controllers, not the IP address (see the Advanced Deployment section). A controller embeds its sysName in the LWAPP Discovery Response message. So if you choose to configure a primary, secondary, and/or tertiary controller at priming time, the access point must learn the IP address of these WLCs at priming time. Make sure the primary, secondary, and/or tertiary controllers are in the mobility group of the "priming" WLC.

Another deployment strategy is to use the "Master Controller" option during the deployment phase. The idea is to have access points join a Master Controller as they are deployed and then have the administrator assign them a primary, secondary, and/or tertiary controller. This is also a good time to place the access points on WCS maps. Here are the basic recommendations for using the Master Controller option:

1. Deploy the WLCs in the network.
2. Create the mobility group for the WLCs and assign the controllers to the same mobility group (see the Advanced Deployment section for further help on this).
3. Select one of the WLCs to be the Master Controller and turn Master Controller Mode on for that controller. To turn Master Controller Mode on, login to the WLC and navigate to Controller | Master Controller Mode. Check the "Master Controller Mode" box and then click on the Apply button. Figure 5 shows the Master Controller Mode interface:

*Figure 5 Master Controller Mode Configuration*



Master Controller Configuration

Master Controller Mode ☑

This switch is currently NOT configured as Master switch for APs

4. Implement a strategy to have the access points learn the Master Controller IP address during the LWAPP Discovery process. For example, configure the Master Controller's Management Interface IP address in the vendor specific Option 43 in the DHCP server.
5. Proceed with deploying the access points. Assuming that the access points have not previously been configured with a primary, secondary, and/or tertiary controller, the access points should join the Master Controller.
6. You may now assign these joined access points to the desired primary, secondary, and/or tertiary WLCs (see the Advanced Deployment section). This is also a good time to place the access points in maps in the WCS.

7. After completing your access point deployment, Cisco recommends that you turn Master Controller Mode off.

## Powering the Access Points

Once the infrastructure foundation is laid, connecting the access points is usually as simple as plugging them into the switchport. In lightweight mode, there is no manual access point configuration required. The only consideration is figuring out how to provide power to the access points. There are three options:

- Power over Ethernet (PoE)
- Power Injector
- Power bricks

The basic power requirements for Cisco Lightweight Access Points are listed in :

*Table 2 Cisco Access Point Power Capabilities*

| Cisco Access Point | Power over Ethernet Capabilities | Power Draw in Watts |
|---|---|---|
| Cisco 1000 Series | 802.3af | 12 |
| Cisco Aironet 1130AG | 802.3af, Cisco PoE | 12.2 |
| Cisco Aironet 1240AG | 802.3af, Cisco PoE | 12.95 |
| Cisco Aironet 1200 (802.11g only) | Cisco PoE | 6.5 |
| Cisco Aironet 1200 (802.11a only) | Cisco PoE | 10.5 |
| Cisco Aironet 1230AG (802.11a and 802.11g) | Cisco PoE | 13 |

Note that the access point power draw in the table does not include other factors like voltage and cable resistance. You need to consider these factors when selecting a power option. An in-depth discussion is beyond the scope of this document and you should consult the Cisco Aironet Power Over Ethernet Application Note for more details on access point power options.

Power over Ethernet is the most desirable since it minimizes the amount of extra equipment to deploy. However, to use PoE, the access point's neighbor switch must support the right flavor of PoE and have enough power capacity to support the number of access points connected to it, as well as any other power drawing devices such as IP phones. Consult the *Cisco Aironet Power Over Ethernet Application Note* for more details on access point power options.

A second-most attractive power option is the use of power injectors. A power injector has two Ethernet ports—one that comes from the switch and one that goes to the access point. The power injector plugs into a standard electrical outlet and converts the power from the jack to the appropriate level for the access point, which it then supplies over the Ethernet connection to the access point. The power injector is attractive since it can be deployed in the IDF closet where there are usually plenty of electrical outlets. It also minimizes the amount of extra cabling to be done. Cisco offers power injectors for all of its access point products. Consult Cisco.com and your Cisco account representatives for more details on access point power injector options.

The AP1130AG and AP1240AG access points might not power their radios when using power injectors. Cisco recommends the following in this situation:

1. Disable CDP for the switchports the access point is connected to and then reset the access points.
2. Once the access points have joined a WLC, issue the following two commands from the WLC CLI:

   ```
   > config ap power pre-standard enable <ap-name>
   > config ap power injector enable <ap-name> <switchport MAC address>
   ```

   The "`ap-name`" parameter refers to the access point's sysName. You can glean this from the "`show ap summary`" command at the WLC CLI. The switchport MAC address should be in XX:XX:XX:XX:XX:XX format. This should be the MAC address of the switchport the access point is connected to.

The least attractive power option is a standard Cisco power brick that supplies 15.4W of -48 VDC from a standard wall outlet. This is the least attractive since it requires an electrical outlet near each access point. This can substantially increase the deployment costs since electrical outlets may need to be run to the access point locations. Consult Cisco.com and your Cisco account representatives for more details on access point power brick options.

## Access Point Locations

Determining access point placement is somewhat of a black art, but can be critical to optimal wireless LAN performance. Access point locations should optimize RF coverage and end-user experience. The location decisions should be governed by the planned applications, antennae patterns, user densities, and RF propagation characteristics of the coverage environment.

Typically, a deployment for serving users with data specific needs will require that a wireless client experience no worse than a -72dBm RSSI at any point in the coverage environment. Data deployments should be engineered to support no more than 15-20 concurrent users per access point. Voice-specific deployments typically require no worse than -68 dBm RSSI at any point in the coverage area. In addition, voice deployments should be engineered so that there are no more than seven concurrent active phone calls per access point. Other important factors to consider when determining RF coverage and access point density requirements are the selection of Cisco access point and corresponding antennae. Adding location-based services also affects access point density requirements. However, an in-depth discussion of determining RF coverage requirements, determining access point placement, and antennae selection is beyond the scope of this document.

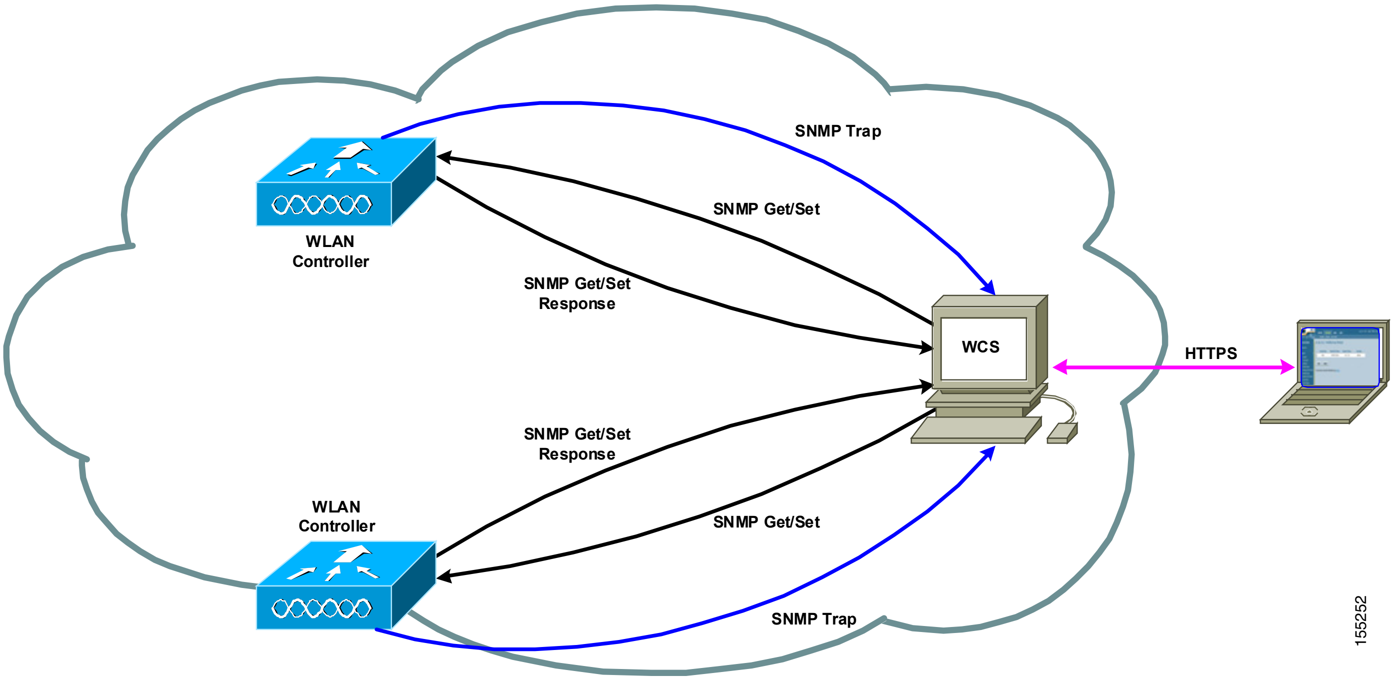
Cisco WCS includes an excellent planning tool that can be used to make access point placement decisions. There are also other advanced, third party planning tools that can be used, but these are often expensive and have a steep learning curve.

As you deploy access points, you should record the access point MAC address and location as precisely as possible. You will need this information for WCS mapping functions.

## Managing the Wireless LAN Controllers with WCS

Figure 6 illustrates how WCS manages WLC devices and how users interact with WCS.

*Figure 6 WCS Management of WLC Devices*



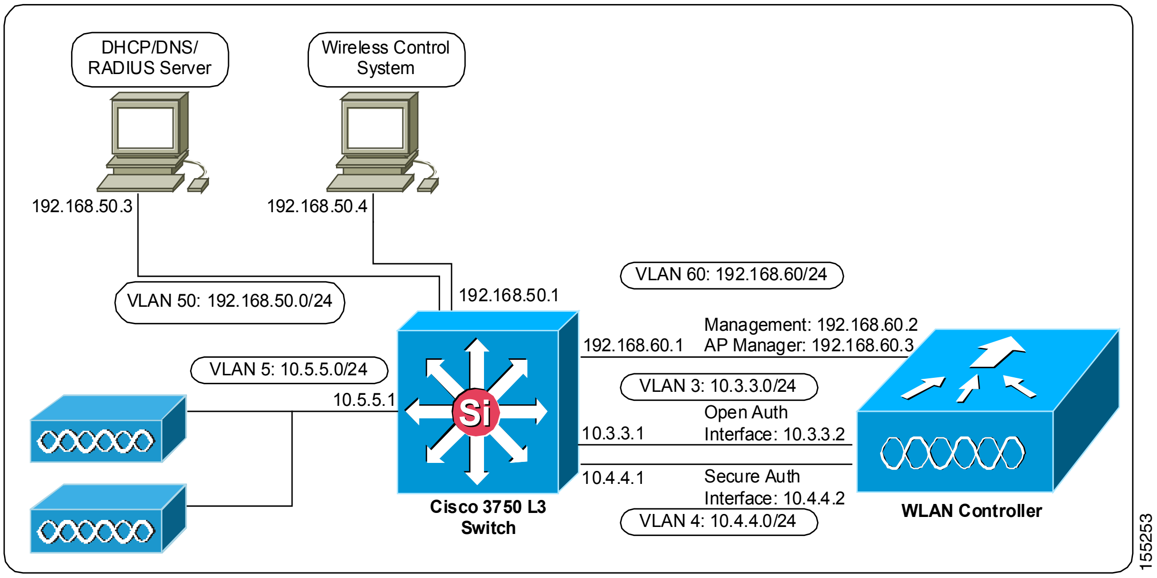
As you can see from Figure 6, data are collected from the managed WLCs at periodic (and customizable) polling intervals. These data samples are used to populate reports, generate alarms, and provide administrators with additional management functionality. The polling protocol is SNMP and SNMP versions 1, 2c, and 3 are fully supported. For SNMPv3, both authorization and authorization with privacy are supported.

As can be seen from Figure 6, asynchronous events such as rogue access point discoveries trigger event notifications to the WCS via SNMP traps. It is important to note that WCS will not show rogue and other event updates when the WCS is not configured as an SNMP trap receiver on the WLCs.

## Basic Setup Example

This example is applicable to the 2006, WLCM, 440x, and WiSM series WLC devices. The sample topology is illustrated in Figure 7:

*Figure 7 Basic Setup Sample Topology*



In this topology example, the WLC is connected to a Cisco 3750 switch using only one physical port (port 1) on the WLC and Gigabit 1/0/1 on the switch. All the interfaces on the WLC are mapped to the physical port 1. Two wireless LANs are configured: one for open authentication (SSID "open") and one for EAP authentication (SSID "secure"). Dynamic interfaces are created for the open SSID and the EAP SSID and mapped to the appropriate VLAN. In the case of the open SSID, VLAN 3 is used and in the case of the EAP SSID, VLAN 4 is used. The Management and AP Manager interfaces are configured to use VLAN 60. To keep this example simple, we will ignore the service-port. All network services (AAA, DHCP, and DNS) are configured on VLAN 50. Access points will be connected to VLAN 5.

## Configuring the Neighbor Switch

As shown in Figure 7, the WLC is connected to the neighboring Cisco 3750 switch using only one port. The neighbor switch port is configured as an 802.1Q trunk and only the appropriate VLANs (VLANs 3 through 4 and 60 in this case) are allowed on the trunk. The Management and AP Manager VLAN (VLAN 60) are tagged and are not configured as the trunk's native VLAN, so when we configure those interfaces on the WLC, we will assign them a VLAN identifier.

The 802.1Q switchport configuration is as follows:

```
interface GigabitEthernet1/0/1
    description Trunk Port to Cisco WLC
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 3-4,60
    switchport mode trunk
    switchport trunk native vlan 60
    no shutdown
```

Notice that the way in which we've configured the neighbor switchport allows only relevant VLANs on the 802.1Q trunk. All other VLANs are pruned. This is not necessary but is a deployment “best practice” because by pruning irrelevant VLANs, the WLC only processes relevant frames, optimizing performance.

## Configuring the Cisco Wireless LAN Controller

The initial configuration of the WLC is done through a console cable connected to the WLC. The WLC is connected to the appropriate switchport and powered up with the serial console cable attached. The serial console settings are the Cisco standard "9600-8-N-1." You will have to configure the system using a setup script through the WLC CLI. After initial configuration, you may configure the WLC through the console CLI or through the WLC web interface. In this example, we'll use the GUI.

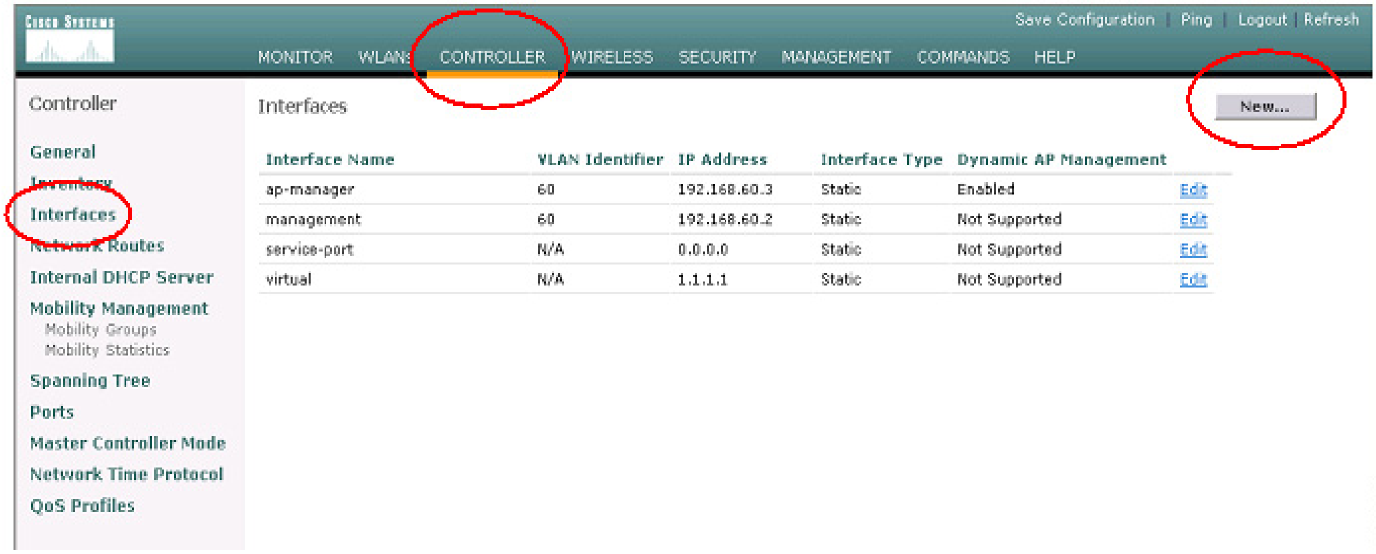
The setup script is used to configure the system name, WLC administrative user credentials, the Management, AP Manager, and virtual interfaces, the mobility group name, one SSID, any RADIUS server(s), and other desired options. In this example, the default values for the other options are accepted and are covered in further detail in a later section. The setup script for the example is as follows:

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_40:e6:23]: c4402-smlab-1
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (24 characters max): *****

Service Interface IP Address Configuration [none][DHCP]: DHCP

Enable Link Aggregation (LAG) [yes][NO]: No

Management Interface IP Address: 192.168.60.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.60.1
Management Interface VLAN Identifier (0 = untagged): 60
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 192.168.50.3

AP Transport Mode [layer2][LAYER3]: LAYER3
AP Manager Interface IP Address: 192.168.60.3

AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (192.168.50.3): 192.168.50.3

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: smlab

Network Name (SSID): secret
Allow Static IP Addresses [YES][no]: yes

Configure a RADIUS Server now? [YES][no]: yes
Enter the RADIUS Server's Address: 192.168.50.3
Enter the RADIUS Server's Port [1812]: 1645
Enter the RADIUS Server's Secret: secret

Enter Country Code (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes
```

All configuration of the WLC from this point forward is done through the WLC web interface. Point to the WLC's Management interface IP address using Internet Explorer to access web-interface. (Please note that only Internet Explorer is supported.) Only HTTPS is enabled by default, so the URL should be https://Management_Interface_IP.

Dynamic interfaces for both VLAN 3 and VLAN 4 will have to be created through the WLC web interface. Navigate to **Controller | Interfaces** and select the **New** button (see Figure 8).

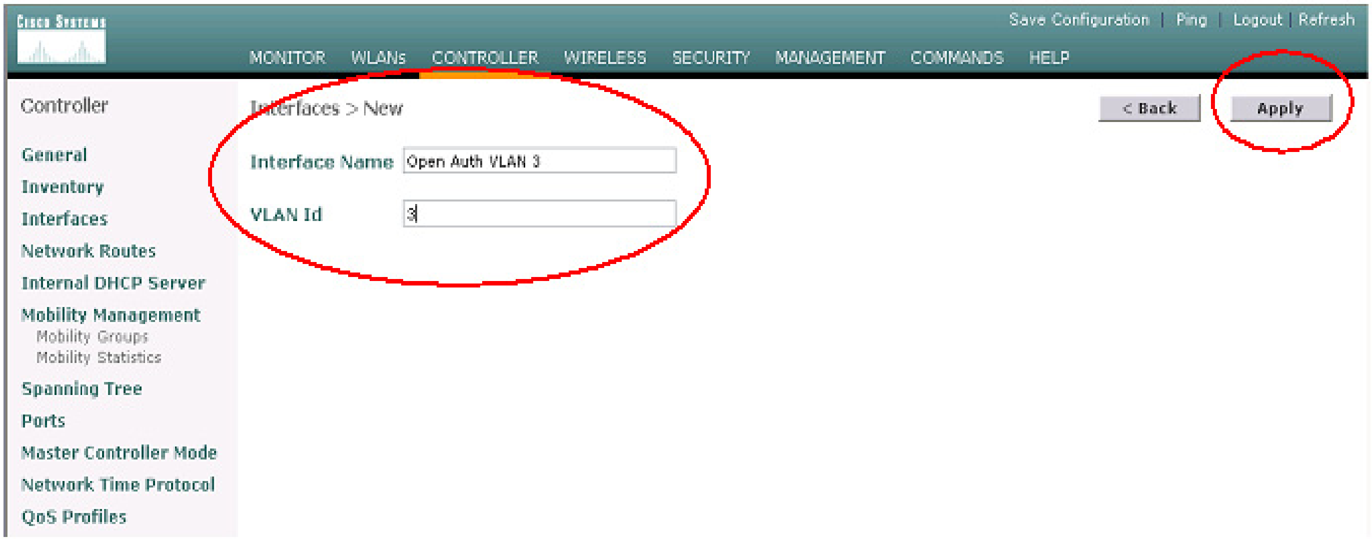
*Figure 8* *WLC Controller Interface Configuration*



| Interface Name | VLAN Identifier | IP Address | Interface Type | Dynamic AP Management | |
|---|---|---|---|---|---|
| ap-manager | 60 | 192.168.60.3 | Static | Enabled | Edit |
| management | 60 | 192.168.60.2 | Static | Not Supported | Edit |
| service-port | N/A | 0.0.0.0 | Static | Not Supported | Edit |
| virtual | N/A | 1.1.1.1 | Static | Not Supported | Edit |

Enter an interface name and VLAN tag and click on the Apply button. Figure 9 illustrates the configuration of the VLAN 3 interface:

*Figure 9* *Dynamic Interface Configuration*

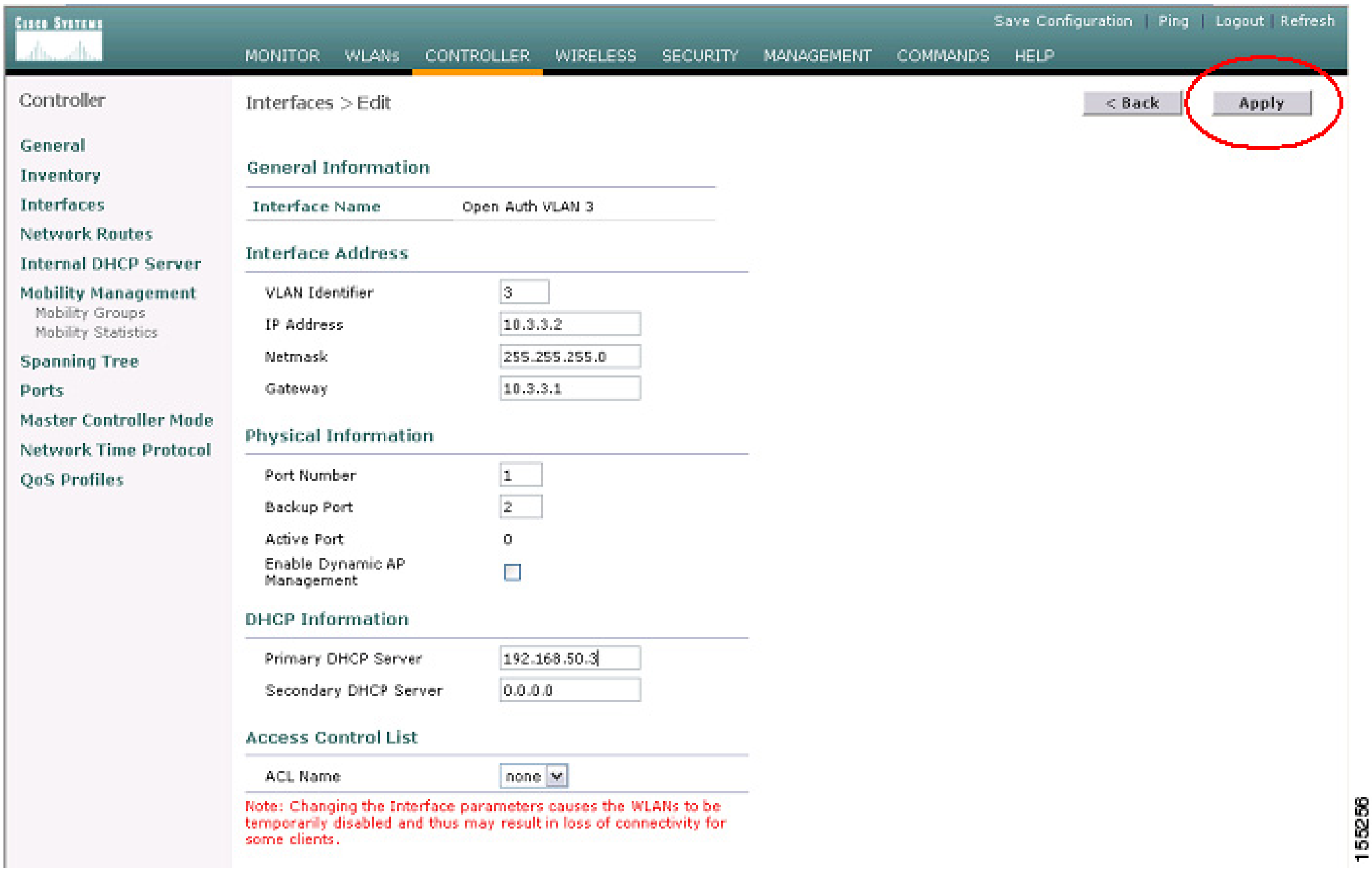


Interface Name: Open Auth VLAN 3

VLAN Id: 3

Enter the appropriate information in the next form and click the **Apply** button (see Figure 10). Note that the port number and primary DHCP server are mandatory parameters for proper operation of your setup.

*Figure 10 Dynamic Interface Configuration*



Interfaces > Edit

General Information

| | |
|---|---|
| Interface Name | Open Auth VLAN 3 |

Interface Address

| | |
|---|---|
| VLAN Identifier | 3 |
| IP Address | 10.3.3.2 |
| Netmask | 255.255.255.0 |
| Gateway | 10.3.3.1 |

Physical Information

| | |
|---|---|
| Port Number | 1 |
| Backup Port | 2 |
| Active Port | 0 |
| Enable Dynamic AP Management | □ |

DHCP Information

| | |
|---|---|
| Primary DHCP Server | 192.168.50.3 |
| Secondary DHCP Server | 0.0.0.0 |

Access Control List

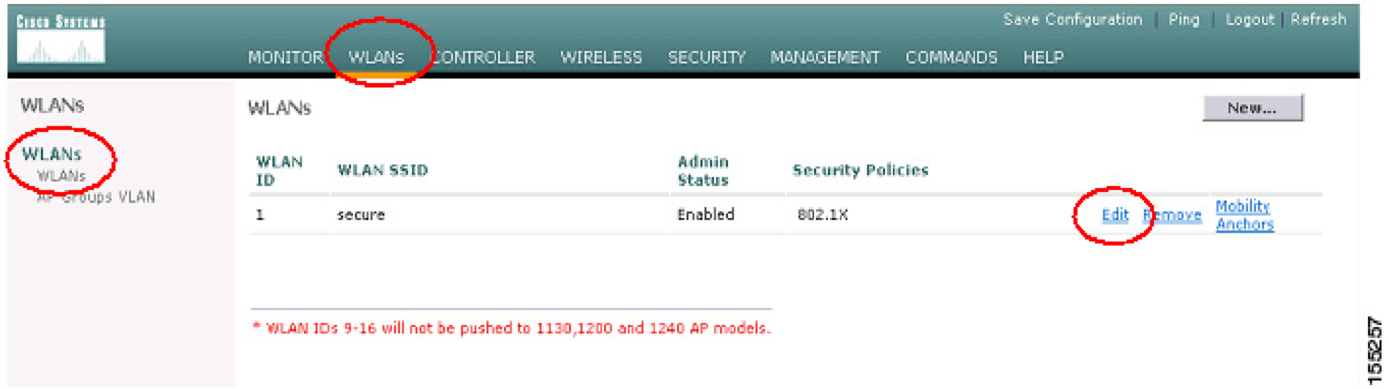
| | |
|---|---|
| ACL Name | none |

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

This process is repeated for each dynamic interface.

Wireless LANs are configured by navigating to the **WLANs | WLANs| WLANs** interface (see Figure 11). The wireless LAN configured with the setup script-the "secure" SSID-should be already listed (see Figure 11). This wireless LAN is, by default, mapped to the Management interface and should be moved to the VLAN 4 interface to continue with our example. Select the Edit link (see Figure 11).

*Figure 11 WLAN Configuration*



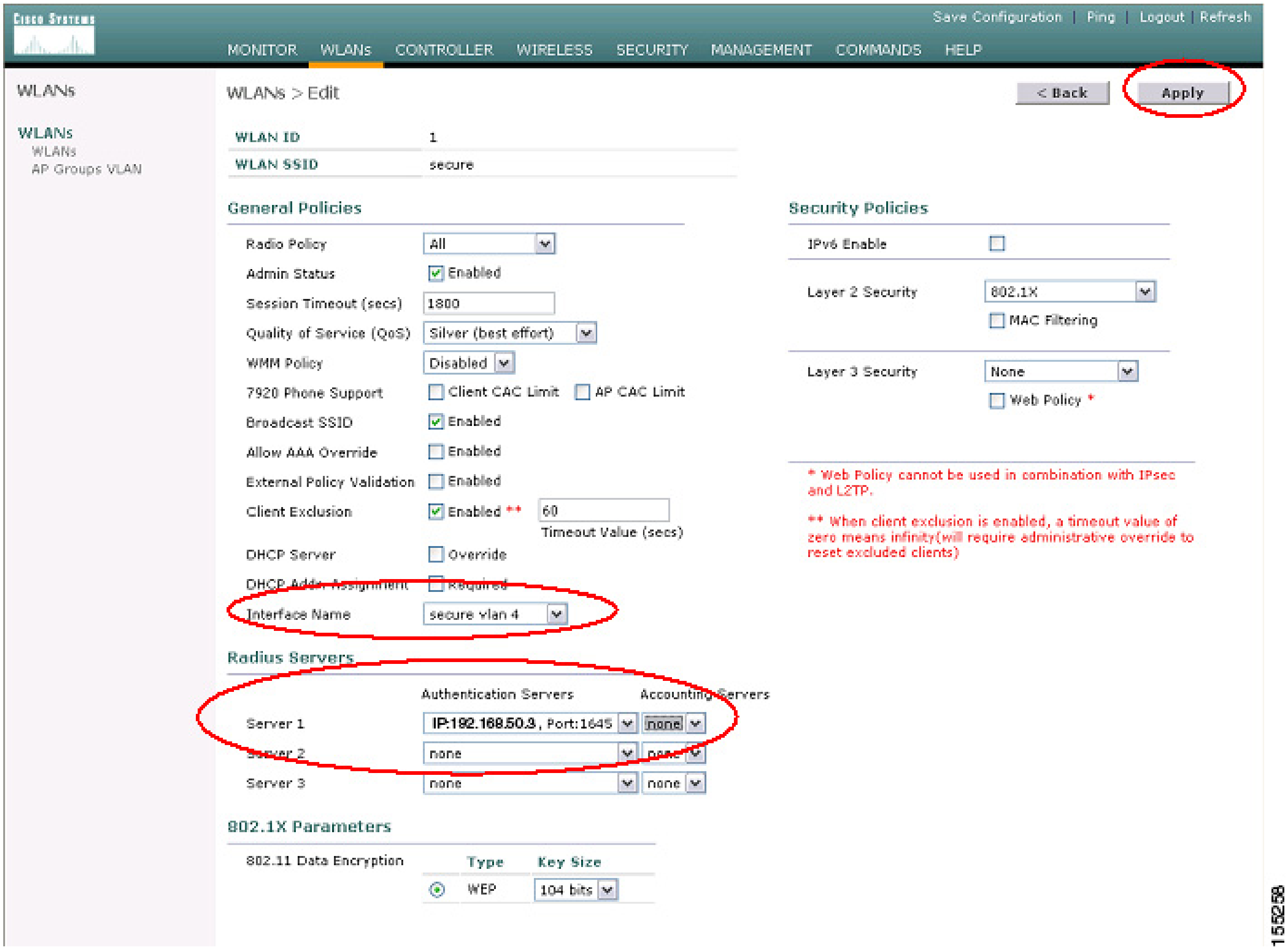
WLANs

| WLAN ID | WLAN SSID | Admin Status | Security Policies | | | |
|---|---|---|---|---|---|---|
| 1 | secure | Enabled | 802.1X | Edit | Remove | Mobility Anchors |

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

Remember to change the Interface Name parameter to the appropriate VLAN. Other security parameters, such as the appropriate RADIUS server and encryption settings must also be configured as per your requirements. Once the configuration is completed, click on the Apply button (see Figure 12).

*Figure 12 WLAN Configuration*



WLANs > Edit

| | |
|---|---|
| WLAN ID | 1 |
| WLAN SSID | secure |

General Policies

| | |
|---|---|
| Radio Policy | All |
| Admin Status | ☑ Enabled |
| Session Timeout (secs) | 1800 |
| Quality of Service (QoS) | Silver (best effort) |
| WMM Policy | Disabled |
| 7920 Phone Support | □ Client CAC Limit □ AP CAC Limit |
| Broadcast SSID | ☑ Enabled |
| Allow AAA Override | □ Enabled |
| External Policy Validation | □ Enabled |
| Client Exclusion | ☑ Enabled ** 60<br>Timeout Value (secs) |
| DHCP Server | □ Override |
| DHCP Addr. Assignment | □ Required |
| Interface Name | secure vlan 4 |

Security Policies

| | |
|---|---|
| IPv6 Enable | □ |
| Layer 2 Security | 802.1X<br>□ MAC Filtering |
| Layer 3 Security | None<br>□ 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)

Radius Servers

| | Authentication Servers | Accounting Servers |
|---|---|---|
| Server 1 | IP:192.168.50.3, Port:1645 | none |
| Server 2 | none | none |
| Server 3 | none | none |

802.1X Parameters

| 802.11 Data Encryption | | Type | Key Size |
|---|---|---|---|
| | ● | WEP | 104 bits |

In the next step, add a wireless LAN for the "open" SSID, by clicking on the **New** button and completing the configuration form as appropriate.

## Setting the Controller Date and Time

Remember that when access points try to join WLCs, there is an exchange of signed X.509 certificates. These X.509 certificates have validity intervals with a start and end time (and date). The validity interval begins at the time the X.509 certificate is provisioned on the access point at the factory, so it is extremely important to keep the WLC date and time accurate and current. For further detail, refer to the explanation in Managing the WLC Date and Time (page 98) in the Controller Maintenance section of this document.

## Preparing the Network for Access Points

In this simple example, the access points will connect to VLAN 5 and the controller management interface is on VLAN 60. This means that our WLC controller discovery options are DHCP Option 43, DNS resolution of "CISCO-LWAPP-CONTROLLER.*localdomain*", or OTAP. Since this is the initial deployment, we'll rule out OTAP which requires at least one access point joined to the controller. DHCP Option 43 is configured under the appropriate DHCP scope. DNS is also configured in the locally significant name space. For our sample deployment, let's assume we're using DHCP Option 43.

Also recall that in our basic example, all routing is done on the Cisco 3750 Layer 3 switch and the default gateway for a VLAN is the VLAN interface on the switch. So we configure VLAN 5 on the Cisco 3750 as follows:

```
interface VLAN5
 description AP VLAN
 ip address 10.5.5.1 255.255.255.0
 ip helper-address 192.168.50.3
```

The "`ip helper-address`" command instructs the interface to relay DHCP requests to the DHCP server at address 192.168.50.3. A scope for the network 10.5.5.0/24 is created on the DHCP server, including Option 43 pointing to the WLC management interface (192.168.60.2). See Appendices C, D, and E for details on configuring vendor specific DHCP Options.

While the Cisco WLCs always connect to 802.1Q trunks, Cisco lightweight access points do not understand VLAN tagging and should be connected only to the access ports on the neighbor switch. Here's an example switchport configuration from the Cisco 3750:

```
interface GigabitEthernet1/0/22
 description Access Port Connection to Cisco Lightweight AP
 switchport access vlan 5
 switchport mode access
 no shutdown
```

The infrastructure is now ready for us to connect the access points.

## Connecting the Access Points to the Network

In our sample deployment, the Cisco 3750 switch supports both 802.3af and Cisco inline power, so we will use PoE. We still need to make sure the switch can supply enough power for all of our access points and make sure that we don't exceed the maximum power output capabilities of the switch. Consult the Cisco Aironet Power Over Ethernet Application Note for more details. You can see the inline power statistics including available power on a Cisco switch using the 'show power inline all' IOS CLI command.

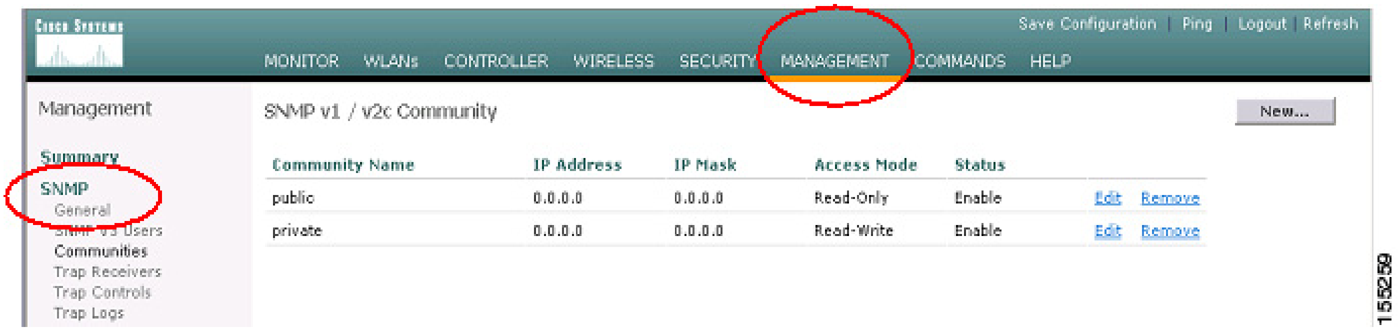
## Managing the Controller with WCS

WCS is management software that is used to manage one or more WLC devices and all of the access points joined to the WLCs. WCS also provides advanced management tools like wireless coverage display and location-based services. WCS uses SNMP to manage WLC devices, so the WLC devices need to have SNMP configured correctly.

The WCS can run on the Windows 2000 Server, Windows 2003 Server or RedHat Enterprise 3.0 ES Linux platform. Installing the operating system and WCS is beyond the scope of this document. Consult the appropriate product documentation for greater details. For this example, it is assumed WCS is already installed and running.

In the example, SNMPv2 is used. SNMPv2 is configured through the WLC web interface by navigating to **Management | SNMP | Communities**. The WLC defaults are read-only community "public" and read-write community "private" (see Figure 13). As a management and security best practice, the default SNMP communities should always be changed. However, to keep this example simple, the default values are used.

***Figure 13 SNMP Community Configuration***



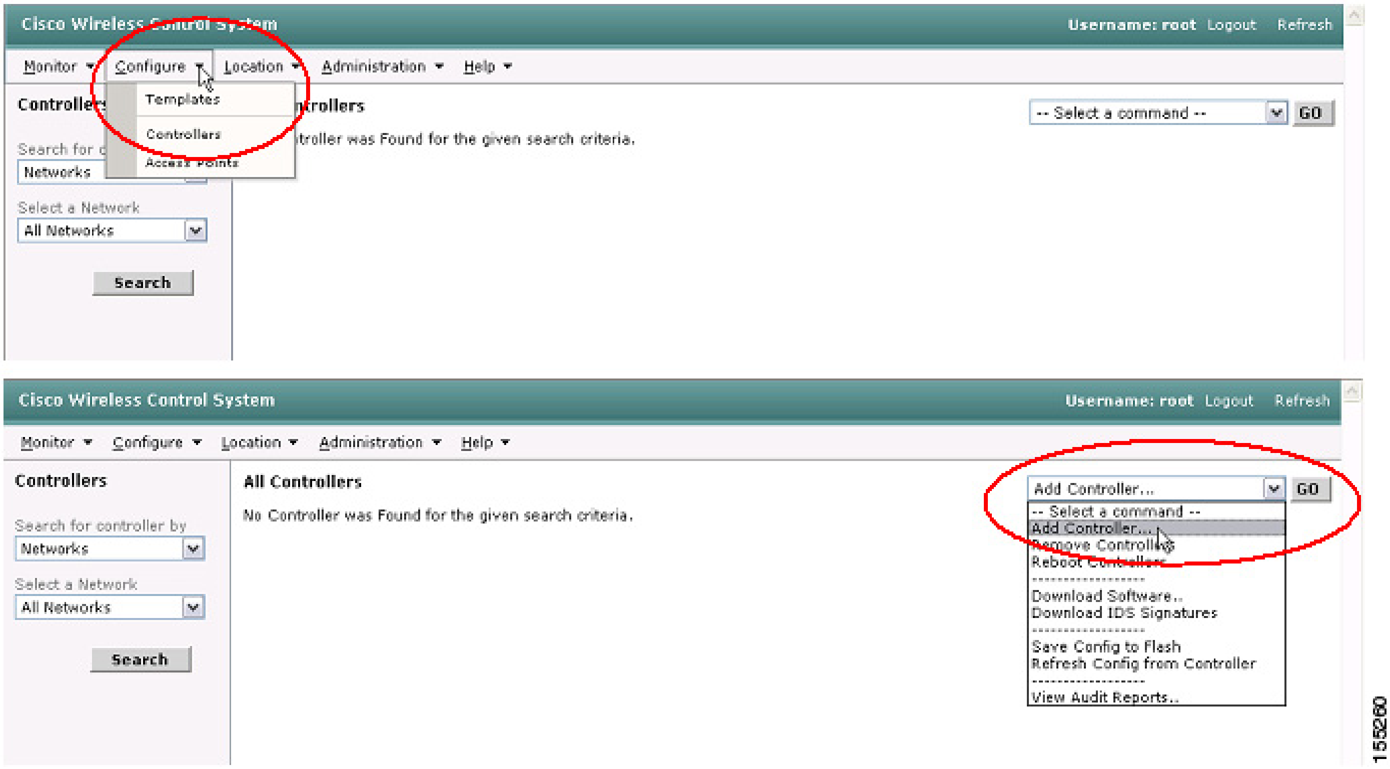
SNMP v1 / v2c Community

| Community Name | IP Address | IP Mask | Access Mode | Status | | |
|---|---|---|---|---|---|---|
| public | 0.0.0.0 | 0.0.0.0 | Read-Only | Enable | Edit | Remove |
| private | 0.0.0.0 | 0.0.0.0 | Read-Write | Enable | Edit | Remove |

You should take a few moments and configure the SNMP General parameters in the **Management | General interface** as a management best practice.

Access the WCS web-interface using the URL:https://WCS_IP_Address. WLCs are added to WCS by navigating to the Configure | Controllers interface. Select "Add Controller" from the drop-down box on the right-hand side, then click Go (see Figure 14).

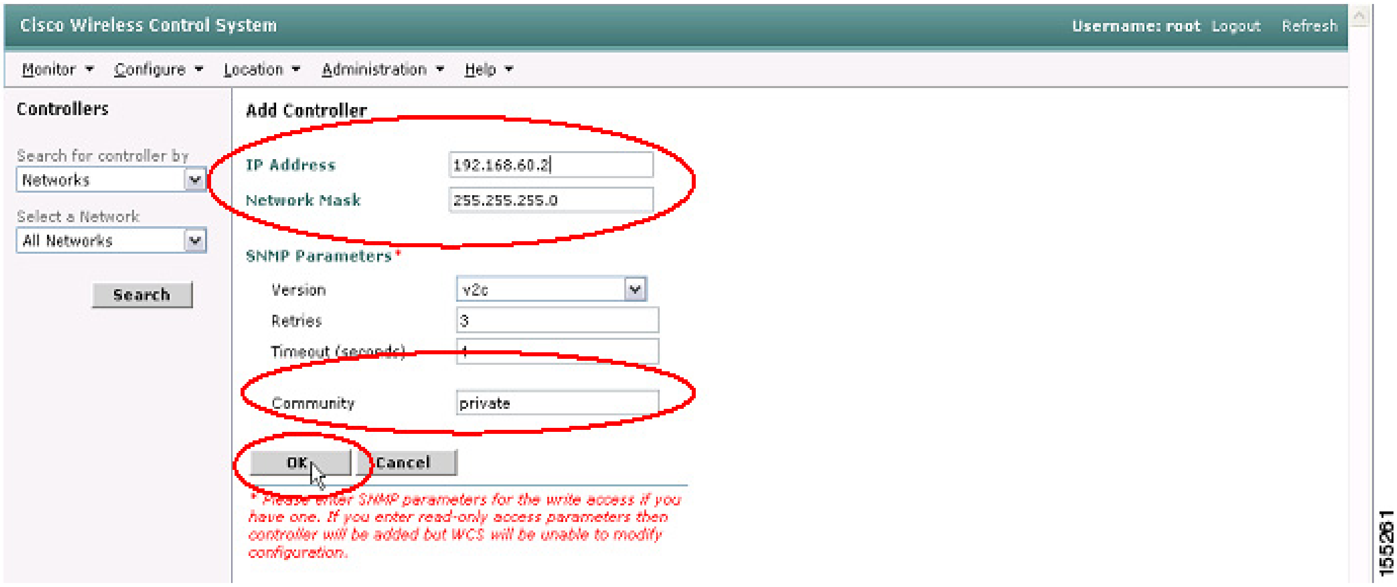
***Figure 14 Adding a Controller to WCS***



No Controller was Found for the given search criteria.

Enter the IP address of the WLC Management interface and configure the appropriate SNMP parameters, then click OK (see Figure 15). The WCS should "discover" the WLC. If the WCS cannot find the WLC, verify the IP reach-ability from the WCS to the WLC and the SNMP community configuration.

*Figure 15 Adding a Controller to WCS*



Search for controller by: Networks

Select a Network: All Networks

IP Address: 192.168.60.2

Network Mask: 255.255.255.0

SNMP Parameters*

Version: v2c

Retries: 3

Timeout (seconds): 4

Community: private

* Please enter SNMP parameters for the write access if you have one. If you enter read-only access parameters then controller will be added but WCS will be unable to modify configuration.

The WCS machine must be configured as an SNMP trap receiver to have full management functionality through the WCS. When you add the WLC to WCS, WCS should provision the WLC to use the WCS machine as an SNMP trap receiver.

# Advanced Deployment Concepts

Advanced deployment concepts are outlined below:

- Mobility
- Mobility Groups
- Radio Management and RF Domains
- Redundancy and Access Point Load Balancing
- Scaling WLCs to support more than 48 Access Points
- IP Addressing Considerations
- Access Point Groups and Site Specific VLANs
- Wireless LAN Override

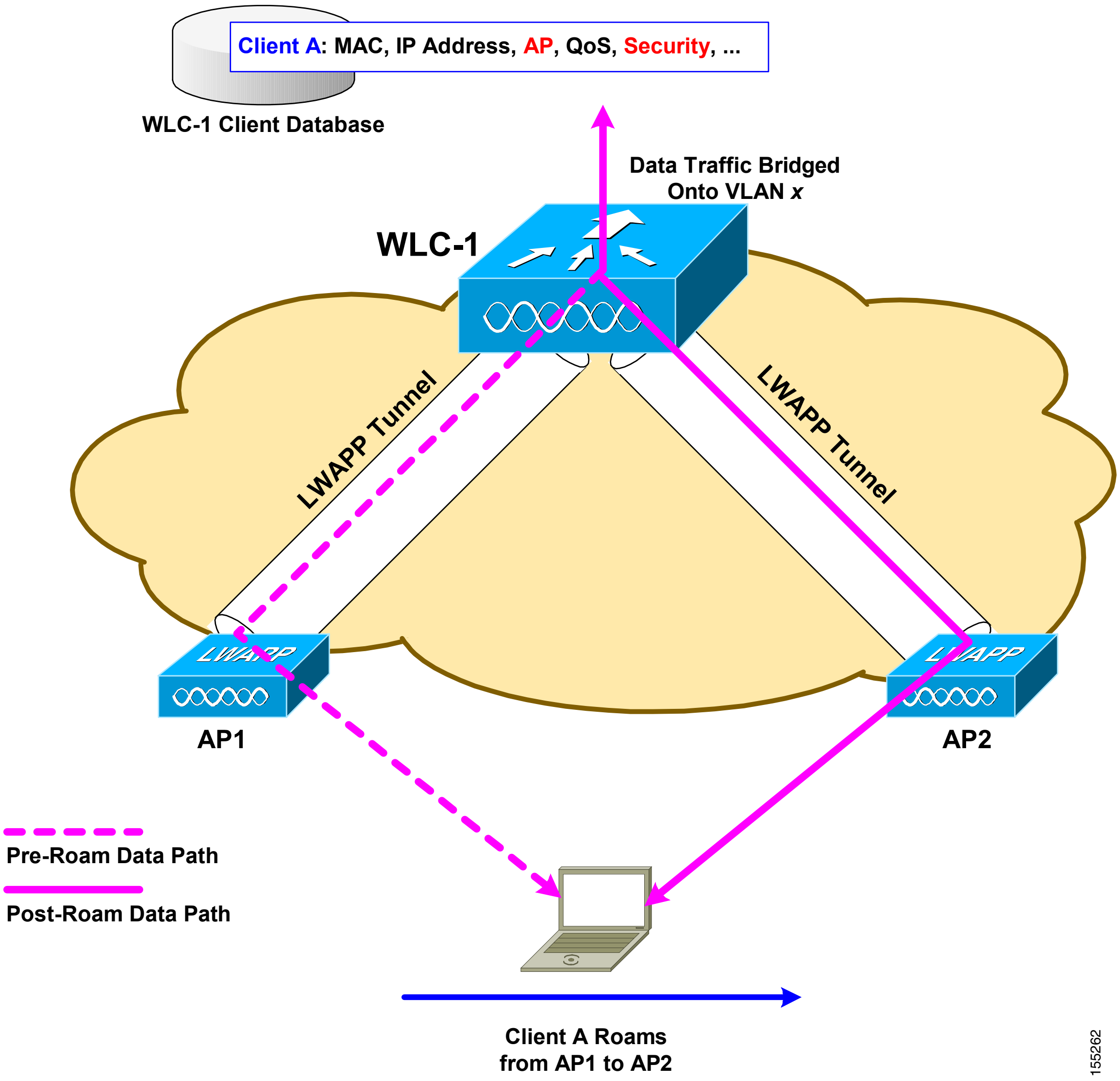
These concepts are critical to scaling the solution and taking advantage of the architecture's important and complete functionality.

## Mobility

One can argue that the greater benefit derived from wireless networks is mobility, but mobility introduces challenges in a network implementation. A wireless LAN client must be able to maintain its association seamlessly from one access point to another securely and with as little latency as possible. These mobility requirements are completely supported by the Cisco Unified Wireless Network architecture. This section covers the basic operational theory to keep the deployment guide simple and easy to understand. For further information, please refer to the product documentation for a complete overview of the solution.

When a wireless client associates and authenticates to an access point, the access point's joined WLC places an entry for that client in its client database. This entry includes the client's MAC and IP addresses, security context and associations, and QoS context, wireless LAN and associated access point. The WLC uses this information to forward frames and manage traffic to and from the wireless client. Now, let's look at what happens when the wireless client roams from one access point to another when both access points are joined to the same WLC. This is illustrated in Figure 16:

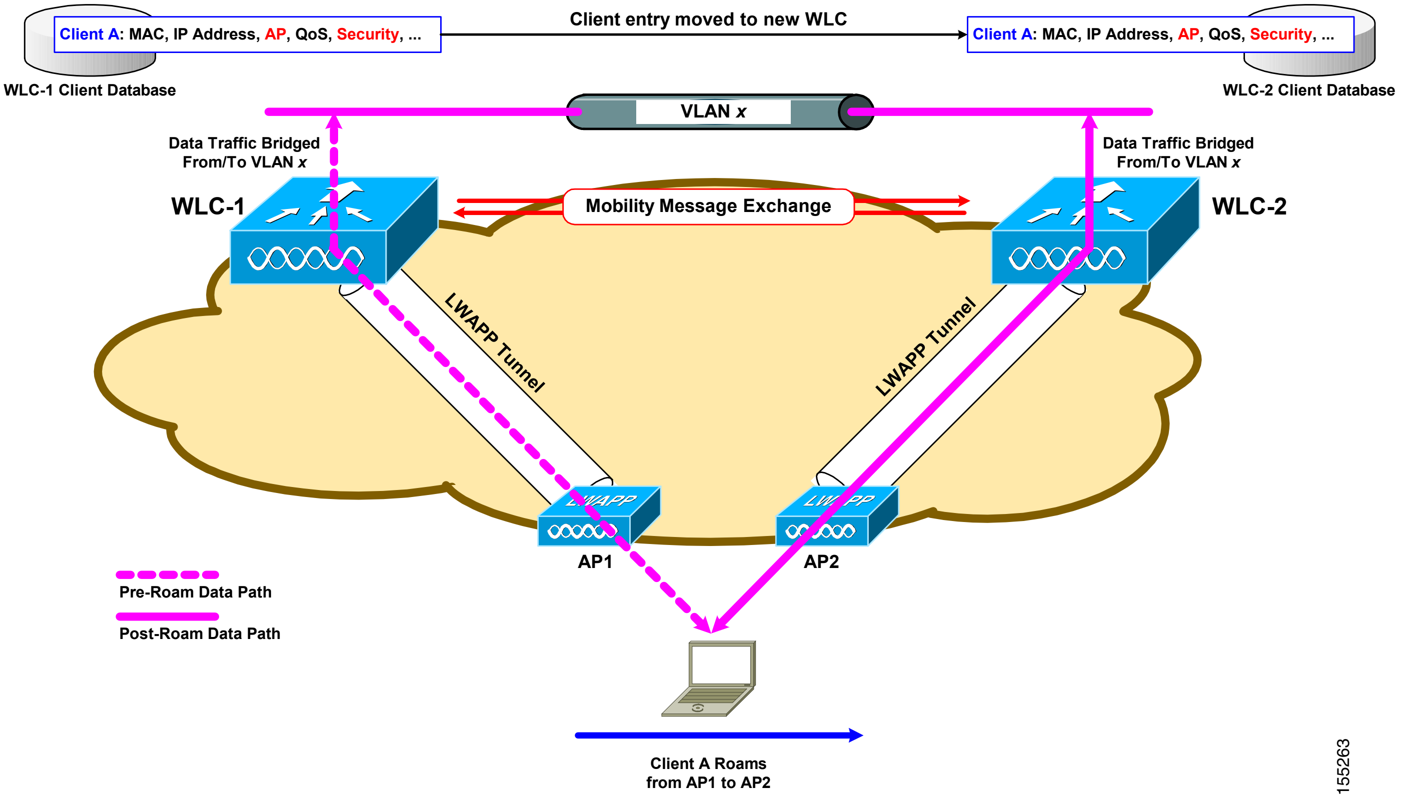
*Figure 16 OL-10043-02-Controller Roaming*


Client A: MAC, IP Address, AP, QoS, Security, ...
WLC-1 Client Database
Data Traffic Bridged Onto VLAN *x*
WLC-1
LWAPP Tunnel
LWAPP Tunnel
LWAPP
LWAPP
AP1
AP2
Pre-Roam Data Path
Post-Roam Data Path
Client A Roams from AP1 to AP2
155262

When the wireless client moves its association from one access point to another, the WLC simply updates the client database with the new associated access point. If necessary, new security context and associations are established as well.[1] Now let's consider what happens when a client roams from an access point joined to one WLC and an access point joined to a different WLC. Figure 17 illustrates an inter-controller roam in the event of a "Layer 2" roam:

[1] Wireless LAN clients are always re-authenticated by the system in some way on a roam. This is always necessary to protect against client spoofing. When wireless clients support Pair-wise Master Key (PMK) caching as defined in the 802.11i and WPAv2 specifications, Cisco wireless LAN controllers support full, secure roaming and re-keying without re-authenticating the client with the AAA server in the back-end. This is true for both Layer 2 and Layer 3 intra- and inter-controller roaming. This feature is called Proactive Key Caching (PKC). While no special client-side software is required to support roaming, PKC requires client-side supplicant support. Please refer to the appropriate documentation for a detailed explanation of PKC.

*Figure 17 Layer 2 Inter-Controller Roaming*

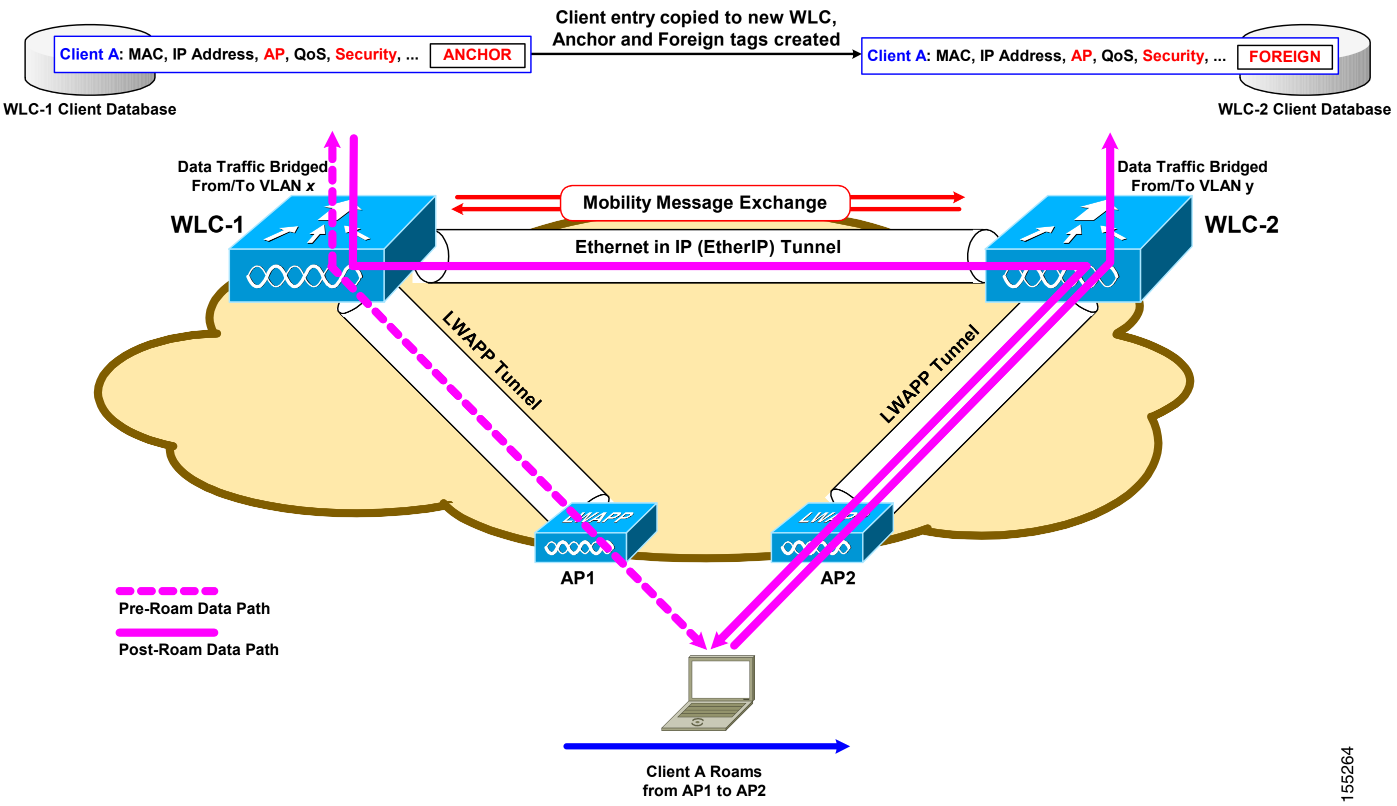

Client A: MAC, IP Address, AP, QoS, Security, ...
Client entry moved to new WLC
Client A: MAC, IP Address, AP, QoS, Security, ...
WLC-1 Client Database
WLC-2 Client Database
VLAN x
Data Traffic Bridged From/To VLAN x
Data Traffic Bridged From/To VLAN x
WLC-1
Mobility Message Exchange
WLC-2
LWAPP Tunnel
LWAPP Tunnel
LWAPP
LWAPP
AP1
AP2
Pre-Roam Data Path
Post-Roam Data Path
Client A Roams from AP1 to AP2
155263

As you can see from Figure 17, a Layer 2 roam occurs when the controller wireless LAN interfaces are on the same IP subnet. When the client re-associates to an access point connected to a new WLC, the new WLC exchanges mobility messages with the original WLC and the client database entry is moved to the new WLC. New security context and associations are established if necessary and the client database entry is updated for the new access point. All of this is transparent to the end-user.

As you can see from Figure 18, a Layer 3 roam occurs when the wireless LAN interfaces configured on the different controllers are on different IP subnets. The inter-controller roaming is similar to Layer 2 roaming in that the WLCs exchange mobility messages on the client roam. However, instead of moving the client's entry to the new controller's client database, the original wireless LAN controller marks the client with an "Anchor" entry in its own client database. The database entry is copied to the new controller client database and marked with a "Foreign" entry in the new WLC. The roam is still transparent to the wireless client and the wireless client maintains its original IP address. Security credentials and context are established if necessary.

Figure 18 illustrates an inter-controller roam in the event of a "Layer 3" roam:

*Figure 18 Layer 3 Inter-Controller Roaming*


Client entry copied to new WLC,
Anchor and Foreign tags created
Client A: MAC, IP Address, AP, QoS, Security, ...
ANCHOR
WLC-1 Client Database
Client A: MAC, IP Address, AP, QoS, Security, ...
FOREIGN
WLC-2 Client Database
Data Traffic Bridged From/To VLAN x
Data Traffic Bridged From/To VLAN y
WLC-1
WLC-2
Mobility Message Exchange
Ethernet in IP (EtherIP) Tunnel
LWAPP Tunnel
LWAPP Tunnel
LWAPP
LWAPP
AP1
AP2
Pre-Roam Data Path
Post-Roam Data Path
Client A Roams from AP1 to AP2
155264

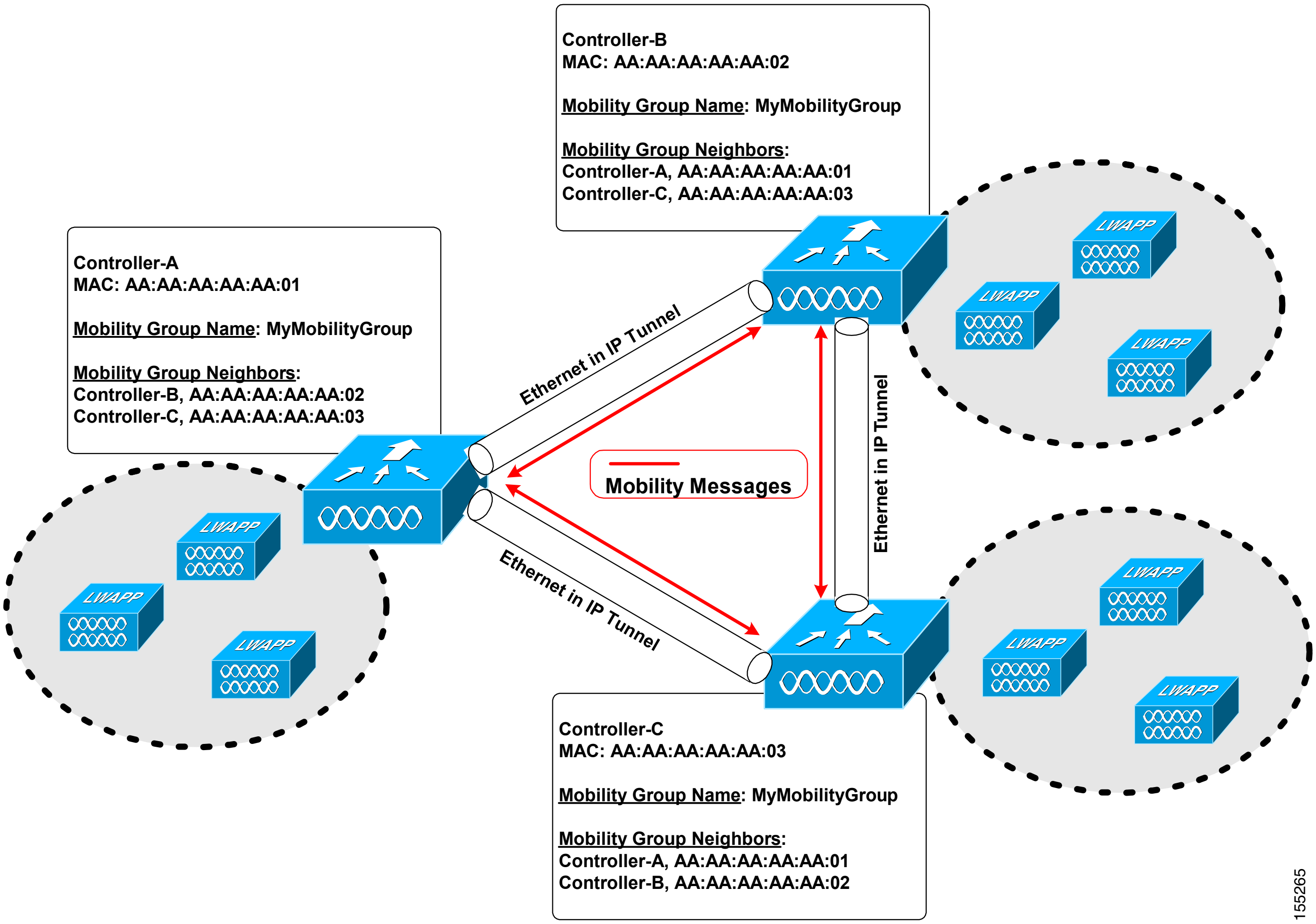
As you can see from Figure 18, after a Layer 3, roam data to and from the wireless client flows in an asymmetric traffic path. Traffic from the client to the network is forwarded directly into the network by the foreign WLC. Traffic to the client arrives at the Anchor WLC, which forwards the traffic to the Foreign WLC in an Ethernet in IP (EtherIP) tunnel. The Foreign WLC then forwards the data to the client. EtherIP is defined by IETF RFC 3378.

If a wireless client roams to a new Foreign WLC, the client database entry is moved from the original Foreign WLC to the new Foreign WLC, but the original Anchor WLC is always maintained.

## Mobility Groups

A set of WLC devices can be configured as a Mobility Group. A Mobility Group allows you to deploy multiple WLC devices in a network and have the devices dynamically share important information between them and also to forward data traffic when inter-controller roaming occurs. The important information shared includes client device's context and state, and WLC loading information. With this information, the network can support inter-controller wireless LAN device roaming, access point load balancing, and controller redundancy. Figure 19 illustrates the mobility group concept:

*Figure 19 Mobility Group*


Controller-B
MAC: AA:AA:AA:AA:AA:02
Mobility Group Name: MyMobilityGroup
Mobility Group Neighbors:
Controller-A, AA:AA:AA:AA:AA:01
Controller-C, AA:AA:AA:AA:AA:03
Controller-A
MAC: AA:AA:AA:AA:AA:01
Mobility Group Name: MyMobilityGroup
Mobility Group Neighbors:
Controller-B, AA:AA:AA:AA:AA:02
Controller-C, AA:AA:AA:AA:AA:03
Ethernet in IP Tunnel
Mobility Messages
Ethernet in IP Tunnel
Ethernet in IP Tunnel
LWAPP
Controller-C
MAC: AA:AA:AA:AA:AA:03
Mobility Group Name: MyMobilityGroup
Mobility Group Neighbors:
Controller-A, AA:AA:AA:AA:AA:01
Controller-B, AA:AA:AA:AA:AA:02
155265

As you can see from Figure 19, each WLC in the Mobility Group is configured with a list of the other members of the Mobility Group. Each WLC device builds a neighbor relationship with every other member of the group. When client data is forwarded between members of a Mobility Group to support Layer 3 roaming, the packets are carried over an Ethernet in IP (EtherIP) tunnel. There is an option to configure IPSec encryption for the inter-controller mobility messages.

A Mobility Group can include up to 24 WLC devices of any flavor. The number of access points supported in a Mobility Group will be bounded by the number of controllers and controller types in the mobility group. For example, a Mobility Group made up of twenty-four 4404-100 WLC devices will support up to 2400 access points since a 4404-100 supports up to 100 access points per WLC (24 * 100 = 2400 access points). A Mobility Group made up of 12 4402-25 and 12 4402-50 WLC devices will support up to 900 access points since the 4402-25 supports up to 25 access points and the 4402-50 supports up to 50 access points (12 * 25 + 12 * 50 = 300 + 600 = 900 access points) and so on. A WiSM controller module counts as two controllers in a Mobility Group, so a maximum of 12 WiSM modules can be supported in a single Mobility Group.

Typically, WLCs should be placed in the same Mobility Group when an inter-controller roam is possible. If there is not the possibility of a roaming event, then it may make sense to not put WLCs in the same Mobility Group. For example, suppose you have deployed two separate WLCs in two buildings, with each WLC managing the access points in its building. If the buildings are separated by a large parking area with no RF coverage, then a wireless LAN client is not going to roam from an access point in one building to an access point in the other building. So, the WLCs don't necessarily need to be members of the same Mobility Group.

Redundant WLCs should be in the same Mobility Group. When access points join a WLC, it learns the IP addresses of the other WLCs in the Mobility Group from its joined WLC. These addresses are remembered and used the next time the access point does an LWAPP discovery. More details on redundancy are covered in the redundancy section.

## Mobility Group Requirements

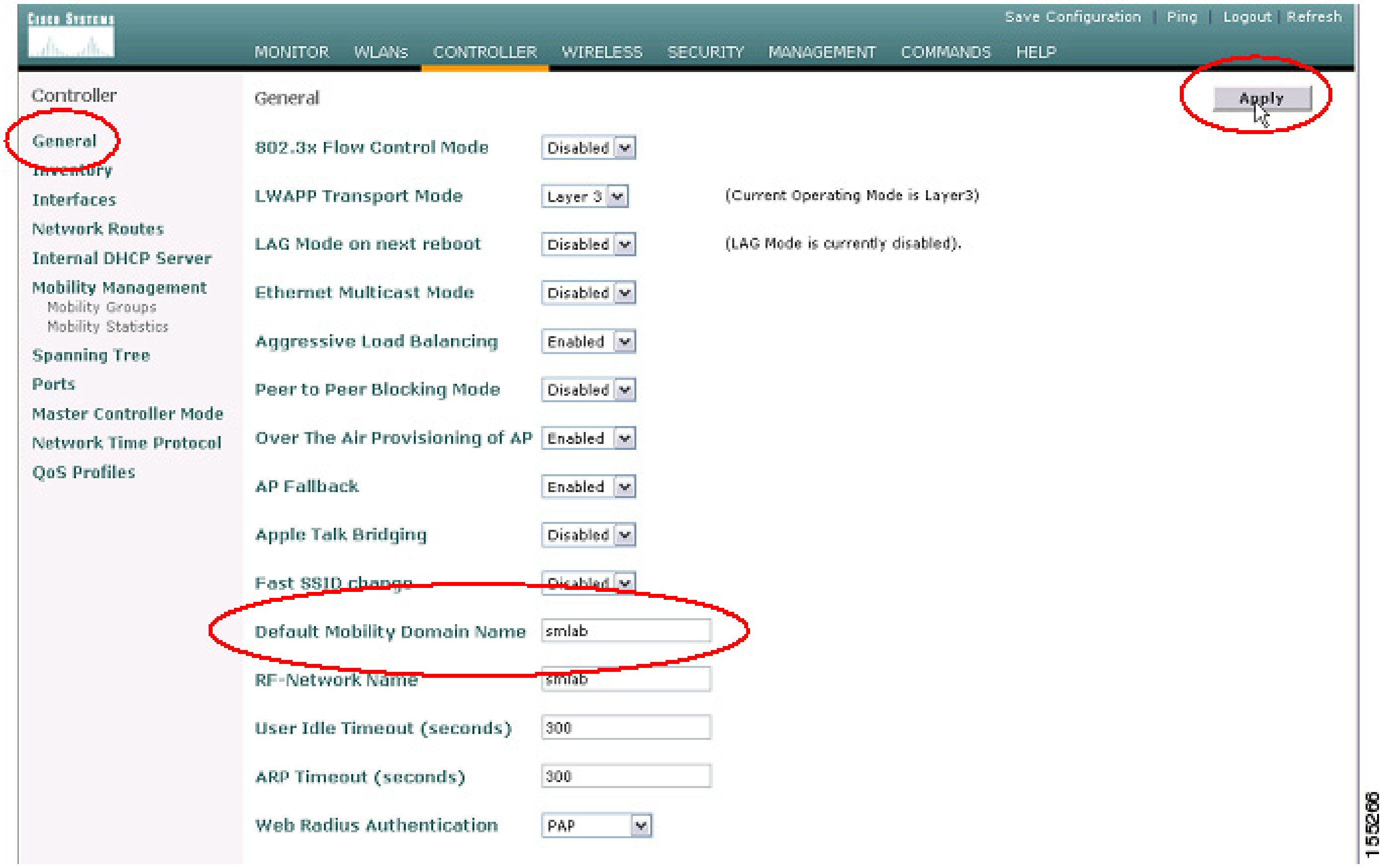
The basic requirements for WLC devices to exist in a Mobility Group are:

- IP connectivity between the management interfaces of all WLC devices
- All WLC devices must be configured with the SAME MOBILIY GROUP NAME. The mobility group name IS case-sensitive.
- All WLC devices must be configured to use the SAME VIRTUAL INTERFACE IP ADDRESS
- Each WLC device is configured with the MAC address and IP address of all the other Mobility Group members

We will now look at how Mobility Groups are configured first through the WLC interface and then using WCS. WCS is the recommended option.

The first requirement is to verify that all the WLCs you plan to add into the Mobility Group meet the above-mentioned requirements. You should verify IP connectivity between the WLCs. Typically, you can do this by pinging the WLCs. Care should be taken to verify that each WLC in the Mobility Group has the same Virtual Interface IP address. if necessary, change the Mobility Group Name parameter. Normally, you set the Mobility Group Name at deployment time in the WLC setup script. But if you need to change the mobility group, the best way is to change the **Default Mobility Domain Name** field in the **Controller | General interface.** This is shown in Figure 20. Remember that the Mobility Group Name must be the same on every controller in the Mobility Group. To gather the MAC address and IP address parameters for the other WLC devices in the Mobility Group, you can look at the **Controller | Mobility Groups** interface on the other WLC devices you plan on adding to the Mobility Group.

*Figure 20 Mobility Group Name Configuration*



General

802.3x Flow Control Mode: Disabled

LWAPP Transport Mode: Layer 3 (Current Operating Mode is Layer3)

LAG Mode on next reboot: Disabled (LAG Mode is currently disabled).

Ethernet Multicast Mode: Disabled

Aggressive Load Balancing: Enabled

Peer to Peer Blocking Mode: Disabled

Over The Air Provisioning of AP: Enabled

AP Fallback: Enabled

Apple Talk Bridging: Disabled

Fast SSID change: Disabled

Default Mobility Domain Name: smlab

RF-Network Name: smlab

User Idle Timeout (seconds): 300

ARP Timeout (seconds): 300

Web Radius Authentication: PAP

## Configuring a Mobility Group Using the WLC Interface

Use the following steps to add the Mobility Group members using the WLC:

**Step 1** Navigate to Controller | Mobility Management | Mobility Groups. (See Figure 21 below.)

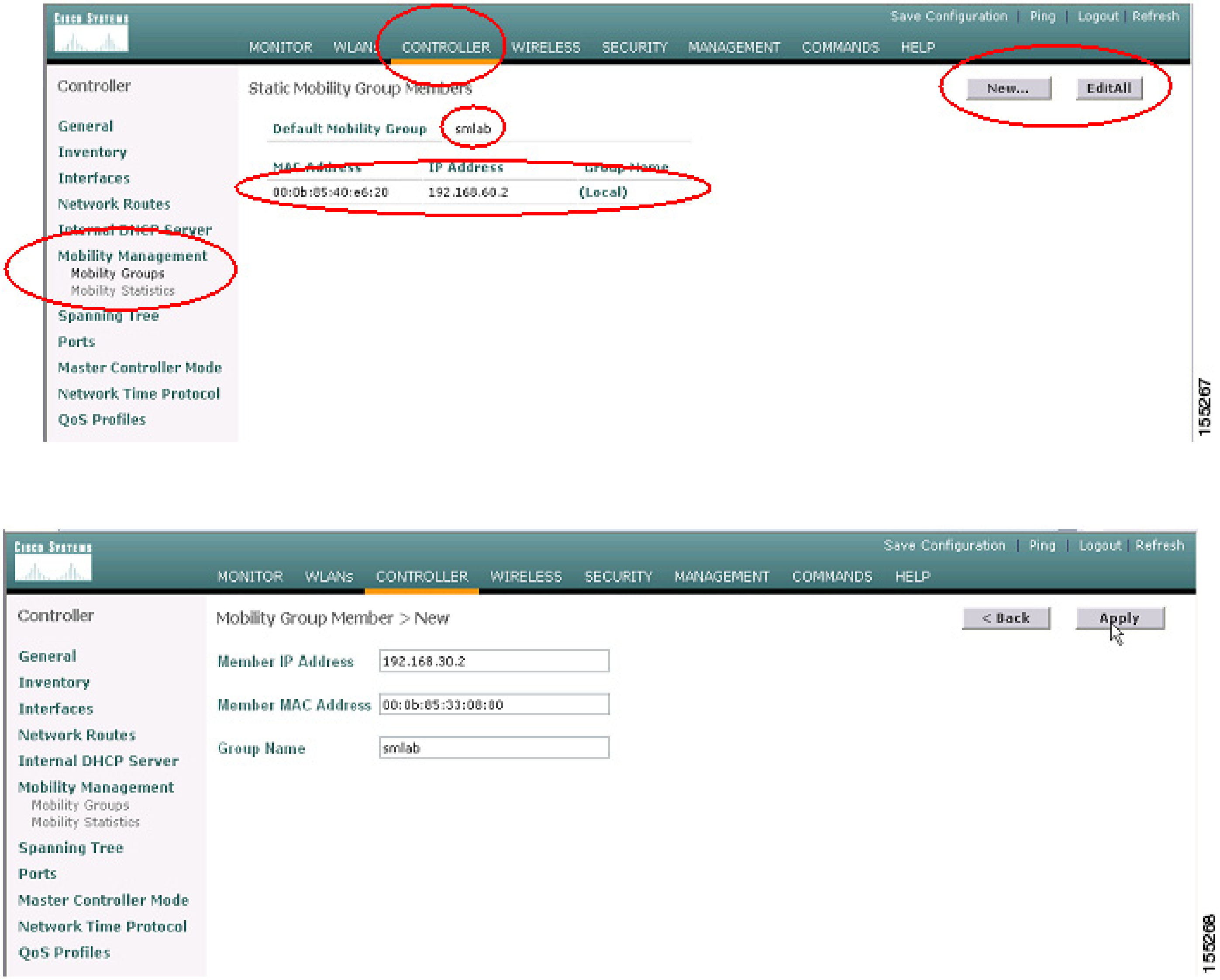
**Step 2** In Figure 21 you will see the Mobility Group name in the Default Mobility Group field. You will also see all of the members of the Mobility Group that have already been added. Remember, though, that each WLC member of a Mobility Group must have the same Mobility Group name configured. You will also see the WLC MAC address and IP address listed.

**Step 3** Click on the New button (see Figure 21) to access the add Mobility Group Member screen, shown in Figure 22.

**Step 4** Add the Management Interface of each neighbor WLC into **Member IP Address** field. Add the **Member MAC Address** of the neighbor WLC and the **Group Name**. This Group Name parameter should be the Mobility Group Name. You must add all the WLCs in the Mobility Group. Note that you can also bulk add members by selecting the **Edit All** button in the **Controller | Mobility Management | Mobility Groups** interface (Figure 21). This interface is shownin Figure 23.

**Step 5** Repeat Steps **1** through **4** for each WLC device in the mobility group.

*Figure 21 Mobility Group Configuration*



Static Mobility Group Members

Default Mobility Group smlab

| MAC Address | IP Address | Group Name |
|---|---|---|
| 00:0b:85:40:e6:20 | 192.168.60.2 | (Local) |

Mobility Group Member > New

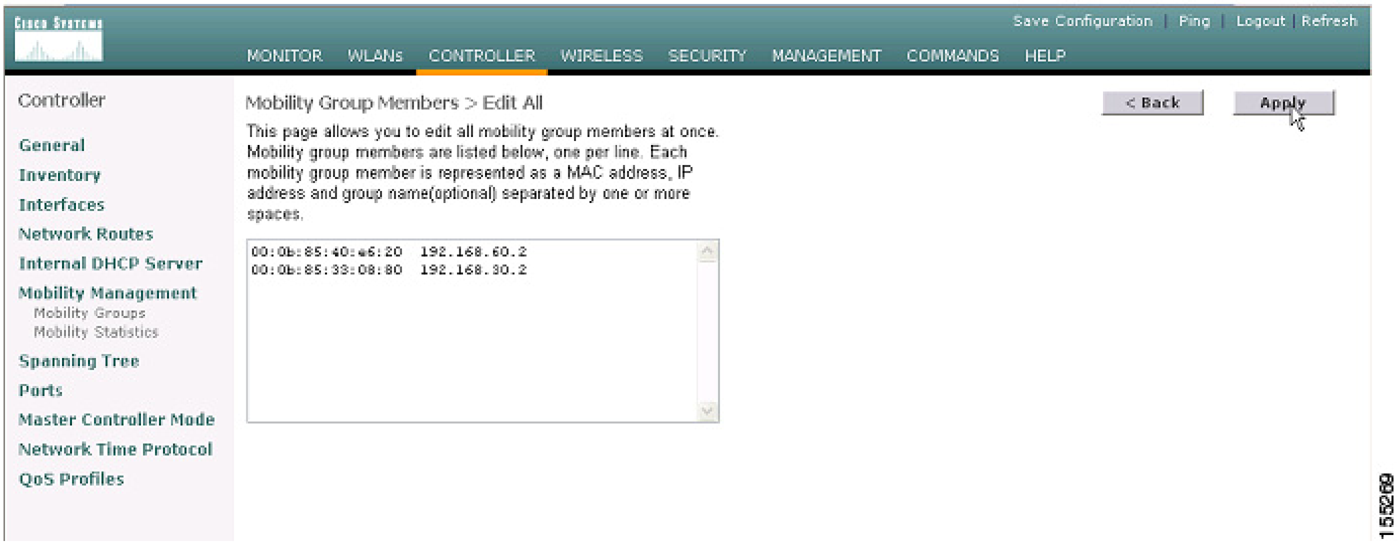
Member IP Address 192.168.30.2

Member MAC Address 00:0b:85:33:08:80

Group Name smlab

*Figure 22 Add Mobility Group Member*

*Figure 23 Mobility Group EditAll*



Mobility Group Members > Edit All

This page allows you to edit all mobility group members at once. Mobility group members are listed below, one per line. Each mobility group member is represented as a MAC address, IP address and group name(optional) separated by one or more spaces.

```
00:0b:85:40:e6:20  192.168.60.2
00:0b:85:33:08:80  192.168.30.2
```

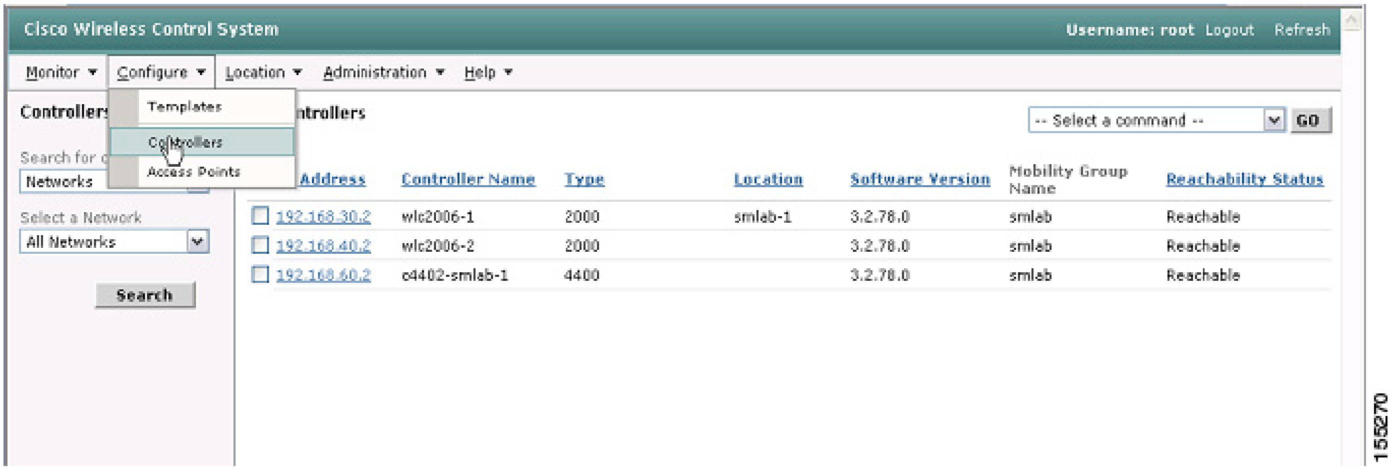
## Configuring a Mobility Group Using WCS

The steps for configuring the mobility group through WCS are as follows:

**Step 1** Add each WLC controller in the Mobility Group to WCS.

**Step 2** Navigate through the WCS interface to Configure | Controllers. You should see a list of all the controllers you added in Step **1**. (See Figure 24.)

*Figure 24 Mobility Group Configuration in WCS*

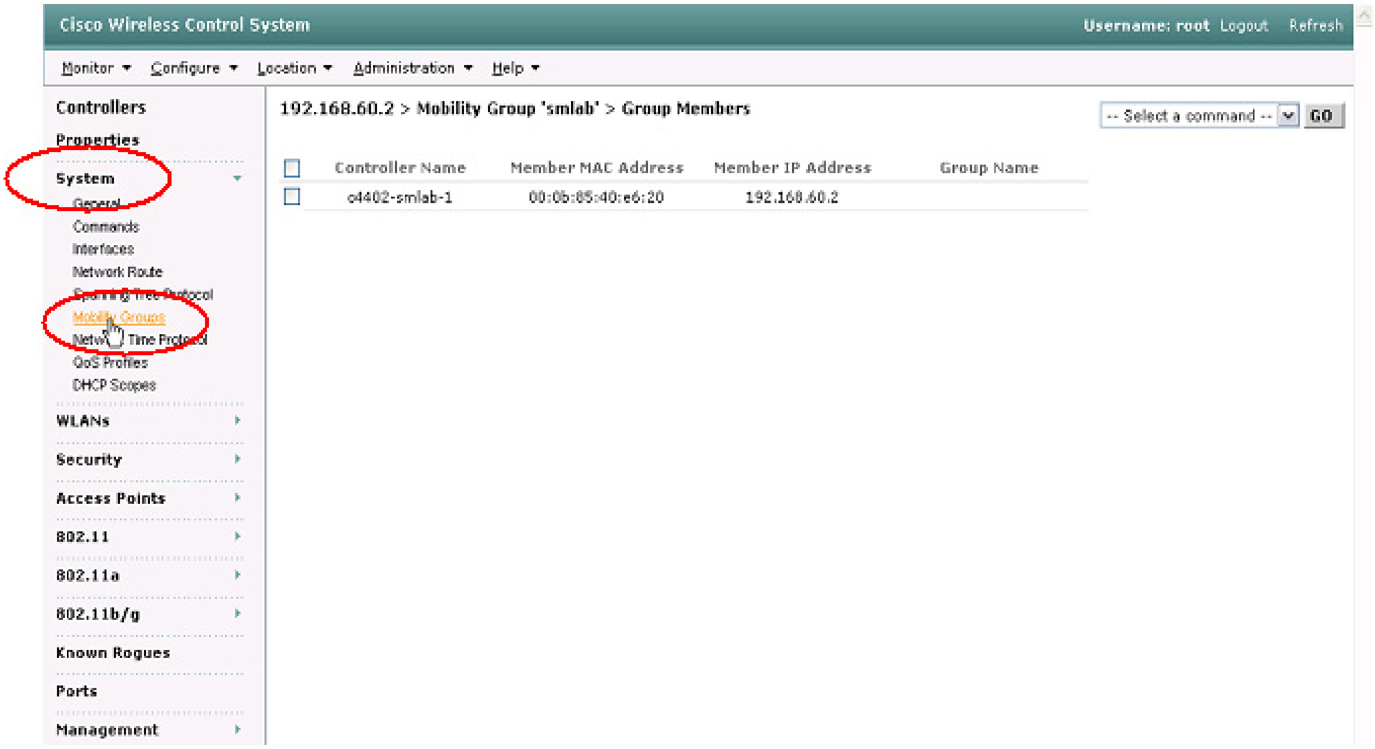


| | IP Address | Controller Name | Type | Location | Software Version | Mobility Group Name | Reachability Status |
|---|---|---|---|---|---|---|---|
| □ | 192.168.30.2 | wlc2006-1 | 2000 | smlab-1 | 3.2.78.0 | smlab | Reachable |
| □ | 192.168.40.2 | wlc2006-2 | 2000 | | 3.2.78.0 | smlab | Reachable |
| □ | 192.168.60.2 | c4402-smlab-1 | 4400 | | 3.2.78.0 | smlab | Reachable |

**Step 3** Select the first controller by clicking on the WLC IP address. This should access the controller templates interface for the controller you are managing.

**Step 4** Select **System | Mobility Groups** on the left-hand side. You should see the existing Mobility Group members listed in the page that's loaded. (See Figure 25.)

*Figure 25 Mobility Group Configuration in WCS*

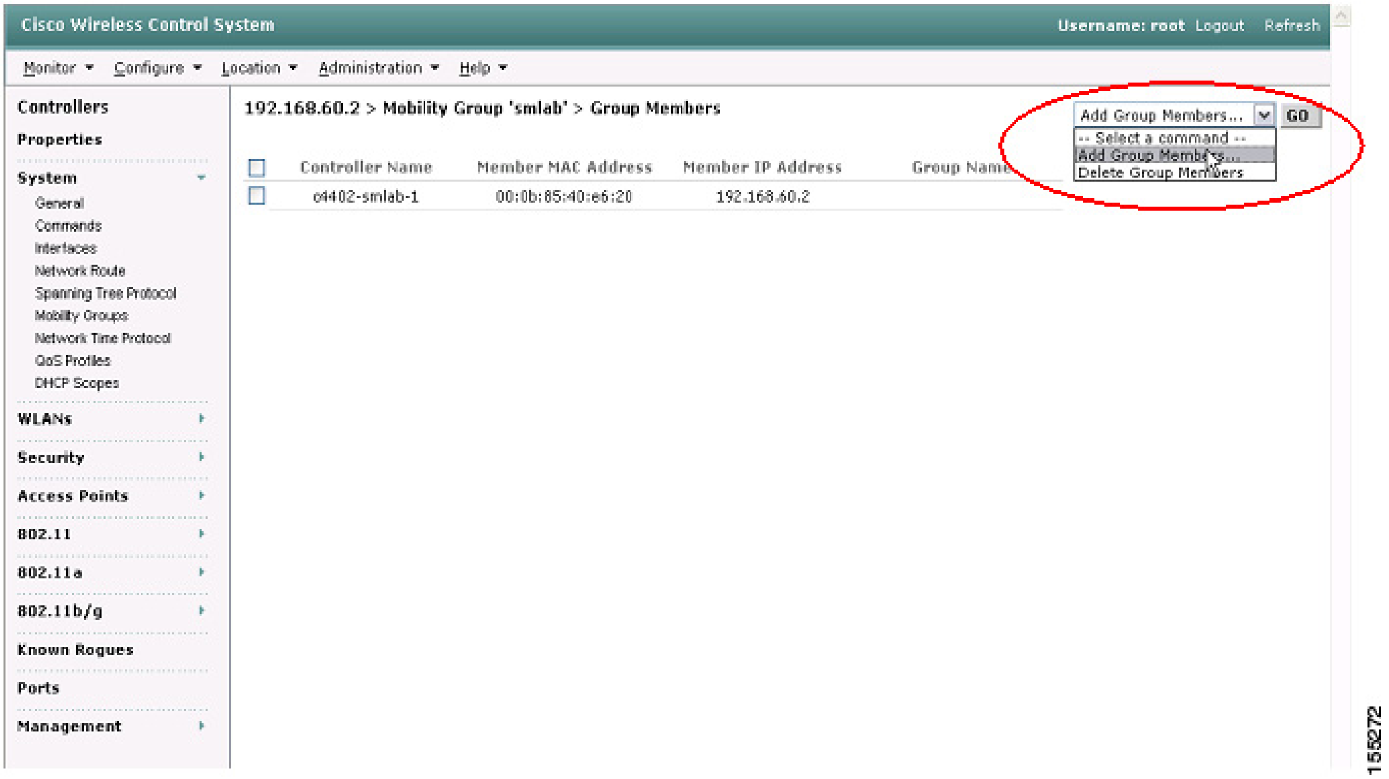


192.168.60.2 > Mobility Group 'smlab' > Group Members

| □ | Controller Name | Member MAC Address | Member IP Address | Group Name |
|---|---|---|---|---|
| □ | c4402-smlab-1 | 00:0b:85:40:e6:20 | 192.168.60.2 | |

**Step 5** In the drop-down box in the upper-right-hand corner, select **Add Group Members** and then click **Go** (see Figure 26).

*Figure 26 Mobility Group Configuration in WCS*

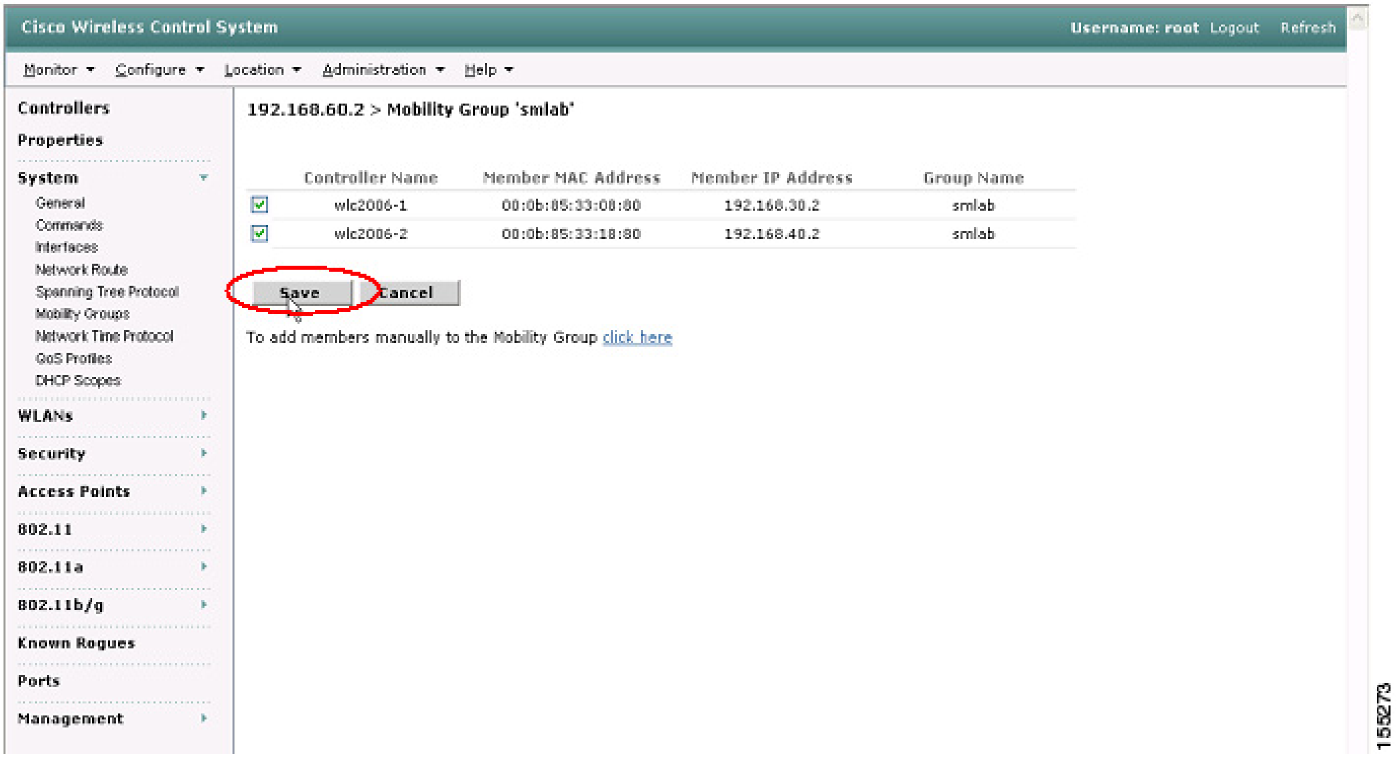


192.168.60.2 > Mobility Group 'smlab' > Group Members

| □ | Controller Name | Member MAC Address | Member IP Address | Group Name |
|---|---|---|---|---|
| □ | c4402-smlab-1 | 00:0b:85:40:e6:20 | 192.168.60.2 | |

**Step 6** You will see a list of available controllers. Select the desired WLCs and then click **Save** (see Figure 27).

*Figure 27 Mobility Group Configuration in WCS*



192.168.60.2 > Mobility Group 'smlab'

| | Controller Name | Member MAC Address | Member IP Address | Group Name |
|---|---|---|---|---|
| ☑ | wlc2006-1 | 00:0b:85:33:08:80 | 192.168.30.2 | smlab |
| ☑ | wlc2006-2 | 00:0b:85:33:18:80 | 192.168.40.2 | smlab |

To add members manually to the Mobility Group click here

**Step 7** Repeat Steps **2** through **6** for the remaining WLC devices in the same Mobility Group.

# Radio Management and RF Domains

An RF Domain, also known as an RF Group, is another critical deployment concept. An RF Domain is a cluster of WLC devices type that coordinate their dynamic radio resource management (RRM) calculations on a per 802.11 PHY type. An RF Domain exists for each 802.11 PHY type. Clustering WLCs into RF Domains allows the dynamic radio resource management (RRM) algorithms to scale beyond a single WLC and span building floors, buildings, and even campuses. An in depth discussion of RRM is beyond the scope of this document, but we offer an abbreviated explanation in the following paragraphs.

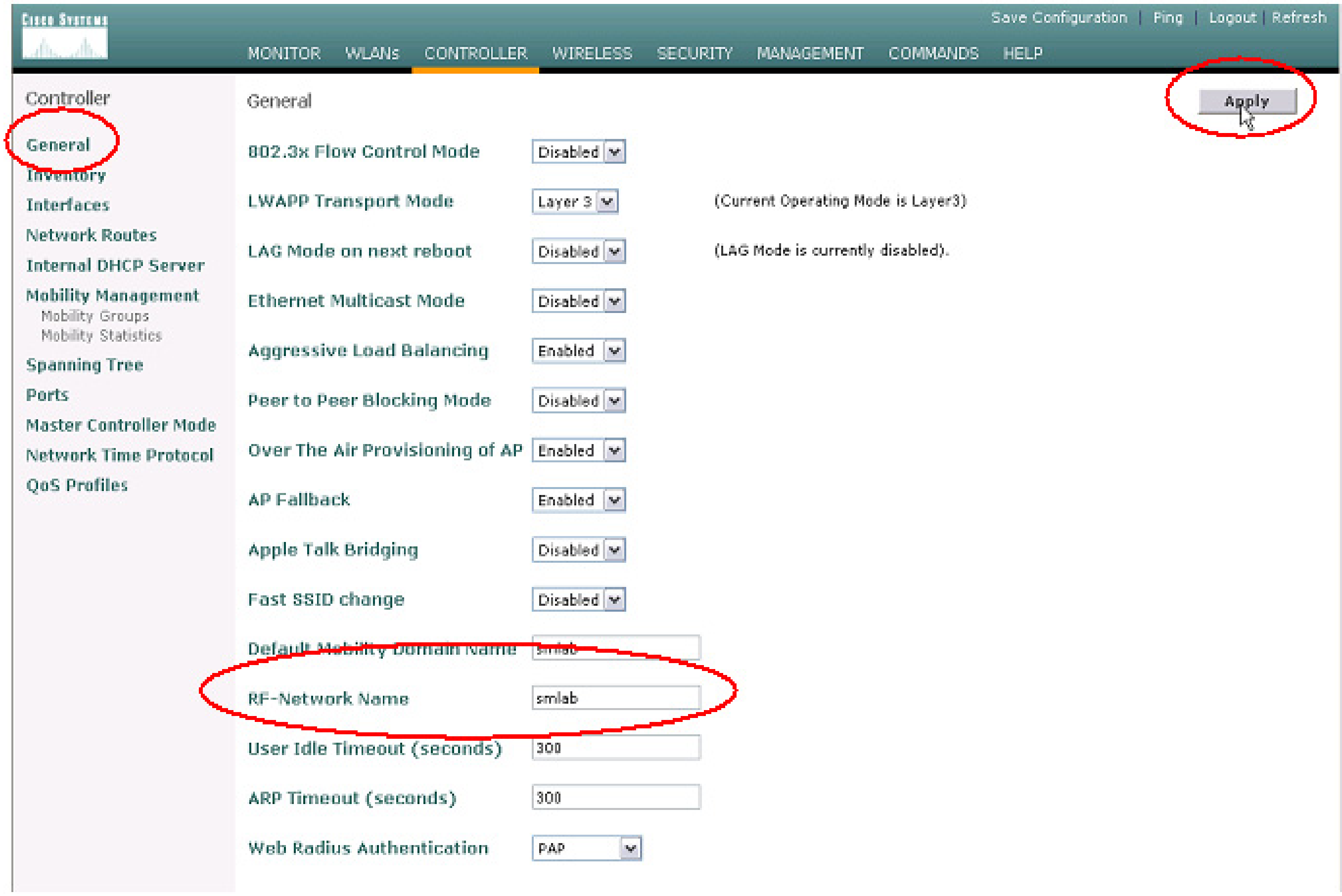
Lightweight access points periodically send out neighbor messages over the air that includes the WLC IP address and a hashed message integrity check (MIC) from the timestamp and BSSID of the access point. The hashing algorithm uses a shared secret that is configured on the WLC and pushed out to each access point. Access points sharing the same secret are able to validate messages from each other via the MIC. When access points on different WLCs hear validated neighbor messages at a signal strength of -80 dBm or stronger, the controllers dynamically form an RF Group.

The members of an RF Domain elect an RF Domain leader to maintain a "master" power and channel scheme for the RF Group. The RF Domain leader analyzes real-time radio data collected by the system and calculates the master power and channel plan. The RRM algorithms try to optimize around signal strength of -65 dBm between all access points and to avoid 802.11 co-channel interference and contention as well as non-802.11 interference. The RRM algorithms employ dampening calculations to minimize system-wide dynamic changes. The end result is dynamically calculated, near-optimal power and channel planning that is responsive to an always changing RF environment.

The RF Group leader and members exchange RRM messages at a specified updated interval which is 600 seconds by default. Between update intervals, the RF Group leader sends keepalive messages to each of the RF Group Members and collects real-time RF data.

A WLC is configured with an RF Domain Name parameter and this parameter is pushed down to all the access points joined to the WLC. The RF Domain Name is used by the access points as the shared secret for generating the hashed MIC in the neighbor messages. So to create an RF Domain, you simply configure all of the WLCs with the same RF Domain Name parameter. The RF Domain Name parameter is configured in **RF - Network Name** field under the **Controller | General interface**. Figure 28 shows this interface.

*Figure 28 Group Name Configuration*



General

| | | |
|---|---|---|
| 802.3x Flow Control Mode | Disabled | |
| LWAPP Transport Mode | Layer 3 | (Current Operating Mode is Layer3) |
| LAG Mode on next reboot | Disabled | (LAG Mode is currently disabled). |
| Ethernet Multicast Mode | Disabled | |
| Aggressive Load Balancing | Enabled | |
| Peer to Peer Blocking Mode | Disabled | |
| Over The Air Provisioning of AP | Enabled | |
| AP Fallback | Enabled | |
| Apple Talk Bridging | Disabled | |
| Fast SSID change | Disabled | |
| Default Mobility Domain Name | smlab | |
| RF-Network Name | smlab | |
| User Idle Timeout (seconds) | 300 | |
| ARP Timeout (seconds) | 300 | |
| Web Radius Authentication | PAP | |

The RF Domain and Mobility Group concepts are similar in that they both define clusters of WLCs, but they are different in terms of their purpose. These two concepts often get confused because the Mobility Group and RF Network Name parameters are configured to be the same in the WLC setup script[1]. Most of the time, all of the WLCs in an RF Domain will also be in the same Mobility Group, and vice-versa. However, the RF Domain concept facilitates scalable, system-wide dynamic RF management while the Mobility Group concept is designed to facilitate scalable, system-wide mobility and controller redundancy.

If there is any possibility that an access point joined to one WLC will hear RF transmissions from an access point joined to a different WLC, the WLC should be configured in the same RF Domain. If RF transmissions between access points can be heard, then system-wide RRM is recommended to avoid

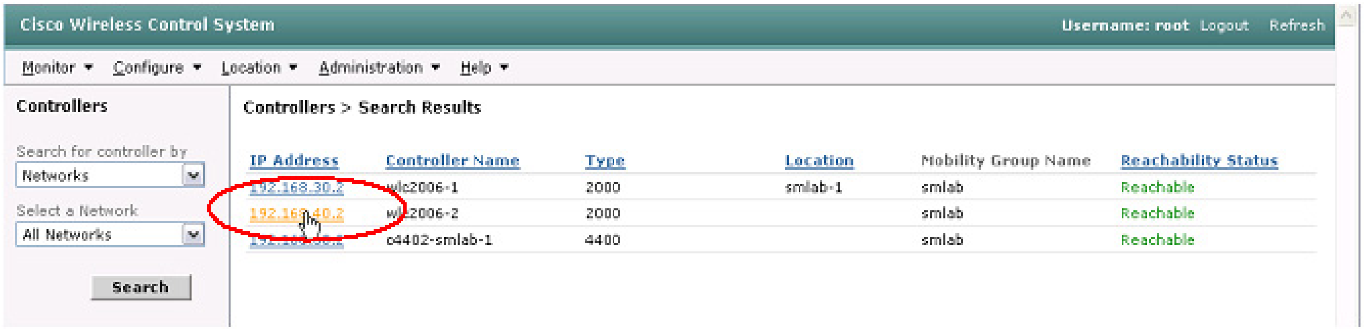
[1] In the WLC setup script, this is called the "RF Group Name".

802.11 interference and contention as much as possible. Furthermore, when an access point records neighbor messages that it cannot validate via the hashed MIC the transmitting access point is reported as a rogue device. So if WLCs are managing neighboring access points that can hear each other and the WLCs are not in the same RF Domain, spurious rogue access point reports will be generated; legitimate access points will be reported as rogues.

You can view the RF Domain status and information in WCS as follows:

**Step 1** Navigate to **Monitor | Devices | Controller**. Select a WLC (see Figure 29).

*Figure 29 WCS Find Controller*

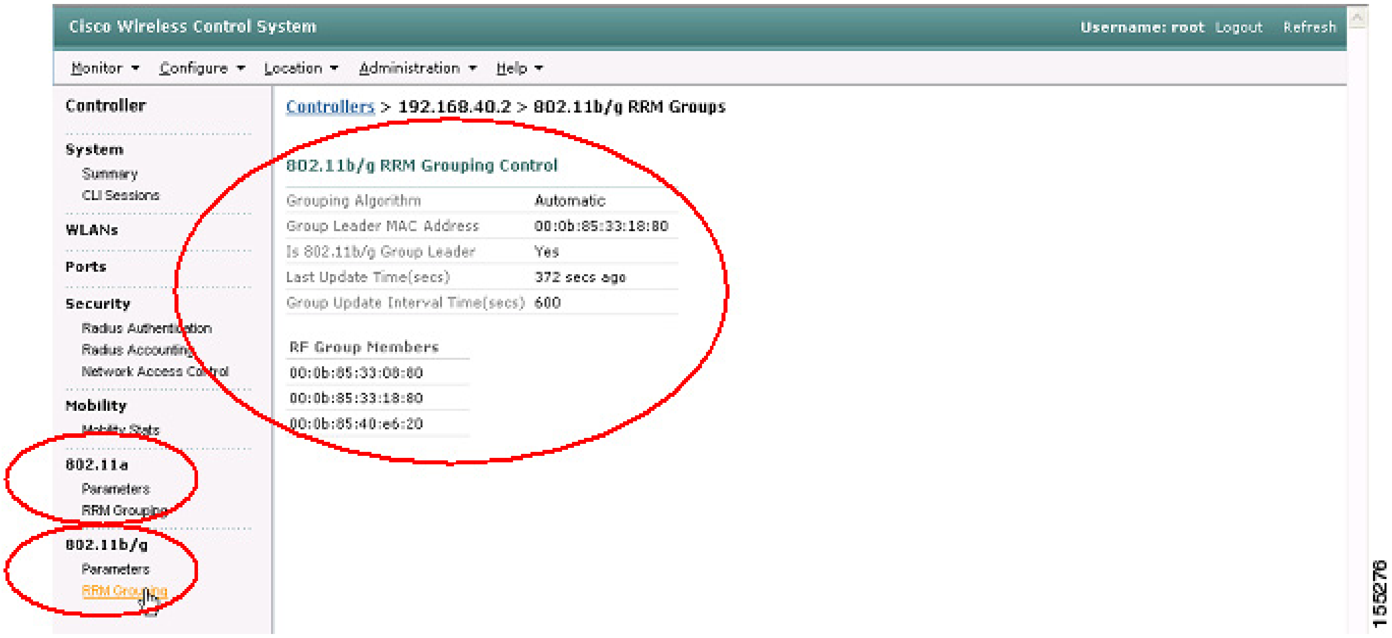


Controllers > Search Results

| IP Address | Controller Name | Type | Location | Mobility Group Name | Reachability Status |
|---|---|---|---|---|---|
| 192.168.30.2 | wlc2006-1 | 2000 | smlab-1 | smlab | Reachable |
| 192.168.40.2 | wlc2006-2 | 2000 | | smlab | Reachable |
| [illegible] | c4402-smlab-1 | 4400 | | smlab | Reachable |

**Step 2** On the left-hand side, select the **RRM Grouping** option for either 802.11a or 802.11b/g. This will show you information about the RRM Grouping for the WLC (see Figure 30).

*Figure 30 WCS RF Group Information*



Controllers > 192.168.40.2 > 802.11b/g RRM Groups

802.11b/g RRM Grouping Control

| | |
|---|---|
| Grouping Algorithm | Automatic |
| Group Leader MAC Address | 00:0b:85:33:18:80 |
| Is 802.11b/g Group Leader | Yes |
| Last Update Time(secs) | 372 secs ago |
| Group Update Interval Time(secs) | 600 |

| RF Group Members |
|---|
| 00:0b:85:33:08:80 |
| 00:0b:85:33:18:80 |
| 00:0b:85:40:e6:20 |

**Step 3** Repeat Step **2** for the other PHY type if desired.

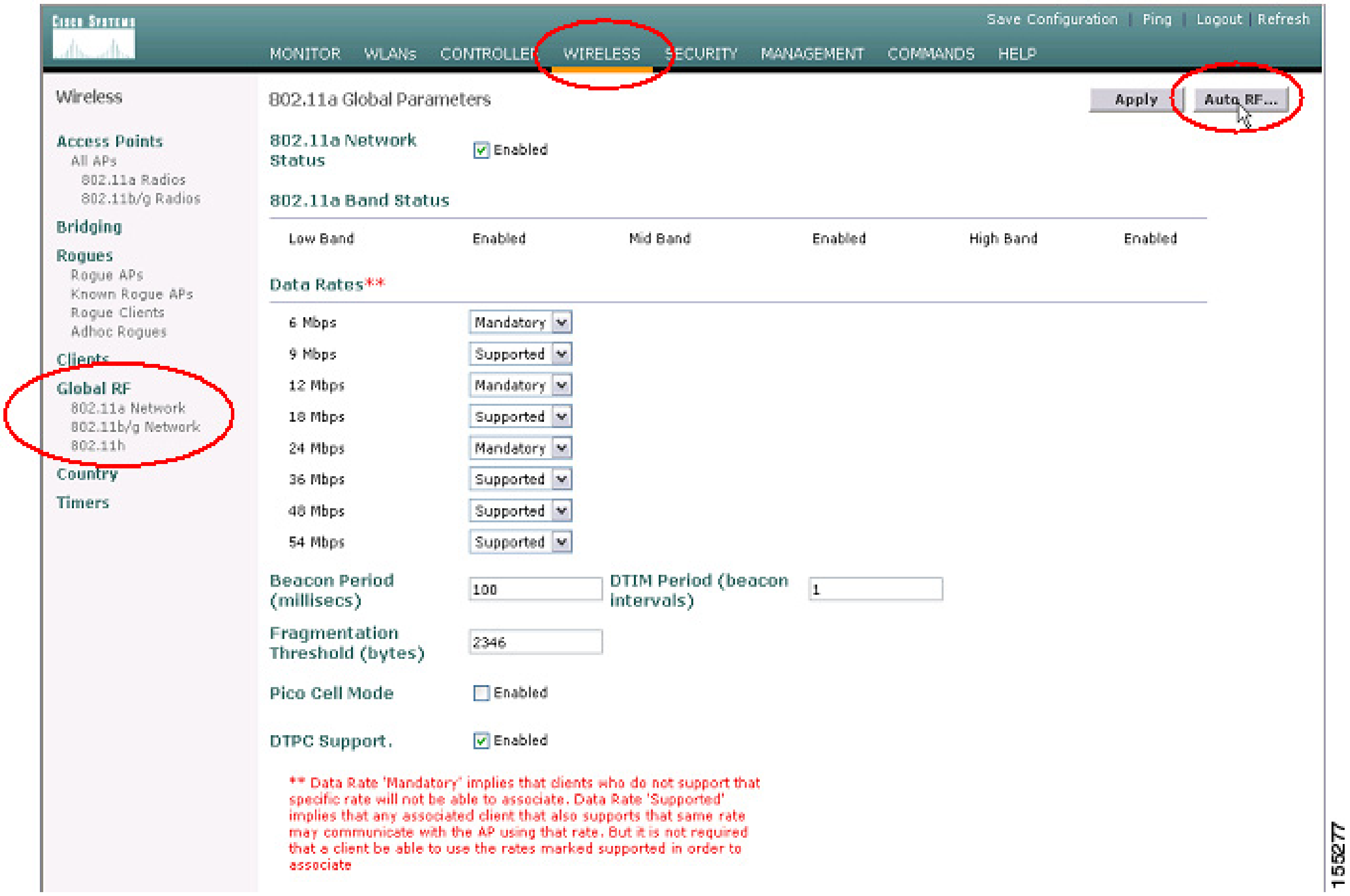
This interface will tell you whether the WLC is participating in automatic grouping for the PHY type, the group leader's MAC address, whether that particular WLC is the group leader, the last update time, the group update interval, and the members of the RF Group (see Figure 30).

The same information is available via the WLC Web Interface. Follow these instructions to view the RF Domain status and information in the WLC Web Interface:

**Step 1** Navigate in the WLC Web Interface to **Wireless | Global RF**. Select a PHY type (either 802.11a or 802.11b/g).

**Step 2** Click **Auto RF** in the upper-right-hand corner (see Figure 31).

***Figure 31 WLC Auto RF Selection***



802.11a Global Parameters

802.11a Network Status ☑ Enabled

802.11a Band Status

| Low Band | Enabled | Mid Band | Enabled | High Band | Enabled |
|---|---|---|---|---|---|

Data Rates**

| | |
|---|---|
| 6 Mbps | Mandatory |
| 9 Mbps | Supported |
| 12 Mbps | Mandatory |
| 18 Mbps | Supported |
| 24 Mbps | Mandatory |
| 36 Mbps | Supported |
| 48 Mbps | Supported |
| 54 Mbps | Supported |

Beacon Period (millisecs) 100 DTIM Period (beacon intervals) 1

Fragmentation Threshold (bytes) 2346

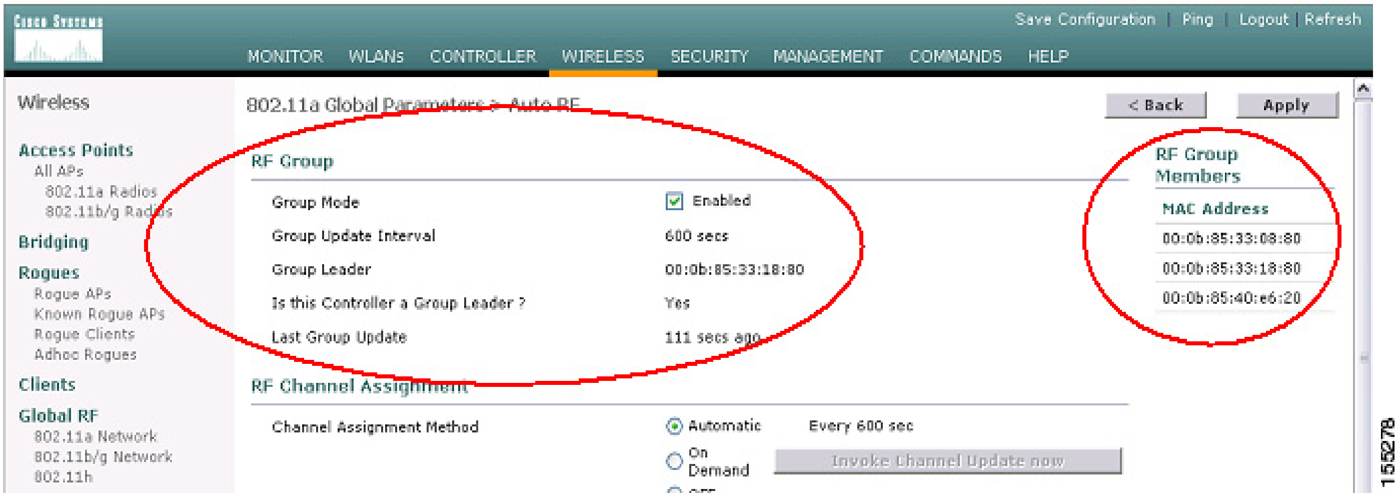
Pico Cell Mode □ Enabled

DTPC Support. ☑ Enabled

** Data Rate 'Mandatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate

**Step 3** You can see the RF Group details including the group leader MAC address, whether the WLC is the group leader, the last update time, the group update interval, and the members of the RF Group at the top of the page (see Figure 32).

*Figure 32 WLC RF Group Parameters*



802.11a Global Parameters > Auto RF

RF Group

| | |
|---|---|
| Group Mode | ☑ Enabled |
| Group Update Interval | 600 secs |
| Group Leader | 00:0b:85:33:18:80 |
| Is this Controller a Group Leader ? | Yes |
| Last Group Update | 111 secs ago |

RF Group Members

| MAC Address |
|---|
| 00:0b:85:33:08:80 |
| 00:0b:85:33:18:80 |
| 00:0b:85:40:e6:20 |

RF Channel Assignment

Channel Assignment Method ● Automatic Every 600 sec
○ On Demand
○ Off

**Step 4** Repeat Steps **1** through **3** for the other PHY type if desired.

## Overriding Automatic RF Group Participation

Unless there is good reason for a WLC to not participate in Automatic RF Grouping, you should leave the feature on. You can override dynamic RRM settings without disabling Automatic RF Group Participation. However, the capability to override Automatic RF Grouping exists in both the WLC Web Interface and the WCS.

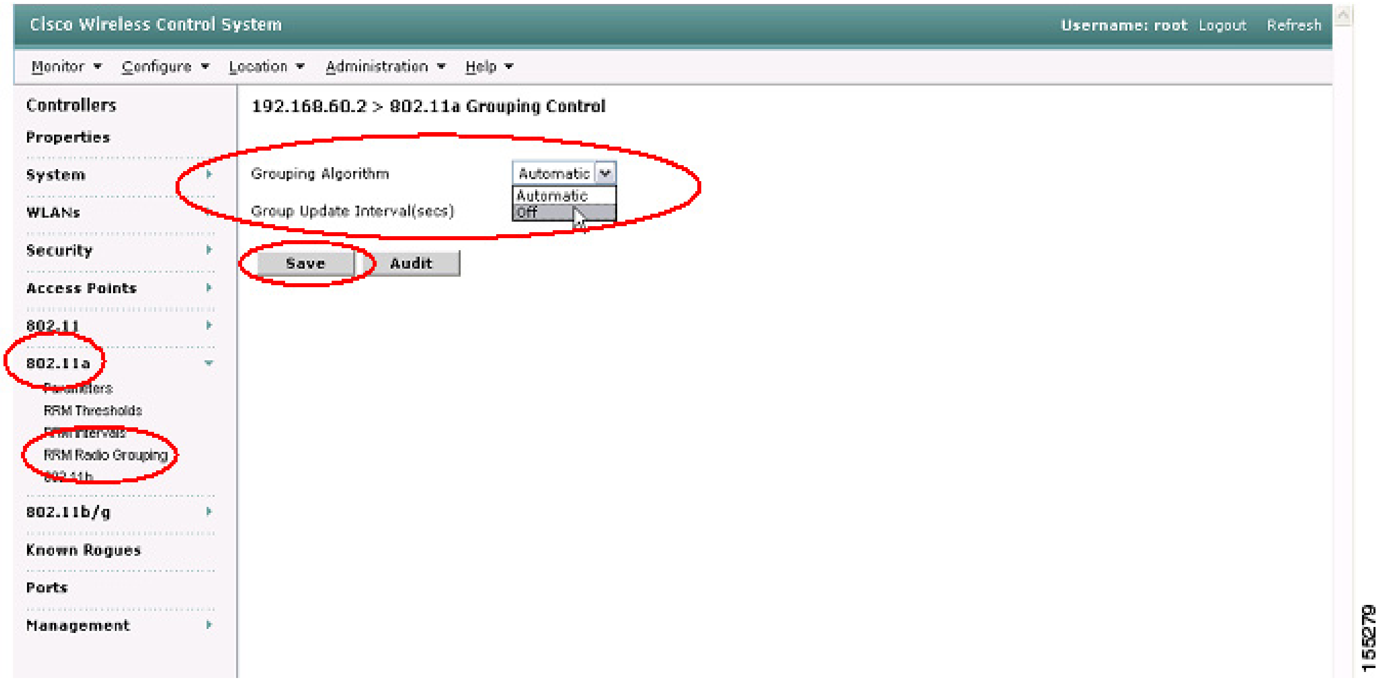
To turn off automatic RF grouping in WCS, follow these steps:

**Step 1** Navigate to **Configure | Controllers**. Select a WLC.

**Step 2** Select the PHY type (for example, 802.11a) on the left-hand-side, and then select the **RRM Radio Grouping** option (see Figure 33).

**Step 3** Change the **Grouping Algorithm** parameter to **Off** and then click **Save** (see Figure 33).

*Figure 33 WCS Automatic RF Group Disable*



192.168.60.2 > 802.11a Grouping Control

Grouping Algorithm: Automatic (Automatic / Off)

Group Update Interval(secs)

**Step 4** Repeat Steps **2** through **3** for the other PHY type if desired.

**Step 5** Repeat Steps **1** through **4** for every WLC as desired.

To turn off Automatic RF Grouping from the WLC Web Interface, follow these steps:

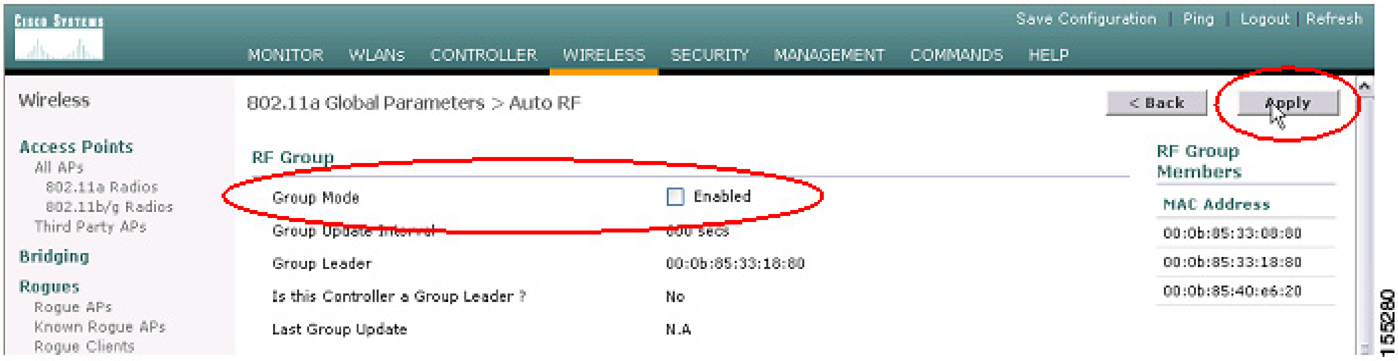
---

**Step 1** Navigate in the WLC Web Interface to **Wireless | Global RF**. Select a PHY type (either 802.11a or 802.11b/g).

**Step 2** Click **Auto RF** in the upper-right-hand corner (see Figure 31.)

**Step 3** Uncheck the **Group Mode** option under the **RF Group** parameters and then click **Apply** (see Figure 34).

*Figure 34 WLC Automatic RF Group Disable*



802.11a Global Parameters > Auto RF

RF Group

| | |
|---|---|
| Group Mode | □ Enabled |
| Group Update Interval | 600 secs |
| Group Leader | 00:0b:85:33:18:80 |
| Is this Controller a Group Leader ? | No |
| Last Group Update | N.A |

RF Group Members

| MAC Address |
|---|
| 00:0b:85:33:08:80 |
| 00:0b:85:33:18:80 |
| 00:0b:85:40:e6:20 |

**Step 4** Repeat Steps **1** through **3** for the other PHY type if desired.

## Overriding Dynamic RRM

In some deployments, it is desirable to statically assign channel and power setting to the access points instead of relying on the dynamic RRM algorithms provided by Cisco. Typically, this is true in RF challenging environments and "non-standard" deployments, but not the more typical carpeted offices. Even if you choose to statically assign power and channels to your access points and/or disable dynamic power and channel assignment, you should still use Automatic RF Grouping to avoid spurious rogue device events.

You can disable dynamic channel and power assignment globally for a WLC, or you can leave dynamic channel and transmit power assignment on and override specific access point radios by statically configuring them with a channel and power setting. While you can specify a global, default transmit power parameter for each PHY type that will apply to all the access point radios on a WLC, you must set the channel for each access point radio when you disable dynamic channel assignment. You may want to set the transmit power for each access point too instead of leaving the global transmit power in effect.

The necessaryconfigurations can be made with WCS radio templates or in the WLC Web Interface. We'll first consider how to statically assign channel and transmit power settings on a per radio basis and then will move on to the steps required to disable dynamic channel and transmit power assignment.

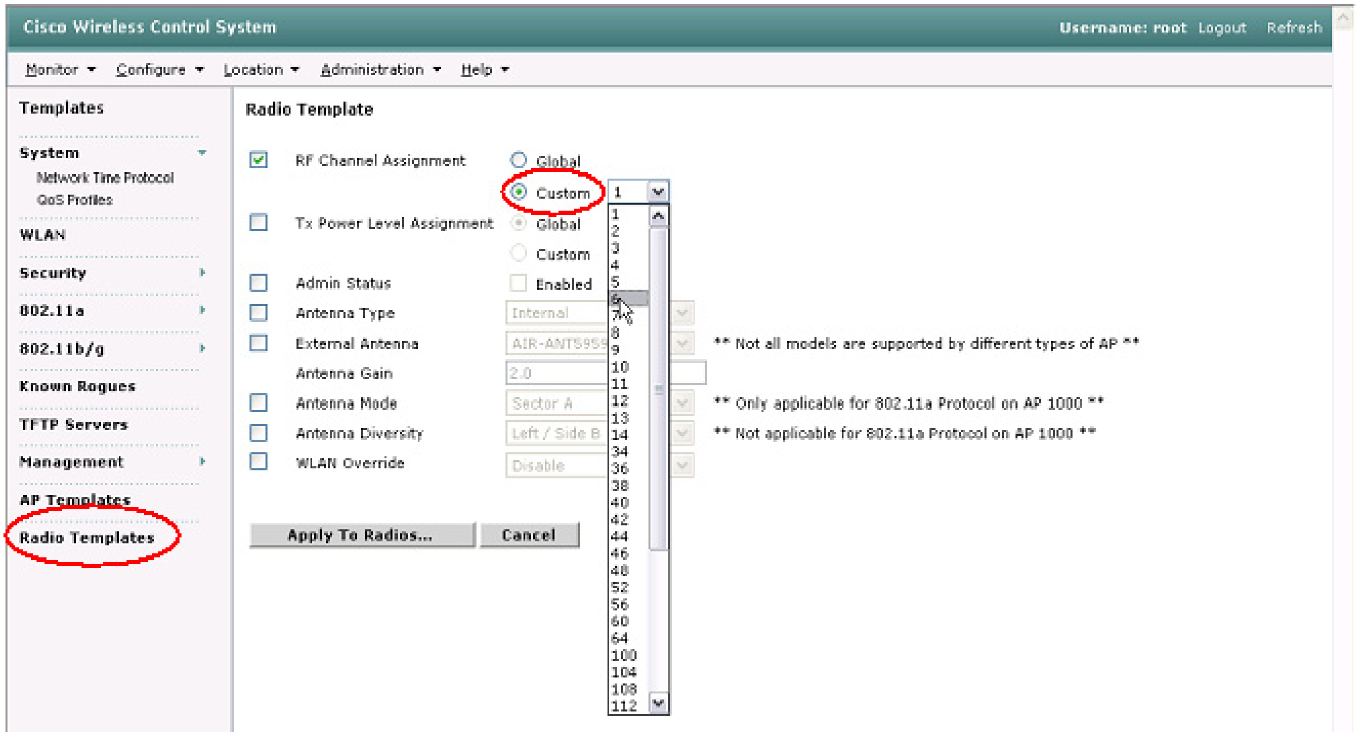
### Statically Assigning Channel and Transmit Power Settings to Access Point Radios

To use WCS radio templates to statically assign channel and transmit power settings to one or more access point radios, follow these steps:

**Step 1** Navigate to **Configuration | Templates | Radio Templates**.

**Step 2** To select an RF Channel, check the RF Channel Assignment box and then select the Custom option. Pick a channel from the drop-down box (see Figure 35). Make sure you select an RF channel that is appropriate for the access point radios you are configuring.

*Figure 35 WCS Static Channel Assignment*



Radio Template

☑ RF Channel Assignment ○ Global ● Custom 1

□ Tx Power Level Assignment ○ Global ○ Custom

□ Admin Status □ Enabled

□ Antenna Type Internal

□ External Antenna AIR-ANT5959 ** Not all models are supported by different types of AP **

Antenna Gain 2.0

□ Antenna Mode Sector A ** Only applicable for 802.11a Protocol on AP 1000 **

□ Antenna Diversity Left / Side B ** Not applicable for 802.11a Protocol on AP 1000 **

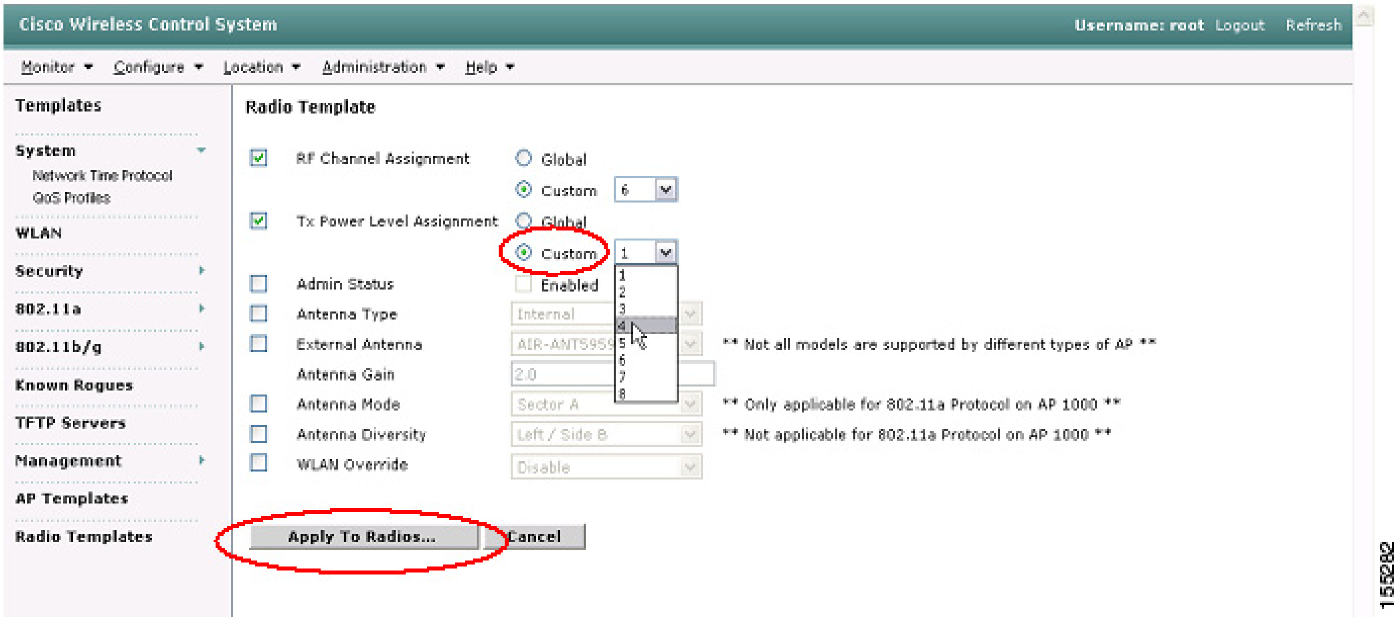
□ WLAN Override Disable

**Step 3** To select a transmit power setting, check the TxPower Level Assignment box and then select the Custom option. Pick a transmit power level from the drop-down box (see Figure 36).

(Make sure you select a transmit power level that is appropriate for the access point radios you are configuring.[1])

[1] In both WCS and the WLC, the Tx Power Level is assigned by an integer value instead of a value in mW or dBm. The integer corresponds to a Tx Power Level that varies depending on the regulatory domain where the access points are deployed. A Tx Power Level of "1" corresponds to the maximum allowed value for the regulatory domain, "2" is 50% of the maximum value, "3" is 25% of the maximum value, and so on. Consult your Cisco representatives for the specifics in your regulatory domain.

Figure 36 WCS Static Transmit Power Assignment



Radio Template

☑ RF Channel Assignment ○ Global ● Custom 6

☑ Tx Power Level Assignment ○ Global ● Custom 1 (1, 2, 3, 4, 5, 6, 7, 8)

□ Admin Status □ Enabled

□ Antenna Type Internal

□ External Antenna AIR-ANT5959 ** Not all models are supported by different types of AP **

Antenna Gain 2.0

□ Antenna Mode Sector A ** Only applicable for 802.11a Protocol on AP 1000 **

□ Antenna Diversity Left / Side B ** Not applicable for 802.11a Protocol on AP 1000 **

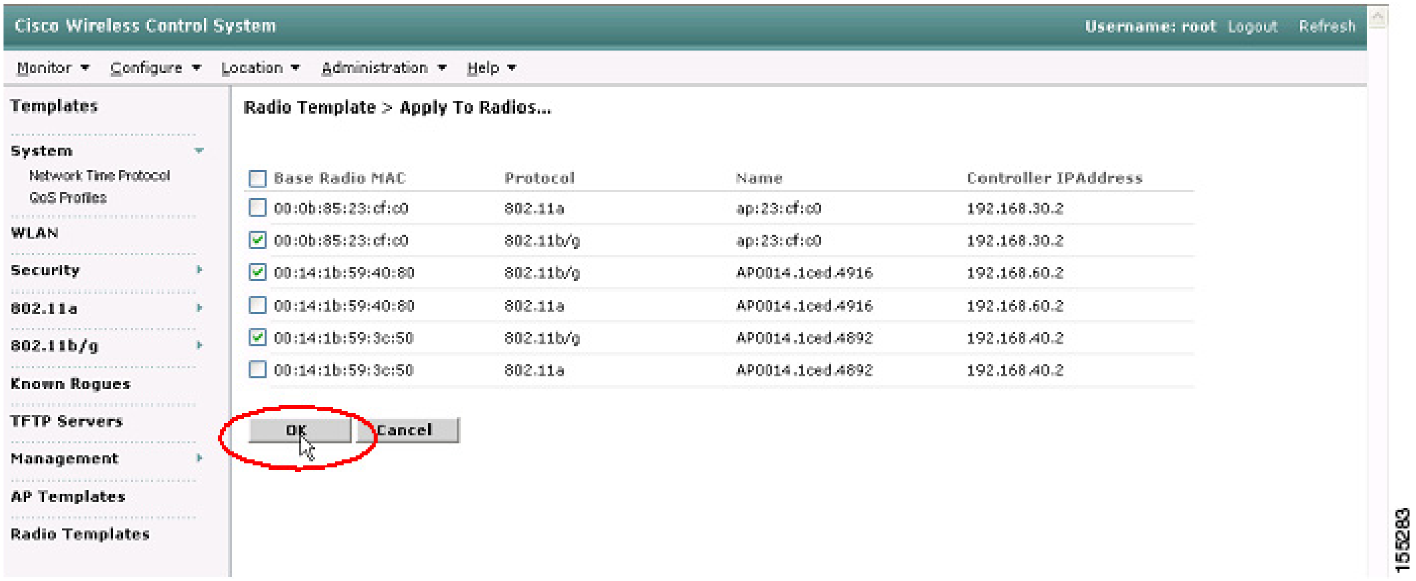
□ WLAN Override Disable

Apply To Radios... Cancel

**Step 4** Click on the Apply to Radios button (see Figure 35 and Figure 36).

**Step 5** Select the desired access point radios and then click on the OK button (see Figure 37). Note that you should select only applicable radio types. For example, if you are setting the RF channel to channel 6, you should not select any 802.11a radios.

Figure 37 Applying WCS Power and Channel Template to Radios



Radio Template > Apply To Radios...

| □ | Base Radio MAC | Protocol | Name | Controller IPAddress |
|---|---|---|---|---|
| □ | 00:0b:85:23:cf:c0 | 802.11a | ap:23:cf:c0 | 192.168.30.2 |
| ☑ | 00:0b:85:23:cf:c0 | 802.11b/g | ap:23:cf:c0 | 192.168.30.2 |
| ☑ | 00:14:1b:59:40:80 | 802.11b/g | AP0014.1ced.4916 | 192.168.60.2 |
| □ | 00:14:1b:59:40:80 | 802.11a | AP0014.1ced.4916 | 192.168.60.2 |
| ☑ | 00:14:1b:59:3c:50 | 802.11b/g | AP0014.1ced.4892 | 192.168.40.2 |
| □ | 00:14:1b:59:3c:50 | 802.11a | AP0014.1ced.4892 | 192.168.40.2 |

OK Cancel

**Step 6** Repeat Steps **1** through **5** as many times as necessary to configure each of the access point radios as desired.

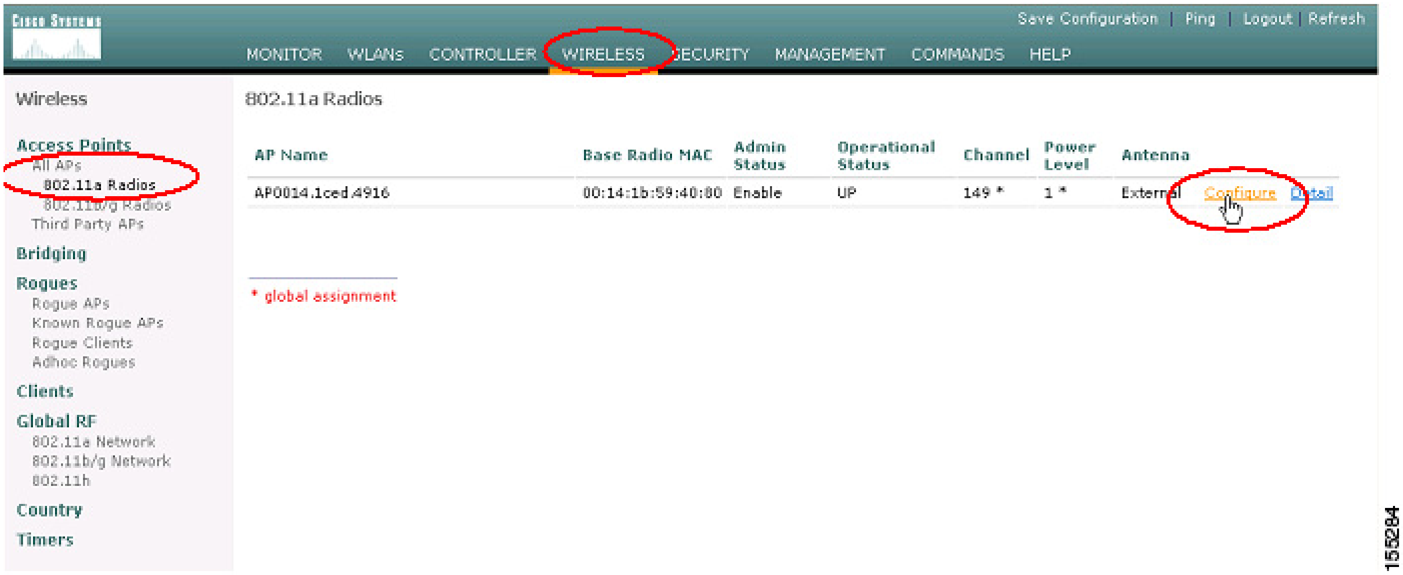
**Step 7** When you have completed Steps **1** through **6**, you should refresh your WLC configurations in WCS to keep WCS current, following the instructions in the Controller Maintenance section.

In the WLC Web Interface, you statically assign power and/or channel settings on a per access point radio basis by following these steps:

**Step 1** Navigate to **Wireless | Access Points | All APs** and select an 802.11 PHY type. For example, if you select 802.11a Radios, all the 802.11a radios joined to the WLC will be shown on the right-hand side (see Figure 38).

**Step 2** Select the **Configure Link** to access the radio configuration (see Figure 38).

***Figure 38 WLC Selecting a Radio to Configure***

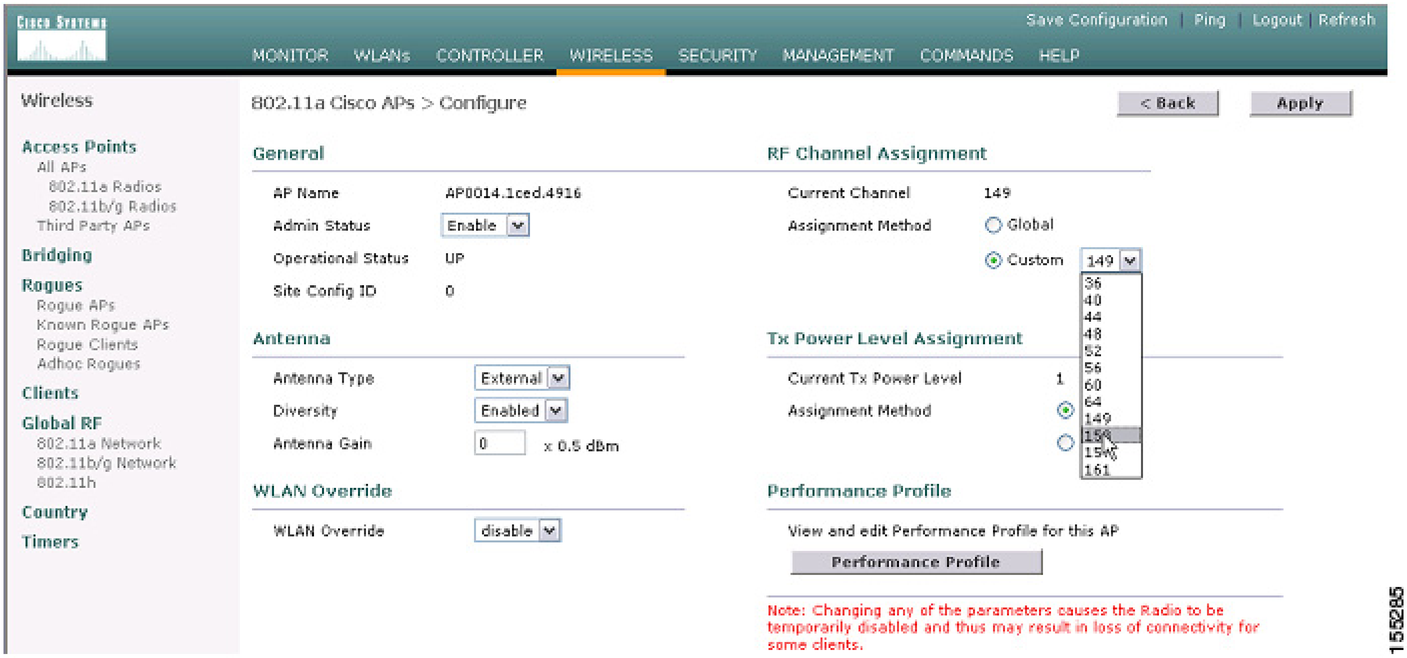


802.11a Radios

| AP Name | Base Radio MAC | Admin Status | Operational Status | Channel | Power Level | Antenna | | |
|---|---|---|---|---|---|---|---|---|
| AP0014.1ced.4916 | 00:14:1b:59:40:80 | Enable | UP | 149 * | 1 * | External | Configure | Detail |

* global assignment

**Step 3** To assign an RF Channel to the access point radio, select the Custom option for RF Channel Assignment and select a channel from the drop-down box (see Figure 39).



802.11a Cisco APs > Configure

General

AP Name AP0014.1ced.4916

Admin Status Enable

Operational Status UP

Site Config ID 0

Antenna

Antenna Type External

Diversity Enabled

Antenna Gain 0 x 0.5 dBm

WLAN Override

WLAN Override disable

RF Channel Assignment

Current Channel 149

Assignment Method ○ Global ● Custom 149

36 40 44 48 52 56 60 64 149 153 157 161

Tx Power Level Assignment

Current Tx Power Level 1

Assignment Method ● ○

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

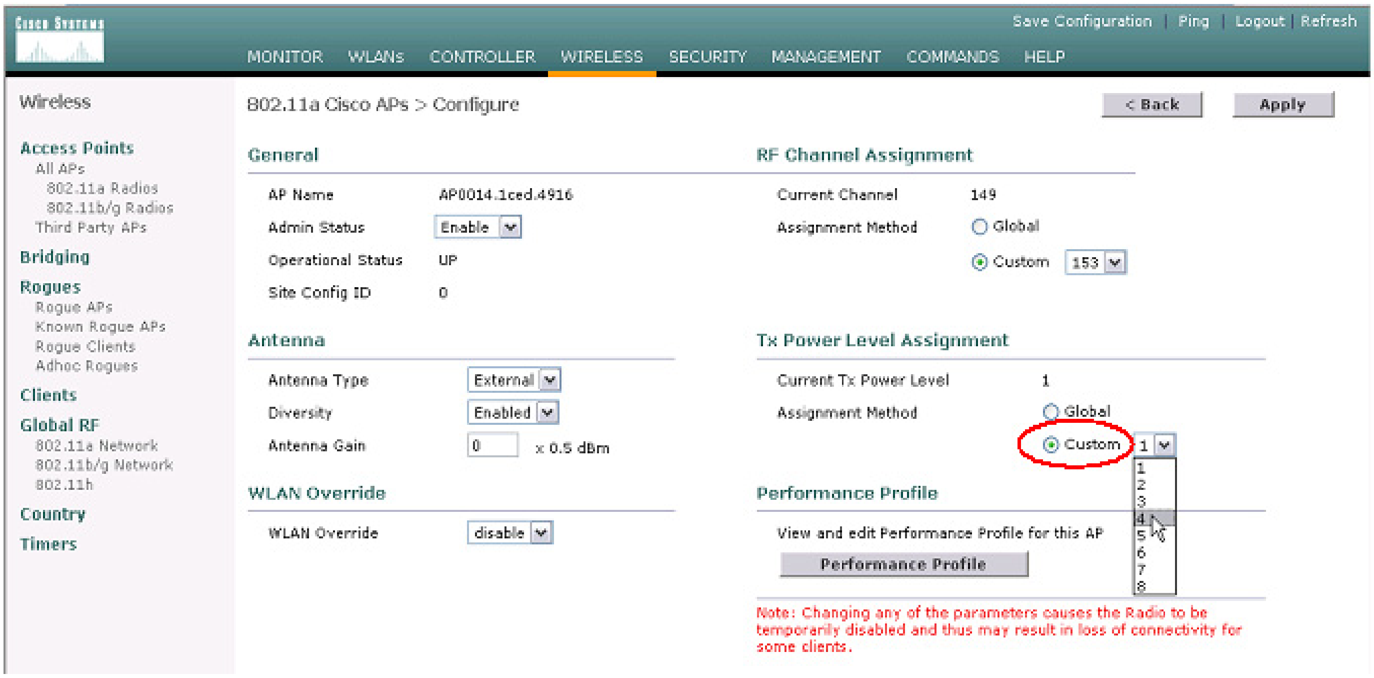
*Figure 39 WLC Static RF Channel Assignment to a Radio*

**Step 4** To assign a transmit power level to the access point radio, select the Custom option for Tx Power Level Assignment and select a transmit power level from the drop-down box (see Figure 40).

(Raw DHCP Option 43 without specifying a VCI should be avoided if possible.[1])

[1] Using a raw DHCP Option 43 limits the DHCP Server to supporting a single device type for vendor specific information per DHCP scope. Also, every DHCP client will receive the Option 43 values in a DHCP Offer, whether the values are relevant to the device or not.

*Figure 40 WLC Static Transmit Power Assignment to a Radio*



802.11a Cisco APs > Configure

General

AP Name AP0014.1ced.4916

Admin Status Enable

Operational Status UP

Site Config ID 0

RF Channel Assignment

Current Channel 149

Assignment Method ○ Global ● Custom 153

Antenna

Antenna Type External

Diversity Enabled

Antenna Gain 0 x 0.5 dBm

Tx Power Level Assignment

Current Tx Power Level 1

Assignment Method ○ Global ● Custom 1

WLAN Override

WLAN Override disable

Performance Profile

View and edit Performance Profile for this AP

Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

**Step 5** Click on Apply commit the changes to the Access Point Radio.

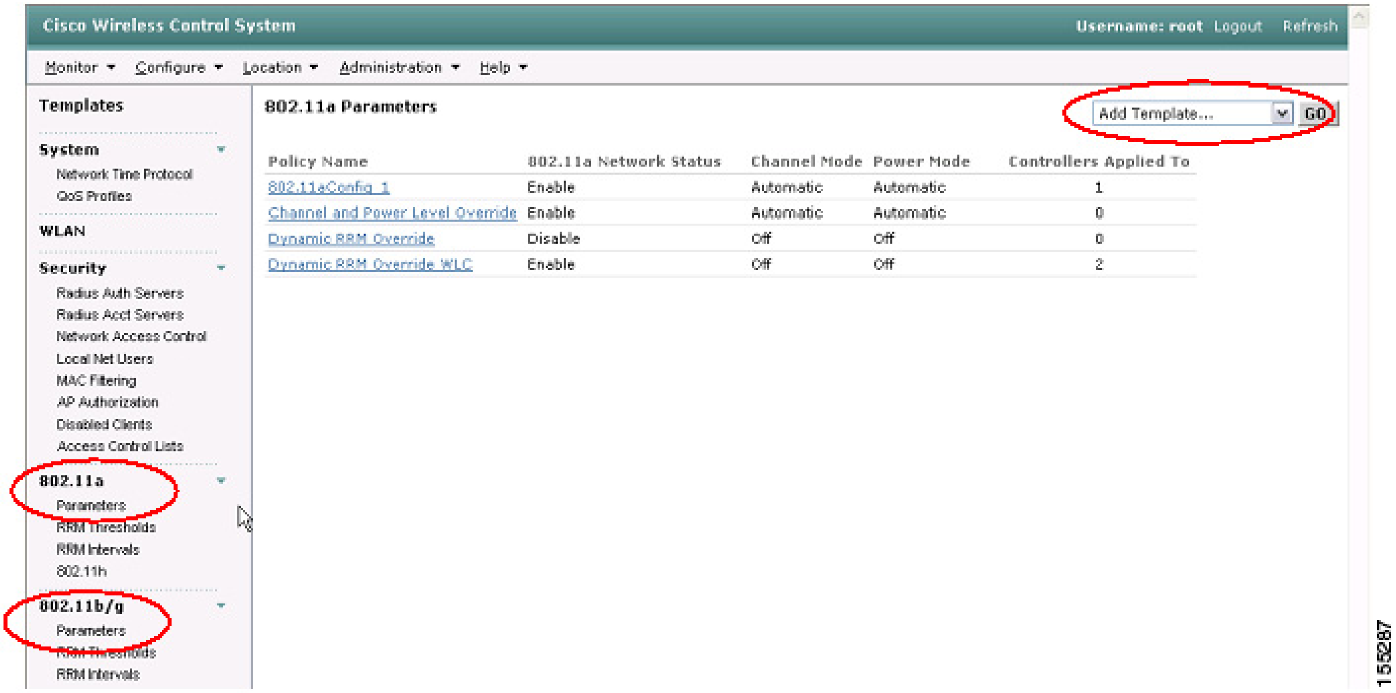
**Step 6** Repeat Steps **1** through **5** for each Access Point Radio that you want to statically assign a static power and/or channel setting for.

## Disabling Dynamic Power and Channel Assignment Globally for a WLC

To disable dynamic power and channel assignment globally for a WLC using WCS, follow these steps:

**Step 1** Navigate to **Configure | Templates**. Select a PHY type on the left-hand side, for example, 802.11a and then select **Parameters**. Select the **Add Template** option from the drop-down box (see Figure 41).

*Figure 41 WCS Radio Parameters Template*



802.11a Parameters

| Policy Name | 802.11a Network Status | Channel Mode | Power Mode | Controllers Applied To |
|---|---|---|---|---|
| 802.11aConfig_1 | Enable | Automatic | Automatic | 1 |
| Channel and Power Level Override | Enable | Automatic | Automatic | 0 |
| Dynamic RRM Override | Disable | Off | Off | 0 |
| Dynamic RRM Override WLC | Enable | Off | Off | 2 |

**Step 2** Assign the template a name in the **Policy Name** field (see Figure 42).

**Step 3** Select the **Enabled** box for the **<PHY Type> Network Status** parameter (see Figure 42).

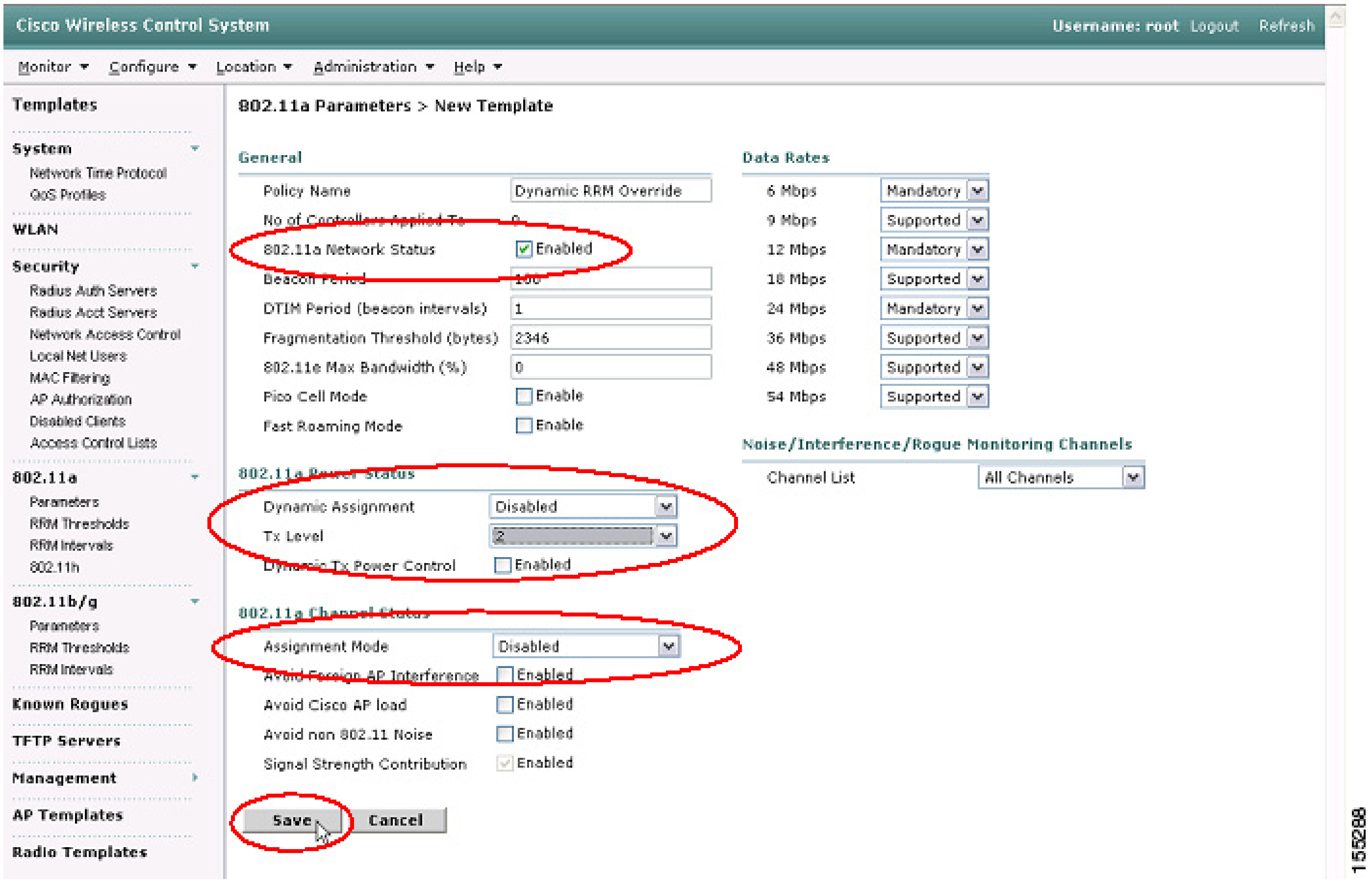
**Step 4** To disable dynamic power assignment, set the **Dynamic Assignment** parameter to **Disabled** under **<PHY Type> Power Status** (see Figure 42).

**Step 5** Select a default transmit power level from the **Tx Level** drop-down box (see Figure 42). Note that this transmit power level will be assigned to all the radios joined to the WLC unless you override the setting on a per-radio basis.

**Step 6** To disable dynamic channel assignment, set the **Assignment Mode** parameter to **Disabled** under **<PHY Type> Channel Status** (see Figure 42). Note that you will now need to statically set the radio channel for each radio joined to the WLC.

**Step 7** Click **Save** (see Figure 42).

*Figure 42 WCS Global Dynamic RRM Override Template*



802.11a Parameters > New Template

General

| | |
|---|---|
| Policy Name | Dynamic RRM Override |
| No of Controllers Applied To | 0 |
| 802.11a Network Status | ☑ Enabled |
| Beacon Period | 100 |
| DTIM Period (beacon intervals) | 1 |
| Fragmentation Threshold (bytes) | 2346 |
| 802.11e Max Bandwidth (%) | 0 |
| Pico Cell Mode | ☐ Enable |
| Fast Roaming Mode | ☐ Enable |

802.11a Power Status

| | |
|---|---|
| Dynamic Assignment | Disabled |
| Tx Level | 2 |
| Dynamic Tx Power Control | ☐ Enabled |

802.11a Channel Status

| | |
|---|---|
| Assignment Mode | Disabled |
| Avoid Foreign AP Interference | ☐ Enabled |
| Avoid Cisco AP load | ☐ Enabled |
| Avoid non 802.11 Noise | ☐ Enabled |
| Signal Strength Contribution | ☑ Enabled |

Data Rates

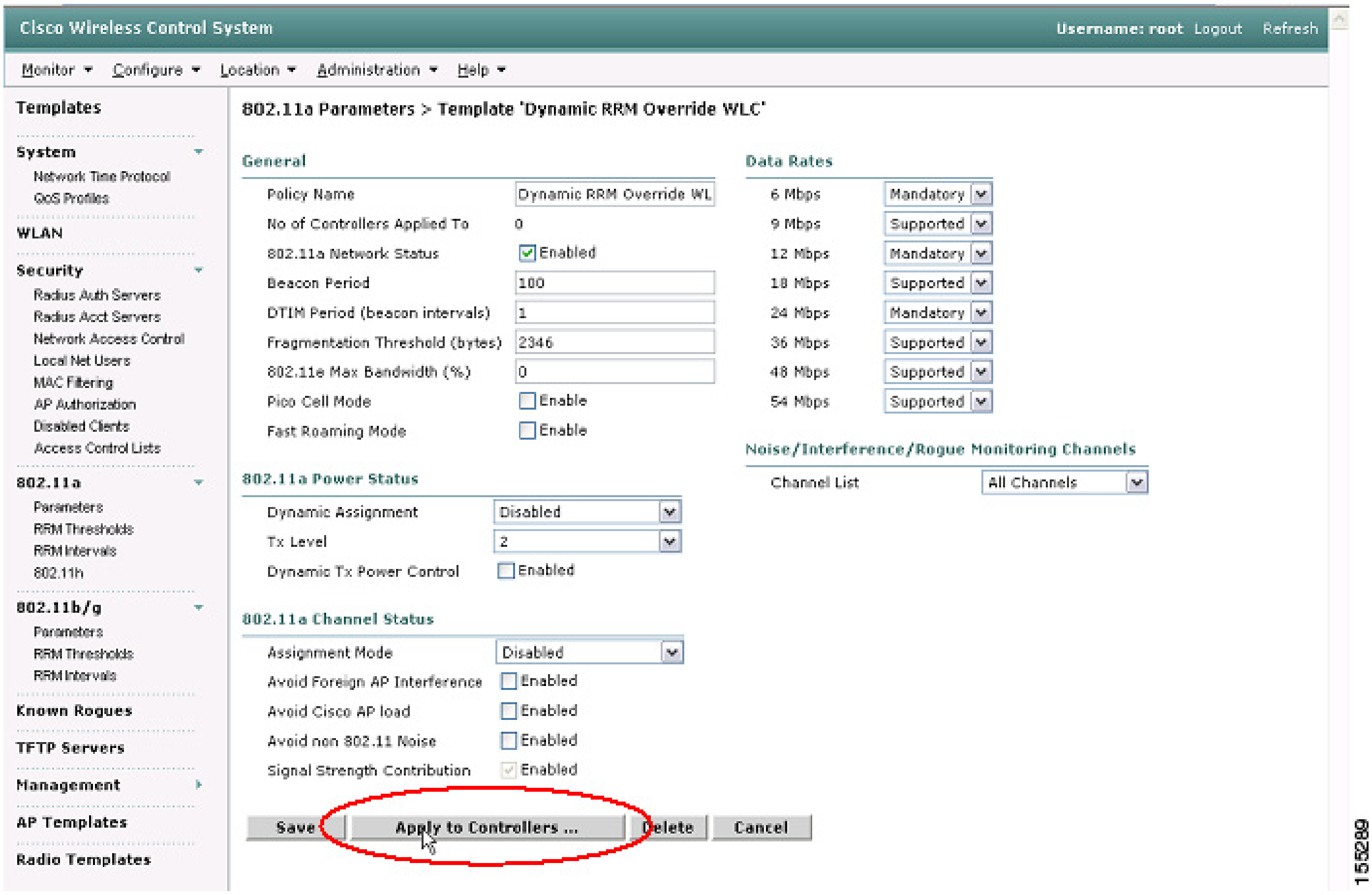
| | |
|---|---|
| 6 Mbps | Mandatory |
| 9 Mbps | Supported |
| 12 Mbps | Mandatory |
| 18 Mbps | Supported |
| 24 Mbps | Mandatory |
| 36 Mbps | Supported |
| 48 Mbps | Supported |
| 54 Mbps | Supported |

Noise/Interference/Rogue Monitoring Channels

| | |
|---|---|
| Channel List | All Channels |

**Step 8** Now click **Apply to Controllers** (see Figure 43).

*Figure 43 WCS Global Dynamic RRM Override Template Apply to Controllers*



802.11a Parameters > Template 'Dynamic RRM Override WLC'

General

| | |
|---|---|
| Policy Name | Dynamic RRM Override WL |
| No of Controllers Applied To | 0 |
| 802.11a Network Status | ☑ Enabled |
| Beacon Period | 100 |
| DTIM Period (beacon intervals) | 1 |
| Fragmentation Threshold (bytes) | 2346 |
| 802.11e Max Bandwidth (%) | 0 |
| Pico Cell Mode | □ Enable |
| Fast Roaming Mode | □ Enable |

802.11a Power Status

| | |
|---|---|
| Dynamic Assignment | Disabled |
| Tx Level | 2 |
| Dynamic Tx Power Control | □ Enabled |

802.11a Channel Status

| | |
|---|---|
| Assignment Mode | Disabled |
| Avoid Foreign AP Interference | □ Enabled |
| Avoid Cisco AP load | □ Enabled |
| Avoid non 802.11 Noise | □ Enabled |
| Signal Strength Contribution | ☑ Enabled |

Data Rates

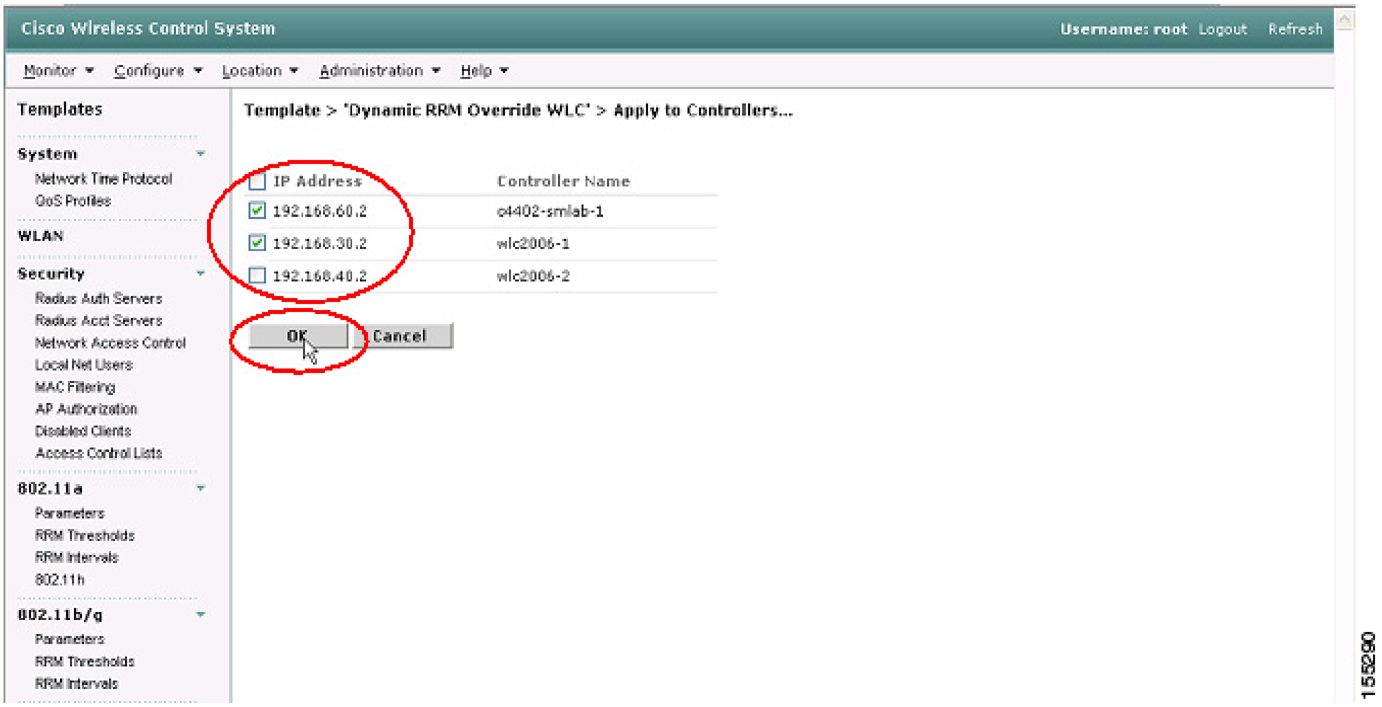
| | |
|---|---|
| 6 Mbps | Mandatory |
| 9 Mbps | Supported |
| 12 Mbps | Mandatory |
| 18 Mbps | Supported |
| 24 Mbps | Mandatory |
| 36 Mbps | Supported |
| 48 Mbps | Supported |
| 54 Mbps | Supported |

Noise/Interference/Rogue Monitoring Channels

| | |
|---|---|
| Channel List | All Channels |

**Step 9** Select the desired WLCs and then click **OK** (see Figure 44).

*Figure 44 WCS Global Dynamic RRM Override Template Apply to Controllers*



Template > 'Dynamic RRM Override WLC' > Apply to Controllers...

| □ IP Address | Controller Name |
|---|---|
| ☑ 192.168.60.2 | c4402-smlab-1 |
| ☑ 192.168.30.2 | wlc2006-1 |
| □ 192.168.40.2 | wlc2006-2 |

**Step 10** Assign static channel and power settings to each of the radios joined to the WLC(s) you selected in Step **9**.

**Step 11** Repeat Steps **1** through **10** for the other PHY type if necessary. For example, if you disabled dynamic power and/or channel settings for the 802.11a radios, repeat those steps for the 802.11b/g radios if necessary.

To disable dynamic power and channel assignment globally for a WLC using the WLC Web Interface, follow these steps:

---

**Step 1** Navigate in the WLC Web Interface to **Wireless | Global RF**. Select a PHY type (either 802.11a or 802.11b/g).

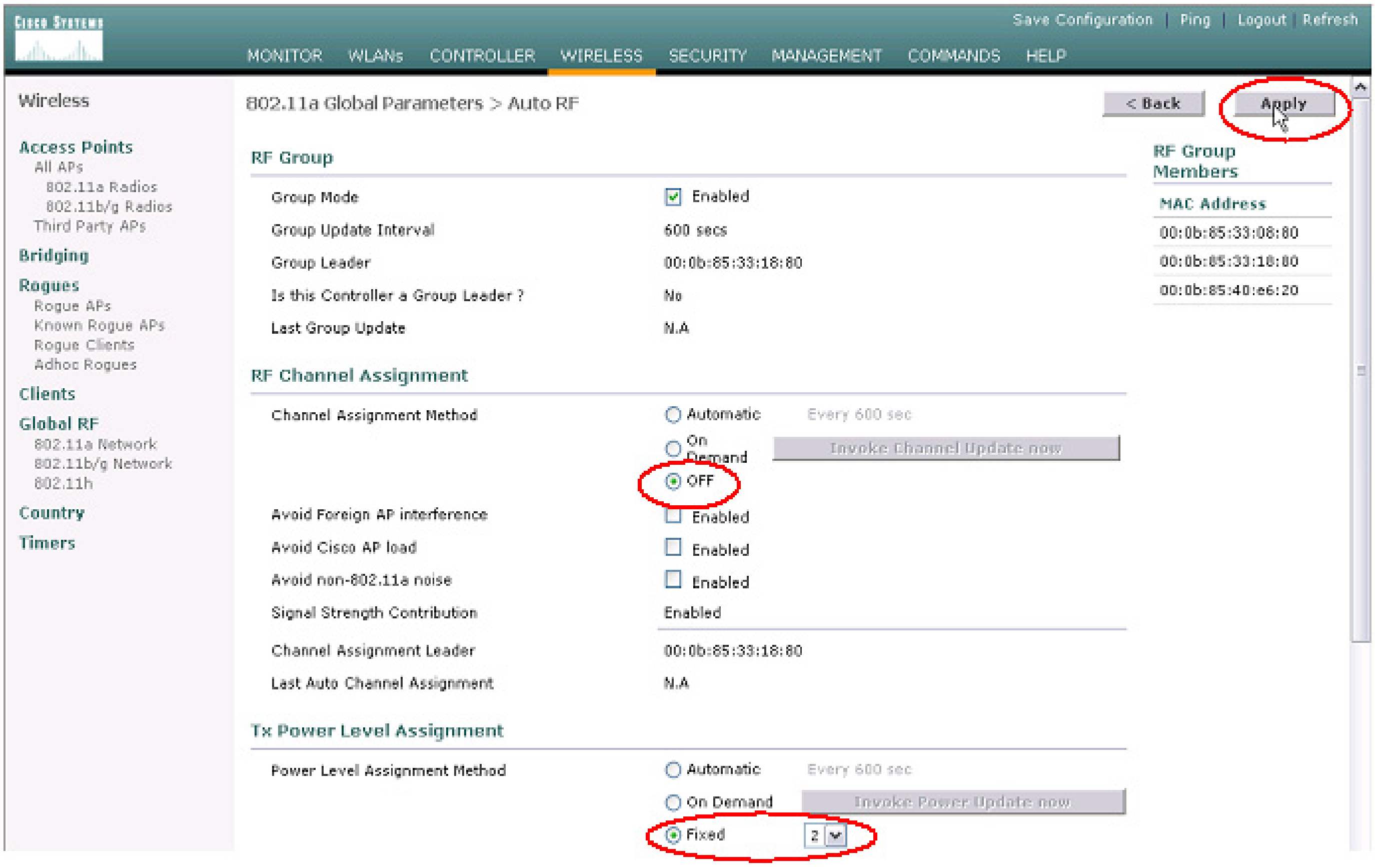
**Step 2** Click **Auto RF** in the upper-right-hand corner (see Figure 31).

**Step 3** To disable dynamic channel assignment, select **Off** under **RF Channel Assignment** (see Figure 45).

**Step 4** To disable dynamic power assignment, select **Fixed** under **Tx Power Level Assignment** and then select a default transmit power level from the drop-down box (see Figure 45).

**Step 5** Click **Apply** to commit the changes to the WLC (see Figure 45).

*Figure 45 WLC Global Dynamic RRM Override*



802.11a Global Parameters > Auto RF

RF Group

| | |
|---|---|
| Group Mode | ☑ Enabled |
| Group Update Interval | 600 secs |
| Group Leader | 00:0b:85:33:18:80 |
| Is this Controller a Group Leader ? | No |
| Last Group Update | N.A |

RF Channel Assignment

| | |
|---|---|
| Channel Assignment Method | ○ Automatic Every 600 sec<br>○ On Demand<br>● OFF |
| Avoid Foreign AP interference | □ Enabled |
| Avoid Cisco AP load | □ Enabled |
| Avoid non-802.11a noise | □ Enabled |
| Signal Strength Contribution | Enabled |
| Channel Assignment Leader | 00:0b:85:33:18:80 |
| Last Auto Channel Assignment | N.A |

Tx Power Level Assignment

| | |
|---|---|
| Power Level Assignment Method | ○ Automatic Every 600 sec<br>○ On Demand<br>● Fixed 2 |

RF Group Members

| MAC Address |
|---|
| 00:0b:85:33:08:80 |
| 00:0b:85:33:18:80 |
| 00:0b:85:40:e6:20 |

**Step 6** Assign static channel and power settings (if you are overriding the default power setting on a per- radio basis) to each of the radios joined to the WLC.

**Step 7** Repeat Steps **1** through **6** for the other PHY type if necessary. For example, if you disabled dynamic power and/or channel settings for the 802.11a radios, repeat those steps for the 802.11b/g radios if necessary.

# Redundancy and Access Point Load Balancing

The Cisco Unified Wirelss Network Architecture offers redundancy at several levels. At the RF level, the system self-heals when one more access points become inactive. The architecture also supports port redundancy per controller and controller device redundancy.

## Access Point Self-Healing

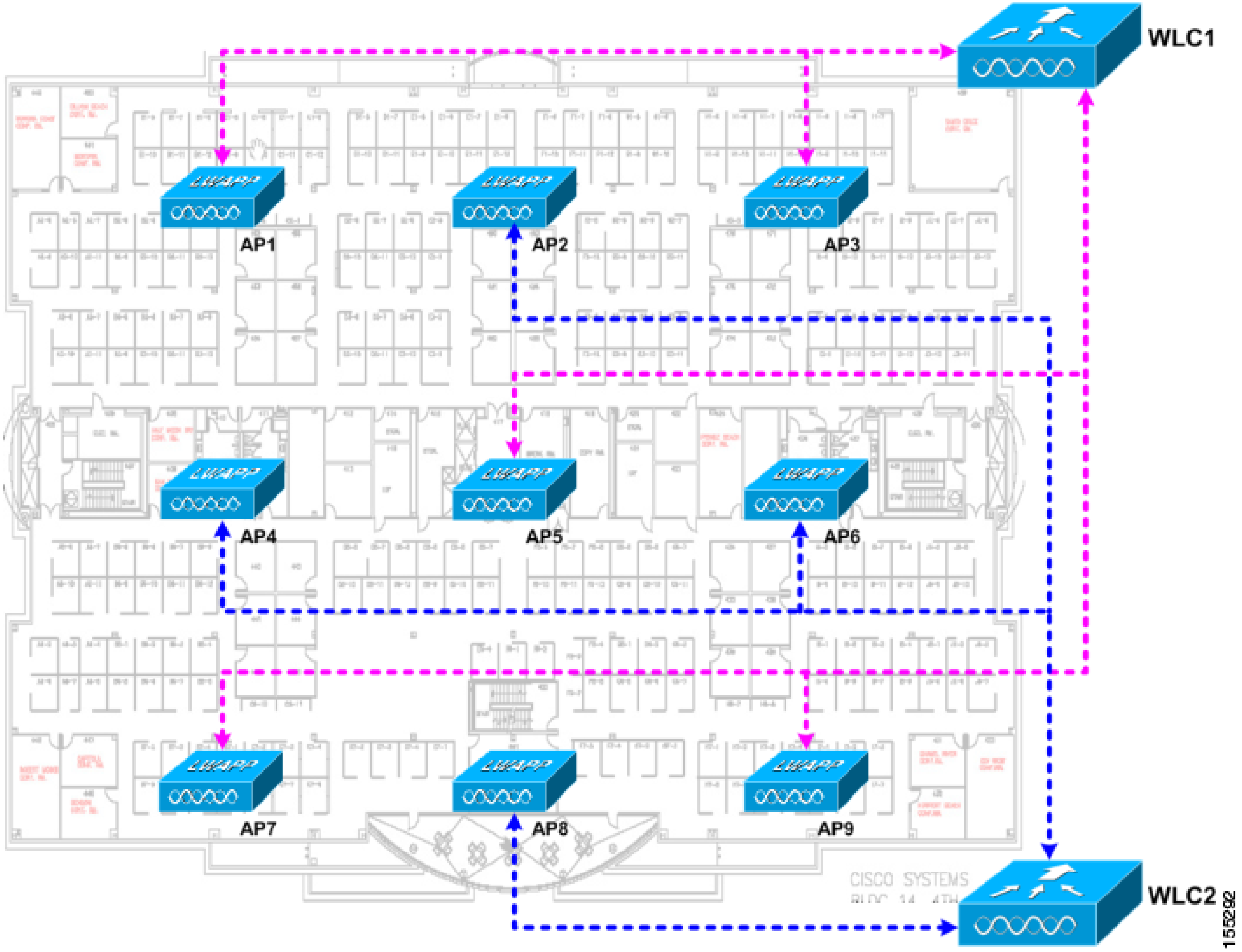
With access point self-healing, the system will raise the power levels and adjust channel selection of neighbor access points to compensate for the lost coverage. An in-depth discussion of the mechanics of RF self-healing are beyond the scope of this document, but simply speaking, an access point is determined to be lost when the neighbor access points no longer see RF neighbor messages from the access point.

It is important to note that the system must be designed to support self-healing capabilities. Specifically, access points must be placed so that the system has at least one power level available to step up if RF self-healing is triggered. It is also important to note that access point self-healing only works for access points configured to be in the same RF Domain.

## Access Point "Salt-and-Pepper" Designs

The Cisco Unified Wireless Network architecture supports salt-and-pepper access point designs, where adjacent access points are joined to different controllers. Figure 46 illustrates the salt-and-pepper access point design concept:

*Figure 46 Salt-and-Pepper Access Point Layout*



In Figure 46, every odd-numbered access point is joined to WLC1 and every even-numbered access point is joined to WLC2. In theory, this design provides for dynamic traffic load-balancing across WLCs and coverage redundancy in the event of a WLC failure.

In practice however, salt-and-pepper designs can result in a large number of inter-controller roaming events and so are generally not widely recommended or deployed. You can get equivalent performance and resiliency without a salt-and-pepper design. Please see the upcoming section on Controller Redundancy and Access Point Load Balancing (Controller Redundancy and Access Point Load Balancing, page 74).

## Controller Interface and Port Redundancy

WLCs can be configured with multiple physical connections to the network. When you have multiple physical connections to the network, WLC interfaces can be mapped to a primary and backup port. In a situation when the primary port is down, the interfaces direct the traffic onto the backup port. There is no load balancing performed across a primary and backup port and only one port is used at a time.

When LAG is enabled, traffic is load balanced across multiple physical ports. Interfaces on a WLC connected to the network via LAG do not have primary and secondary port configuration option available. The system dynamically detects when port is down and automatically maps traffic onto the active links only. LAG configuration is explained in detail in the "Scaling WLCs to Support More Than 48 APs" section. The rest of this section assumes a WLC that is not using LAG so we will consider manually mapped port redundancy.

To configure interface port redundancy through the WLC CLI, follow these steps:

**Step 1** If one or more wireless LANs are mapped to the interface, you must disable the wireless LAN(s) first. To disable a wireless LAN, you need the wireless LAN identifier which is an integer value between 1 and 16. To get the wireless LAN identifier, use the following command:

```
show wlan summary
```

**Step 2** Disable the wireless LAN using the following command:

```
config wlan disable <WLAN ID>
```

**Step 3** Configure the redundant physical ports:

```
config interface port <interface-name> <primary port> <backup port>
```

**Step 4** Re-enable the wireless LAN

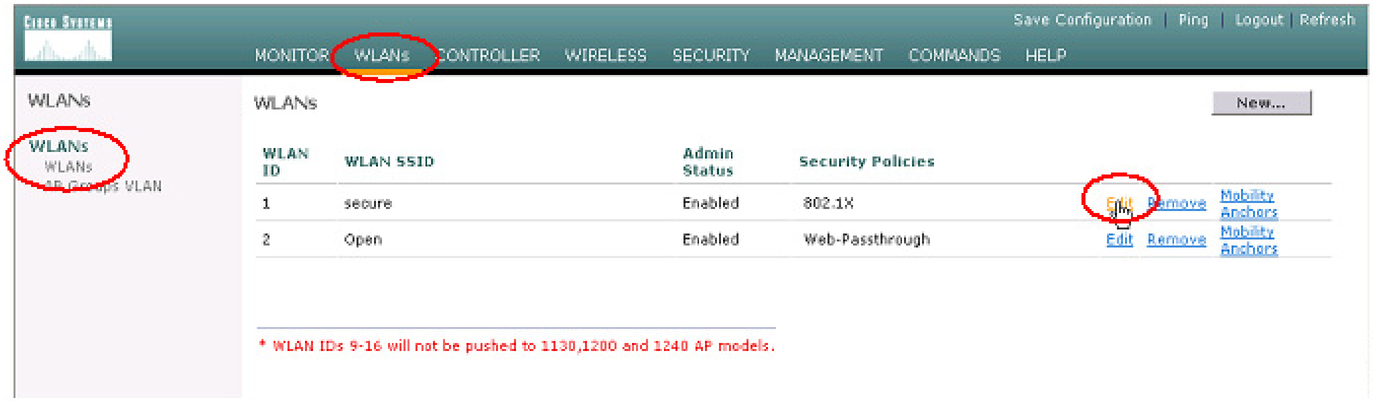
```
config wlan enable <WLAN ID>
```

**Step 5** Repeat Steps **1** through **4** for each interface as necessary.

To configure port redundancy through the WLC, follow these steps:

**Step 1** If a wireless LAN is mapped to the interface, you must disable the wireless LAN first. To disable the wireless LAN, you need the wireless LAN identifier which is an integer value between 1 and 16. To determine the wireless LAN identifier, navigate in the WLC to the **WLANs** tab (see Figure 47):

***Figure 47 WLAN Disable: Edit***



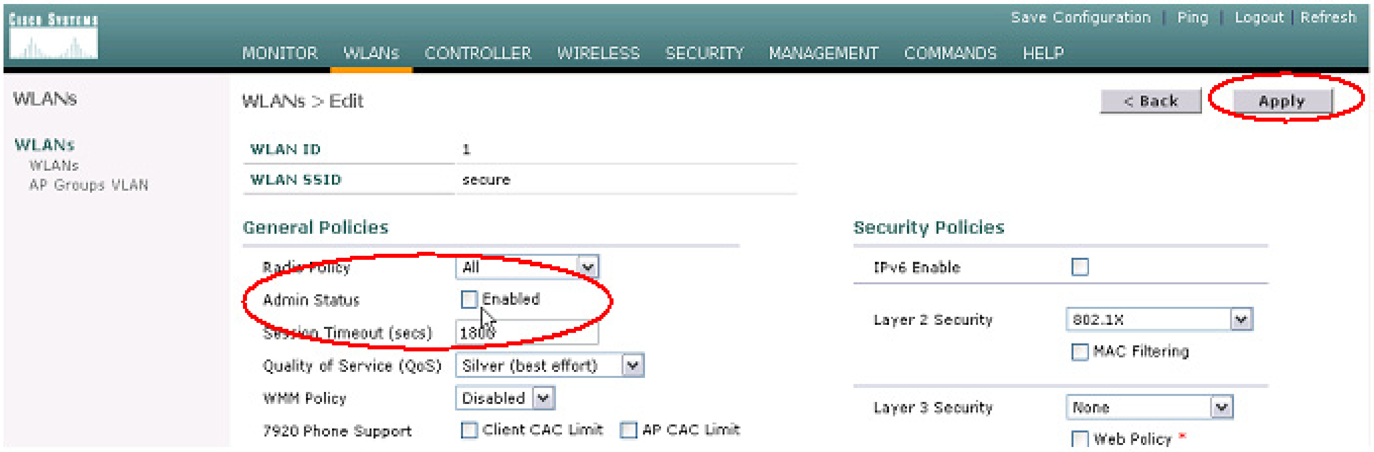
WLANs

| WLAN ID | WLAN SSID | Admin Status | Security Policies | | | |
|---|---|---|---|---|---|---|
| 1 | secure | Enabled | 802.1X | Edit | Remove | Mobility Anchors |
| 2 | Open | Enabled | Web-Passthrough | Edit | Remove | Mobility Anchors |

* WLAN IDs 9-16 will not be pushed to 1130,1200 and 1240 AP models.

**Step 2** Disable the wireless LANs assigned to the interface. Click **Edit** in the WLAN row (see Figure 47). Uncheck the **Admin Status Enabled** box and then click **Apply** (see Figure 48):

***Figure 48 WLAN Disable: Apply***



WLANs > Edit

| | |
|---|---|
| WLAN ID | 1 |
| WLAN SSID | secure |

General Policies

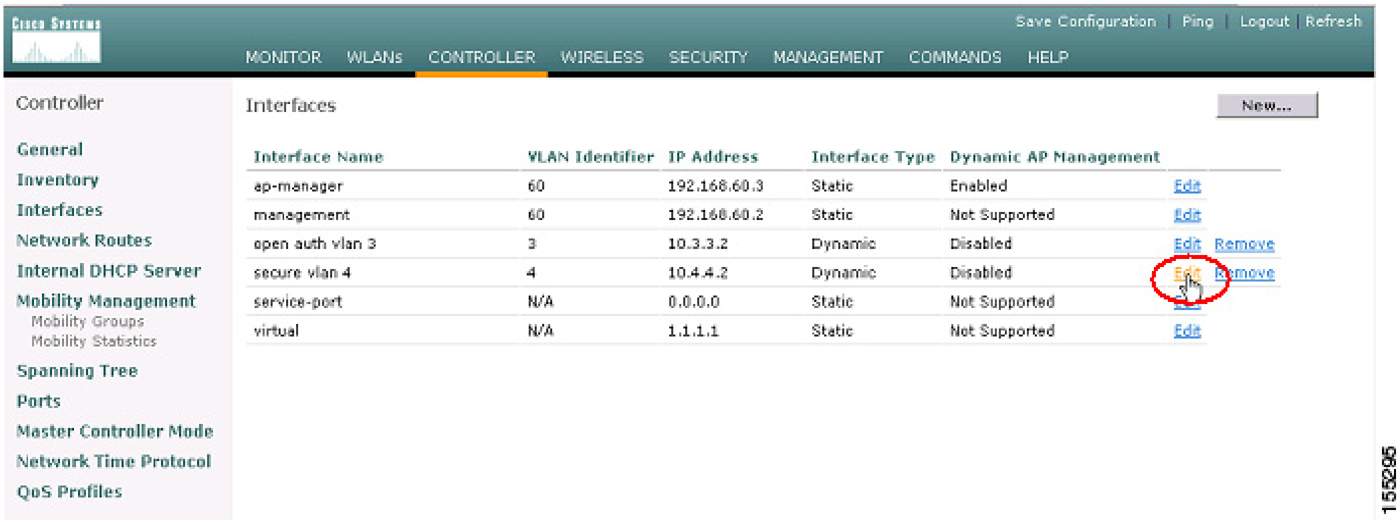
| | |
|---|---|
| Radio Policy | All |
| Admin Status | □ Enabled |
| Session Timeout (secs) | 1800 |
| Quality of Service (QoS) | Silver (best effort) |
| WMM Policy | Disabled |
| 7920 Phone Support | □ Client CAC Limit □ AP CAC Limit |

Security Policies

| | |
|---|---|
| IPv6 Enable | □ |
| Layer 2 Security | 802.1X<br>□ MAC Filtering |
| Layer 3 Security | None<br>□ Web Policy * |

**Step 3** Navigate to the **Controller | Interfaces** screen. Select **Edit** in the appropriate interface row (see Figure 49):

*Figure 49 Dynamic Interface Editing*

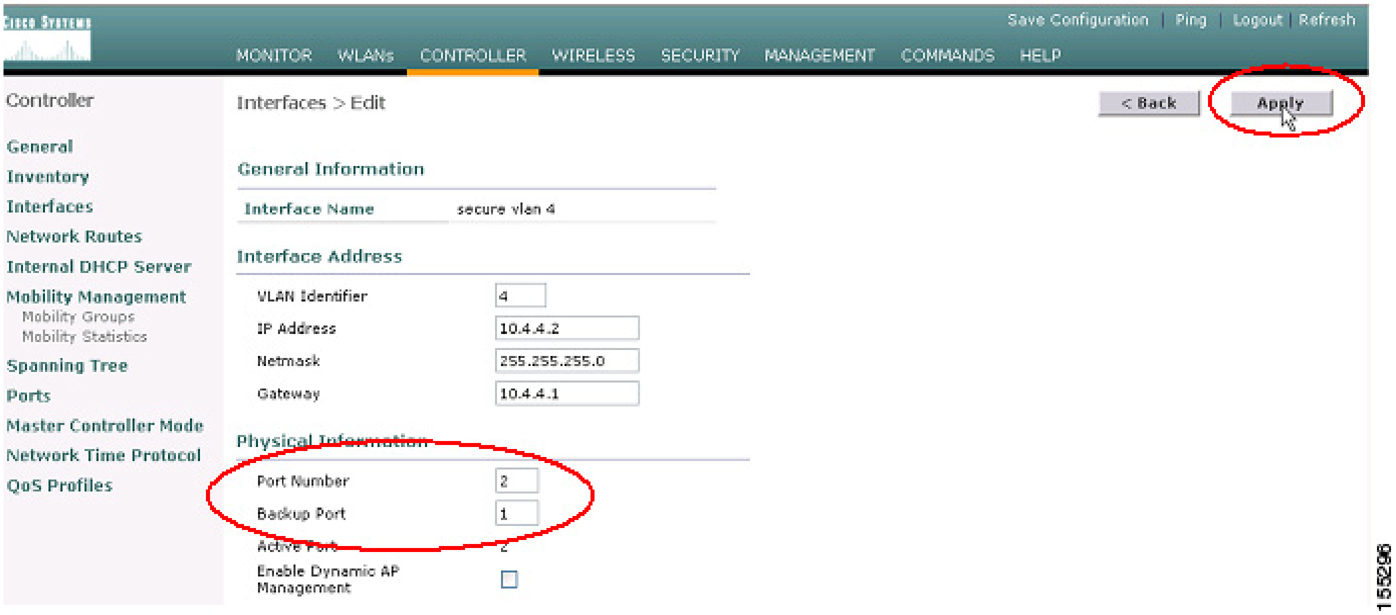


Interfaces

| Interface Name | VLAN Identifier | IP Address | Interface Type | Dynamic AP Management | |
|---|---|---|---|---|---|
| ap-manager | 60 | 192.168.60.3 | Static | Enabled | Edit |
| management | 60 | 192.168.60.2 | Static | Not Supported | Edit |
| open auth vlan 3 | 3 | 10.3.3.2 | Dynamic | Disabled | Edit Remove |
| secure vlan 4 | 4 | 10.4.4.2 | Dynamic | Disabled | Edit Remove |
| service-port | N/A | 0.0.0.0 | Static | Not Supported | Edit |
| virtual | N/A | 1.1.1.1 | Static | Not Supported | Edit |

**Step 4** Enter the primary and backup port numbers in the **Port Number** and **Backup Port** fields, and then click **Apply** (see Figure 50):

*Figure 50 Interface Port Configuration*



Interfaces > Edit

General Information

Interface Name secure vlan 4

Interface Address

VLAN Identifier 4

IP Address 10.4.4.2

Netmask 255.255.255.0

Gateway 10.4.4.1

Physical Information

Port Number 2

Backup Port 1

Active Port 2

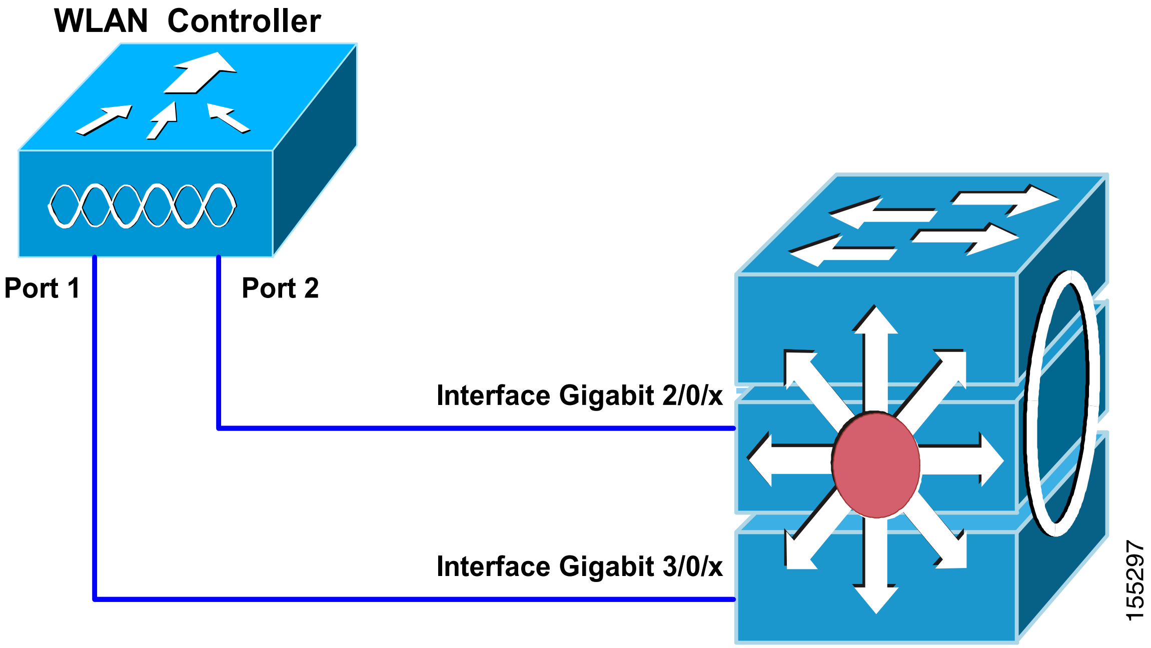
Enable Dynamic AP Management □

**Step 5** Repeat Steps **1** through **4** for each interface as necessary.

**Step 6** Re-enable the default wireless LANs by following Steps **1** and **2**, only checking the **Admin Status Enabled** box this time.

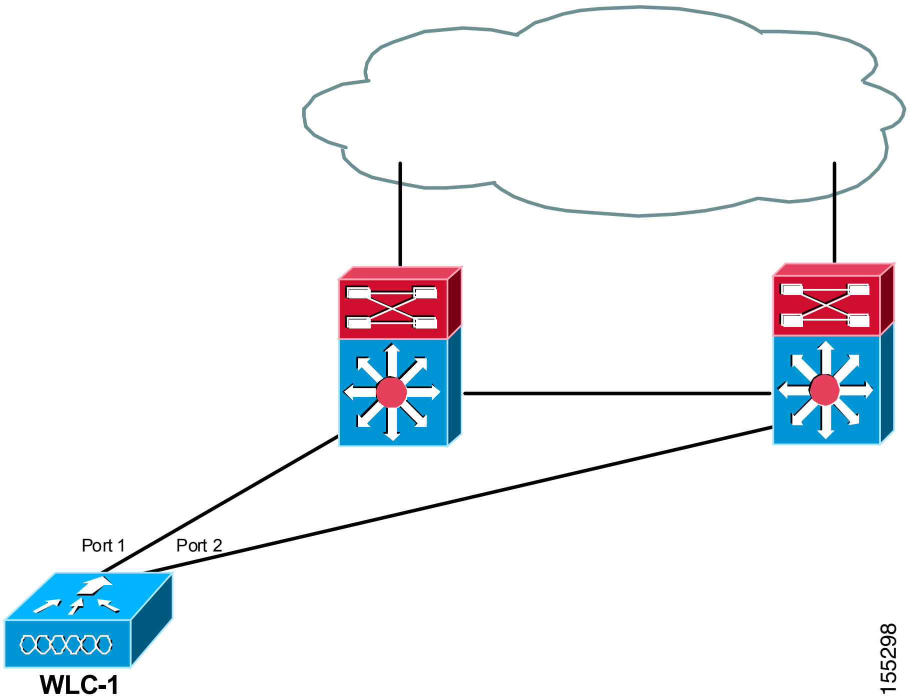
**Step 7** Typically, you want to follow common-sense best practices when configuring port redundancy. For example, suppose you are deploying the WLC in a one-armed configuration off of a Catalyst 4500, 6500, or 3750 stack. You will want to map your primary and secondary ports to different modules or switch stack members to maintain traffic flow in the event of a module or stack member failure. (See Figure 51.)

*Figure 51 Port Redundancy with Single Neighbor Switch or Switch Stack*



Now suppose you are deploying your WLC at the network distribution layer where there are redundant switches. Your primary port should be connected to one of the distribution layer switches and the secondary should be connected to the other distribution layer switch. An example of this configuration is shown in Figure 52:

*Figure 52 Port Redundancy with Redundant Neighbor Switches*



## Controller Redundancy and Access Point Load Balancing

The LWAPP protocol allows for dynamic redundancy and load balancing. For example, if you specify more than one IP address for Option 43, an access point will send LWAPP discovery requests to each of the IP addresses it receives. In the controller LWAPP discovery response, the controller embeds information on its current access point load (defined as the number of access points joined to it at the time), its access point capacity, and the number of wireless clients connected to the controller. The access point will then attempt to join the least loaded controller, defined as the controller with the greatest available access point capacity.

Furthermore, once an access point joins a controller, it learns the IP addresses of the other controllers in the Mobility Group from its joined WLC. Subsequently, the access point will send LWAPP Primary Discovery Requests to each of the WLCs in the Mobility Group. The WLCs respond with a Primary Discovery Response[1] to the access point. The Primary Discovery Response includes information about the WLC type, total capacity, and current access point load. As long as the WLC has the "AP Fallback" parameter enabled, the access point may decide to change over to a less loaded WLC.

This dynamic load-balancing can be a basis for a dynamic controller redundancy scheme. Access points send an LWAPP heartbeat to their WLC every 30 seconds. The WLC responds to the LWAPP heartbeats from the access points in the form of unicast heartbeat acknowledgements. When an access point misses a heartbeat acknowledgement, it resends up to five heartbeat messages at 1-second intervals. If no acknowledgement is received after the five resends, the access point releases and renews its IP address and initiates a new WLC hunting and discovery process to find a new controller. This is how the system supports dynamic WLC redundancy.

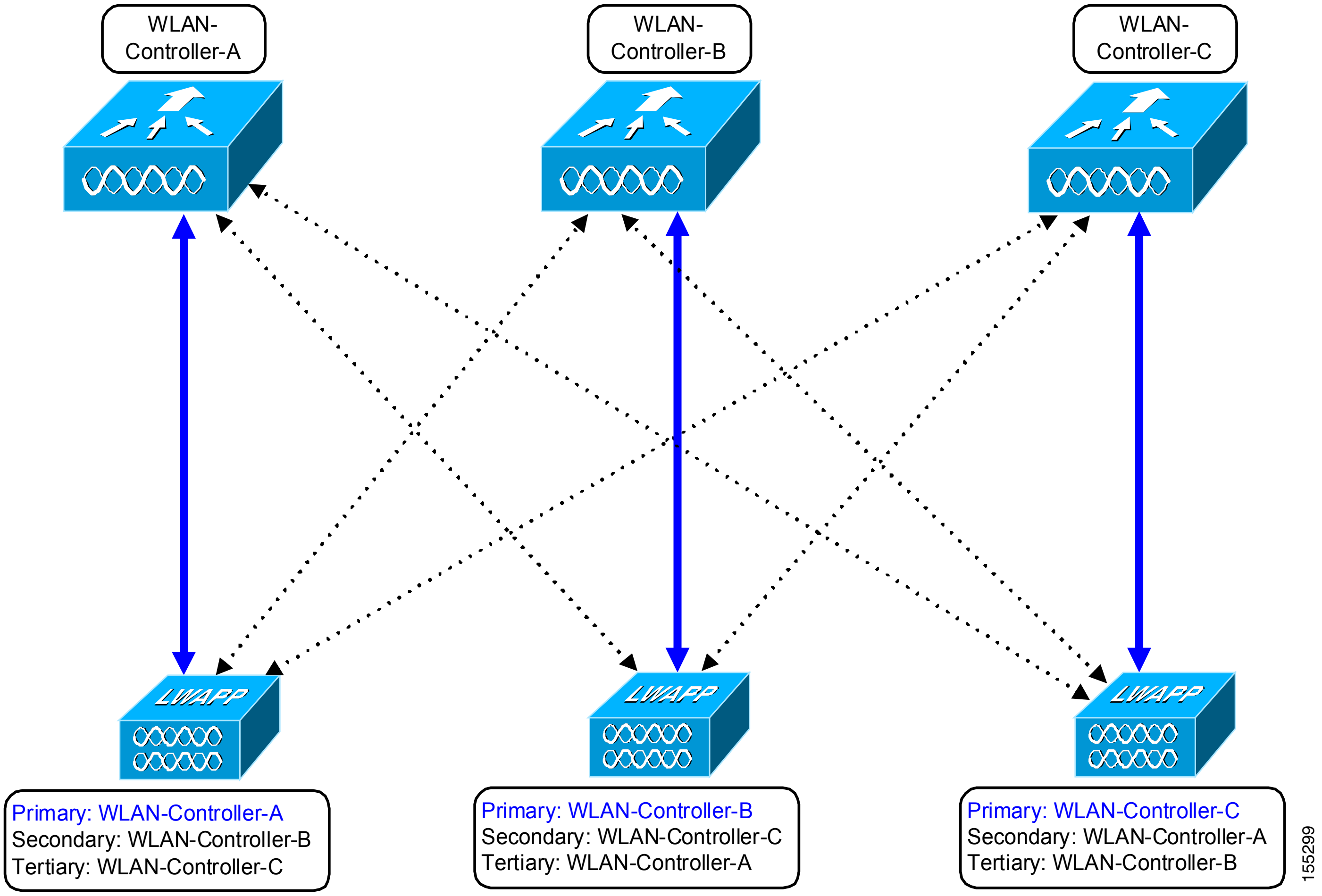
This useful algorithm helps dynamically balance the access point load across the mobility group. However, it is important to consider how it could also have some unintended consequences. For example, suppose we have configured two controllers management interfaces in Option 43 in the DHCP scope. When we deploy our first access point, it may join one controller. Now when we deploy our second access point, it may join the second controller. The next access point will join one of the two controllers; the fourth access point may join the other controller and so on. By the time we've completed the access point deployment for the area, some of the access points will have joined one controller and the other access points will have joined the other controller. The access points will likely be joined to controllers in a salt-and-pepper fashion, where access points are joined to the controllers in no particular order or sequence. This may be perfectly acceptable if there aren't many roaming clients. But consider the impact on the network if many clients are roaming. There will be many inter-controller roaming events that can have a potential impact on aggregate network performance. Secondly, the traffic patterns from wireless clients will be unpredictable making it difficult to implement stateful security mechanisms in the infrastructure and take advantage of some other Cisco switching features. Furthermore, it makes for additional difficulties when you are ready to apply access point templates and add access points to maps in the WCS.

Due to some of these characteristics of dynamic load balancing and redundancy, many customers choose to override the dynamic behavior of LWAPP by assigning access points to specific controllers to balance the load by assigning access points a primary, secondary, and/or tertiary controller. By doing this, WLC redundancy behavior is deterministic. Furthermore, it has an additional benefit that when an access point has a primary, secondary and/or tertiary WLC configured, the access point failover occurs more quickly.

[1] The LWAPP Primary Discovery Request and Primary Discovery Response are LWAPP Control Types 0x20 and 0x21 respectively. These should not be confused with the LWAPP Discovery Request (Type 0x01) and LWAPP Discovery Response (0x02).

Figure 53 illustrates deterministic WLC redundancy:

*Figure 53 Deterministic Redundancy with Primary, Secondary, and Tertiary WLCs*


WLAN-Controller-A
WLAN-Controller-B
WLAN-Controller-C
LWAPP
LWAPP
LWAPP
Primary: WLAN-Controller-A
Secondary: WLAN-Controller-B
Tertiary: WLAN-Controller-C
Primary: WLAN-Controller-B
Secondary: WLAN-Controller-C
Tertiary: WLAN-Controller-A
Primary: WLAN-Controller-C
Secondary: WLAN-Controller-A
Tertiary: WLAN-Controller-B
155299

When an access point declares its primary controller unreachable due to missed heartbeat acknowledgements, it will attempt to join the secondary controller. If it fails to join the secondary controller, it attempts to join the tertiary controller. If neither the primary, secondary, nor tertiary controllers are available, access points will resort to the dynamic LWAPP algorithms to connect to the least-loaded available controller.

The WLC has a configurable parameter for **AP Fallback**. When the WLC AP Fallback option is enabled, access points will return to their primary controllers after a failover event when the primary controller comes back online. This feature is enabled by default and many administrators choose to leave the AP Fallback default value in place.

However, when an access point falls back to its primary controller, there will be a brief window of time, usually on the order of 30 seconds, during which service to wireless clients is interrupted because the access points are re-joining the primary WLC. Also, if connectivity to the primary WLC has become unstable for some reason, the access point might end up "flapping" back and forth between a primary and the backup WLCs. Many wireless LAN administrators prefer to disable AP Fallback and move the access points back to the primary in a controlled manner during a scheduled service window.

Remember that when you engineer your WLC infrastructure for redundancy, you need to account for the extra capacity on the secondary and/or tertiary controllers in the event of a catastrophic failure.

## Configuring an Access Point's Primary, Secondary, and Tertiary Controller Using the WLC Interface

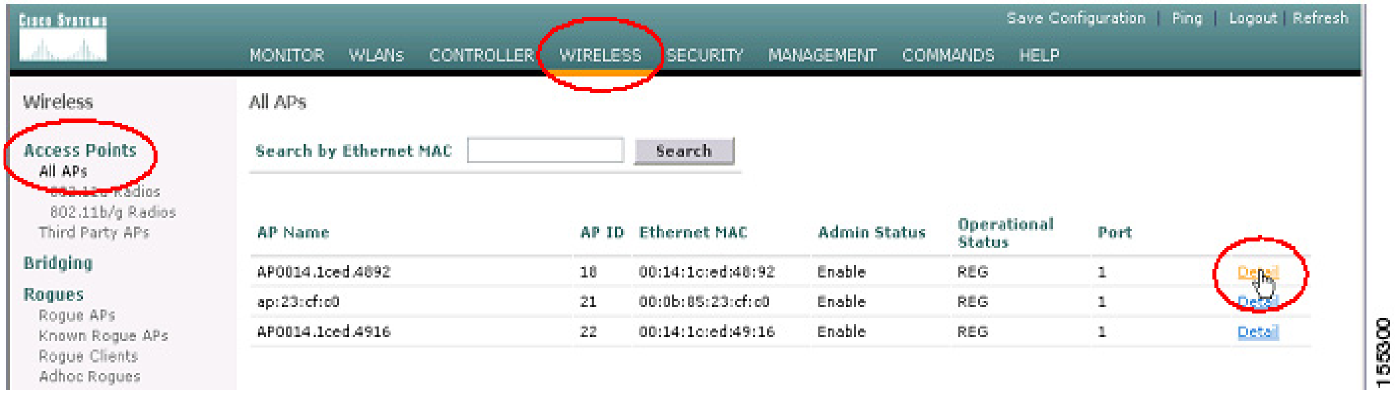
Follow these steps to configure controller redundancy through the WLC:

**Step 1** Place the primary, secondary, and tertiary controllers into a mobility group.

**Step 2** Navigate to **Wireless | Access Points | All APs.**

**Step 3** Select an AP and click **Detail** to access the access point configuration screen (see Figure 54).

*Figure 54 Configuring the Access Point's Primary, Secondary, and Tertiary Controller in the WLC GUI*



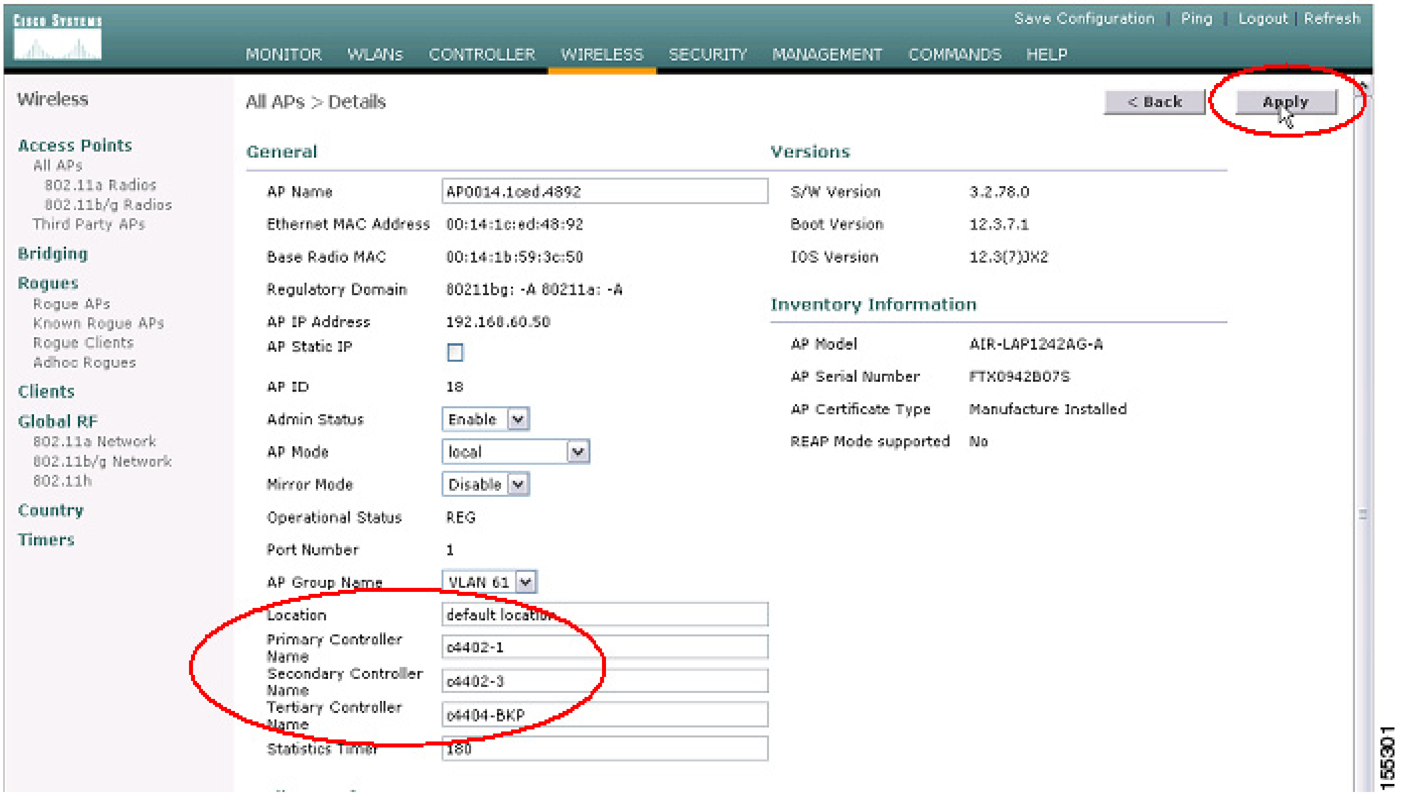
| AP Name | AP ID | Ethernet MAC | Admin Status | Operational Status | Port | |
|---|---|---|---|---|---|---|
| AP0014.1ced.4892 | 18 | 00:14:1c:ed:48:92 | Enable | REG | 1 | Detail |
| ap:23:cf:c0 | 21 | 00:0b:85:23:cf:c0 | Enable | REG | 1 | Detail |
| AP0014.1ced.4916 | 22 | 00:14:1c:ed:49:16 | Enable | REG | 1 | Detail |

**Step 4** Input the appropriate values (controller sysName) in the **Primary Controller Name**, **Secondary Controller Name**, and/or **Tertiary Controller Name** fields and then click **Apply** (see Figure 55).

(The controller name is the name that the controller is identified by within the mobility group.[1])

[1] The controller name can be retrieved via the "show sysinfo" command at the WLC CLI or in GUI in the Monitor | Summary screen in the "System Name" field. This value is case-sensitive.

*Figure 55 Configuring the Access Point's Primary, Secondary, and Tertiary Controller in the WLC GUI*



All APs > Details

General

AP Name: AP0014.1ced.4892
Ethernet MAC Address: 00:14:1c:ed:48:92
Base Radio MAC: 00:14:1b:59:3c:50
Regulatory Domain: 80211bg: -A 80211a: -A
AP IP Address: 192.168.60.50
AP Static IP: ☐
AP ID: 18
Admin Status: Enable
AP Mode: local
Mirror Mode: Disable
Operational Status: REG
Port Number: 1
AP Group Name: VLAN 61
Location: default locatio
Primary Controller Name: c4402-1
Secondary Controller Name: c4402-3
Tertiary Controller Name: c4404-BKP
Statistics Timer: 180

Versions

S/W Version: 3.2.78.0
Boot Version: 12.3.7.1
IOS Version: 12.3(7)JX2

Inventory Information

AP Model: AIR-LAP1242AG-A
AP Serial Number: FTX0942B07S
AP Certificate Type: Manufacture Installed
REAP Mode supported: No

**Step 5** Repeat Steps **2** through **4** for each access point.

Since the configurations just described must be performed on each access point, this is a laborious exercise. Fortunately, using the WCS makes this job easier.

## Configuring an Access Point's Primary, Secondary, and Tertiary Controller Using WCS

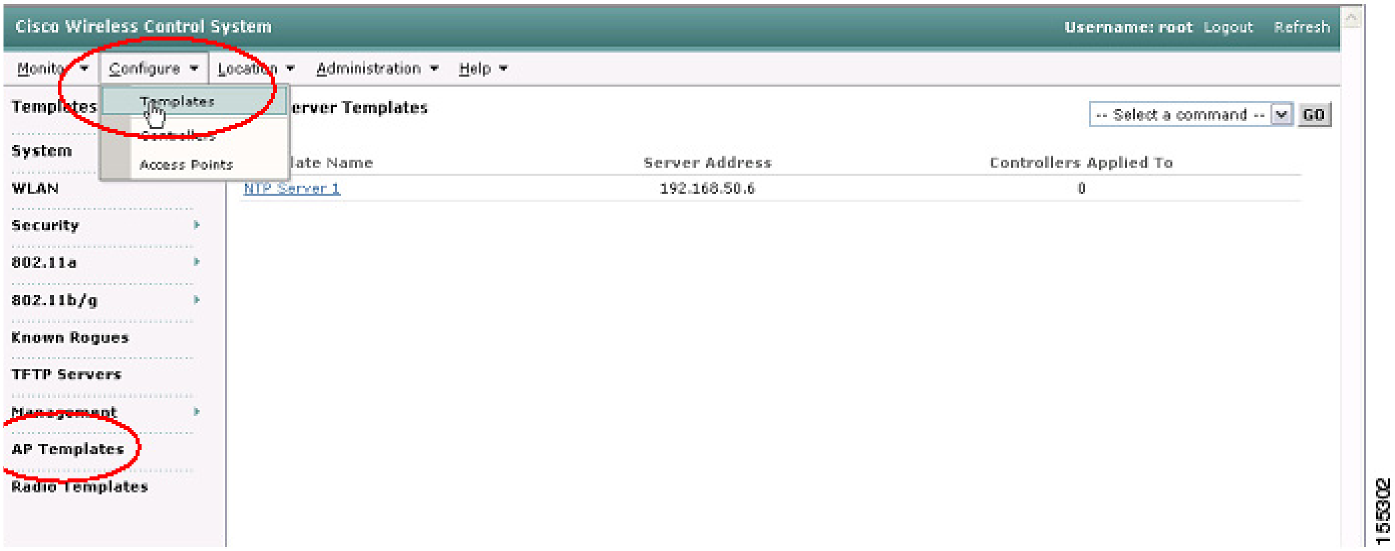
Follow these steps to configure controller redundancy using WCS:

**Step 1** Place the primary, secondary, and tertiary controllers into a mobility group.

**Step 2** Make sure to add all the controllers to WCS.

**Step 3** Navigate in the WCS to **Configure | Templates | AP Templates** (see Figure 56).

Figure 56 Configuring an Access Point's Primary, Secondary, and Tertiary Controller Using WCS



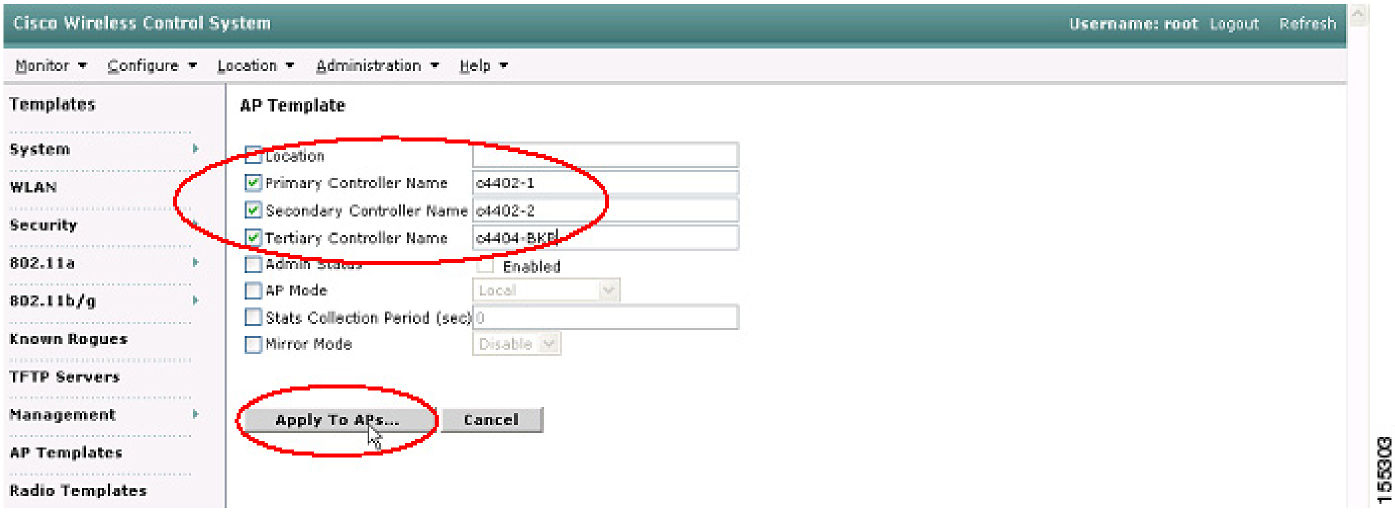
...erver Templates

| ...late Name | Server Address | Controllers Applied To |
|---|---|---|
| NTP Server 1 | 192.168.50.6 | 0 |

**Step 4** Input the appropriate values (controller sysName) in the **Primary Controller Name**, **Secondary Controller Name**, and/or **Tertiary Controller Name** fields and then click **Apply to APs** (see Figure 57).

(The controller name is the name that the controller is identified with within the mobility group.[1])

Figure 57 Configuring an Access Point's Primary, Secondary, and Tertiary Controller Using WCS



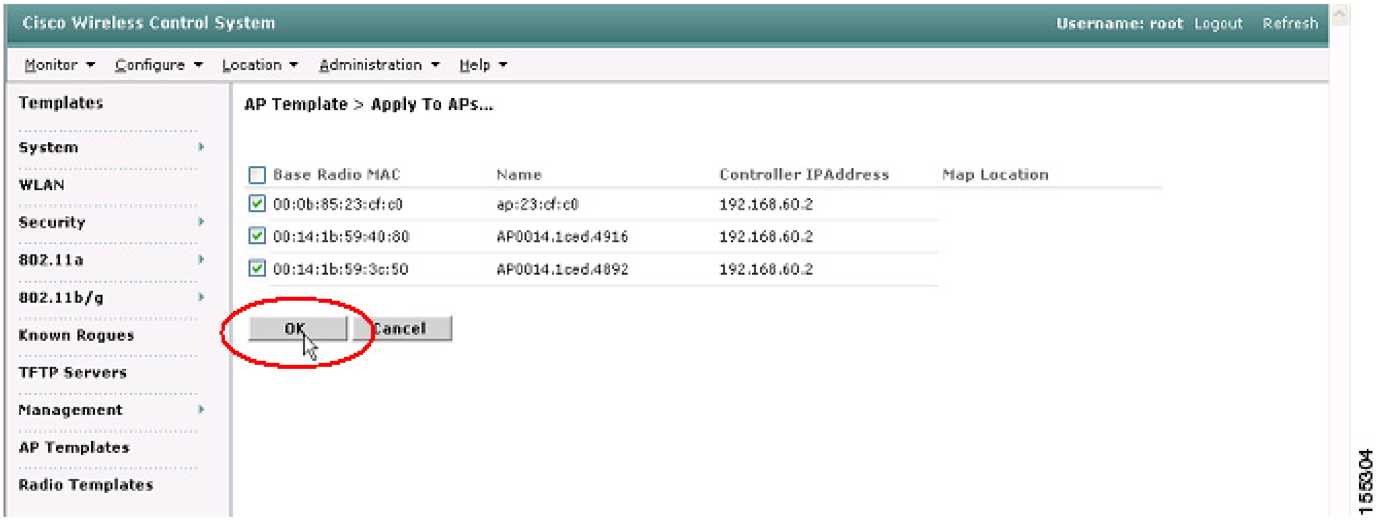
AP Template

☐ Location
☑ Primary Controller Name c4402-1
☑ Secondary Controller Name c4402-2
☑ Tertiary Controller Name c4404-BKP
☐ Admin Status ☐ Enabled
☐ AP Mode Local
☐ Stats Collection Period (sec) 0
☐ Mirror Mode Disable

**Step 5** Select all the appropriate access points in the **Apply to APs** interface and then click **OK** (see Figure 58).

[1] The controller name can be retrieved via the "show sysinfo" command at the WLC CLI or in GUI in the **Monitor | Summary** screen in the "System Name" field. This value is case-sensitive.

*Figure 58 Configuring an Access Point's Primary, Secondary, and Tertiary Controller Using WCS*



Cisco Wireless Control System — Username: root Logout Refresh

Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾

Templates

- System ▸
- WLAN
- Security ▸
- 802.11a ▸
- 802.11b/g ▸
- Known Rogues
- TFTP Servers
- Management ▸
- AP Templates
- Radio Templates

AP Template > Apply To APs...

| □ Base Radio MAC | Name | Controller IPAddress | Map Location |
|---|---|---|---|
| ☑ 00:0b:85:23:cf:c0 | ap:23:cf:c0 | 192.168.60.2 | |
| ☑ 00:14:1b:59:40:80 | AP0014.1ced.4916 | 192.168.60.2 | |
| ☑ 00:14:1b:59:3c:50 | AP0014.1ced.4892 | 192.168.60.2 | |

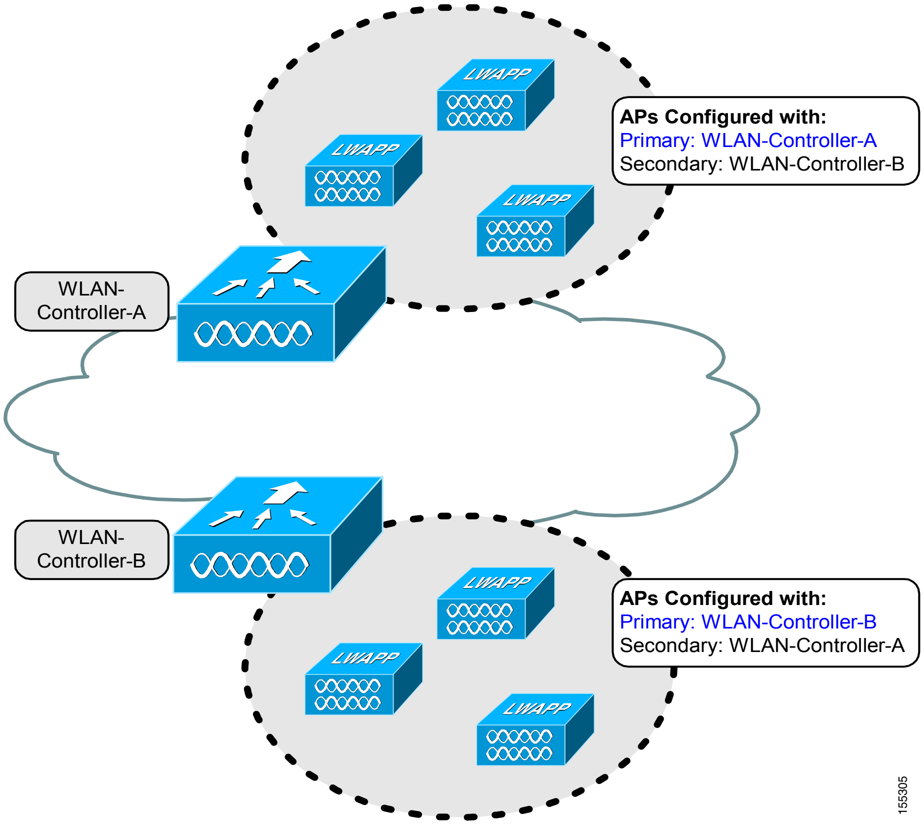
OK Cancel

155304

## Controller Redundancy Designs

The Cisco Unified Wireless Network architecture gives you flexibility in WLC redundancy options. For example, Figure 59 illustrates an "N+N" redundancy configuration:

*Figure 59 Redundancy*

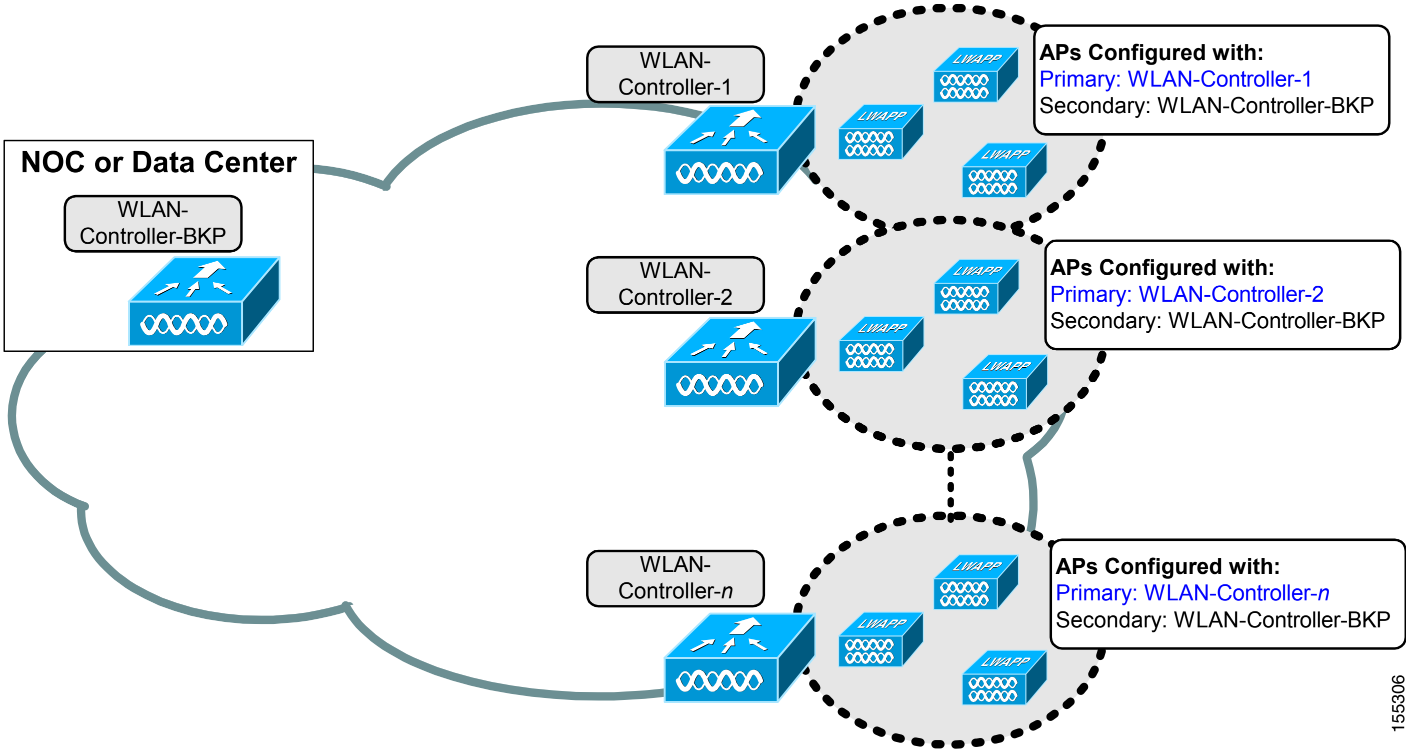

LWAPP
APs Configured with:
Primary: WLAN-Controller-A
Secondary: WLAN-Controller-B
WLAN-Controller-A
WLAN-Controller-B
APs Configured with:
Primary: WLAN-Controller-B
Secondary: WLAN-Controller-A
155305

In this configuration, there are two controllers. Some of the access points are configured with controller A as primary and controller B as secondary. The other access points are configured to use controller B as primary and controller A as secondary. In this design, you should try to load balance the access point capacity across both controllers. But you should also try to logically group access points on controllers to minimize inter-controller roaming events. For example, if you are supporting a four floor building with two redundant controllers, you might configure the access points on floors 1 and 2 to use one controller as primary and the access points on floors 3 and 4 to use the other controller as primary.

It may seem obvious, but it needs to be noted: be sure that there is enough excess capacity on each controller to handle a failover situation.

Another popular WLC redundancy option is an "N+1" configuration. This is a good option when there are many WLC controller devices and capital expenditure costs are a big consideration. Figure 60 illustrates N+1 redundancy:

***Figure 60 N+1 Redundancy***

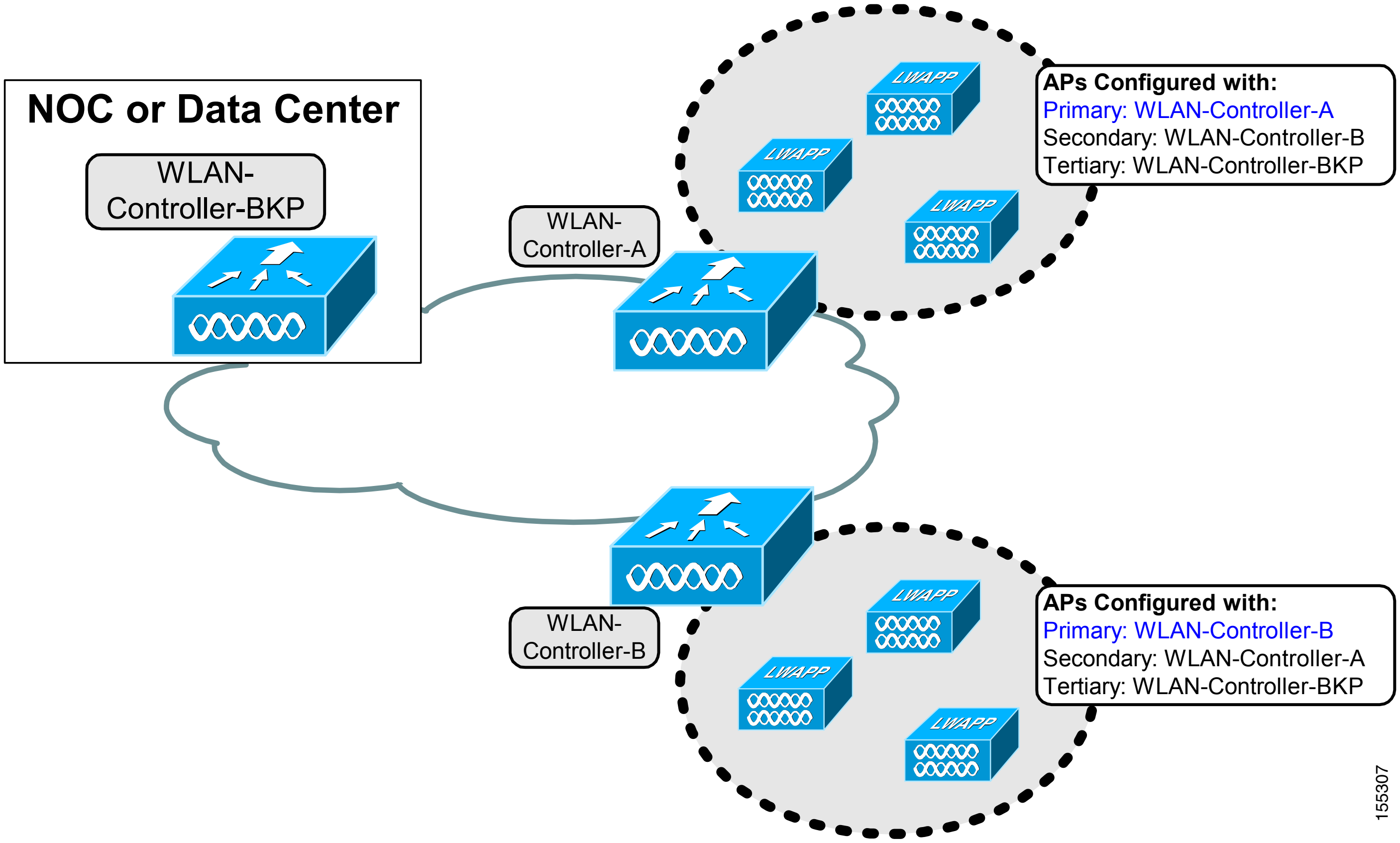

NOC or Data Center
WLAN-Controller-BKP
WLAN-Controller-1
WLAN-Controller-2
WLAN-Controller-*n*
LWAPP
APs Configured with:
Primary: WLAN-Controller-1
Secondary: WLAN-Controller-BKP
APs Configured with:
Primary: WLAN-Controller-2
Secondary: WLAN-Controller-BKP
APs Configured with:
Primary: WLAN-Controller-*n*
Secondary: WLAN-Controller-BKP
155306

In this configuration, the redundant controller is placed in a NOC or data center and acts a backup for multiple WLCs. Each access point is configured with a WLC as primary and all access points point to the #1 redundant controller as secondary.

As you can probably see, the redundant controller could become oversubscribed with access points if there are multiple primary WLC failures, which is usually unlikely. Once a WLC has reached the maximum number of joined access points, it accepts no more LWAPP Join requests. So when the backup WLC becomes oversubscribed, some access points might be stuck with no WLC. When designing an N+1 redundant solution you should assess the risks of multiple WLC failures and the consequences of an oversubscribed backup WLC.

Another redundancy option is an "N+N+1" configuration, as illustrated in Figure 61:

*Figure 61 N+N+1 Redundancy*


NOC or Data Center
WLAN-Controller-BKP
WLAN-Controller-A
WLAN-Controller-B
LWAPP
APs Configured with:
Primary: WLAN-Controller-A
Secondary: WLAN-Controller-B
Tertiary: WLAN-Controller-BKP
APs Configured with:
Primary: WLAN-Controller-B
Secondary: WLAN-Controller-A
Tertiary: WLAN-Controller-BKP
155307

In this configuration, some of the access points are configured with controller A as primary and controller B as secondary and all access points are configured to use the same backup controller as tertiary. Typically, the primary and secondary controllers are placed at the network distribution level and the "1" tertiary controller placed in a NOC or data center. Multiple distribution blocks can be configured with the same tertiary controller.

When selecting a redundancy option, you should consider the risks of WLC failure and the service level agreement (SLA) required to be maintained by your wireless LAN. The higher the SLA, the more robust of a redundancy scheme your designed solution should provide.

## Scaling the 440x WLC Beyond 48 Access Points

Cisco 440x-based WLC platforms normally support no more than 48 access points per port. This limitation applies to the 440x appliance controllers (4402-50, 4404-100) and the integrated WiSM module. There are two ways to scale beyond 48 access points:

- Use multiple AP Manager interfaces
- Use Link Aggregation (LAG)

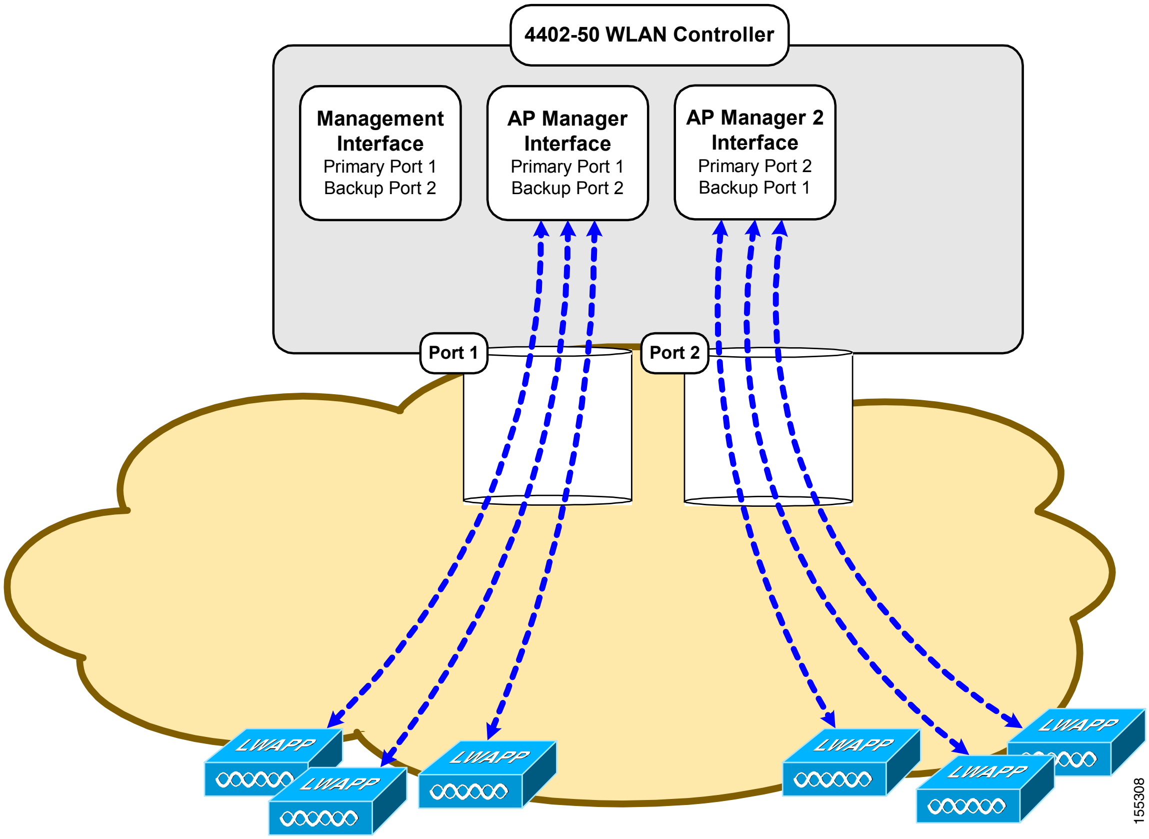
LAG is the only option for the WiSM. For the 440x appliance controllers however, there are situations where the multiple AP Manager option is preferable.

**Note** LAG is supported only on L3 LWAPP.

## Using Multiple AP Manager Interfaces

Figure 62 illustrates the use of multiple AP Managers with the 4402-50 WLC:

*Figure 62 Multiple AP Managers*



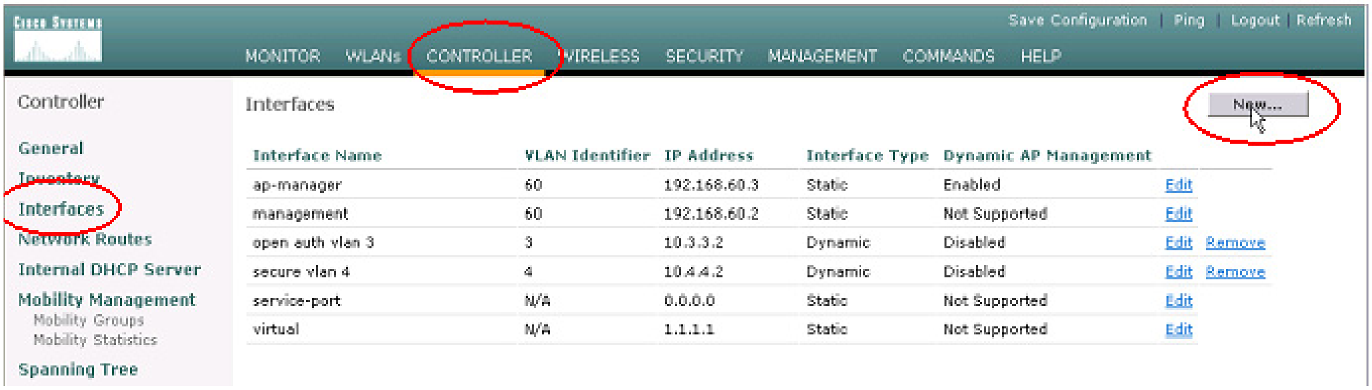
As you can see from Figure 62, two (or more) AP Manager Interfaces are created, each mapped to a different physical port. All AP Manager IP addresses are included in the LWAPP Discovery Response message from a WLC to an access point along with information on how many access points are currently using each AP Manager IP address. The access point will select an AP Manager IP address to use for the LWAPP Join Request, preferring the least loaded AP Manager interface. Therefore, the access point load is dynamically distributed across the multiple AP Manager interfaces.

Multiple AP Manager Interfaces can exist on the same VLAN and IP subnet, or they can be configured on different VLANs and IP subnets. Cisco recommends that you configure all AP Manager Interfaces on the same VLAN and IP subnet.

To configure one of more additional AP Manager Interfaces, follow these steps:

**Step 1** Navigate to **Controller | Interfaces** and click **New** (see Figure 63):

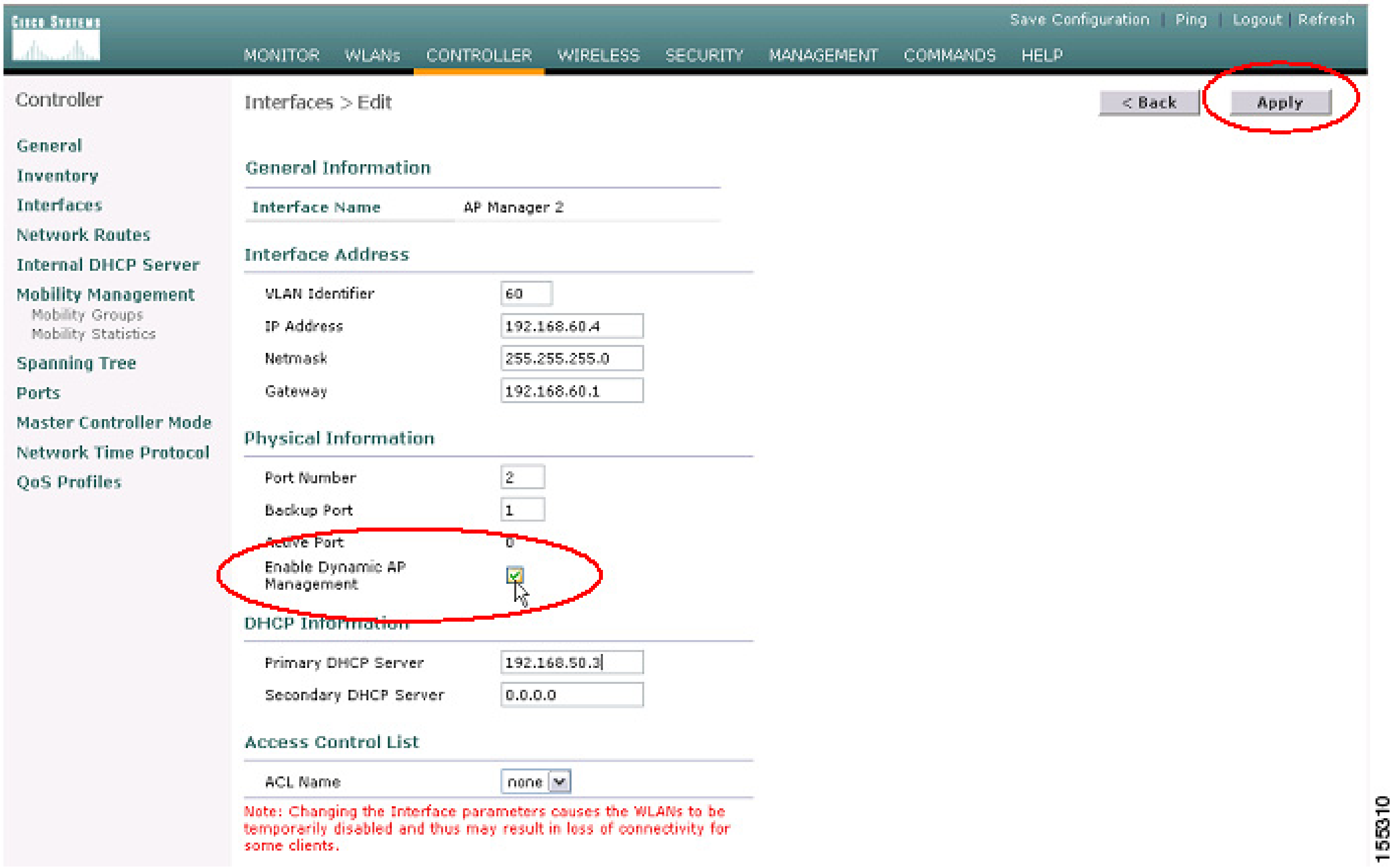
*Figure 63 AP Manager Interface Configuration*



| Interface Name | VLAN Identifier | IP Address | Interface Type | Dynamic AP Management | | |
|---|---|---|---|---|---|---|
| ap-manager | 60 | 192.168.60.3 | Static | Enabled | Edit | |
| management | 60 | 192.168.60.2 | Static | Not Supported | Edit | |
| open auth vlan 3 | 3 | 10.3.3.2 | Dynamic | Disabled | Edit | Remove |
| secure vlan 4 | 4 | 10.4.4.2 | Dynamic | Disabled | Edit | Remove |
| service-port | N/A | 0.0.0.0 | Static | Not Supported | Edit | |
| virtual | N/A | 1.1.1.1 | Static | Not Supported | Edit | |

**Step 2** Enter the appropriate interface parameters. You would usually want to just clone the static AP Manager configuration, except of course, the IP Address and the primary and backup port configurations. To make the interface an AP Manager Interface, check the **Enable Dynamic AP Management** check box and then click **Apply** (Figure 64).

*Figure 64 AP Manager Interface Configuration*



Interfaces > Edit

General Information

| | |
|---|---|
| Interface Name | AP Manager 2 |

Interface Address

| | |
|---|---|
| VLAN Identifier | 60 |
| IP Address | 192.168.60.4 |
| Netmask | 255.255.255.0 |
| Gateway | 192.168.60.1 |

Physical Information

| | |
|---|---|
| Port Number | 2 |
| Backup Port | 1 |
| Active Port | 0 |
| Enable Dynamic AP Management | ☑ |

DHCP Information

| | |
|---|---|
| Primary DHCP Server | 192.168.50.3 |
| Secondary DHCP Server | 0.0.0.0 |

Access Control List

| | |
|---|---|
| ACL Name | none |

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

**Step 3** Repeat Steps **1** and **2** for each desired AP Manager interface.

It's important to consider how multiple AP Managers impacts your port and WLC redundancy engineering. Let's consider first the 4402-50 WLC. This device supports a maximum of 50 access points and has 2 ports. So obviously, to support the maximum number of access points, you need to create two AP Manager Interfaces. A problem arises, though, if you want to support port redundancy. Look again at Figure 62.

The static AP Manager is assigned port 1 as primary port and port 2 as secondary. The second AP Manager interface is assigned port 2 as primary and port 1 as secondary. If either port fails, though, a situation arises where the WLC is trying to support 50 access points on a port that supports only 48 access points. Two access points will be unable to communicate with the WLC and will be forced to look for an alternate WLC. You must take this into consideration when engineering redundancy.

The 4404-100 supports up to 100 access points and has 4 ports. If we want to support a maximum number of access points, we need three (or more) AP Manager Interfaces. Figure 65 represents one option, which is to configure three AP Manager Interfaces, each with a unique primary port and sharing the same backup port. In the event of a single primary port failure, all access points are able to communicate with the WLC using the backup port. However, if more than one primary port fails, there is an "oversubscription" problem with the backup port. You must take this into consideration when engineering redundancy.

*Figure 65 4404-100 with Three Access Point Managers*

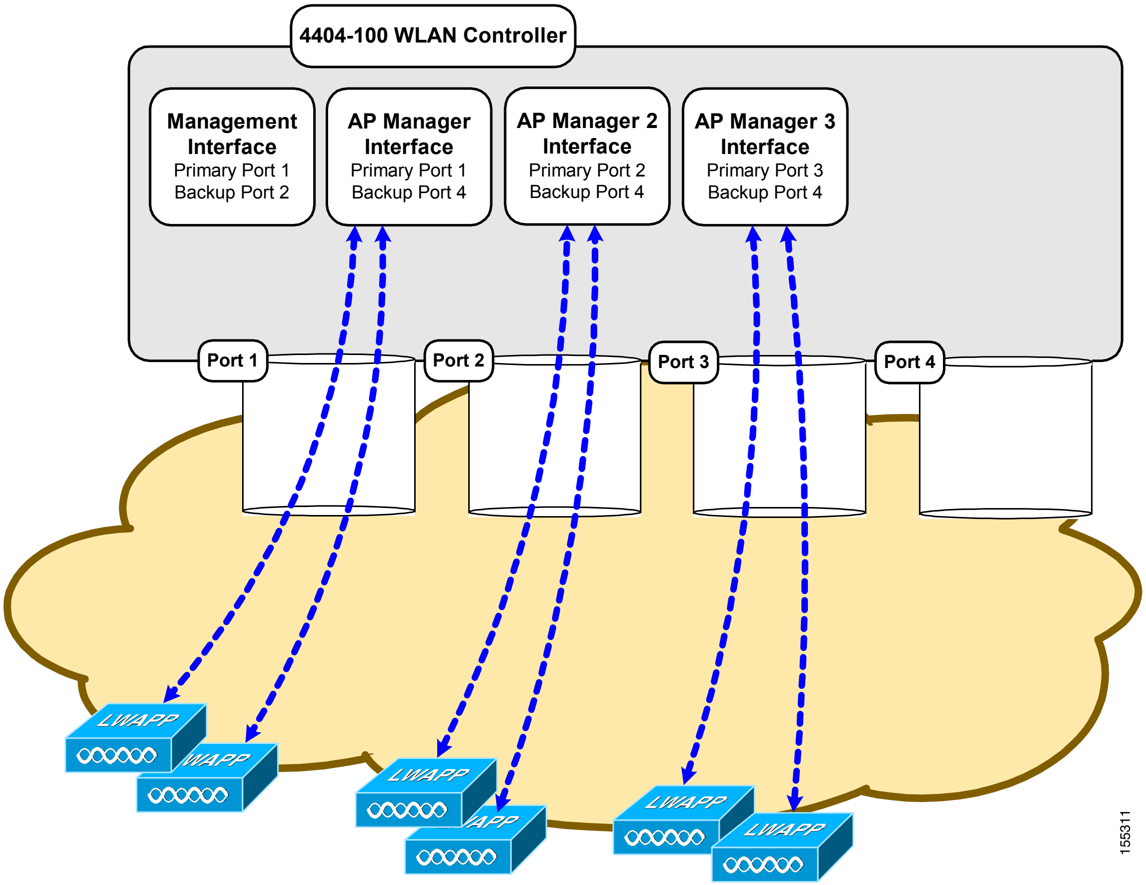
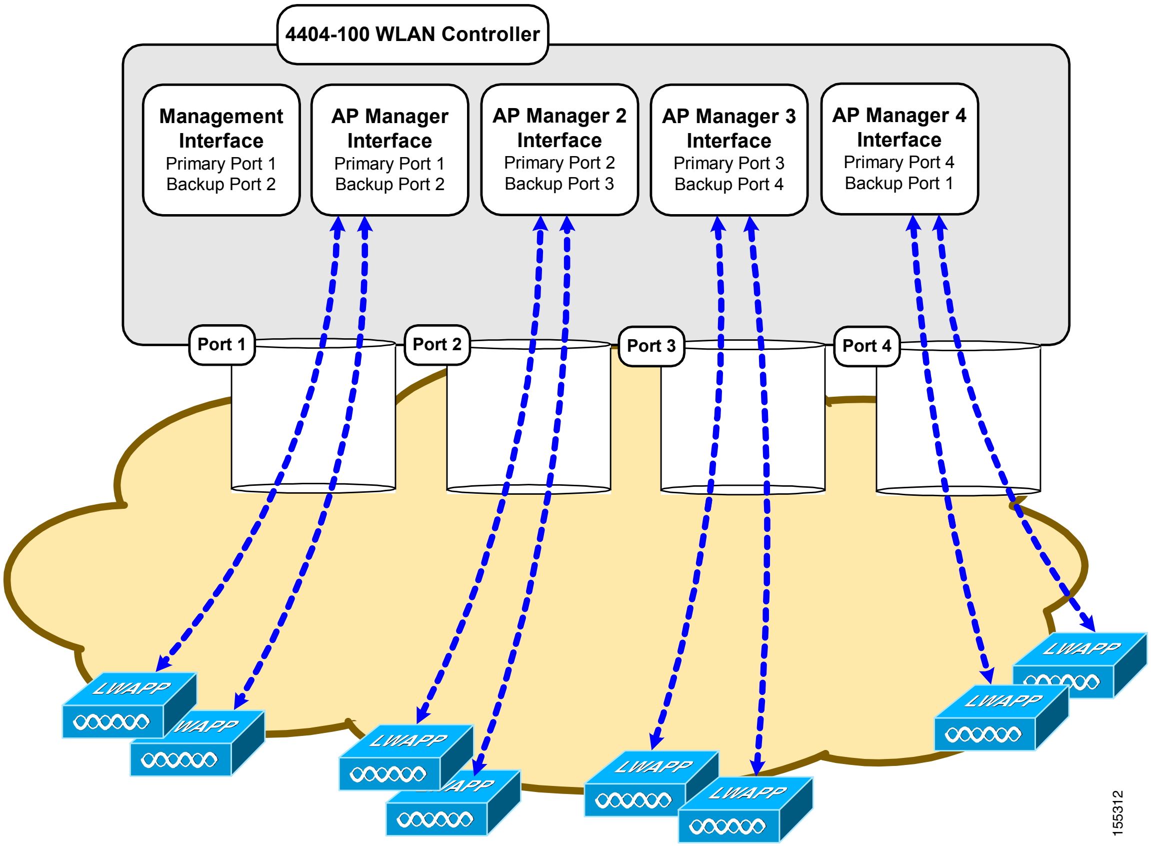


Figure 66 illustrates the use of four AP Manager Interfaces to support 100 access points. Each has a unique primary port, but each port is also a backup port for one of the AP Manager interfaces.

*Figure 66 4404-100 with Four Access Point Managers*



This configuration has the advantage of load-balancing all 100 access points evenly across all 4 ports; each AP Manager and port combination will be supporting 25 access points. But in the event a primary port goes down, the WLC will be trying to support 50 access points on a port that supports 48 access points. So two access points will be unable to communicate with the WLC and will be forced to look for an alternate WLC. You must take this into consideration when engineering redundancy.

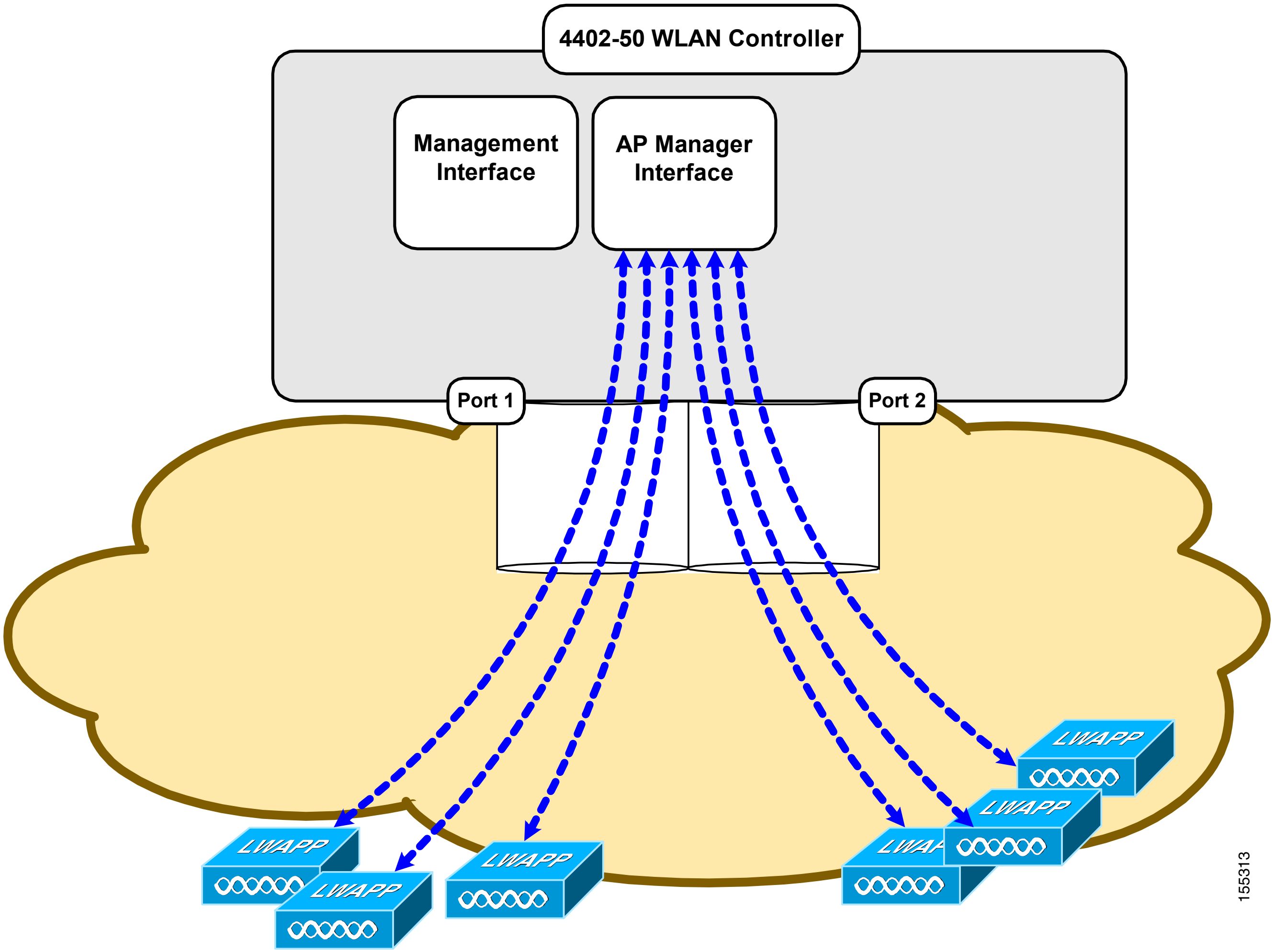
## Using Link Aggregation (LAG)

An alternative to using multiple AP Managers is to use Link Aggregation (LAG). LAG bundles all of the ports (excluding the service port) on a WLC into a single 802.3ad port channel. The system load balances access points transparently to the user. When LAG is implemented, only one AP Manager Interface is required.

**Note** LAG operates only with Layer 3 LWAPP.

Figure 67 illustrates LAG:

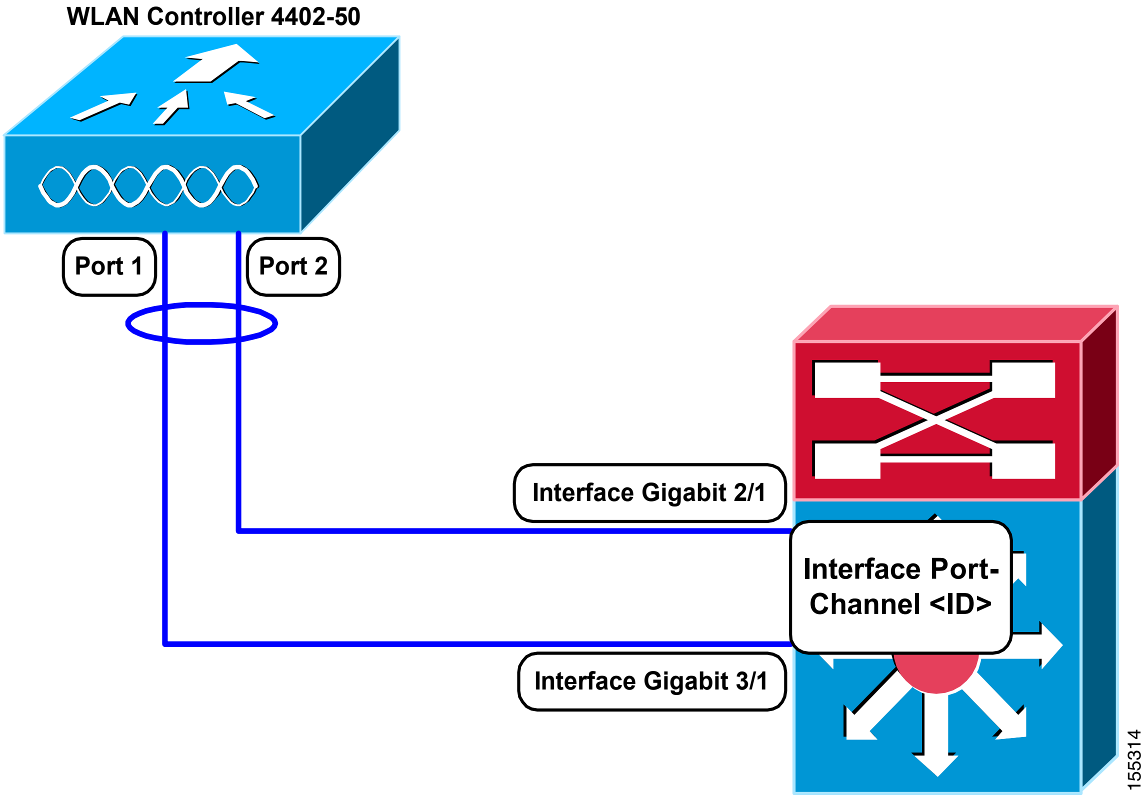
*Figure 67 Link Aggregation*



LAG handles port redundancy dynamically. You cannot configure primary and backup ports when LAG is enabled. The 48 access point per port limitation does not apply when LAG is enabled.

A common practice when configuring bundled ports is span modules with your port channel when you connect to a modular switch like a Catalyst 6500. This provides protection in the case of a module failure. Figure 68 illustrates just such a scenario where a 4402-50 is connected to a Catalyst 6500 with Gigabit modules in slots 2 and 3. The 4402-50's port 1 is connected to Gigabit interface 2/1 and the 4402-50's port 2 is connected to Gigabit interface 3/1 on the Catalyst 6500. On the Catalyst switch, the two interfaces are assigned to the same channel group.

*Figure 68 Link Aggregation with Catalyst 6500 Neighbor Switch*



The current WLC platform supports only 1 LAG group per controller. So when LAG is enabled, all the physical ports, excluding the service port, are included in the bundle. This means you cannot connect a WLC in LAG mode to more than one neighbor device.

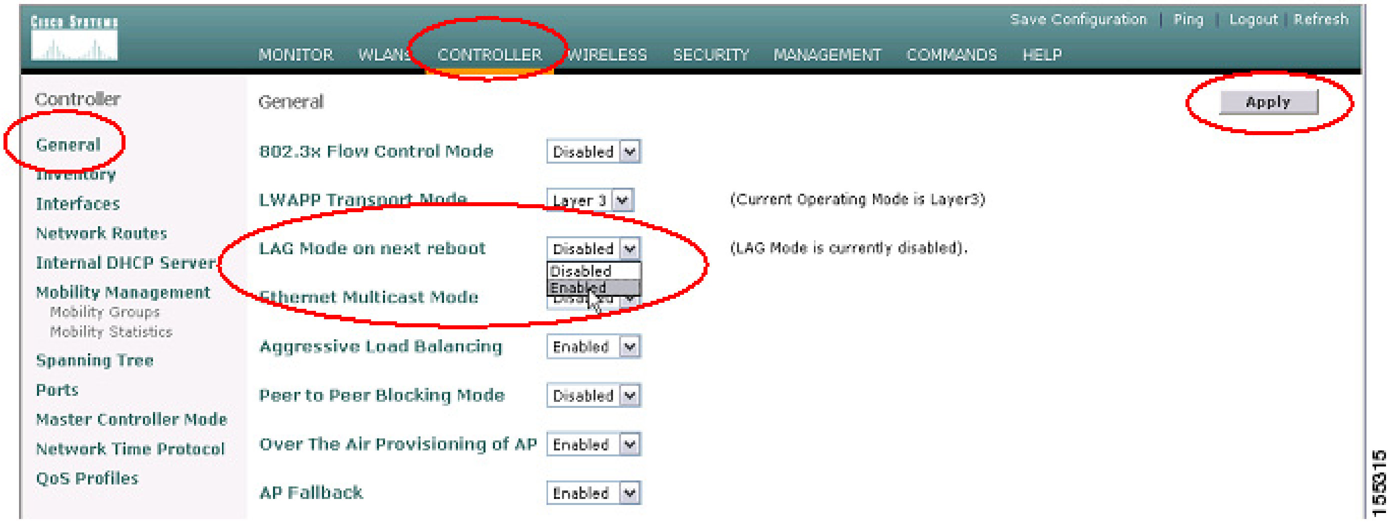
You can configure a 440x WLC to use LAG when you run the WLC setup script.

If you want to configure LAG mode after the WLC is already running, follow these steps:

**Step 1** Navigate to the **Controller | General interface** (see Figure 69).

**Step 2** Change the **LAG Mode on next reboot** parameter to **Enabled** (see Figure 69).

*Figure 69 WLC LAG Configuration*



General

802.3x Flow Control Mode: Disabled

LWAPP Transport Mode: Layer 3 (Current Operating Mode is Layer3)

LAG Mode on next reboot: Disabled (LAG Mode is currently disabled).

Disabled
Enabled

Ethernet Multicast Mode: Disabled

Aggressive Load Balancing: Enabled

Peer to Peer Blocking Mode: Disabled

Over The Air Provisioning of AP: Enabled

AP Fallback: Enabled

**Step 3** Reboot the WLC.

Each neighbor port that the WLC is connected to should be configured as follows:

```
interface GigabitEthernet <interface id>
    switchport
    channel-group <id> mode on
    no shutdown
```

Configure the port-channel on the neighbor switch as follows:

```
interface port-channel <id>
   switchport
   switchport trunk encapsulation dot1q
   switchport trunk native vlan <native vlan id>
   switchport trunk allowed vlan <allowed vlans>
   switchport mode trunk
   no shutdown
```

# IP Addressing Considerations

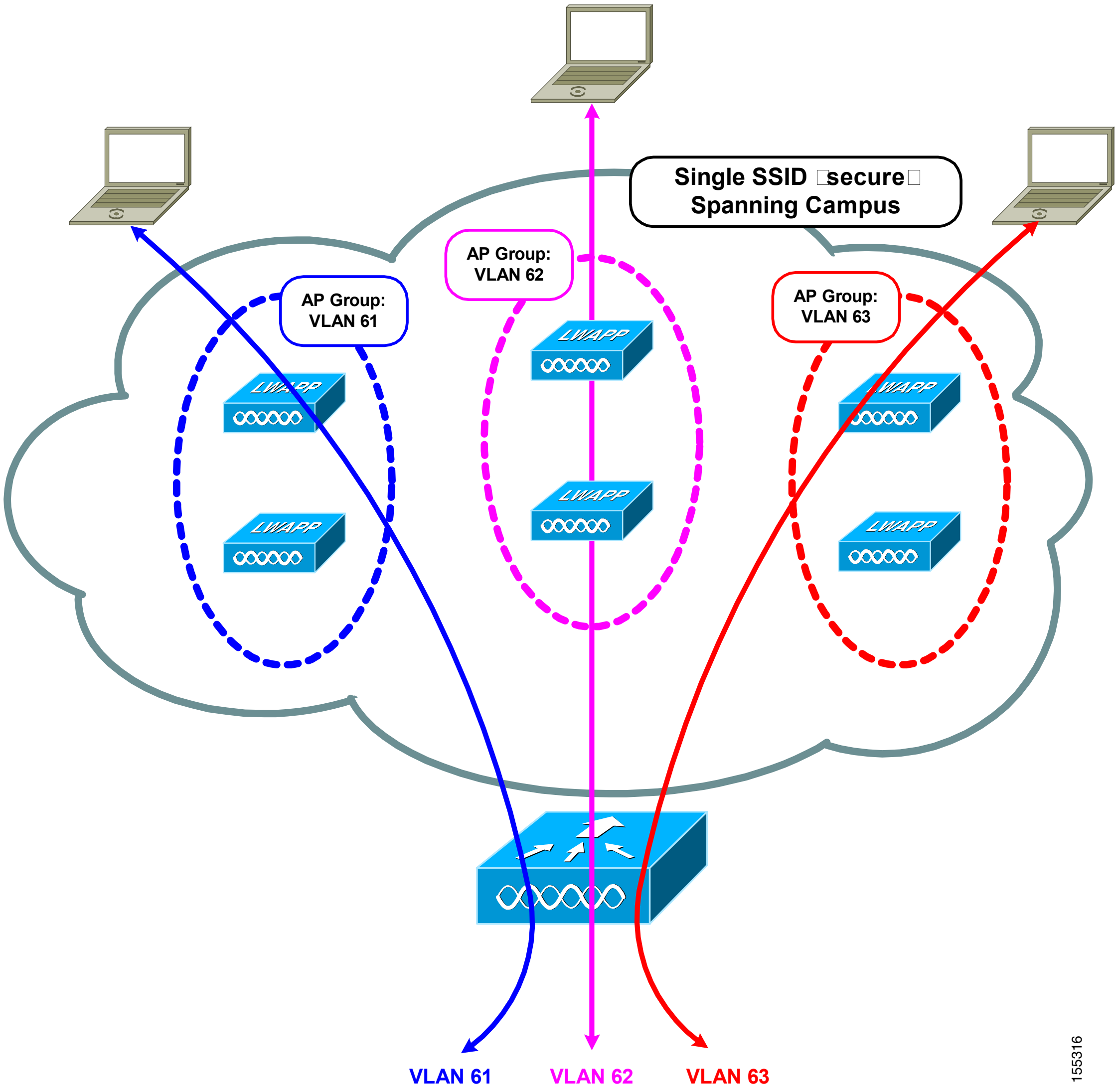
Let's review how IP addresses are assigned to wireless clients. Remember that a wireless client gets an IP address on the same IP network as the wireless LAN's assigned interface. You need to be sure to allot enough address space to support your users. User network IP address allocation should be calculated based on worst-case scenarios, and even then, it may make sense to allow for extra IP addresses.

For example, if you have 50 access points joined to the WLC and you're operating on a worst-case assumption of 20 simultaneous users per access point for the wireless LAN, you need to allocate enough IP addresses for 1000 users (50 access points * 20 users). So you would, at a minimum, select an IP subnet with a /22 subnet mask, which would yield 1022 total usable IP addresses. Once you subtract out the routed interfaces and the WLC interface from the 1022 addresses, you have a buffer (beyond the 1000 users) of only about 15 IP addresses. If there's an unexpectedly high number of users you could run out of IP addresses for your wireless clients. Therefore, you might choose to allocate a /21 IP subnet instead. Of course, a /21 subnet mask yields 2046 usable IP addresses so there could be a large number of unused IP addresses that might be considered "wasted." You'll need to select an IP address space that best meets the needs of your network.

## Access Points Groups and Site-Specific VLANs

In a default deployment, a wireless LAN is mapped to a single interface per WLC. Consider a deployment scenario, where you have a 4404-100 WLC supporting the maximum number of access points, which is 100. Now, let's consider a near-worst-case scenario with 25 users associated to each access point. In the default configuration then, you have 2500 users on the same VLAN. This may not be a problem since LWAPP is an overlay architecture; there's no spanning tree that has to span all 100 access points. However there could be broadcast or multicast intensive applications running on the wireless LAN end-clients. Also, you may want to distribute the end-client load across multiple interfaces in the infrastructure. To create smaller user domains, you should make use of the AP Groups feature and create Site Specific VLANs. Figure 70 illustrates the AP Groups and Site Specific VLAN concept:

*Figure 70 AP Groups and Site Specific VLANs*



In Figure 70, there are three dynamic interfaces configured, mapping to three Site Specific VLANs: VLANs 61, 62, and 63. These Site Specific VLANs apply to the secure SSID for normal corporate users. A corporate user associating to the secure SSID on an access point in the AP Group corresponding to VLAN 61 will get an IP address on VLAN 61's IP subnet. A corporate user associating to the secure

SSID on an access point in the AP Group corresponding to VLAN 62 will get an IP address on VLAN 62's IP subnet. A corporate user associating to the secure SSID on an access point in the AP Group corresponding to VLAN 63 will get an IP address on VLAN 63's IP subnet. Roaming between Site Specific VLANs is treated internally by the WLC as a Layer 3 roaming event, so the wireless LAN client will maintain their original IP address.

There are three tasks to configure the AP Groups feature to support Site Specific VLANs. The tasks are:

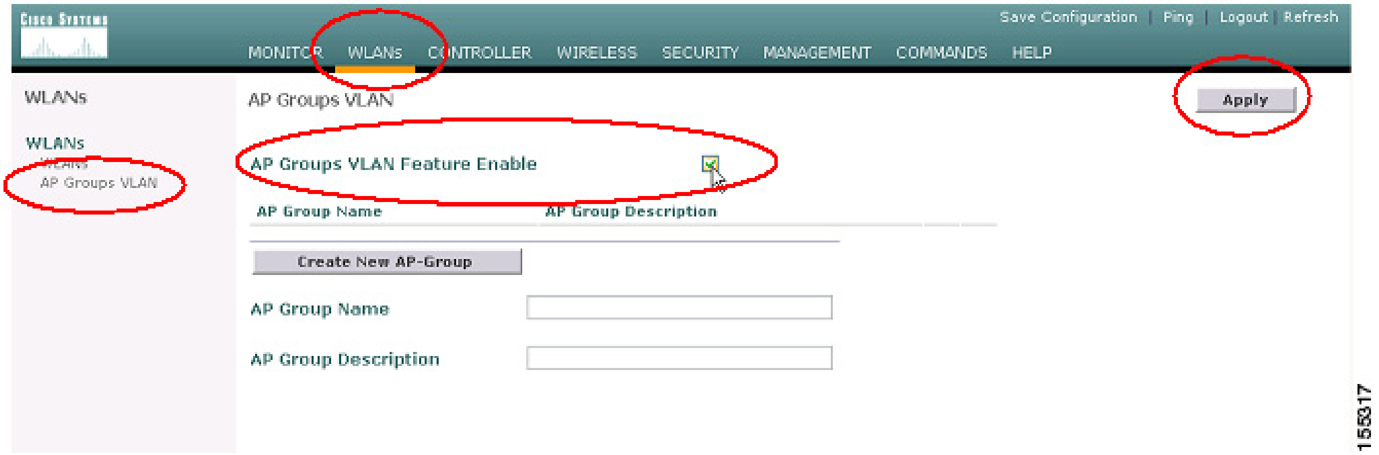
1. Configure the appropriate dynamic interfaces and map them to the desired VLANs.
2. Create the AP Groups.
3. Assign access points to the appropriate AP Group.

The instructions for creating dynamic interfaces have been previously covered. You'll just need to create a dynamic VLAN for each desired AP Group. For example, if you were implementing the network in Figure 70, you would create dynamic interfaces for VLANs 61, 62, and 63 on the WLC.

Once all the access points have been joined to the WLC, you create AP Groups and assign each group one or more wireless LANs and an interface mapping for each wireless LAN. To create an AP Group, follow these steps:

**Step 1** Navigate to **WLAN | WLANs | AP Groups VLAN** in the WLC (see Figure 71).

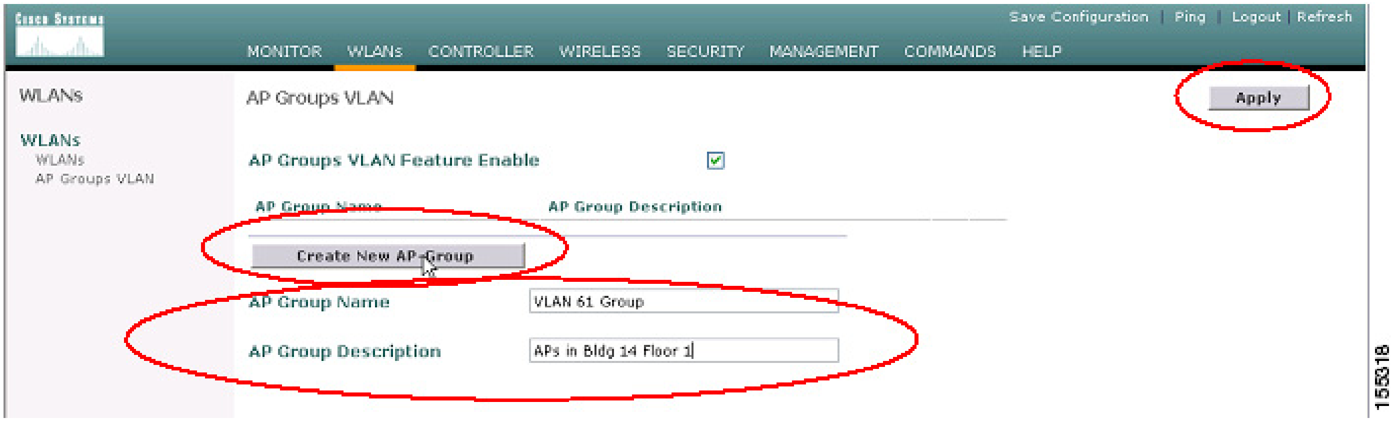
*Figure 71 AP Groups Configuration*



**Step 2** Check the **AP Groups VLAN Feature Enable** box and then click **Apply**. (See Figure 71.)

**Step 3** Enter an **AP Group Name** and **AP Group Description** in the appropriate fields and then click **Create New AP-Group**. (See Figure 72.)

*Figure 72 AP Groups Configuration*



AP Groups VLAN

AP Groups VLAN Feature Enable ☑

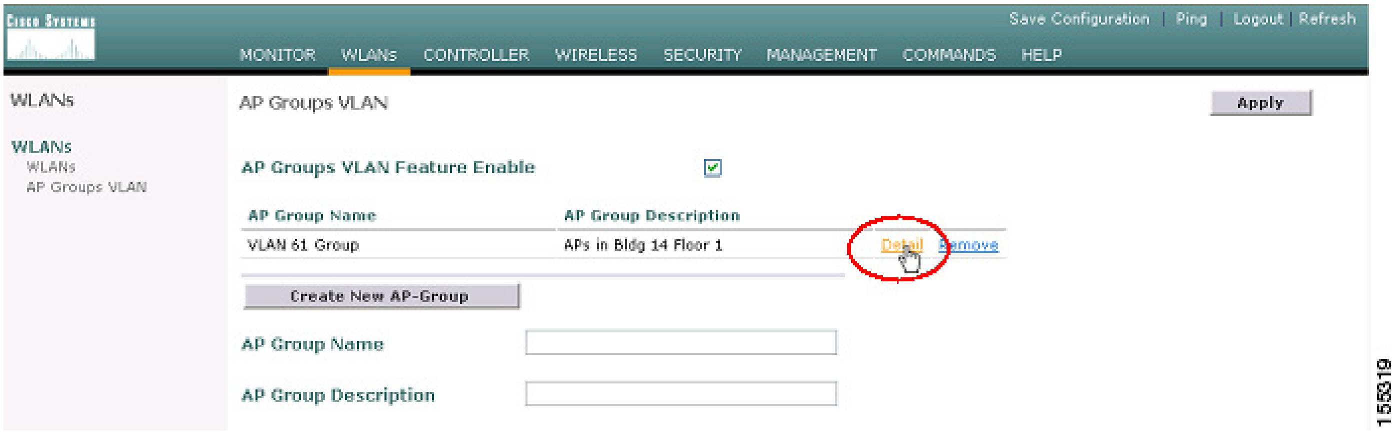
| AP Group Name | AP Group Description |
|---|---|

AP Group Name: VLAN 61 Group

AP Group Description: APs in Bldg 14 Floor 1

**Step 4** For your newly created AP Group, click on the **Detail** link (see Figure 73).

*Figure 73 AP Groups Configuration*



AP Groups VLAN

AP Groups VLAN Feature Enable ☑

| AP Group Name | AP Group Description | |
|---|---|---|
| VLAN 61 Group | APs in Bldg 14 Floor 1 | Detail Remove |

AP Group Name:

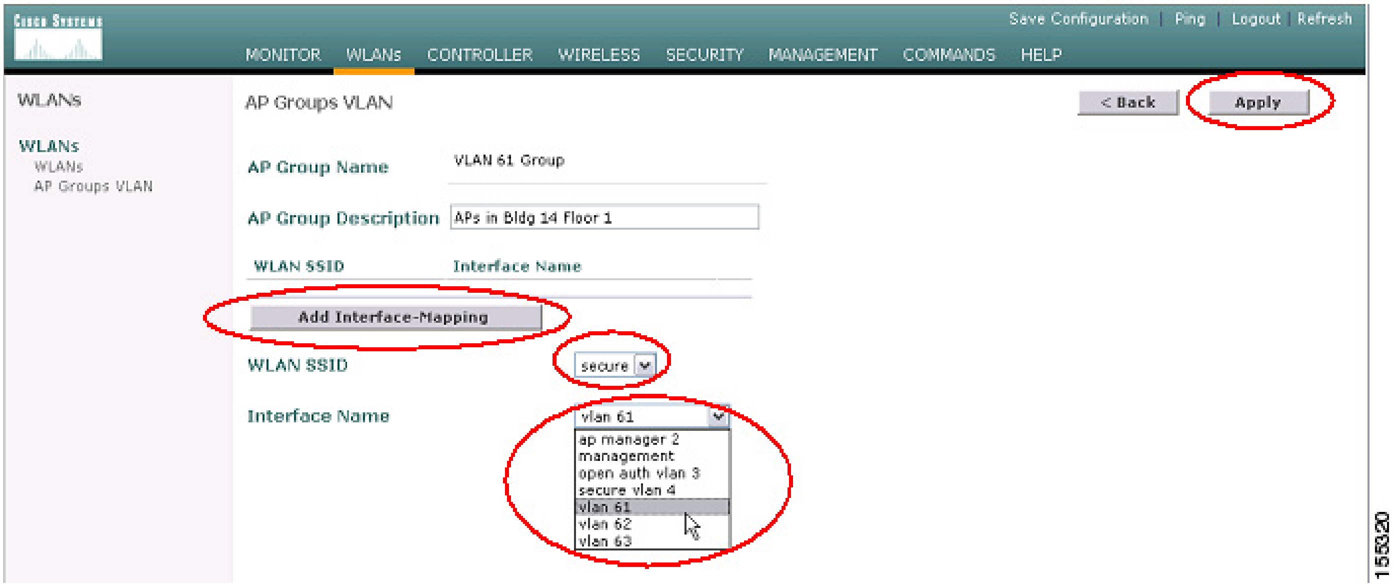
AP Group Description:

**Step 5** Select a **WLAN SSID** and the appropriate **Interface Name** from the drop-down boxes. Then click on **Add Interface-Mapping**. Note that you will need to map every wireless LAN to an interface for the AP Group. Every wireless LAN needs to be included in the AP Group, but not every interface needs to be Site Specific. For example, you might want your guest network to span the campus since you expect fewer users. In this case, you can simply map the guest wireless LAN to the same interface in each AP Group (see Figure 74).

**Step 6** When you are done adding your interface mappings, click **Apply** (see Figure 74).

**Step 7** Repeat Steps **3** through **6** for each AP Group.

*Figure 74 AP Groups Configuration*



AP Groups VLAN

AP Group Name: VLAN 61 Group

AP Group Description: APs in Bldg 14 Floor 1

| WLAN SSID | Interface Name |
|---|---|

WLAN SSID: secure

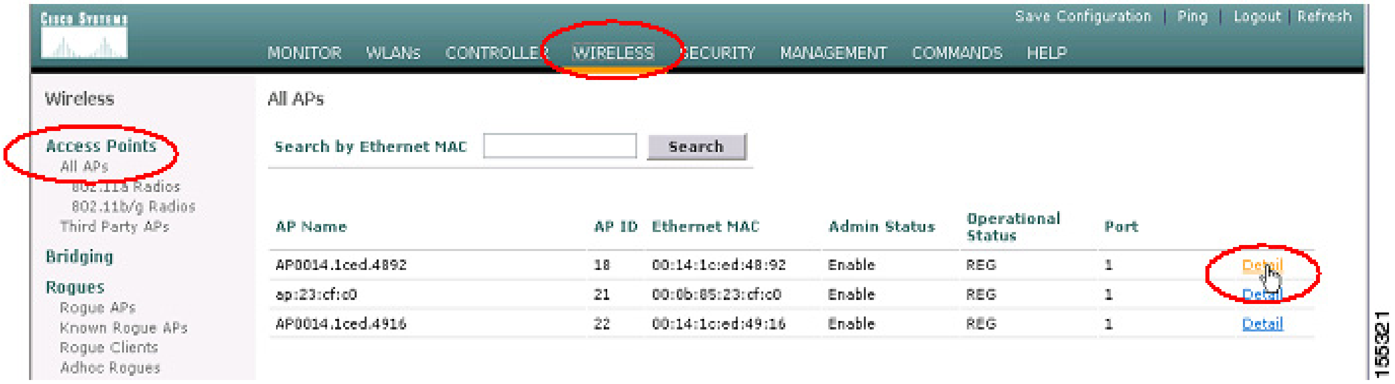
Interface Name: vlan 61

Now you need to assign access points the AP Groups in these steps:

**Step 1** Navigate to **Wireless | Access Points | All APs** in the WLC (see Figure 75).

**Step 2** Click on the **Detail** link for an access point (see Figure 75).

*Figure 75 Adding an Access Point to an AP Group*

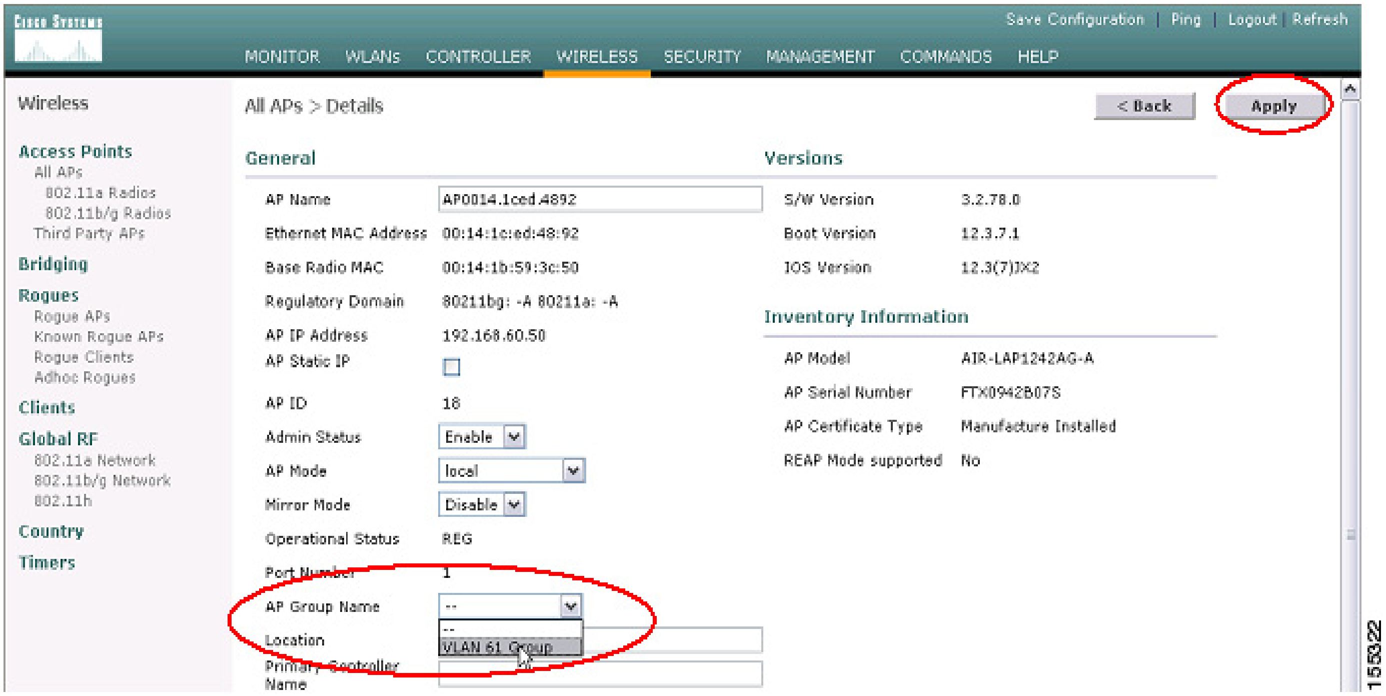


All APs

| AP Name | AP ID | Ethernet MAC | Admin Status | Operational Status | Port | |
|---|---|---|---|---|---|---|
| AP0014.1ced.4892 | 18 | 00:14:1c:ed:48:92 | Enable | REG | 1 | Detail |
| ap:23:cf:c0 | 21 | 00:0b:85:23:cf:c0 | Enable | REG | 1 | Detail |
| AP0014.1ced.4916 | 22 | 00:14:1c:ed:49:16 | Enable | REG | 1 | Detail |

**Step 3** Select the **AP Group** from the **AP Group Name** drop-down box and then click **Apply** (see Figure 76).

*Figure 76 Adding an Access Point to an AP Group*



All APs > Details

General

| | |
|---|---|
| AP Name | AP0014.1ced.4892 |
| Ethernet MAC Address | 00:14:1c:ed:48:92 |
| Base Radio MAC | 00:14:1b:59:3c:50 |
| Regulatory Domain | 80211bg: -A 80211a: -A |
| AP IP Address | 192.168.60.50 |
| AP Static IP | □ |
| AP ID | 18 |
| Admin Status | Enable |
| AP Mode | local |
| Mirror Mode | Disable |
| Operational Status | REG |
| Port Number | 1 |
| AP Group Name | --<br>--<br>VLAN 61 Group |
| Location | |
| Primary Controller Name | |

Versions

| | |
|---|---|
| S/W Version | 3.2.78.0 |
| Boot Version | 12.3.7.1 |
| IOS Version | 12.3(7)JX2 |

Inventory Information

| | |
|---|---|
| AP Model | AIR-LAP1242AG-A |
| AP Serial Number | FTX0942B07S |
| AP Certificate Type | Manufacture Installed |
| REAP Mode supported | No |

**Step 4** Repeat Steps **2** and **3** for each access point.

# WLAN Override

The default system behavior is for a wireless LAN Controller (WLC) to push all wireless LANs to all of its joined access points. Many Cisco customers deploying the Cisco Unified Wireless Network solution want to restrict certain SSIDs to sets of access points. For example, an enterprise might want to offer open guest access in an Executive Briefing Center but no where else on the campus. The way to override the default behavior is to use the WLAN Override feature.

We'll look at two ways to configure the WLAN Override feature-through WCS and through the WLC interface. If you choose the WLC web interface, you need to configure WLAN override on a per-radio (not just per-access point) basis.

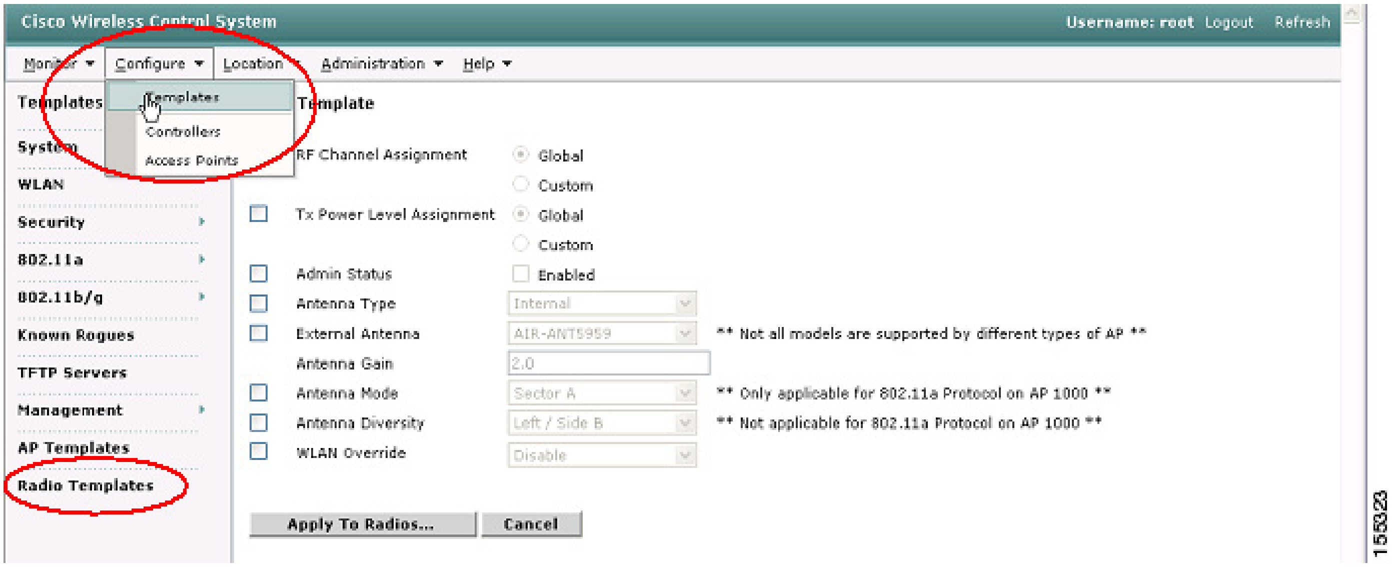
## Configuring WLAN Override Using WCS

The steps for configuring WLAN Override for a wireless LAN using WCS are as follows:

**Step 1** Login to WCS using the https://wcs_ip_address URL and the appropriate credentials.

**Step 2** Navigate to **Configure|Templates|Radio Templates** (see Figure 77).

*Figure 77 WLAN Override Configuration in WCS*



Template

RF Channel Assignment ● Global ○ Custom

□ Tx Power Level Assignment ● Global ○ Custom

□ Admin Status □ Enabled

□ Antenna Type Internal

□ External Antenna AIR-ANT5959 ** Not all models are supported by different types of AP **

Antenna Gain 2.0

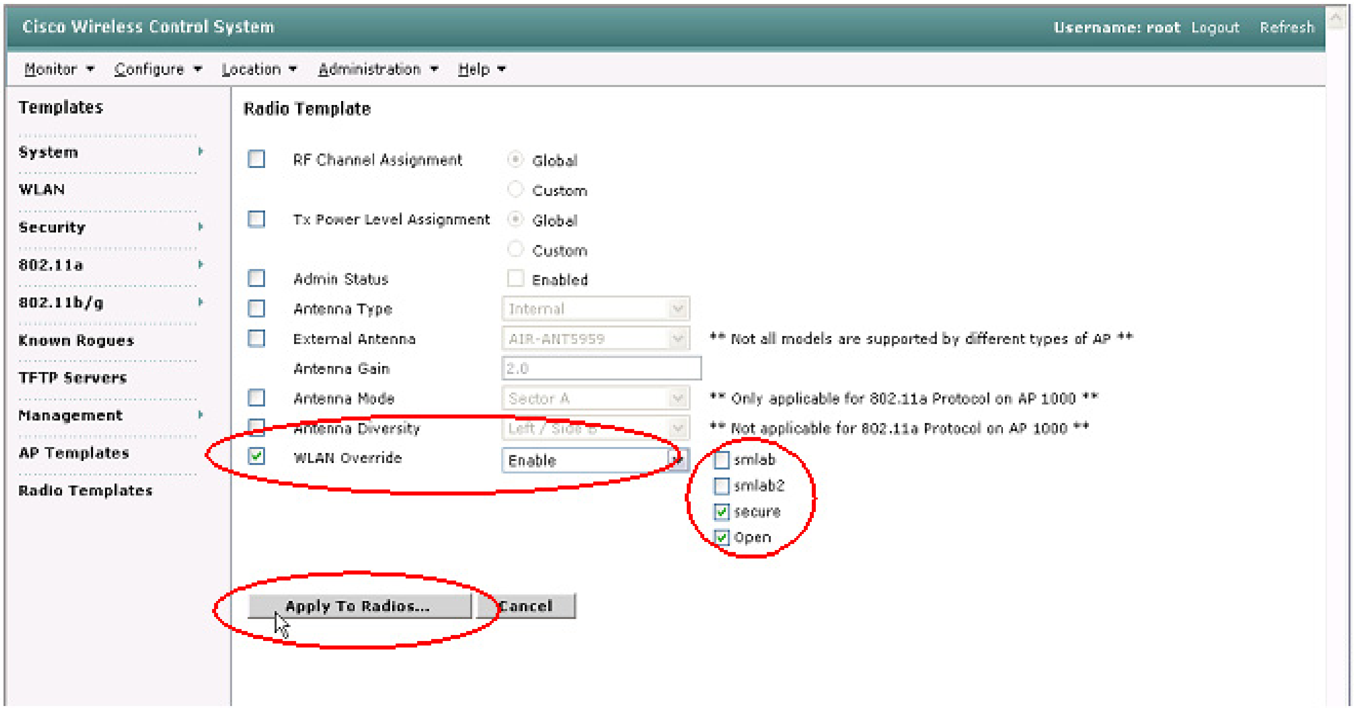
□ Antenna Mode Sector A ** Only applicable for 802.11a Protocol on AP 1000 **

□ Antenna Diversity Left / Side B ** Not applicable for 802.11a Protocol on AP 1000 **

□ WLAN Override Disable

**Step 3** Check the "WLAN Override" box and then select **Enable** from the drop-down box. Your wireless LANs should appear when the box is checked. Select the desired SSID(s) (see Figure 78).

*Figure 78 WLAN Override Configuration in WCS*

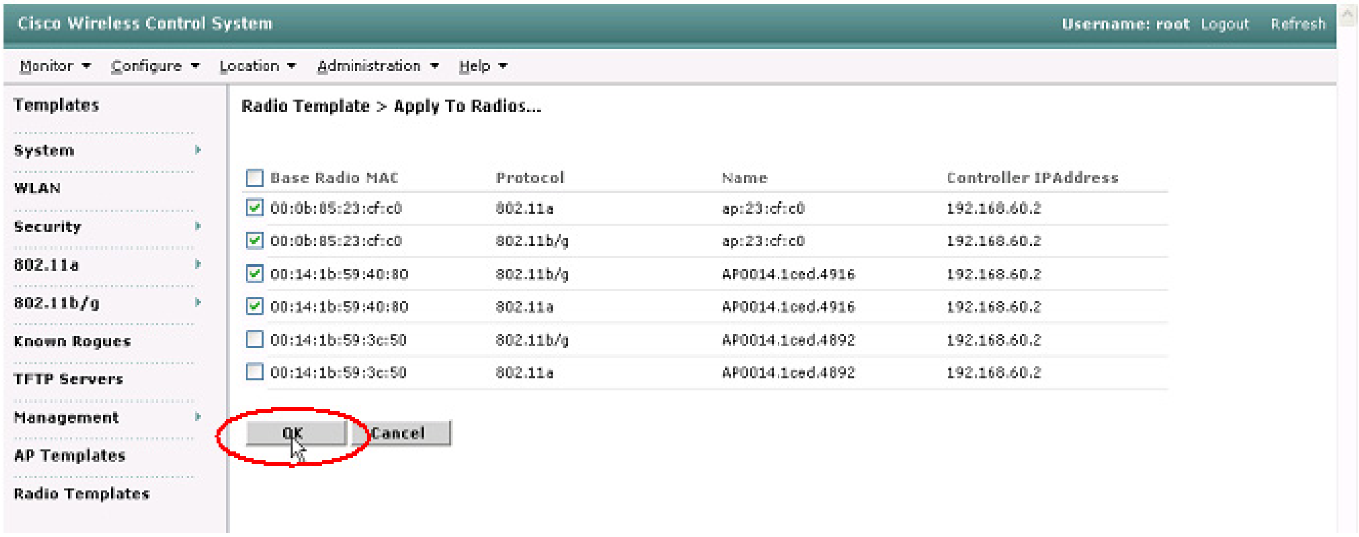


Radio Template

| | | |
|---|---|---|
| □ RF Channel Assignment | ● Global<br>○ Custom | |
| □ Tx Power Level Assignment | ● Global<br>○ Custom | |
| □ Admin Status | □ Enabled | |
| □ Antenna Type | Internal | |
| □ External Antenna | AIR-ANT5959 | ** Not all models are supported by different types of AP ** |
| Antenna Gain | 2.0 | |
| □ Antenna Mode | Sector A | ** Only applicable for 802.11a Protocol on AP 1000 ** |
| □ Antenna Diversity | Left / Side B | ** Not applicable for 802.11a Protocol on AP 1000 ** |
| ☑ WLAN Override | Enable | □ smlab<br>□ smlab2<br>☑ secure<br>☑ Open |

**Step 4** Next, click **Apply to Radios**. Note that this feature is not applied per access point, but rather, per radio. Select the appropriate radios (there is no limit on the number of radios you can select) then click **OK** (see Figure 79).

*Figure 79 WLAN Override Configuration in WCS*



Radio Template > Apply To Radios...

| □ Base Radio MAC | Protocol | Name | Controller IPAddress |
|---|---|---|---|
| ☑ 00:0b:85:23:cf:c0 | 802.11a | ap:23:cf:c0 | 192.168.60.2 |
| ☑ 00:0b:85:23:cf:c0 | 802.11b/g | ap:23:cf:c0 | 192.168.60.2 |
| ☑ 00:14:1b:59:40:80 | 802.11b/g | AP0014.1ced.4916 | 192.168.60.2 |
| ☑ 00:14:1b:59:40:80 | 802.11a | AP0014.1ced.4916 | 192.168.60.2 |
| □ 00:14:1b:59:3c:50 | 802.11b/g | AP0014.1ced.4892 | 192.168.60.2 |
| □ 00:14:1b:59:3c:50 | 802.11a | AP0014.1ced.4892 | 192.168.60.2 |

## Configuring WLAN Override Using the WLC Web Interface

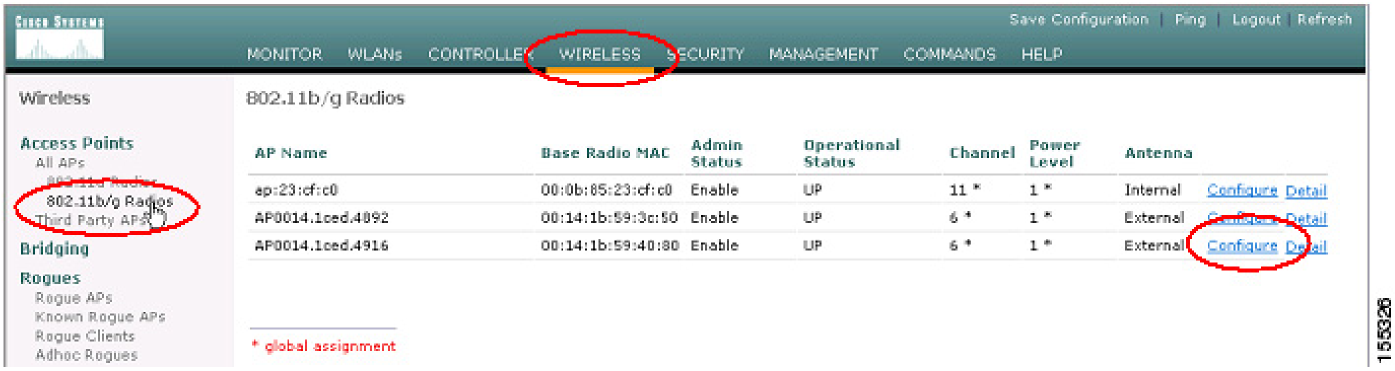
WLAN override must be configured on a per access point radio basis if you choose to use the WLC web interface. The steps for configuring WLAN Override for a wireless LAN using WLC web interface are as follows:

**Step 1** Login to the WLC web interface.

**Step 2** Navigate to the Wireless tab, and then select the radio type under the Access Points "All APs" options on the left-hand side. For example, you might select 802.11b/g Radios (see Figure 80).

**Step 3** All the 802.11b/g radios in your network should be visible  Select the **Configure** link for the appropriate individual radio (see Figure 80).

*Figure 80 WLAN Override Configuration in the WLC Web Interface*



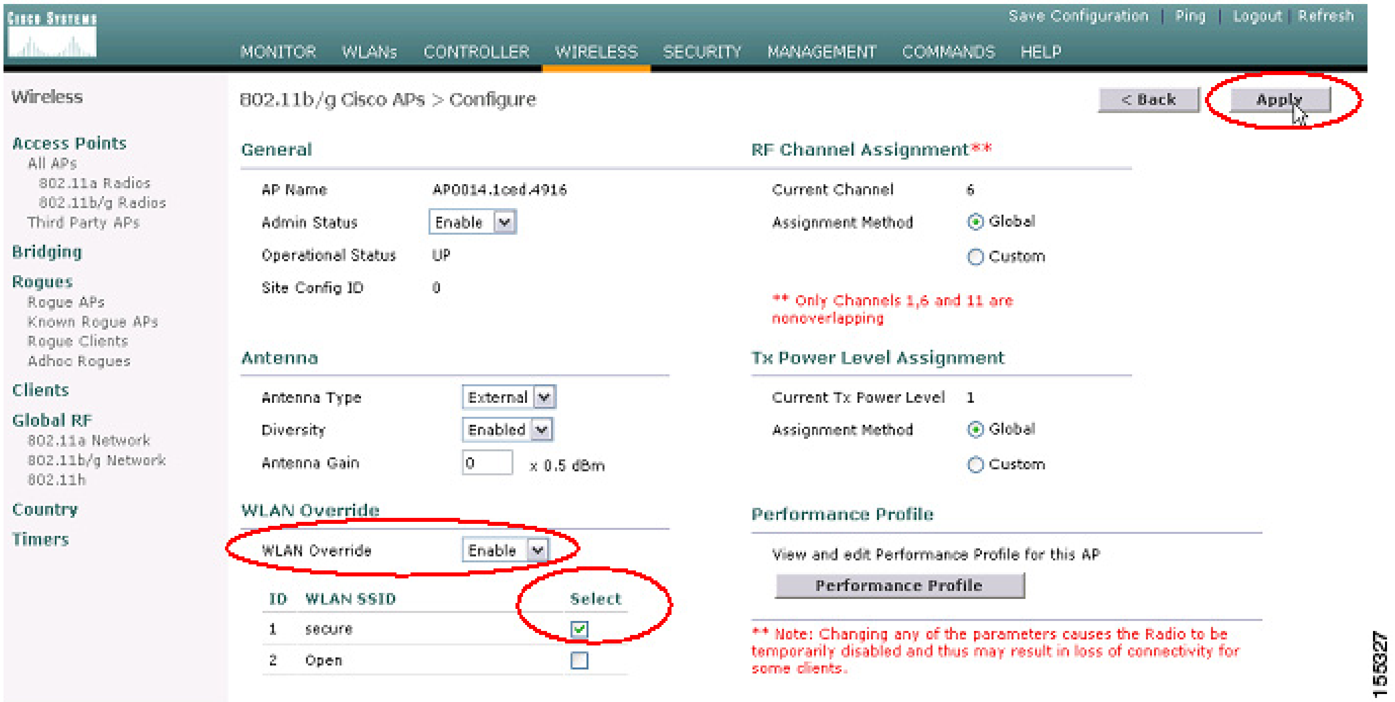
802.11b/g Radios

| AP Name | Base Radio MAC | Admin Status | Operational Status | Channel | Power Level | Antenna | | |
|---|---|---|---|---|---|---|---|---|
| ap:23:cf:c0 | 00:0b:85:23:cf:c0 | Enable | UP | 11 * | 1 * | Internal | Configure | Detail |
| AP0014.1ced.4892 | 00:14:1b:59:3c:50 | Enable | UP | 6 * | 1 * | External | Configure | Detail |
| AP0014.1ced.4916 | 00:14:1b:59:40:80 | Enable | UP | 6 * | 1 * | External | Configure | Detail |

* global assignment

**Step 4** Change the WLAN Override option to **Enable** and then select the appropriate SSIDs and then click **Apply** (see Figure 81).

*Figure 81 WLAN Override Configuration in the WLC Web Interface*



802.11b/g Cisco APs > Configure

**General**

| | |
|---|---|
| AP Name | AP0014.1ced.4916 |
| Admin Status | Enable |
| Operational Status | UP |
| Site Config ID | 0 |

**RF Channel Assignment****

| | |
|---|---|
| Current Channel | 6 |
| Assignment Method | ● Global<br>○ Custom |

** Only Channels 1,6 and 11 are nonoverlapping

**Antenna**

| | |
|---|---|
| Antenna Type | External |
| Diversity | Enabled |
| Antenna Gain | 0 x 0.5 dBm |

**Tx Power Level Assignment**

| | |
|---|---|
| Current Tx Power Level | 1 |
| Assignment Method | ● Global<br>○ Custom |

**WLAN Override**

| | |
|---|---|
| WLAN Override | Enable |

| ID | WLAN SSID | Select |
|---|---|---|
| 1 | secure | ☑ |
| 2 | Open | □ |

**Performance Profile**

View and edit Performance Profile for this AP

** Note: Changing any of the parameters causes the Radio to be temporarily disabled and thus may result in loss of connectivity for some clients.

**Step 5** Repeat Steps **1** through **4** for EACH radio as necessary.

Since you have to configure each radio individually through the WLC web interface, using WCS is obviously a more desirable solution, which is Cisco's recommendation as well.

# Wireless LAN Controller Maintenance

This section describes common WLC maintenance tasks:

- Upgrading WLC Software
- Backing up and Restoring WLC Controller Configuration
- Managing the WLC Date and Time

## Upgrading WLC Software

You can upgrade WLC software any of three ways:

- Through the WLC CLI
- Through the WLC Web Interface
- Through WCS

### Upgrading WLC Software Using the WLC CLI

To upgrade a WLC through the controller CLI, follow these steps:

**Step 1** Copy the code file onto a TFTP server's root directory.

**Step 2** Start the TFTP server if not already running.

**Step 3** Login to the WLC CLI and enter the following commands:

```
> transfer download serverip <TFTP Server IP>
> transfer download path <path>
> transfer download filename <code filename>
> transfer download start
```

Note that if you put the code in the TFTP root directory, the "path" parameter is optional.

**Step 4** Once the code is successfully downloaded and written to the WLC flash, be sure to save the WLC configuration:

```
> save config
```

**Step 5** Reboot the WLC with the following command:

```
> reset system
```

### Upgrading WLC Software Using the WLC Web Interface

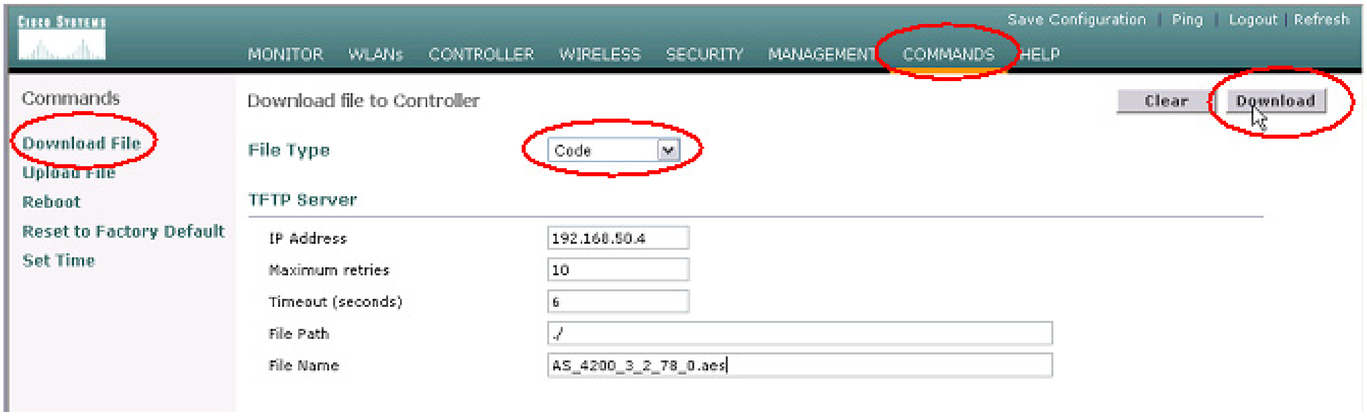
To upgrade a controller through the WLC GUI, follow these steps:

**Step 1** Copy the code file onto a TFTP server's root directory.

**Step 2** Start the TFTP server if not already running.

**Step 3** Navigate through the GUI to **Commands | Download File**. Select **Code** as the File Type, and then enter the TFTP server parameters in the appropriate fields. If you copied the code to the TFTP server root, then enter a period (**.**) in the File Path Field. Click **Download** in the upper right-hand corner to initiate the TFTP download (see Figure 82).

*Figure 82 WLC Code Download*


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download
155328

Download file to Controller

File Type: Code

TFTP Server

IP Address: 192.168.50.4

Maximum retries: 10

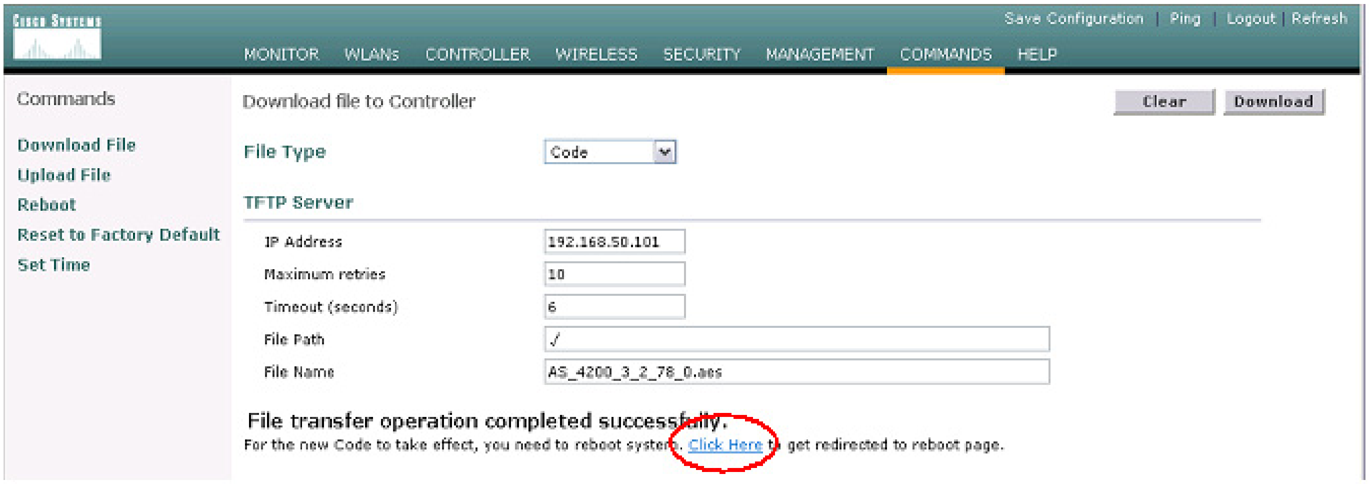
Timeout (seconds): 6

File Path: ./

File Name: AS_4200_3_2_78_0.aes

**Step 4** Once the file transfer is successfully completed, you need to reboot the controller to load the new code. You will see a **Click Here** link at the bottom of the page (see Figure 83). Click on the link to continue the process.

*Figure 83 WLC Code Download*


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download
155329

Download file to Controller

File Type: Code

TFTP Server

IP Address: 192.168.50.101

Maximum retries: 10

Timeout (seconds): 6

File Path: ./

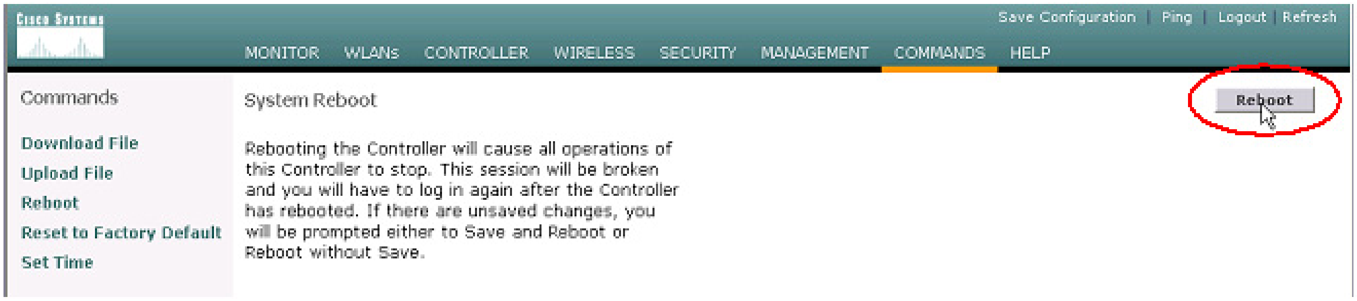
File Name: AS_4200_3_2_78_0.aes

File transfer operation completed successfully.

For the new Code to take effect, you need to reboot system. Click Here to get redirected to reboot page.

**Step 5** At the next screen, you will see a system reboot warning. Read the warning carefully, then click **Reboot** (Figure 84).

*Figure 84 WLC Code Download--Controller Reboot*

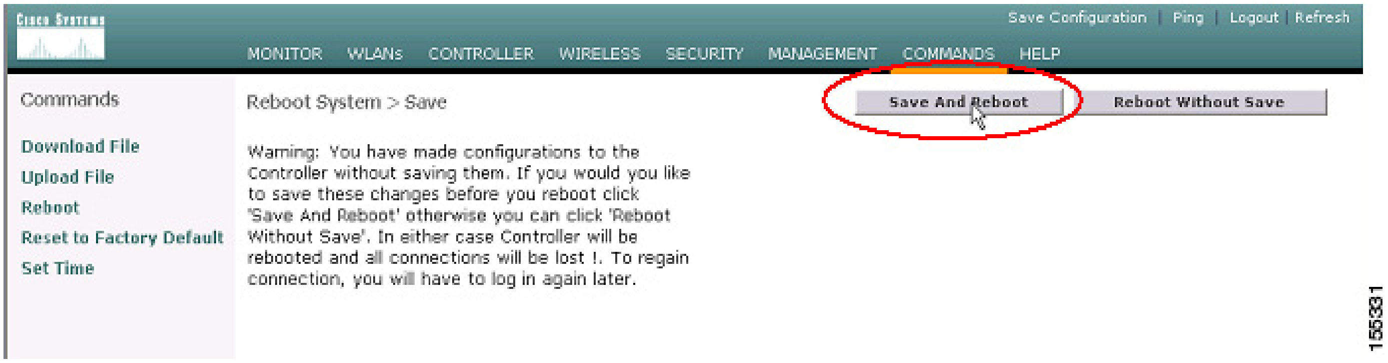

Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Reboot
155330

System Reboot

Rebooting the Controller will cause all operations of this Controller to stop. This session will be broken and you will have to log in again after the Controller has rebooted. If there are unsaved changes, you will be prompted either to Save and Reboot or Reboot without Save.

**Step 6** Be sure to save the WLC configuration by clicking **Save and Reboot** (Figure 85).

*Figure 85 WLC Save and Reboot*



Reboot System > Save

Warning: You have made configurations to the Controller without saving them. If you would you like to save these changes before you reboot click 'Save And Reboot' otherwise you can click 'Reboot Without Save'. In either case Controller will be rebooted and all connections will be lost !. To regain connection, you will have to log in again later.

When the WLC reboots, you will eventually lose browser connectivity with the controller. Wait a couple of minutes and then refresh the page. A successful page refresh indicates a completed update.

## Upgrading WLC Software Using the WCS

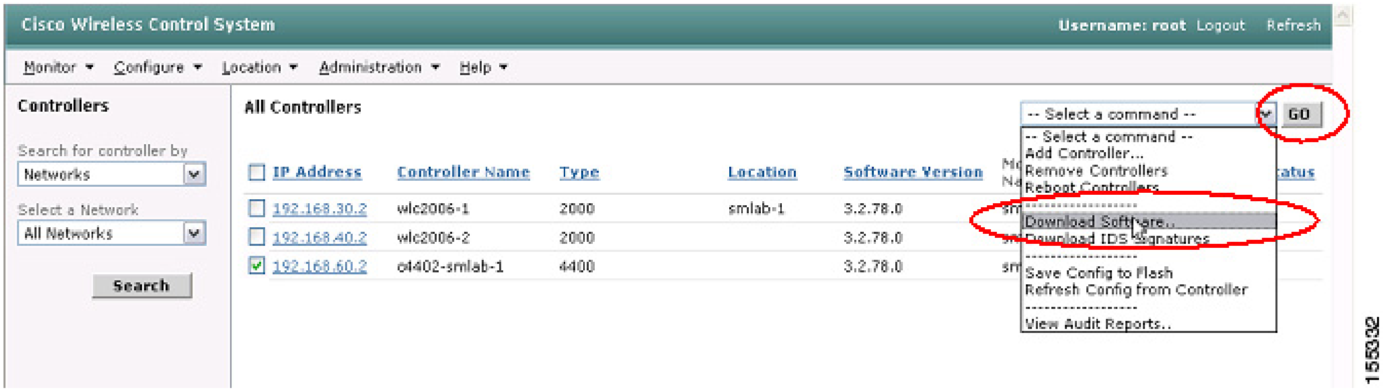
To upgrade a WLC using WCS, follow these steps:

**Step 1** You can initiate a software upgrade to a WLC from either an external TFTP server or from the TFTP server embedded in WCS. In the case of an external TFTP server, copy the WLC code to the TFTP root. With WCS, the file can be copied to the TFTP root directory configured at install time or in a directory on the WCS host machine.

**Step 2** Navigate in the WCS interface to **Configure | Controllers** (see Figure 86).

**Step 3** Select one or more WLCs by checking the appropriate check-boxes. Note that you can upgrade WLCs from a single WLC family at a time. Select the **Download Software** option from the drop-down box and click **Go** (Figure 86).

*Figure 86 WCS Software Download to WLC*

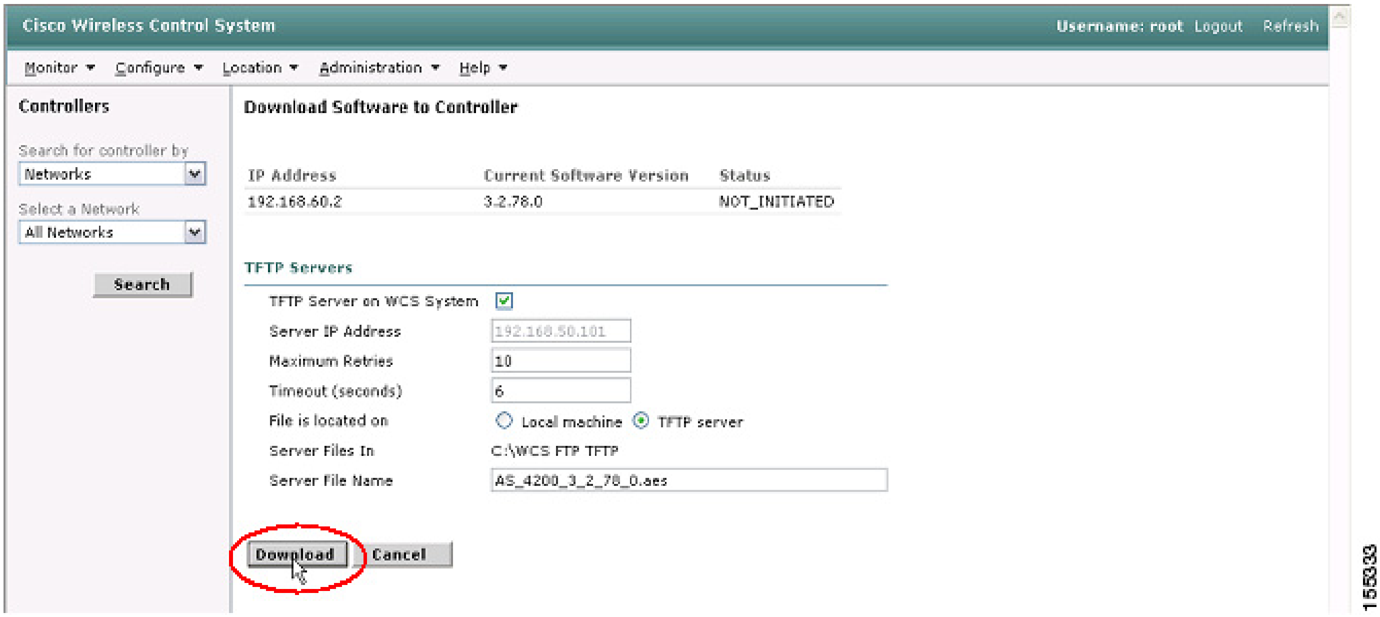


All Controllers

| □ IP Address | Controller Name | Type | Location | Software Version |
|---|---|---|---|---|
| □ 192.168.30.2 | wlc2006-1 | 2000 | smlab-1 | 3.2.78.0 |
| □ 192.168.40.2 | wlc2006-2 | 2000 | | 3.2.78.0 |
| ☑ 192.168.60.2 | c4402-smlab-1 | 4400 | | 3.2.78.0 |

**Step 4** Configure the appropriate parameters. Consult the online help for details on the TFTP server fields. When you have configured the appropriate parameters, click **Download** (Figure 87).

*Figure 87 WCS Software Download to WLC*


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search
Download
Cancel
155333

Search for controller by: Networks

Select a Network: All Networks

Download Software to Controller

| IP Address | Current Software Version | Status |
|---|---|---|
| 192.168.60.2 | 3.2.78.0 | NOT_INITIATED |

TFTP Servers

TFTP Server on WCS System ☑

Server IP Address: 192.168.50.101

Maximum Retries: 10

Timeout (seconds): 6

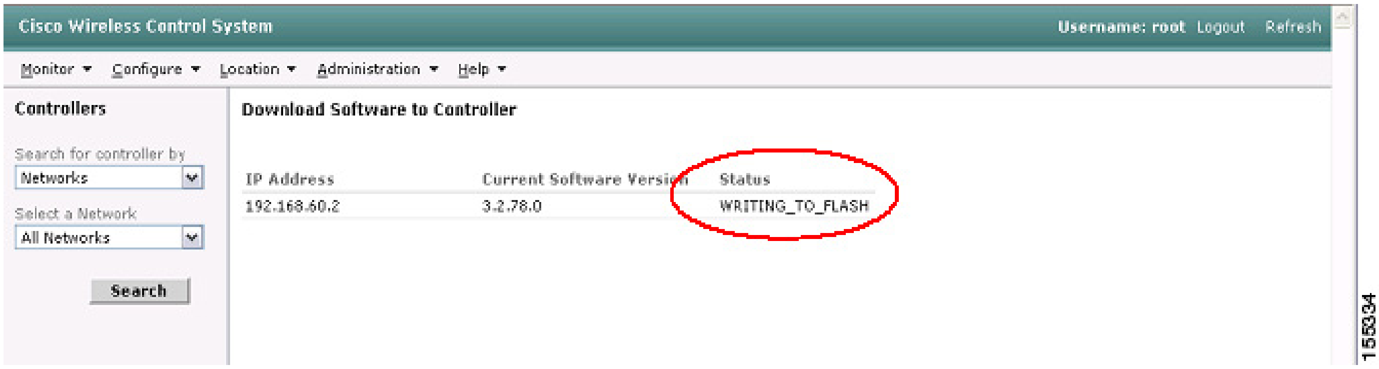
File is located on: ○ Local machine ● TFTP server

Server Files In: C:\WCS FTP TFTP

Server File Name: AS_4200_3_2_78_0.aes

While the code is downloading and the WLC upgrading, you will see status messages in the WCS interface (Figure 88).

*Figure 88 WCS Software Download Status*


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search
155334

Search for controller by: Networks

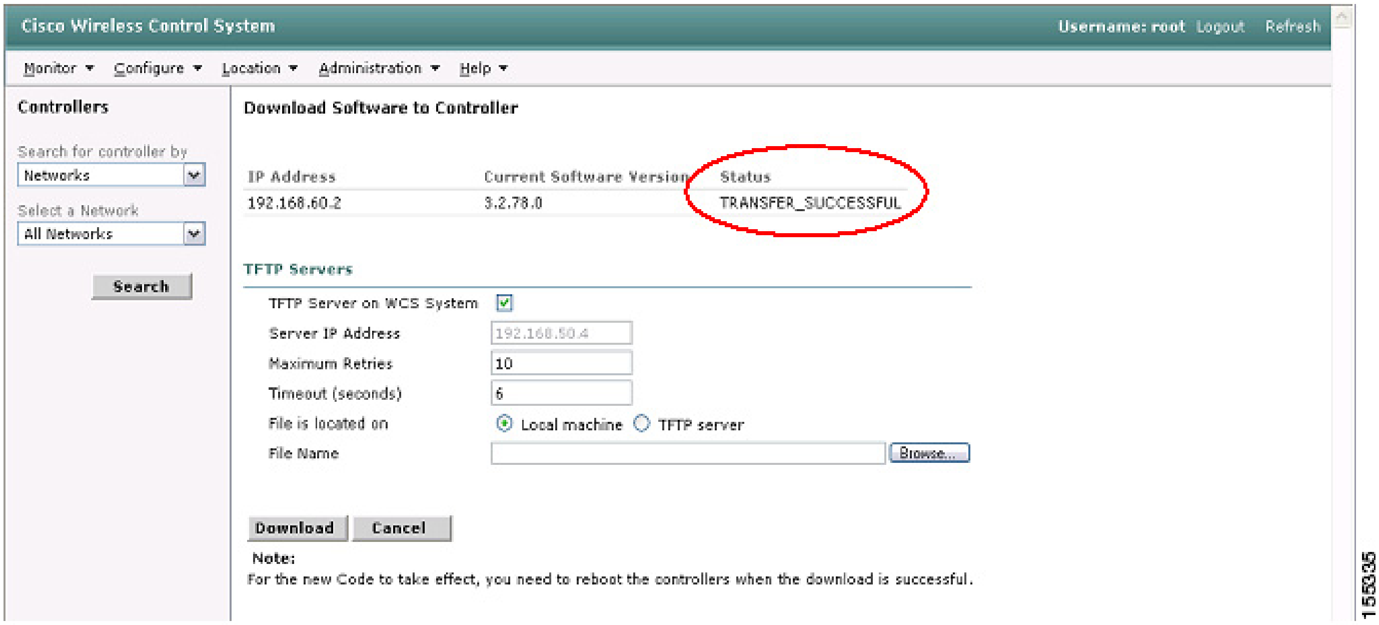
Select a Network: All Networks

Download Software to Controller

| IP Address | Current Software Version | Status |
|---|---|---|
| 192.168.60.2 | 3.2.78.0 | WRITING_TO_FLASH |

**Step 5** When the code download is successful, you will see a TRANSFER_SUCCESSFUL message (Figure 89).

*Figure 89 WCS Software Download Success*


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Search
Browse...
Download
Cancel
155335

Controllers

Search for controller by: Networks

Select a Network: All Networks

Download Software to Controller

| IP Address | Current Software Version | Status |
|---|---|---|
| 192.168.60.2 | 3.2.78.0 | TRANSFER_SUCCESSFUL |

TFTP Servers

TFTP Server on WCS System ☑

Server IP Address: 192.168.50.4

Maximum Retries: 10

Timeout (seconds): 6

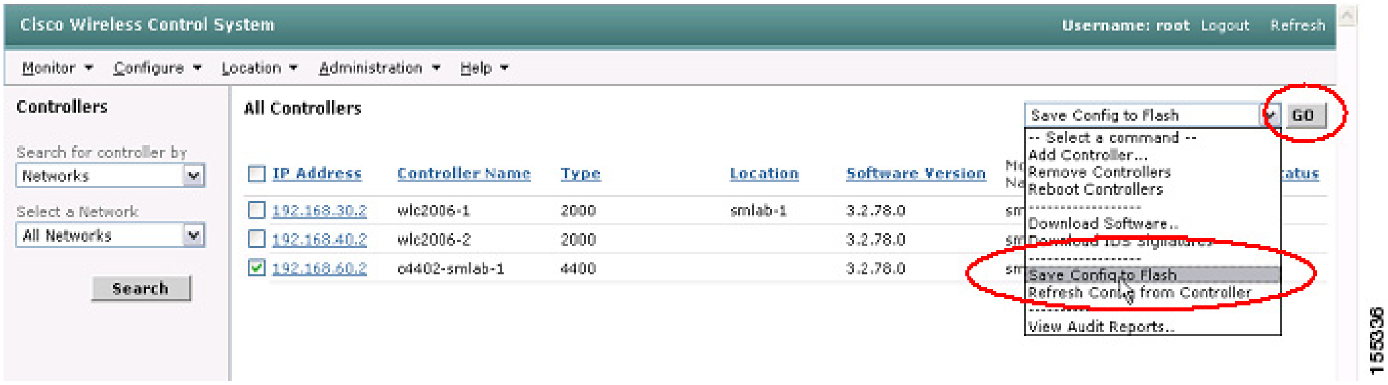
File is located on: ● Local machine ○ TFTP server

File Name:

Note:
For the new Code to take effect, you need to reboot the controllers when the download is successful.

**Step 6** When the code is successfully loaded on the controllers, you must reboot them to load the new code. You should first save the WLC configurations and to do so, navigate to the **Configure | Controllers** interface. Select the controllers, and then choose **Save Config to Flash** from the drop-down box on the right-hand side, and finally click **Go** (see Figure 90).

*Figure 90 WCS Save Configuration to WLC Flash*



Controllers

Search for controller by: Networks

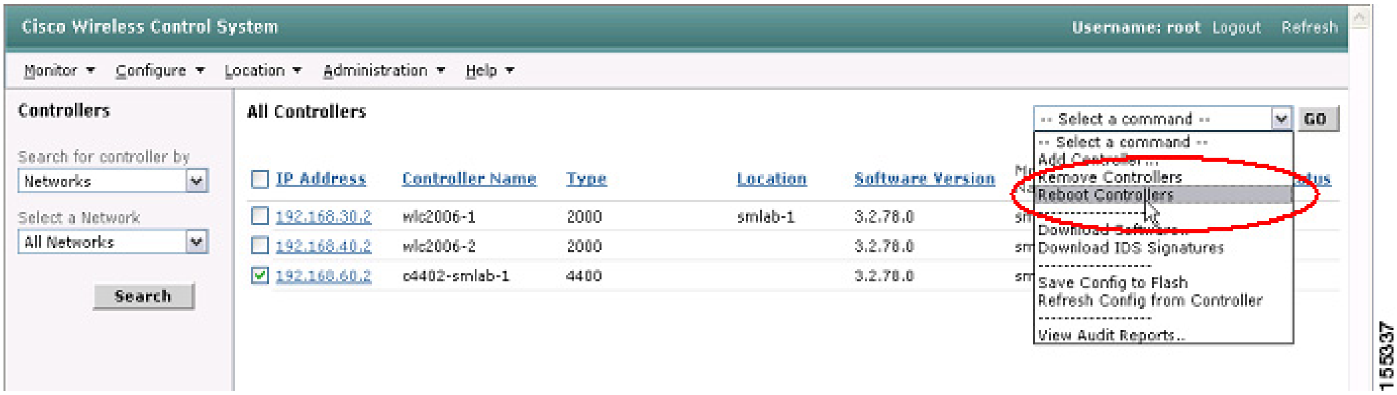
Select a Network: All Networks

All Controllers

| ☐ | IP Address | Controller Name | Type | Location | Software Version |
|---|---|---|---|---|---|
| ☐ | 192.168.30.2 | wlc2006-1 | 2000 | smlab-1 | 3.2.78.0 |
| ☐ | 192.168.40.2 | wlc2006-2 | 2000 | | 3.2.78.0 |
| ☑ | 192.168.60.2 | c4402-smlab-1 | 4400 | | 3.2.78.0 |

**Step 7** After the configuration(s) have been successfully saved, select the controllers and then choose **Reboot Controllers** from the drop-down box on the right-hand side and then click **Go** (see Figure 91).

*Figure 91 WCS Reboot WLC*



Search for controller by: Networks

Select a Network: All Networks

All Controllers

| ☐ | IP Address | Controller Name | Type | Location | Software Version |
|---|---|---|---|---|---|
| ☐ | 192.168.30.2 | wlc2006-1 | 2000 | smlab-1 | 3.2.78.0 |
| ☐ | 192.168.40.2 | wlc2006-2 | 2000 |  | 3.2.78.0 |
| ☑ | 192.168.60.2 | c4402-smlab-1 | 4400 |  | 3.2.78.0 |

## Best Practices for Upgrading WLC Software

A controller can download a new image without disrupting service but it needs to be rebooted manually to load the new code. Once the new code is loaded on reboot, the upgrade of all access point code is automatically triggered. Cisco controllers currently upgrade four access points at a time. Take this into account when allotting a change window for upgrading your WLC.

To compute the minimum change window, use this formula:

```
Change Window = Controller reboot time + (Number of APs / 4 )* 3 minutes per AP
```

Let's take a worst-case example. Suppose we have a Cisco 4404 controller with 100 access points joined to it. The controller reboot time is approximately 3.5 minutes. So our minimum change window is:

```
4.5 minutes + (100 APs / 4) * 3 minutes per AP = 78.5 minutes = 1 hour 18.5 minutes.
```

You should allow yourself some time for troubleshooting.

As another best practice, if you have multiple WLC devices in the network, **you should keep the software revisions consistent across all WLC devices.** This is because an access point down-revs its code when it joins a WLC with a lower code revision than what is currently running on the access point. This is an issue that leads to increased downtime each time an access point joins a new controller. Keep this in mind when you have multiple controllers in the network and redundancy deployed. You should account for this change in your planned service window.

# WLC Controller Configuration Backup and Restore

Backup and restore operations for a WLC's configurations can be performed from both the WLC itself and the WCS.

## Managing WLC Configurations Using the WLC Web Interface

Follow these steps to backup WLC Configurations from the WLC Web Interface:

**Step 1** Start a TFTP server if necessary.

**Step 2** Navigate in the WLC to **Commands | Upload File** (see Figure 92).

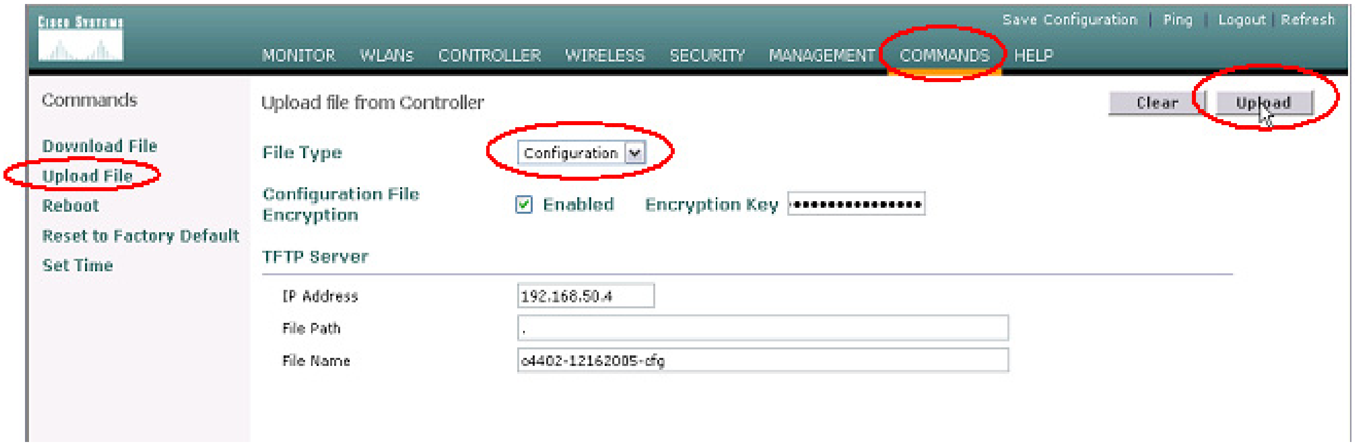
**Step 3** From the File Type drop-down box, select **Configuration** (see Figure 92).

**Step 4** If you want to encrypt the configuration file, check the **Configuration File Encryption Enabled** box and then enter a value in the **Encryption Key** field. The encryption key must be at least 16 characters in length (see Figure 92).

**Step 5** Enter the TFTP Server **IP address**, **File Path**, and **File Name** in the appropriate fields (see Figure 92).

**Step 6** Click on the **Upload** button (see Figure 92).

*Figure 92 WCS Configuration Upload*


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Upload

Upload file from Controller

File Type: Configuration

Configuration File Encryption: ☑ Enabled Encryption Key: ••••••••••••••••

TFTP Server

IP Address: 192.168.50.4

File Path: .

File Name: c4402-12162005-cfg

**Step 7** When the upload is successful, you will see a message that says, "File transfer operation completed successfully."

Follow these steps to reload a configuration to a WLC:

**Step 1** Start a TFTP server and load the backed up controller configuration to the TFTP server.

**Step 2** Navigate in the WLC to **Commands | Download File** (see Figure 93).

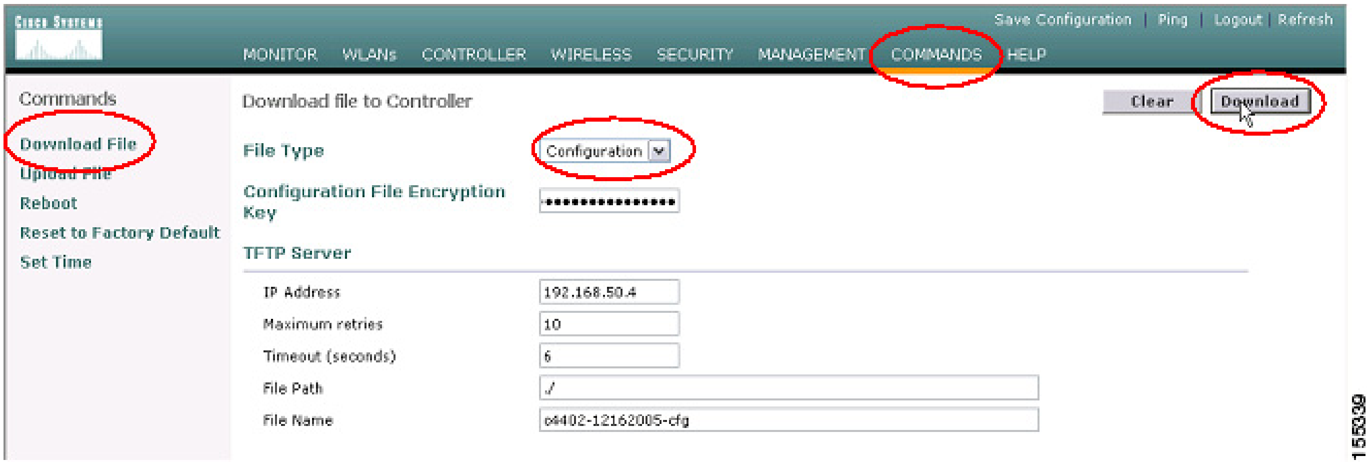
**Step 3** From the File Type drop-down box, select **Configuration** (see Figure 93).

**Step 4** If necessary, enter the file encryption key in the **Configuration File Encryption Key** field (see Figure 93).

**Step 5** Enter the TFTP Server **IP address**, **File Path**, and **File Name** in the appropriate fields (see Figure 93).

**Step 6** Click **Download** (see Figure 93).

*Figure 93 WCS Configuration Download to WLC*


Cisco Systems
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Commands
Download File
Upload File
Reboot
Reset to Factory Default
Set Time
Clear
Download
155339

Download file to Controller

File Type: Configuration

Configuration File Encryption Key: •••••••••••••••

TFTP Server

| | |
|---|---|
| IP Address | 192.168.50.4 |
| Maximum retries | 10 |
| Timeout (seconds) | 6 |
| File Path | ./ |
| File Name | c4402-12162005-cfg |

**Step 7** The WLC will reboot after it successfully loads the configuration.

## Managing WLC Configurations Using WCS

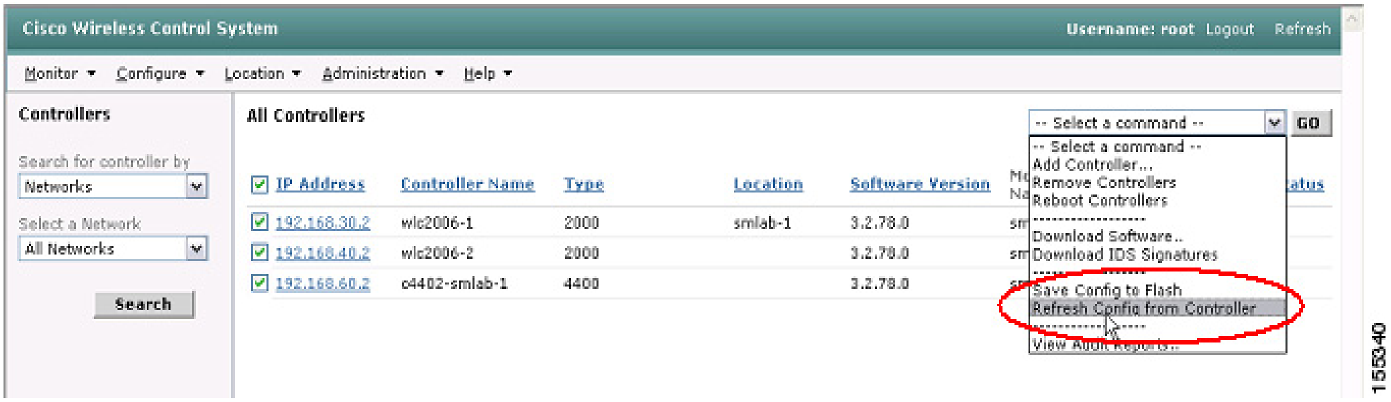
When a controller is added to WCS, its complete configuration is pulled from the WLC and stored locally. When you use the WCS to change a WLC configuration, it is automatically updated in the WCS database.

If you make a change from on the WLC independent of WCS, you can refresh the configuration on WCS using the following steps:

**Step 1** Navigate in WCS to **Configure | Controllers**.

**Step 2** Select one or more WLCs. Select **Refresh Config from Controller** from the drop-down box and click **GO** (see Figure 94).

*Figure 94 WCS Refresh Configuration from WLC*

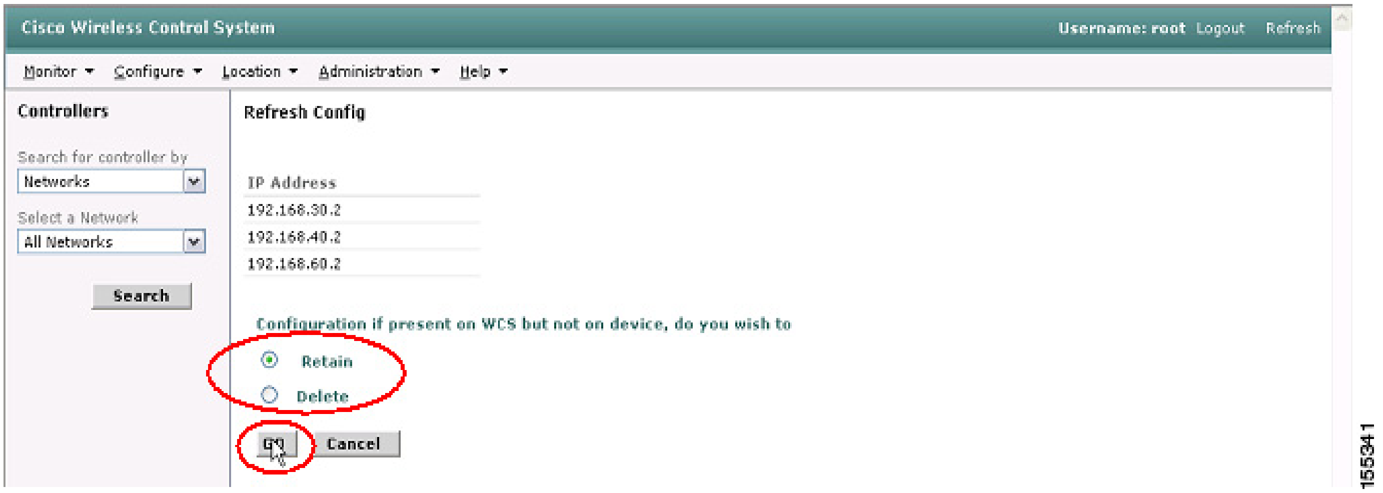


All Controllers

| ☑ IP Address | Controller Name | Type | Location | Software Version |
|---|---|---|---|---|
| ☑ 192.168.30.2 | wlc2006-1 | 2000 | smlab-1 | 3.2.78.0 |
| ☑ 192.168.40.2 | wlc2006-2 | 2000 | | 3.2.78.0 |
| ☑ 192.168.60.2 | c4402-smlab-1 | 4400 | | 3.2.78.0 |

**Step 3** You will also be provided an option to either retain or delete configurations that are on WCS but not the controller. Typically, you would want to select the retain option (in case there's a need to roll-back to previous configurations). Click on **Go** to initiate the configuration refresh from the WLC (see Figure 95).

*Figure 95 WCS Retain Configuration*


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
Search
Go
Cancel
155341

Refresh Config

| IP Address |
|---|
| 192.168.30.2 |
| 192.168.40.2 |
| 192.168.60.2 |

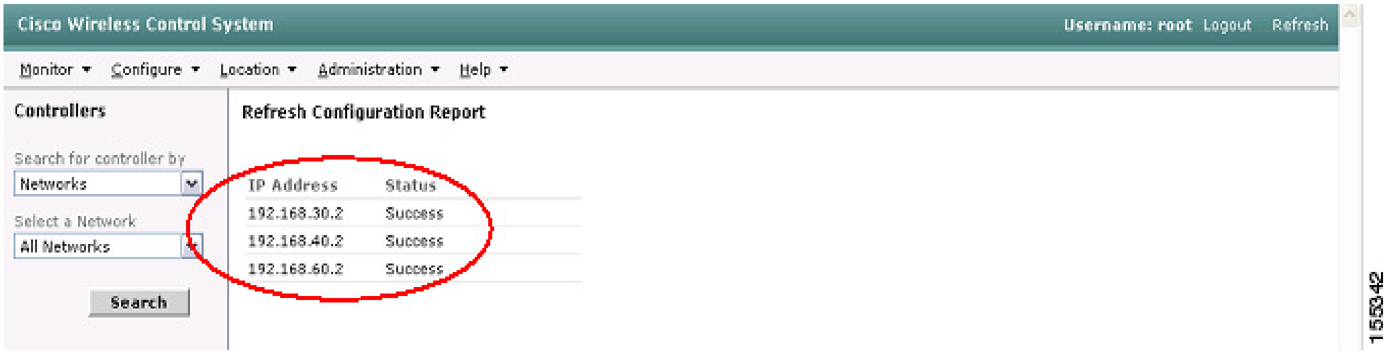
Configuration if present on WCS but not on device, do you wish to

● Retain

○ Delete

**Step 4** When the configurations have been successfully refreshed from the controllers, you will see a "Success" status message (see Figure 96).

*Figure 96 WCS Refresh Configuration Success*


Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Controllers
Search for controller by
Networks
Select a Network
All Networks
Search
155342

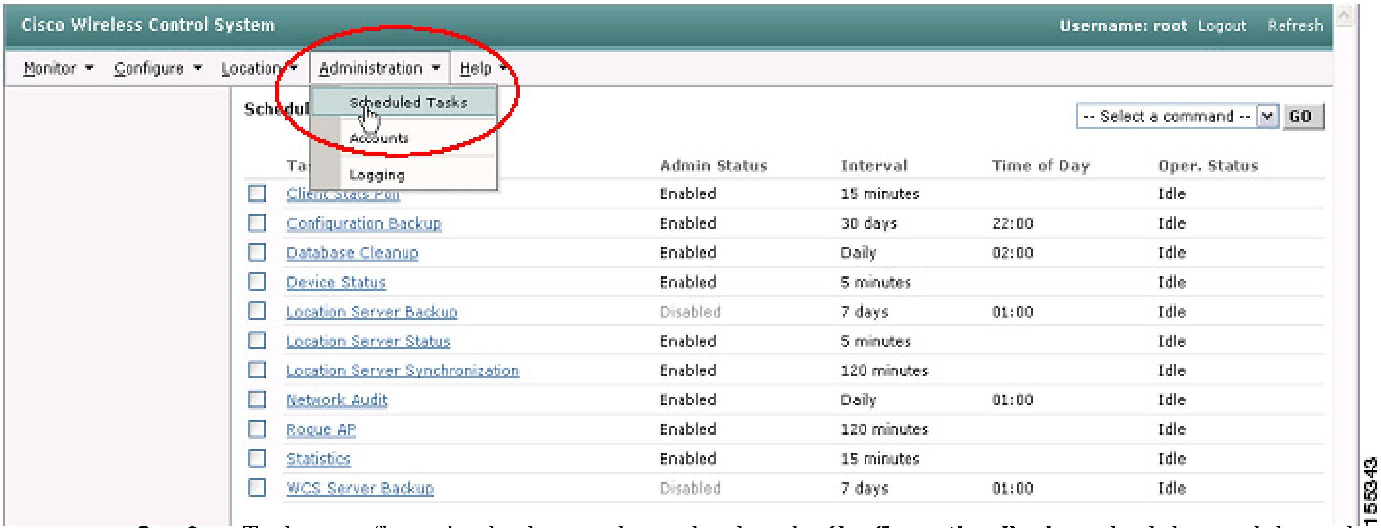
Refresh Configuration Report

| IP Address | Status |
|---|---|
| 192.168.30.2 | Success |
| 192.168.40.2 | Success |
| 192.168.60.2 | Success |

The WCS can also perform scheduled and full on-demand configuration backups:

**Step 1** Navigate in WCS to **Administration | Scheduled Tasks** (see Figure 97).

*Figure 97 WCS Scheduled Configuration Backup*

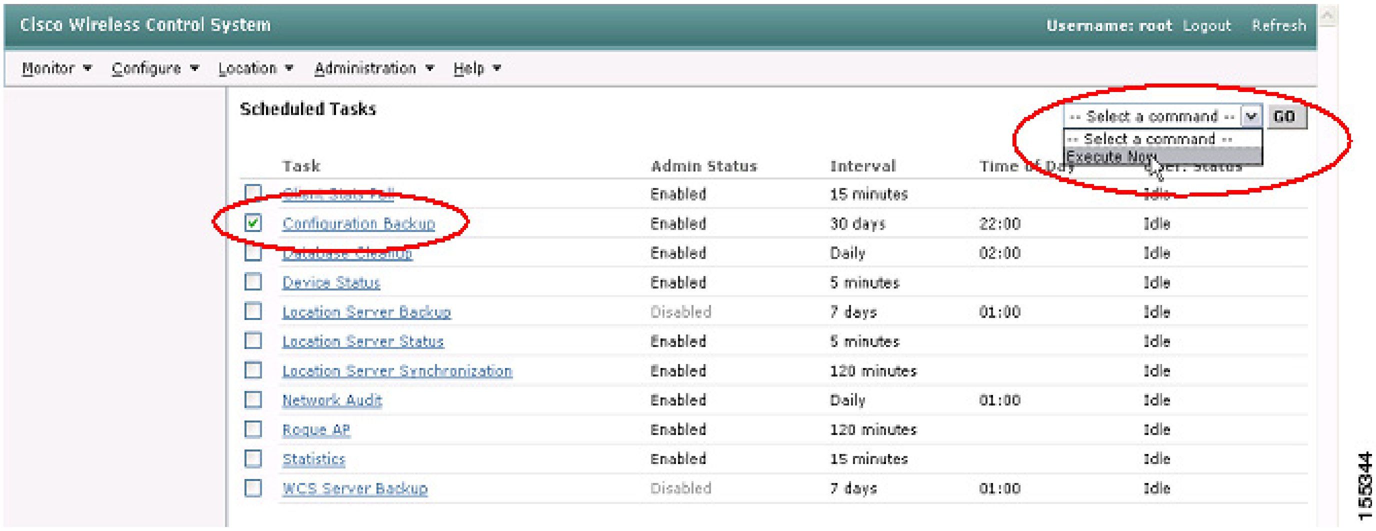

Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Scheduled Tasks
Accounts
Logging
-- Select a command -- GO
155343

Schedul

| | Ta | Admin Status | Interval | Time of Day | Oper. Status |
|---|---|---|---|---|---|
| □ | Client Stats Poll | Enabled | 15 minutes | | Idle |
| □ | Configuration Backup | Enabled | 30 days | 22:00 | Idle |
| □ | Database Cleanup | Enabled | Daily | 02:00 | Idle |
| □ | Device Status | Enabled | 5 minutes | | Idle |
| □ | Location Server Backup | Disabled | 7 days | 01:00 | Idle |
| □ | Location Server Status | Enabled | 5 minutes | | Idle |
| □ | Location Server Synchronization | Enabled | 120 minutes | | Idle |
| □ | Network Audit | Enabled | Daily | 01:00 | Idle |
| □ | Rogue AP | Enabled | 120 minutes | | Idle |
| □ | Statistics | Enabled | 15 minutes | | Idle |
| □ | WCS Server Backup | Disabled | 7 days | 01:00 | Idle |

**Step 2** To do a configuration backup on demand, select the **Configuration Backup** check-box and then select **Execute Now** from the drop-down box and click **Go** (see Figure 98). The backed-up configurations will be stored in the WCS TFTP root directory and labeled with the WLC Management Interface IP address and a timestamp.

*Figure 98 WCS Scheduled Configuration Backup*

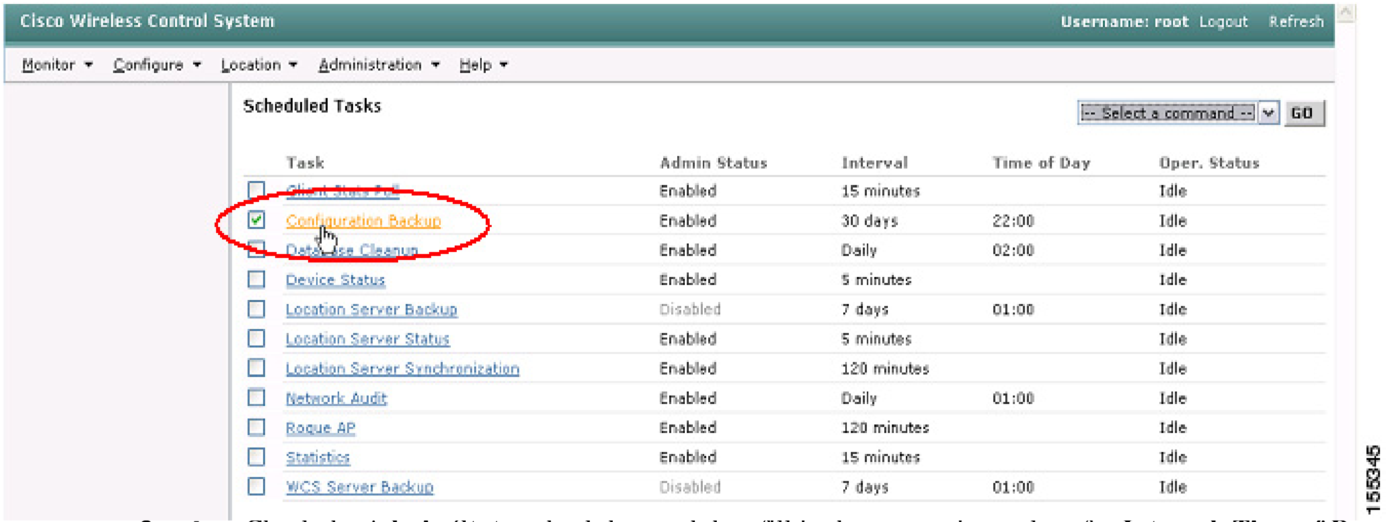

Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
-- Select a command -- GO
-- Select a command --
Execute Now
155344

Scheduled Tasks

| | Task | Admin Status | Interval | Time of Day | Oper. Status |
|---|---|---|---|---|---|
| □ | Client Stats Poll | Enabled | 15 minutes | | Idle |
| ☑ | Configuration Backup | Enabled | 30 days | 22:00 | Idle |
| □ | Database Cleanup | Enabled | Daily | 02:00 | Idle |
| □ | Device Status | Enabled | 5 minutes | | Idle |
| □ | Location Server Backup | Disabled | 7 days | 01:00 | Idle |
| □ | Location Server Status | Enabled | 5 minutes | | Idle |
| □ | Location Server Synchronization | Enabled | 120 minutes | | Idle |
| □ | Network Audit | Enabled | Daily | 01:00 | Idle |
| □ | Rogue AP | Enabled | 120 minutes | | Idle |
| □ | Statistics | Enabled | 15 minutes | | Idle |
| □ | WCS Server Backup | Disabled | 7 days | 01:00 | Idle |

**Step 3** To schedule regular configuration backups, select the **Configuration Backup** link to access the configuration screen (see Figure 99).

*Figure 99 WCS Scheduled Configuration Backup*



Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
-- Select a command -- GO
155345

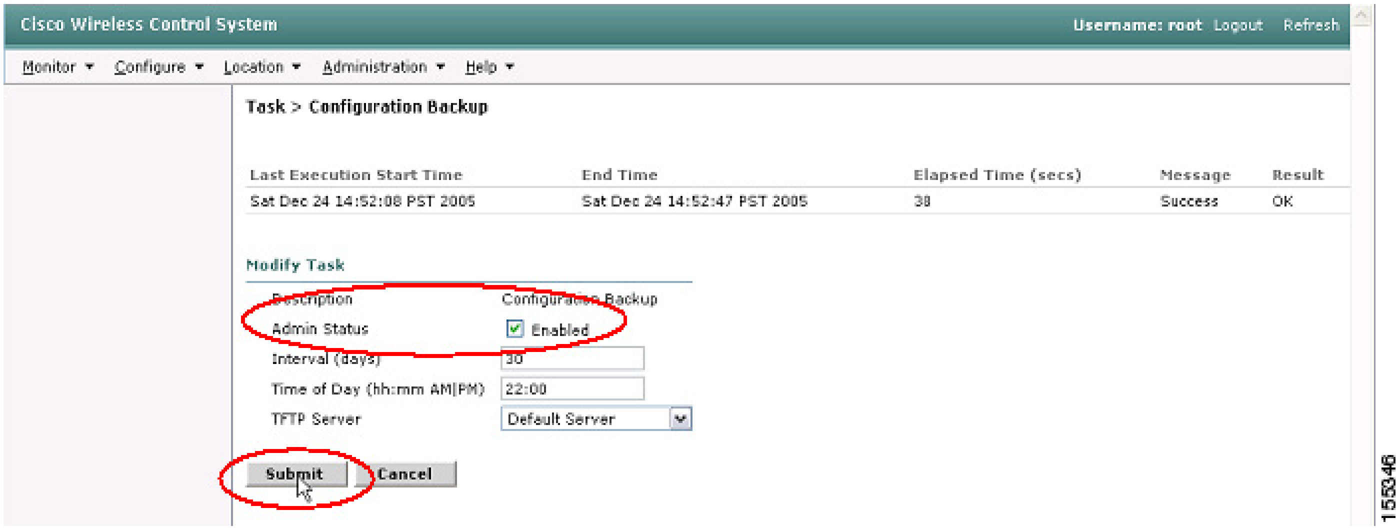
Scheduled Tasks

| | Task | Admin Status | Interval | Time of Day | Oper. Status |
|---|---|---|---|---|---|
| □ | Client Stats Poll | Enabled | 15 minutes | | Idle |
| ☑ | Configuration Backup | Enabled | 30 days | 22:00 | Idle |
| □ | Database Cleanup | Enabled | Daily | 02:00 | Idle |
| □ | Device Status | Enabled | 5 minutes | | Idle |
| □ | Location Server Backup | Disabled | 7 days | 01:00 | Idle |
| □ | Location Server Status | Enabled | 5 minutes | | Idle |
| □ | Location Server Synchronization | Enabled | 120 minutes | | Idle |
| □ | Network Audit | Enabled | Daily | 01:00 | Idle |
| □ | Rogue AP | Enabled | 120 minutes | | Idle |
| □ | Statistics | Enabled | 15 minutes | | Idle |
| □ | WCS Server Backup | Disabled | 7 days | 01:00 | Idle |

**Step 4** Check the **Admin Status** check-box and then fill in the appropriate values for **Interval**, **Time of Day**, and **TFTP Server** (see Figure 100).

**Step 5** Click **Submit** to commit the changes (see Figure 100).

*Figure 100 WCS Scheduled Configuration Backup*



Cisco Wireless Control System
Username: root Logout Refresh
Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾
Submit
Cancel
155346

Task > Configuration Backup

| Last Execution Start Time | End Time | Elapsed Time (secs) | Message | Result |
|---|---|---|---|---|
| Sat Dec 24 14:52:08 PST 2005 | Sat Dec 24 14:52:47 PST 2005 | 38 | Success | OK |

Modify Task

| | |
|---|---|
| Description | Configuration Backup |
| Admin Status | ☑ Enabled |
| Interval (days) | 30 |
| Time of Day (hh:mm AM\|PM) | 22:00 |
| TFTP Server | Default Server |

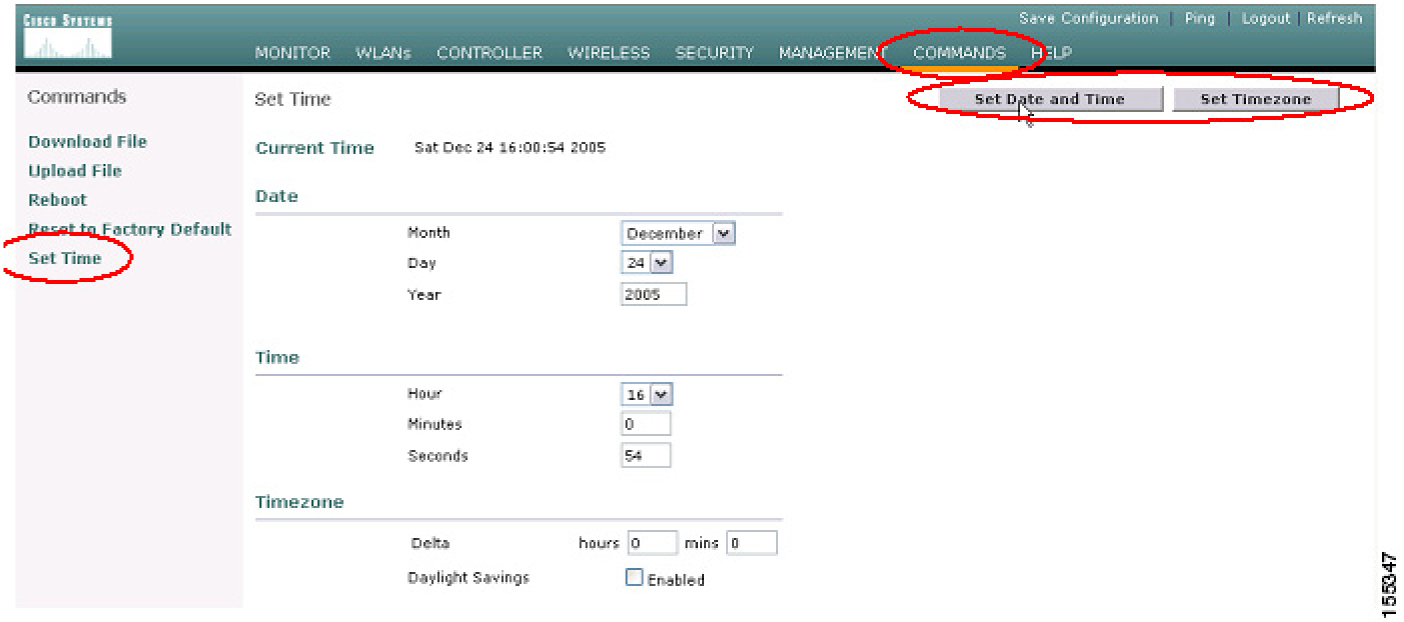
When you want to reset a WLC configuration from the WCS, you may use the Configure | Controllers interface. Select the WLC and then select the appropriate templates to apply to the WLC.

## Managing the WLC Date and Time

Remember that when access points try to join WLCs, there is an exchange of signed X.509 certificates. These X.509 certificates have validity intervals with a start and end time. The validity interval begins at the time the X.509 certificate is provisioned on the access point at the factory, so it is extremely important to keep the WLC's date and time accurate (and current).

To configure the date and time use the WLC GUI interface **Commands | Set Time**. This is displayed in Figure 101:

*Figure 101 WLC Set Date and Time and Timezone*



Set Time

Current Time Sat Dec 24 16:00:54 2005

Date

| | |
|---|---|
| Month | December |
| Day | 24 |
| Year | 2005 |

Time

| | |
|---|---|
| Hour | 16 |
| Minutes | 0 |
| Seconds | 54 |

Timezone

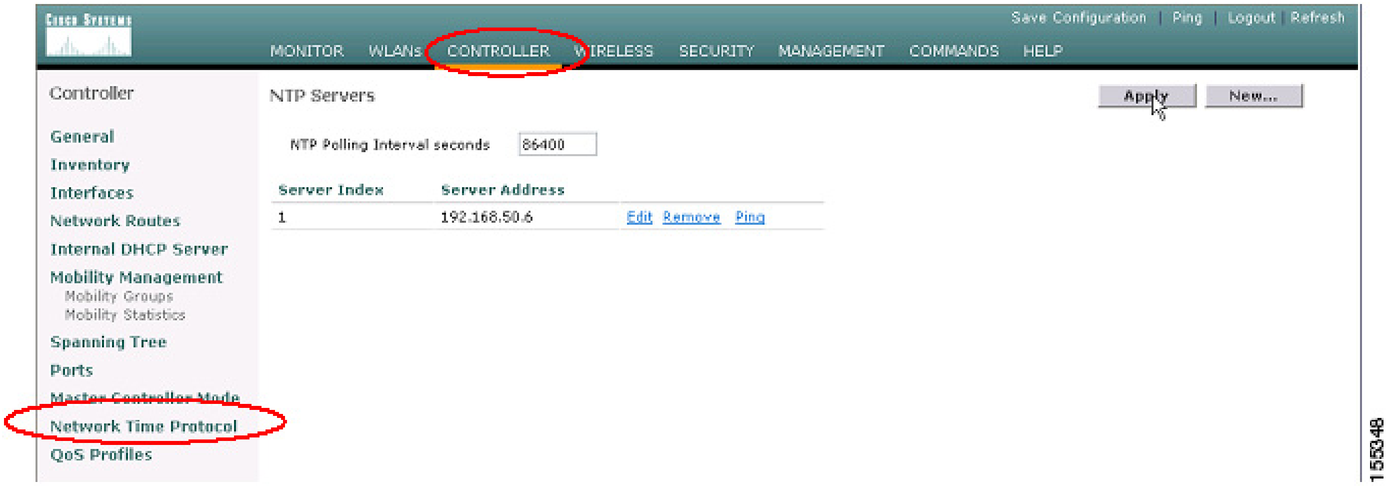
Delta hours 0 mins 0

Daylight Savings □ Enabled

Use this same interface to set the WLC timezone offset (see Figure 101).

When possible, you should configure the WLC to use NTP. To configure NTP through the WLC GUI, use the **Controller | Network Time Protocol** interface as shown in Figure 102:

*Figure 102 WLC NTP Configuration*



NTP Servers

NTP Polling Interval seconds 86400

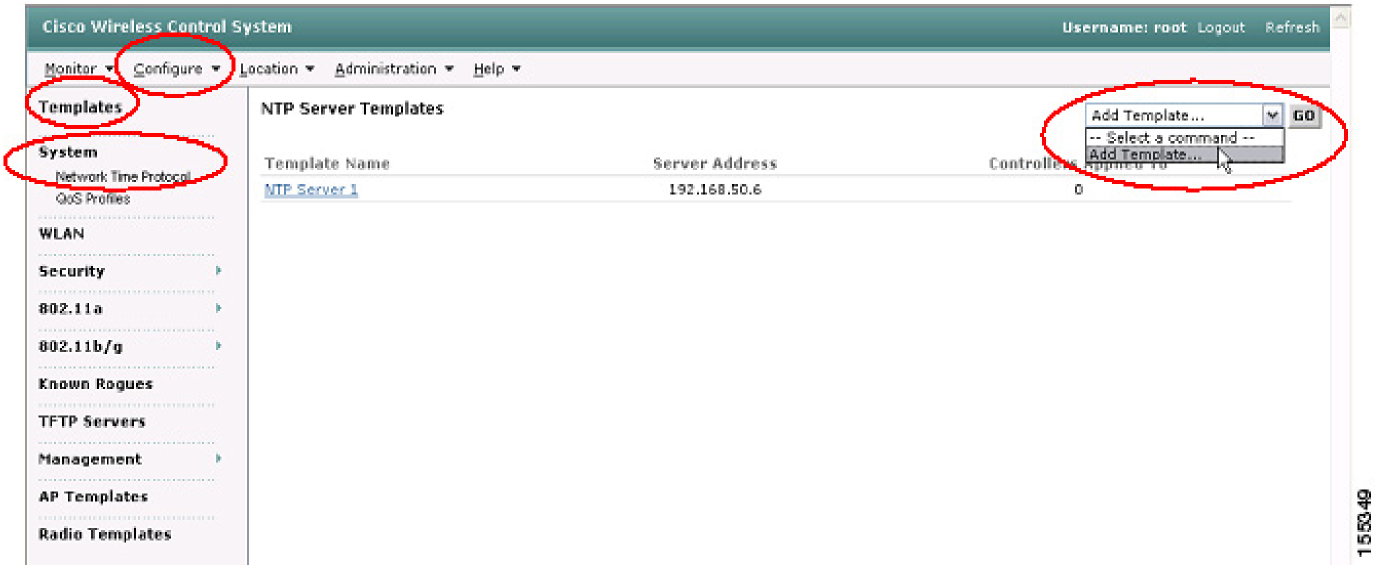
| Server Index | Server Address | |
|---|---|---|
| 1 | 192.168.50.6 | Edit Remove Ping |

You can use WCS to configure NTP:

**Step 1** Navigate in WCS to **Configure | Templates | System | Network Time Protocol** (see Figure 103).

**Step 2** Select **Add Template** from the drop-down box, and then click **Go** (see Figure 103).

*Figure 103 WCS NTP Configuration*



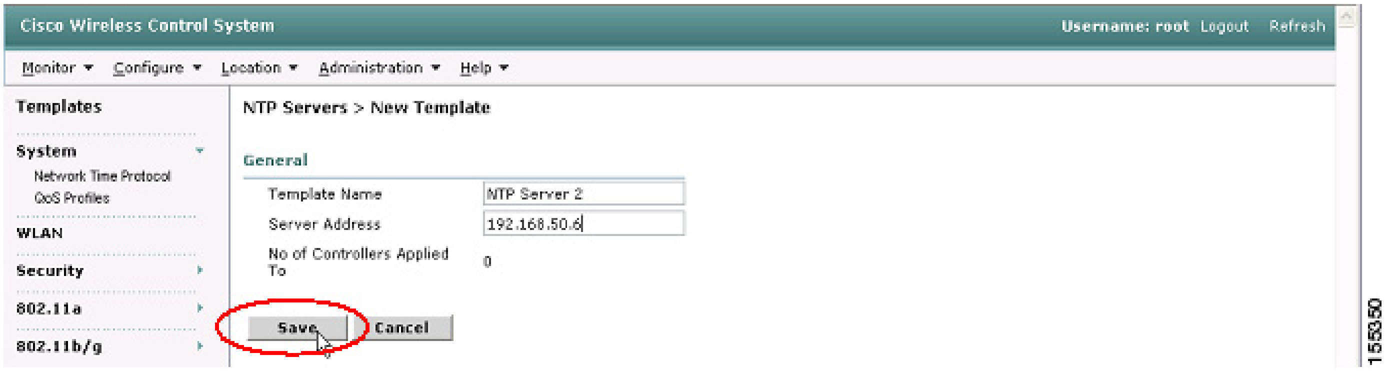
NTP Server Templates

| Template Name | Server Address | Controllers Applied To |
|---|---|---|
| NTP Server 1 | 192.168.50.6 | 0 |

**Step 3** Enter a **Template Name** and **NTP Server Address** in the appropriate fields (see Figure 104).

**Step 4** Click **Save** (see Figure 104).

*Figure 104 WCS NTP Configuration*



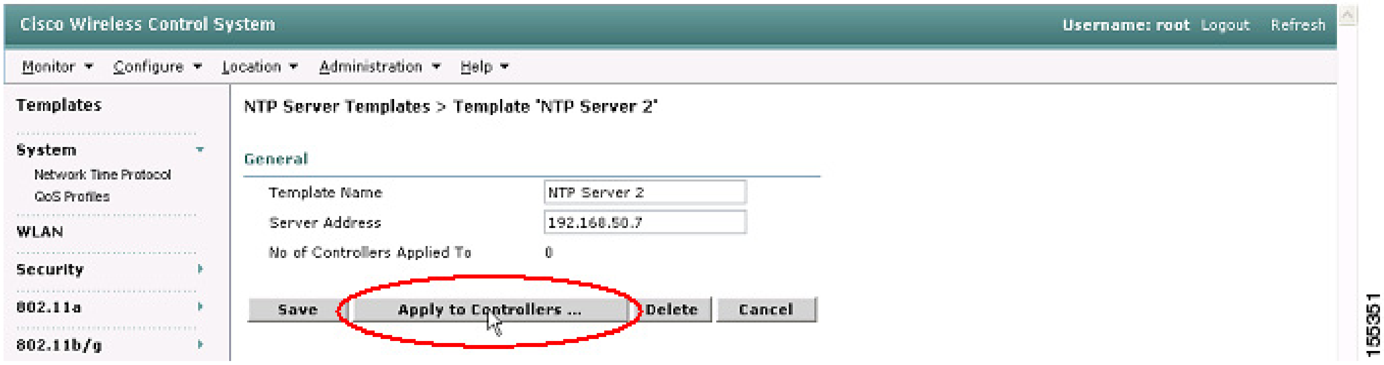
NTP Servers > New Template

General

Template Name: NTP Server 2
Server Address: 192.168.50.6
No of Controllers Applied To: 0

**Step 5** Click **Apply to Controller** (see Figure 105).

*Figure 105 WCS NTP Configuration*



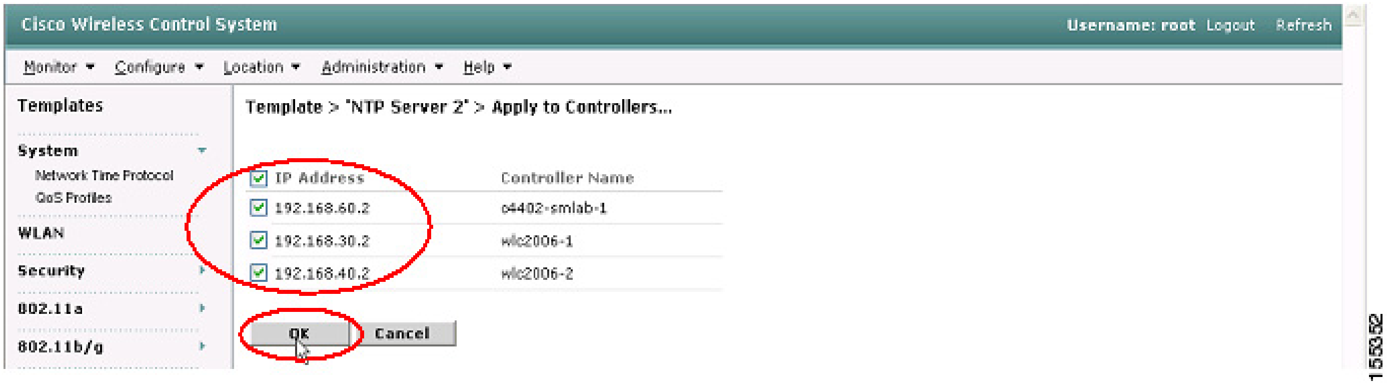
NTP Server Templates > Template 'NTP Server 2'

General

Template Name: NTP Server 2
Server Address: 192.168.50.7
No of Controllers Applied To: 0

**Step 6** Select the appropriate WLCs and then click **OK** (see Figure 106).

*Figure 106 WCS NTP Configuration*



Template > 'NTP Server 2' > Apply to Controllers...

| ☑ IP Address | Controller Name |
|---|---|
| ☑ 192.168.60.2 | c4402-smlab-1 |
| ☑ 192.168.30.2 | wlc2006-1 |
| ☑ 192.168.40.2 | wlc2006-2 |

**Note** When you configure NTP, there is no provision NTP timeout and offset. When you use NTP, you should use UTC settings across the board.

# Conclusion

In this document, we've reviewed the LWAPP architecture and looked at the basics of the Cisco implementation of LWAPP in the Cisco Unified Wireless Network architecture. We reviewed deployment basics, including how Cisco WLC devices connect to networks. We also investigated how the solution supports advanced features like mobility and dynamic radio management. We then considered redundancy, access point load balancing and solution scaling strategies. The document closes by highlighting the basic WLC maintenance tasks.

Additional information about the Cisco Unified Wireless Solution can be found on Cisco.com at http://www.cisco.com/go/wireless.

Consult with your Cisco account representatives as you prepare for new deployments, expansion of an existing deployment, or a migration to the Cisco Unified Wireless Network Solution.

# Appendix A: Relevant Cisco Unified Wireless Nerwork Products

Table 3 lists and describes the Cisco Unified Wireless Network Controller products and accessories.

*Table 3 Cisco Unified Wireless Network Controllers*

| Part Number | Description |
|---|---|
| AIR-WLC4404-100-K9 | 4400 series wireless LAN controller with 4 gigabit fiber ports, 1 copper 10/100 service port. Supports up to 100 Cisco lightweight access points. |
| AIR-WLC4402-50-K9 | 4400 series wireless LAN controller with 2 gigabit fiber ports, 1 copper 10/100 service port. Supports up to 50 Cisco lightweight access points. |
| AIR-WLC4402-25-K9 | 4400 series wireless LAN controller with 2 gigabit fiber ports, 1 copper 10/100 service port. Supports up to 25 Cisco lightweight access points. |
| AIR-WLC4402-12-K9 | 4400 series wireless LAN controller with 2 gigabit fiber ports, 1 copper 10/100 service port. Supports up to 12 Cisco lightweight access points. |
| WS-SVC-WISM-1-K9 | Cisco Catalyst 6500 series wireless services module with support for up to 300 Cisco Aironet lightweight access points. Requires Catalyst 6500 host switch. |
| NM-AIR-WLC6-K9 | Cisco wireless LAN controller module for managing up to 6 lightweight access points (when sold as part of an Integrated Services Router (ISR) system. Requires Cisco 2800, 3700, and 3800 series (excluding Cisco 2801 routers) ISR |
| NM-AIR-WLC6-K9= | Cisco wireless LAN controller module for up to 6 lightweight access points (spare, ordered as an individual unit). Requires Cisco 2800, 3700, and 3800 series (excluding Cisco 2801 routers) ISR |
| AIR-WLC2006-K9 | Cisco 2000 series wireless LAN controller with 4 10/100 copper ports. Supports up to 6 Cisco lightweight access points. |
| AIR-PWR-4400-AC | AC power supply for Cisco 4400 series wireless LAN controllers |

For more details on ordering appliance-based Cisco Wireless LAN Controllers (2006 and 440x Series), please consult the following document:

http://www.cisco.com/en/US/docs/wireless/technology/guest_access/technical/reference/4.0/GAccess.html

For more details on ordering the Cisco Wireless LAN Service Module (WiSM), please consult the following document:

http://www.cisco.com/en/US/prod/collateral/modules/ps2706/ps6526/product_data_sheet0900aecd80364340.html

For more details on ordering the Cisco Wireless LAN Controller Module (WLCM) for the ISR product family, please consult the following document:

http://www.cisco.com/en/US/prod/collateral/modules/ps2797/ps6730/product_data_sheet0900aecd80364432.html

Table 4 lists Cisco access points that can be used with Cisco wireless LAN controller products:

*Table 4 Cisco Access Point Options for the Cisco Unified Wireless Network Architecture*

| Cisco Access Point Part Numbers | Comments |
|---|---|
| AIR-AP1010-x-K9(see Note) | Cisco 1000 Series Access Point with internal antennae only. Supports 802.11a/b/g. |
| AIR-AP1020-x-K9(see Note) | Cisco 1000 Series Access Point with internal antennae and RPC-TNC connectors for external antennae. Supports 802.11a/b/g. |
| AIR-AP1030-x-K9(see Note) | Cisco 1000 Series Access Point with internal antennae and RPC-TNC connectors for external antennae. Includes Remote Edge Access Point (REAP) support. Supports 802.11a/b/g. |
| AIR-PWR-1000 | Power supply brick for Cisco 1000 Series Access Point. |
| AIR-ACC-WBRKT1000 | Wall-mount bracket kit for Cisco 1000 Series Access Point. |
| AIR-ACC-CEBZL1000 | Ceiling-mount bezel kit for Cisco 1000 Series Access Point. |
| AIR-PWRINJ-1000AF | 802.3af power injector for Cisco 1000 Series Access Point. |
| AIR-AP1131AG-x-K9(see Note) | Cisco 1130AG Series Access Point. This is the autonomous IOS-based version that must be loaded with a special IOS software version using an upgrade utility from Cisco to work in lightweight mode. Supports 802.11a/b/g. This is a non-modular access point with integrated antennae. |
| AIR-LAP1131AG-x-K9(see Note) | Cisco 1130AG Series Access Point. This is the lightweight IOS-based version that works from the factory with Cisco Wireless LAN Controllers. Supports 802.11a/b/g. This is a non-modular access point with integrated antennae. |
| AIR-PWR-A | Power supply for the 1130AG, 1210, 1230AG and 1240AG Series access points. |
| AIR-PWRINJ3 | Cisco Aironet power injector for the Cisco 1130AG, 1210, 1230AG and 1240AG Series access points. |
| AIR-PWRINJ-FIB | Cisco Aironet power injector media converter (fiber to copper) for Cisco 1130AG and 1240AG Series access points. |
| AIR-AP1242AG-x-K9(see Note) | Cisco 1240AG Series Access Point. This is the autonomous IOS-based version that must be loaded with a special IOS software version using an upgrade utility from Cisco to work in lightweight mode. Supports 802.11a/b/g. This is a non-modular access point with RPC-TNC connectors for external antennae. |
| AIR-LAP1242AG-x-K9(see Note) | Cisco 1130AG Series Access Point. This is the lightweight IOS-based version that works from the factory with Cisco Wireless LAN Controllers. Supports 802.11a/b/g. This is a non-modular access point with RPC-TNC connectors for external antennae. |
| Antennae and accessories for the Cisco 1000, 1210, 1230, and 1240 series access points; Consult the Cisco Aironet Antenna Reference Guide | http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html |
| AIR-AP1232AG-x-K9(see Note) | Cisco 1230AG Series Access Point based on the AIR-AP1210 chassis. This is the autonomous IOS-based version that must be loaded with a special IOS software version using an upgrade utility from Cisco to work in lightweight mode. Supports modular 802.11a and 802.11b/g radios. The 802.11b/g radios have RPC-TNC connectors for external antennae. The 802.11a radios can be selected as either the AIR-RM21A, which has a fixed antennae or the AIR-RM22A radio which has RPC-TNC connectors. |

| Cisco Access Point Part Numbers | Comments |
|---|---|
| AIR-LAP1232AG-x-K9(see Note) | Cisco 1230AG Series Access Point based on the AIR-AP1210 chassis. This is the lightweight IOS-based version that works from the factory with Cisco Wireless LAN Controllers. Supports modular 802.11a and 802.11b/g radios. The 802.11b/g radios have RPC-TNC connectors for external antennae. The 802.11a radios can be selected as either the AIR-RM21A, which has a fixed antennae or the AIR-RM22A radio which has RPC-TNC connectors. |
| AIR-AP1231G-x-K9(see Note) | Cisco 1230G Series Access Point based on the AIR-AP1210 chassis. This is the autonomous IOS-based version that must be loaded with a special IOS software version using an upgrade utility from Cisco to work in lightweight mode. This access point comes from the factory with ONLY 802.11b/g radios with RPC-TNC connectors for external antennae. An 802.11A radio (AIR-RM21A-x-K91 or AIR-RM22A-x-K91) can be added as a module. |
| AIR-LAP1231G-x-K9(see Note) | Cisco 1230G Series Access Point based on the AIR-AP1210 chassis. This is the lightweight IOS-based version that works from the factory with Cisco Wireless LAN Controllers. This access point comes from the factory with ONLY 802.11b/g radios with RPC-TNC connectors for external antennae. An 802.11A radio (AIR-RM21A-x-K91 or AIR-RM22A-x-K91) can be added as a module. |
| AIR-AP1210 | Cisco 1210 Series Access Point chassis. This is the autonomous IOS-based version that must be loaded with a special IOS software version using an upgrade utility from Cisco to work in lightweight mode. This access point chassis has RPC-TNC connectors for external antennae for the AIR-MP21G-x-K91 radio module. An 802.11A radio (AIR-RM21A-x-K91 or AIR-RM22A-x-K91) can also be added as a module. |
| AIR-LAP1210 | Cisco 1210 Series Access Point chassis. This is the lightweight IOS-based version that works from the factory with Cisco Wireless LAN Controllers. This access point chassis has RPC-TNC connectors for external antennae for the AIR-MP21G-x-K91 radio module. An 802.11A radio (AIR-RM21A-x-K91 or AIR-RM22A-x-K91) can also be added as a module. |
| AIR-MP21G-x-K9(see Note) | 802.11G module for the Cisco Aironet 1210 Series access point. |
| AIR-RM21A-x-K9(see Note) | 802.11A module for the Cisco Aironet 1210 Series access point with integrated "paddle" antenna. |
| AIR-RM22A-x-K9(see Note) | 802.11A module for the Cisco Aironet 1210 Series access point with RPC-TNC connectors for external antenna. |

**Note** Each access point is configured with a regulatory domain code in the part number. In the table above, these values have been abstracted with an "x". You should substitute in the appropriate value for your access point part numbers.

The values are as follows:

- A = FCC
- C = China
- E = ETSI
- I = Israel
- J = Japan

- K = Korea
- N = North America (excluding FCC).
- P = Japan 2
- S = Singapore
- T = Taiwan

For more details on compliance, please consult the following resource:

- http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps6087_Products_Data_Sheet.html

  Note that Cisco 1000 Series Access Points support only A, E, and J.

For more details on ordering Cisco access points, consult the following documents:

- Cisco 1000 Series Lightweight Access Point:

  http://www.cisco.com/en/US/products/ps6306/
- Cisco Aironet 1130AG Series Ordering Guide:

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6087/product_data_sheet0900aecd801b901c.html
- Cisco Aironet 1200 Series Access Point Ordering Guide:

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/product_data_sheet0900aecd801b91d4.html
- Cisco Aironet 1230AG Series Access Point Ordering Guide:

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6108/product_data_sheet0900aecd801b9266.html
- Cisco Aironet 1240AG Series Access Point Ordering Guide:

  http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps6521/product_data_sheet0900aecd8031c968.html
- Cisco Aironet Antenna Reference Guide:

  http://www.cisco.com/en/US/prod/collateral/wireless/ps7183/ps469/product_data_sheet09186a008008883b.html

# Appendix B: Protocols and Protocol Ports Used by the Cisco Unified Wireless Network Solution

When the Cisco Unified Wireless Network Solution is deployed in the network, it may be necessary to allow protocols and protocol ports through firewalls and/or access control lists. This appendix reviews the protocol ports that must be opened and where they should be opened. This apendix does not contain security best practices and/or recommendations. It simply lists the protocols and ports used in the Cisco Unified Wireless Network Solution. Best practices for securing your network should always be followed. Cisco security best practices can be found here: http://www.cisco.com/go/safe.

In some cases, protocol ports can be changed. It is assumed that the protocols are using the defaults and well known ports if and where applicable. If default ports have been changed in your network, you'll need to adapt the information here to your network.

## LWAPP Protocols and Ports

All packets transmitted between the WLC and its joined access points are LWAPP encapsulated. The WLC(s) use(s) **UDP port 12222 for LWAPP Data Packets and UDP port 12223 for LWAPP Control Messages.** The access point uses an ephemeral port that is derived from a hash of its MAC address. So an LWAPP Data Packet transmitted from the access point to the WLC would be transported in a UDP packet using the ephemeral port as the source port and UDP port 12222 as the destination port. An LWAPP Data Packet traveling the reverse path from WLC to the access point uses UDP port 12222 as source and the access point ephemeral port as the destination port. An LWAPP Control Message sent from the WLC to an access point uses UDP port 12223 as the source port and the access point ephemeral port as the destination port. An LWAPP Control Message sent from the access point to the WLC uses the access point ephemeral port as source and UDP port 12223 as the destination.

## Mobility Protocols and Protocol Ports

Forwarded data traffic, including data traffic forwarded as a result of layer 3 roaming and the "guest tunneling" feature, between WLCs in a mobility group is carried in Ethernet in IP (EtherIP) tunnels. EtherIP is defined in RFC 3378. EtherIP defines a simple mechanism whereby Ethernet frames are encapsulated in IP packets. The IP packet headers have the 8-bit protocol field set to a decimal value of 97 (0x61). IP Protocol 97 must be allowed through any firewalls and ACLs.

Mobility control messages are exchanged between WLCs in UDP packets. The mobility protocol ports are UDP 16666, or 16667 if the mobility messages are encrypted. **UDP ports 16666 and/or 16667** must be bi-directionally opened to support Mobility Groups.

## RF Group Protocols and Protocol Ports

The members of an RF Group will exchange RRM messages. At the RF Group update interval (by default, every 600 seconds), the RF Group leader and members exchange RRM messages during a re-evaluation of the current radio and channel plan. Between the update intervals, the non-leader members of the RF Group send periodic update messages and data to the RF Group leader. All messages are carried in UDP datagrams. For all 802.11b/g RRM messages, the UDP datagrams use UDP ports 12124 (client) and 12134 (manager). For all 802.11a RRM messages, the UDP datagrams use UDP ports 12125 (client) and 12135 (manager). **UDP ports 12124, 12134, and 12135** must be allowed between all WLCs belonging to an RF Group.

## WLC Management Protocols and Ports

WCS communicates with the WLCs using SNMP for both polling and configuration. WLCs send asynchronous SNMP Traps to the WCS to notify the WCS of certain events. SNMP uses UDP as transport and the well known **UDP ports 161 and 162.** You may override the default ports if you choose to do so. In the default case, you need to allow bi-directional traffic using UDP port 161 as the destination port between the WCS and each WLC for SNMP polling and configuration. You'll need to allow traffic using UDP port 162 from the WLC to the WCS to allow SNMP traps through.

If you've configured a WLC to send SYSLOG messages to a SYSLOG server, you'll need to make sure you allow the messages through any firewall or ACL between the WLC and SYSLOG server. SYSLOG uses the well-known **UDP port 514** so you'll need to open that port for SYSLOG messages from the WLC to the SYSLOG server.

If you've configured the WLCs to use NTP for time, then you need to allow the NTP synchronizations between the WLC and the NTP server. NTP is assigned the well-known **port 123 (both TCP and UDP)**, so you'll need to allow bi-directional traffic using port 123 between the WLC and NTP server.

When you're using 802.1X authentication, you'll need to allow RADIUS communications between the WLC Management Interface and the RADIUS Server. RADIUS is assigned **UDP port 1812 for authentication and port 1813 for RADIUS accounting. Cisco ACS also uses ports 1645 for authentication and 1646 for accounting.** Other RADIUS servers may use non-standard ports. Consult your vendor documentation for the RADIUS ports used by the product.

The WLC also acts as a DHCP proxy for wireless LAN clients by forwarding broadcast client DHCP requests to the DHCP server. You'll need to allow these DHCP messages. DHCP is assigned well-known **port 67 for DHCP clients and port 68 for DHCP servers**. You need to allow DHCP between the WLC and DHCP server.

You'll also want to allow TFTP from the WLC to the TFTP servers you use to upgrade code and backup configurations. This could be the WCS, or some other TFTP server. TFTP uses **UDP port 69** so this needs to be allowed.

## Management Access Protocols and Ports

WCS can be accessed only remotely and only via web browser using HTTPS. The default (and well-known) port for HTTPS is **TCP port 443**. This can be overridden at the time WCS is installed. Whichever port is used, web browser access needs to be allowed to the port for TCP traffic.

WLC devices are only accessible via console port, SSH and secure HTTP by default. The default HTTPS port is TCP port 443. This cannot be overridden in the case of the WLC, although HTTPS access can be disabled. As long as HTTPS access is enabled, you need to allow web browser access to TCP port 443 on the WLC. You can also disable SSH if you want. But if you leave SSH enabled, you need to allow SSH traffic to TCP port 22.

Telnet and HTTP can also be enabled on the WLC. If you enable HTTP, you need to allow web browser access to TCP port 80. When you enable telnet on the WLC, you need to allow access to TCP port 23.

# Appendix C: How the Vendor-Specific DHCP Option (Option 43) is Used to Faclitate Controller Discovery

Appendix C describes how to use vendor-specific options to facilitate controller discovery by the access point. RFC 2132 defines two DHCP Options-Option 60 and Option 43-that are relevant. DHCP Option 60 is the Vendor Class Identifier (VCI). The VCI is a text string that uniquely identifies a type of vendor device. Table 4 lists the VCIs used by Cisco access points.

*Table 5 Cisco Access Point Vendor Class Identifiers*

| Access Point Model | Vendor Class Identifier (VCI) |
|---|---|
| Cisco Aironet 1000 series | Airespace.AP1200 |
| Cisco Aironet 1100 series | Cisco AP c1100 |
| Cisco Aironet 1130 series | Cisco AP c1130 |
| Cisco Aironet 1140 Series | Cisco AP c1140 |
| Cisco Aironet 1200 series | Cisco AP c1200 |
| Cisco Aironet 1230 series | Cisco AP c1200 |
| Cisco Aironet 1240 series | Cisco AP c1240 |
| Cisco Aironet 1250 Series | Cisco AP c1250 |
| Cisco Aironet 1300 series | Cisco AP c1300 |
| Cisco Aironet 1500 series | Cisco AP c1500[1]<br>Cisco AP.OAP1500[2]<br>Cisco AP.LAP1505[3]<br>Cisco AP.LAP1510[4]<br>Cisco AP c1520<br>Airespace.AP1200[5] |
| Cisco 3201 Lightweight Access Point | Cisco Bridge/AP/WGB c3201 |
| Cisco 521 Wireless Express Access Point | Cisco AP c520 |
| AP801 (embedded in 86x/88x series ISRs | Cisco AP801 |

[1] Any 1500 Series AP that runs 4.1 software

[2] 1500 OAP AP that runs 4.0 software

[3] 1505 Model AP that runs 4.0 software

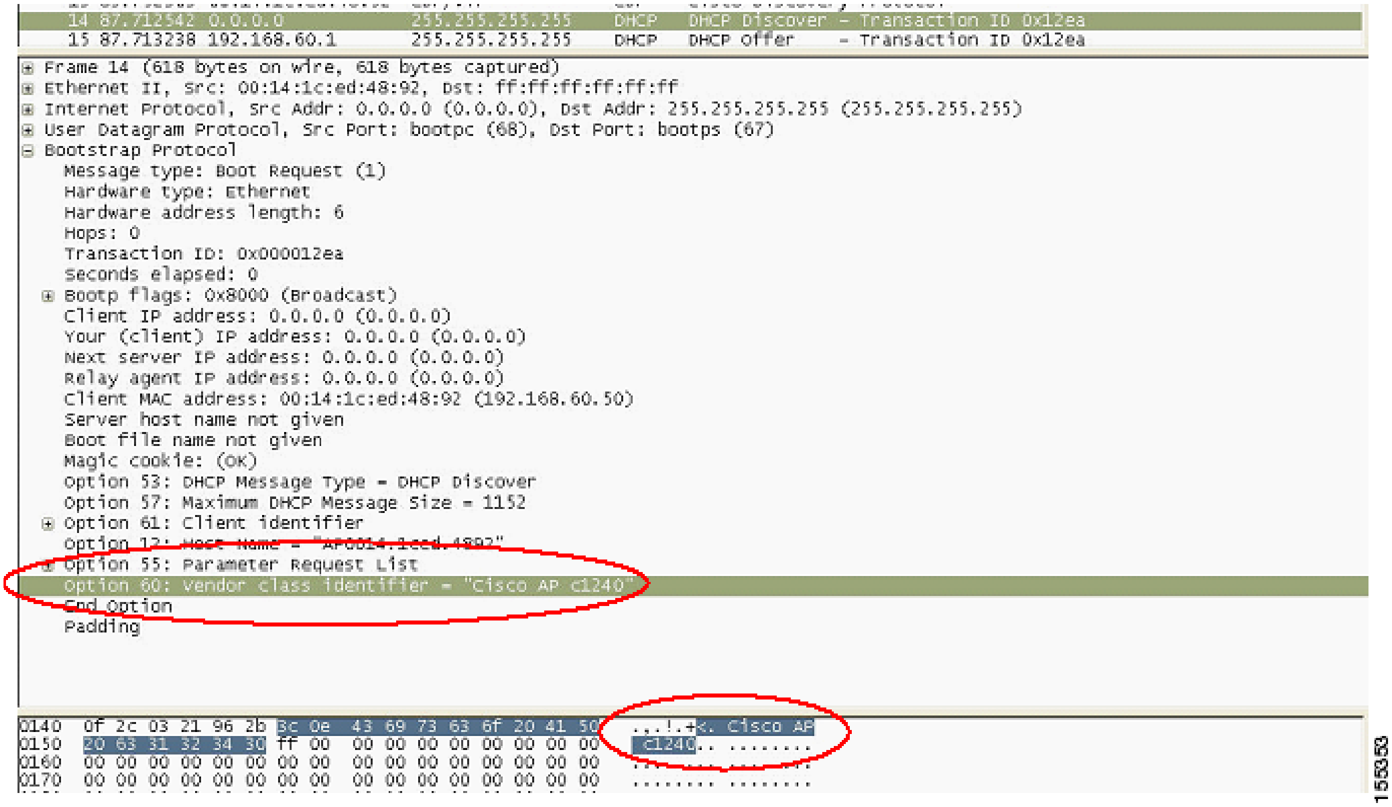
[4] 1510 Model AP that runs 4.0 software

[5] Any 1500 Series AP that runs 3.2 software

The VCI values listed in Table 4 are embedded as DHCP Option 60 in DHCP DISCOVER packets from Cisco access points that is broadcast by  the access point as a DHCP client in search of an address.

Figure 107 shows a decoded DHCP DISCOVER packet send by a Cisco Aironet 1240 Series access point that includes the VCI:

*Figure 107 DHCP Option 60 Decode*

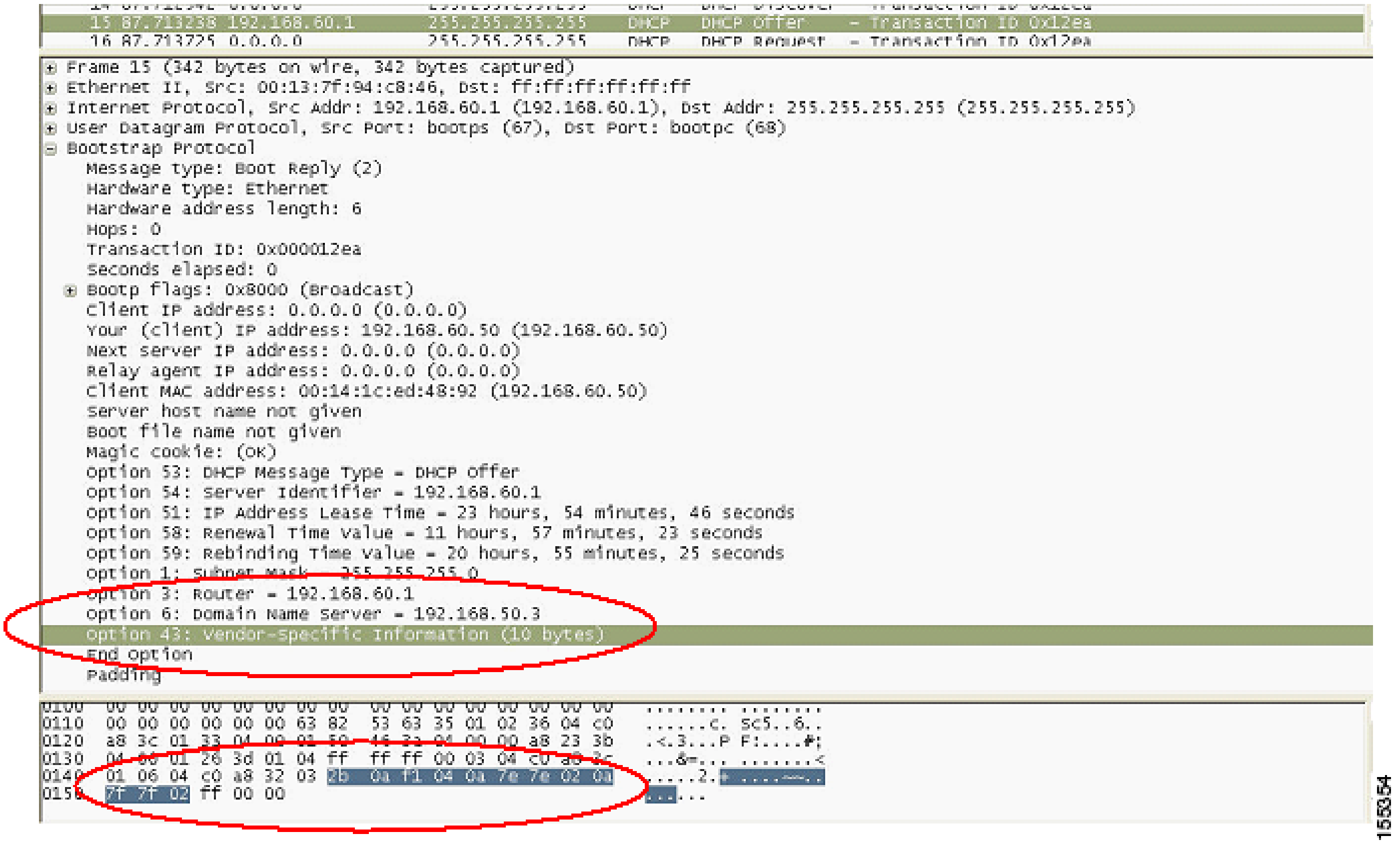


```
 14 87.712542 0.0.0.0          255.255.255.255   DHCP   DHCP Discover - Transaction ID 0x12ea
 15 87.713238 192.168.60.1     255.255.255.255   DHCP   DHCP Offer    - Transaction ID 0x12ea
⊞ Frame 14 (618 bytes on wire, 618 bytes captured)
⊞ Ethernet II, Src: 00:14:1c:ed:48:92, Dst: ff:ff:ff:ff:ff:ff
⊞ Internet Protocol, Src Addr: 0.0.0.0 (0.0.0.0), Dst Addr: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊟ Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x000012ea
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:14:1c:ed:48:92 (192.168.60.50)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Discover
    Option 57: Maximum DHCP Message Size = 1152
  ⊞ Option 61: Client identifier
    Option 12: Host Name = "AP0014.1ced.4892"
  ⊞ Option 55: Parameter Request List
    Option 60: Vendor class identifier = "Cisco AP c1240"
    End Option
    Padding

0140  0f 2c 03 21 96 2b 3c 0e  43 69 73 63 6f 20 41 50   .,.!.+<. Cisco AP
0150  20 63 31 32 34 30 ff 00  00 00 00 00 00 00 00 00    c1240.. ........
0160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

On the DHCP Server, vendor specific information is mapped to the VCI text string. When the DHCP server sees a recognizable VCI in a DHCP DISCOVER from a DHCP client, it returns the mapped (to the VCI) vendor specific information in its DHCP OFFER to the client as DHCP Option 43.

Figure 108 shows a decoded DHCP OFFER to a Cisco Aironet 1240 Series access point that includes Option 43 values:

*Figure 108 DHCP Option 43 Decode*



```
   14 87.712942 0.0.0.0          255.255.255.255   DHCP    DHCP Discover   - Transaction ID 0x12ea
   15 87.713238 192.168.60.1     255.255.255.255   DHCP    DHCP Offer      - Transaction ID 0x12ea
   16 87.713725 0.0.0.0          255.255.255.255   DHCP    DHCP Request    - Transaction ID 0x12ea
⊞ Frame 15 (342 bytes on wire, 342 bytes captured)
⊞ Ethernet II, Src: 00:13:7f:94:c8:46, Dst: ff:ff:ff:ff:ff:ff
⊞ Internet Protocol, Src Addr: 192.168.60.1 (192.168.60.1), Dst Addr: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
⊟ Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x000012ea
    Seconds elapsed: 0
  ⊞ Bootp flags: 0x8000 (Broadcast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 192.168.60.50 (192.168.60.50)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: 00:14:1c:ed:48:92 (192.168.60.50)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Offer
    Option 54: Server Identifier = 192.168.60.1
    Option 51: IP Address Lease Time = 23 hours, 54 minutes, 46 seconds
    Option 58: Renewal Time Value = 11 hours, 57 minutes, 23 seconds
    Option 59: Rebinding Time Value = 20 hours, 55 minutes, 25 seconds
    Option 1: Subnet Mask = 255.255.255.0
    Option 3: Router = 192.168.60.1
    Option 6: Domain Name Server = 192.168.50.3
    Option 43: Vendor-Specific Information (10 bytes)
    End Option
    Padding

0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0110  00 00 00 00 00 00 63 82  53 63 35 01 02 36 04 c0   ......c. Sc5..6..
0120  a8 3c 01 33 04 00 01 50  46 3a 04 00 00 a8 23 3b   .<.3...P F:....#;
0130  04 00 01 26 3d 01 04 ff  ff ff 00 03 04 c0 a8 3c   ...&=... .......<
0140  01 06 04 c0 a8 32 03 2b  0a f1 04 0a 7e 7e 02 0a   .....2.+ ....~~..
0150  7f 7f 02 ff 00 00                                  ......
```

To facilitate access point discovery of wireless LAN controllers using DHCP Option 43, the DHCP Server should be programmed to return one or more WLAN Controller Management Interface IP addresses based on the access point's VCI. Typically, this involves programming the DHCP Server to recognize the VCI for each access point type and then defining the vendor specific information that is returned in Option 43 on a per scope or super-scope basis for each VCI.

RFC 2132 defines the format that DHCP Servers should return vendor specific information as DHCP Option 43. The RFC allows for vendors to define encapsulated vendor-specific "sub-option" codes between 0 and 255 exclusive. The sub-options are all included in the DHCP Offer as type-length-value (TLV) blocks embedded within Option 43. The definition of the sub-option codes and their corresponding message format is left to the vendors.

When programming DHCP Servers to offer WLAN Controller IP addresses as Option 43 for Cisco 1000 series access points, the sub-option TLV block is defined as follows:

**Type:** 0x66 (decimal 102)

**Length:** The length of the ASCII string in the Value field. The length is a count of the characters in ASCII string in the value field. Length should include the commas if there are more than one controller specified, but not a zero-terminator.

**Value:** A non-zero terminated ASCII string that is a comma-separated list of controllers. No spaces should be embedded in the list.

When programming DHCP Servers to offer WLAN Controller IP addresses as Option 43 for Cisco Aironet 1130, 1200, and/or 1240 series access points, the sub-option TLV block is defined as follows:

**Type:** 0xf1 (decimal 241)

**Length:** Number of controller IP addresses * 4

**Value**: List of WLC management interfaces (typically translated to hexadecimal values)

The semantics of DHCP Server configuration vary per DHCP Server vendor. Appendix D contains specific instructions on configuring vendor specific options for access points to discover wireless LAN controllers in the IOS DHCP Server. Appendix E contains specific details for configuring vendor specific options for access points to discover wireless LAN controllers in the Windows 2000 and 2003 DHCP Server. For other DHCP Server products, consult the vendor documentation for instructions on configuring vendor specific options.

## Software Requirements

Cisco 1000 series access points require version 3.2 or later code to be pre-loaded on the access point in order to use the Vendor Class Identifier feature of DHCP (Option 60). If code earlier than 3.2 is loaded on the access point, then an alternate controller discovery method may be necessary. Suggested alternate methods for access point discovery of the Wireless LAN Controller (WLC) are:

1. Placing the access point in same subnet/VLAN as the WLC management interface (priming the access point)
2. Mapping the host name CISCO-LWAPP-CONTROLLER to the IP address of the WLC management interface in DNS.

   The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.*localdomain* or CISCO-CAPWAP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.
3. Over the Air Provisioning (OTAP) from a neighboring access point
4. Raw DHCP Option 43 (without specifying a VCI) [1]

There are no software limitations on Cisco Aironet 1130, 1200, and 1240 lightweight access points.

[1] Raw DHCP Option 43 without specifying a VCI should be avoided if possible. Using a raw DHCP Option 43 limits the DHCP Server to supporting a single device type for vendor specific information per DHCP scope. Also, every DHCP client will receive the Option 43 values in a DHCP Offer, whether the values are relevant to the device or not.

# Appendix D: Configuring Vendor-Specific DHCP Options (Option 43) in the Cisco IOS DHCP Server

This appendix entry describes the configurations necessary on the IOS DHCP server to use DHCP Option 43 for wireless LAN controller discovery.

The IOS DHCP Server only allows Option 43 definitions for one device type per DHCP address pool so only one access point type can be supported per DHCP address pool.

## Cisco Aironet Series Access Points (Cisco Aironet 1130, 1200, 1240 Series)-Embedded IOS DHCP Server

The steps to configure DHCP Option 43 for lightweight Cisco Aironet access points in the embedded IOS DHCP server are:

**Step 1** Enter configuration mode at the IOS CLI.

**Step 2** Create the DHCP pool, including the necessary parameters such as default router and name server. An example DHCP scope is as follows:

```
ip dhcp pool <pool name>
    network <IP Network> <Netmask>
    default-router <Default router>
    dns-server <DNS Server>
```

**Step 3** Add the option 60 line using the following syntax:

```
option 60 ascii "VCI string"
```

For the VCI string, use the value from Table 4. The quotation marks must be included.

**Step 4** Add the option 43 line using the following syntax:

```
option 43 hex <hexadecimal string>
```

The hexadecimal string in Step **4** is assembled by concatenating the TLV values for the Option 43 sub-option.

```
Type + Length + Value
```

"Type" is always the sub-option code 0xf1. "Length" is the number of controller management IP addresses times 4 in hex. "Value" is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to 0a7e7e02 (10.126.126.2) and 0a7f7f02 (10.127.127.2). Assembling the string then yields f1080a7e7e020a7f7f02. The IOS command then added to the DHCP scope is:

```
option 43 hex f1080a7e7e020a7f7f02
```

# Cisco 1000 Series Access Points-Embedded IOS DHCP Server

The steps to configure DHCP Option 43 for lightweight Cisco 1000 Series access points in the embedded IOS DHCP server are:

**Step 1** Enter configuration mode at the IOS CLI.

**Step 2** Create the DHCP pool, including the necessary parameters such as default router and name server. An example DHCP scope is as follows:

```
ip dhcp pool <pool name>
 network <IP Network> <Netmask>
 default-router <Default router>
 dns-server <DNS Server>
```

**Step 3** Add the option 60 line using the following syntax:

```
option 60 ascii "Airespace.AP1200"
```

The quotation marks must be included.

**Step 4** Add the option 43 line using the following syntax:

```
option 43 ascii "Comma Separated IP Address List"
```

The quotation marks must be included. Note that no sub-option value needs to be defined in the IOS DHCP Server for Cisco 1000 Series access points.

For example, if you are configuring option 43 for Cisco 1000 series access points using the controller values 10.126.126.2 and 10.127.127.2, add the following line to the DHCP pool in the IOS CLI:

```
option 43 ascii "10.126.126.2,10.127.127.2"
```

# Appendix E: Configuring Vendor-Specific DHCP Options (Option 43) in the Windows 2000 and 2003 DHCP Server

This Appendix section describes how to configure a Microsoft Windows 2000 DHCP Server and Microsoft Windows 2003 DHCP Server to send the appropriate value for DHCP Option 43 to Cisco Lightweight access points.

## Configuring Vendor-Specific DHCP Options for Cisco 1000 Series Access Points

In this section, we'll take a look at how the Windows DHCP Server is used to configured to return vendor specific information to Cisco 1000 access points. Key information you'll need to know are:

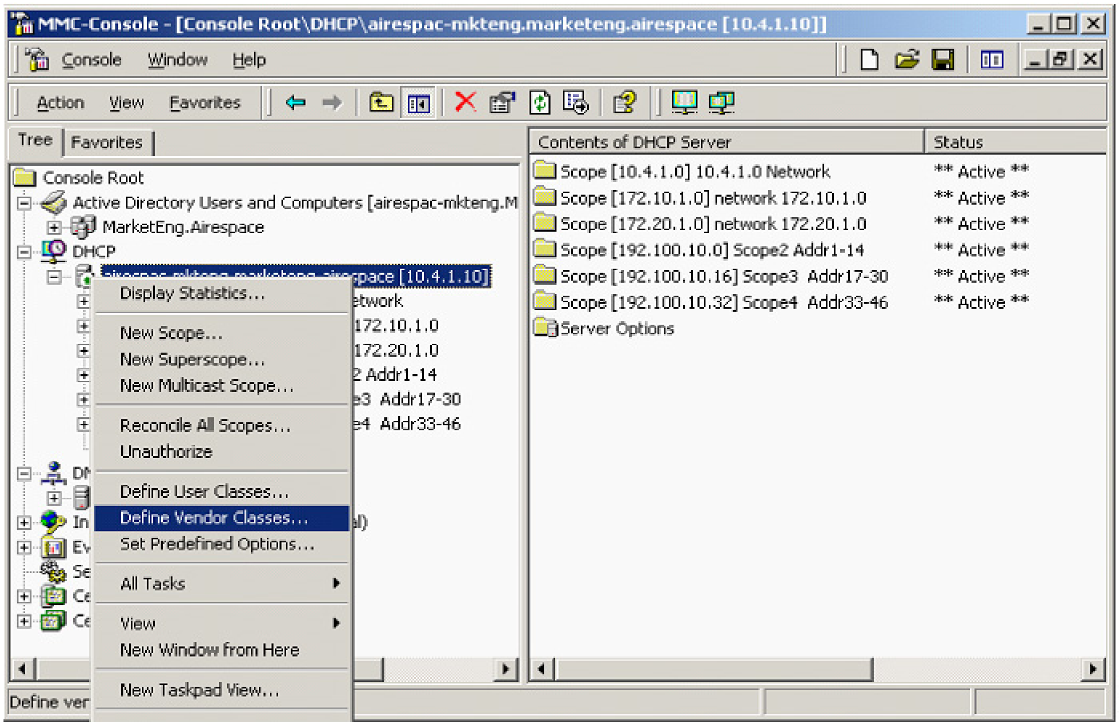
- Vendor Class Identifier (VCI)
- Option 43 sub-option code
- Management IP address(es) of wireless LAN controller(s)

From Table 4, the VCI for a Cisco 1000 Series Access Point will always be "Airespace.AP1200". Also, as stated in Appendix C, the Option 43 sub-option code for Cisco 1000 Series access points is type 102 (0x66).

The example configurations are done using the Windows MMC Console utility. You can also use the DHCP Server Utility. The steps are virtually identical.

The first step is to create a new vendor class to program the DHCP Server to recognize the VCI "Airespace.AP1200". In the MMC console, right click on the DHCP server icon and choose **Define Vendor Classes**. This is shown in Figure 109:

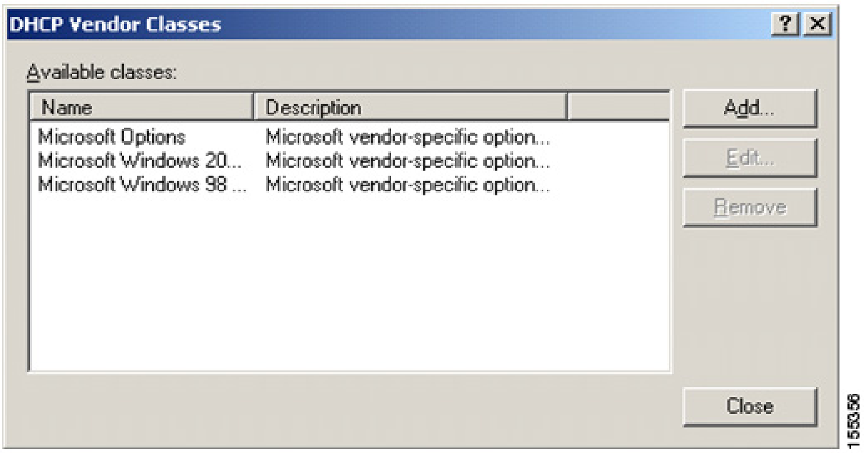
*Figure 109 Defining a Vendor Class*



| Contents of DHCP Server | Status |
|---|---|
| Scope [10.4.1.0] 10.4.1.0 Network | ** Active ** |
| Scope [172.10.1.0] network 172.10.1.0 | ** Active ** |
| Scope [172.20.1.0] network 172.20.1.0 | ** Active ** |
| Scope [192.100.10.0] Scope2 Addr1-14 | ** Active ** |
| Scope [192.100.10.16] Scope3 Addr17-30 | ** Active ** |
| Scope [192.100.10.32] Scope4 Addr33-46 | ** Active ** |
| Server Options | |

Select **Add** to create the new class. The procedure is shown in Figure 110:

*Figure 110 Defining a Vendor Class*

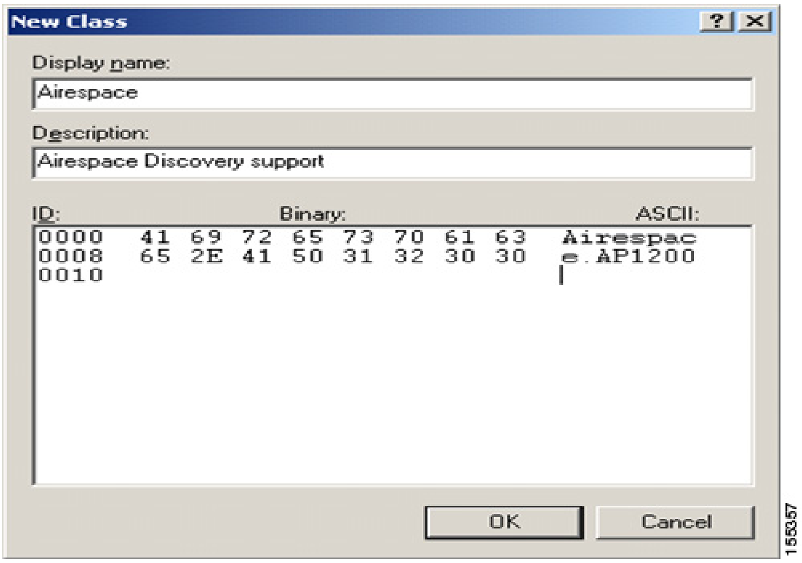


| Name | Description |
|---|---|
| Microsoft Options | Microsoft vendor-specific option... |
| Microsoft Windows 20... | Microsoft vendor-specific option... |
| Microsoft Windows 98 ... | Microsoft vendor-specific option... |

Enter a value for the **Display Name**.

In Figure 111, you can see that the value **Airespace** is entered for the Display Name. You should also add a short description of the vendor class in the **Description Field**. Add the Vendor Class Identifier string by clicking on the ASCII field and typing in the appropriate value, in this case **Airespace.AP1200**. Click on **OK** when finished. This is shown in Figure 111:

*Figure 111 Defining a Vendor Class*



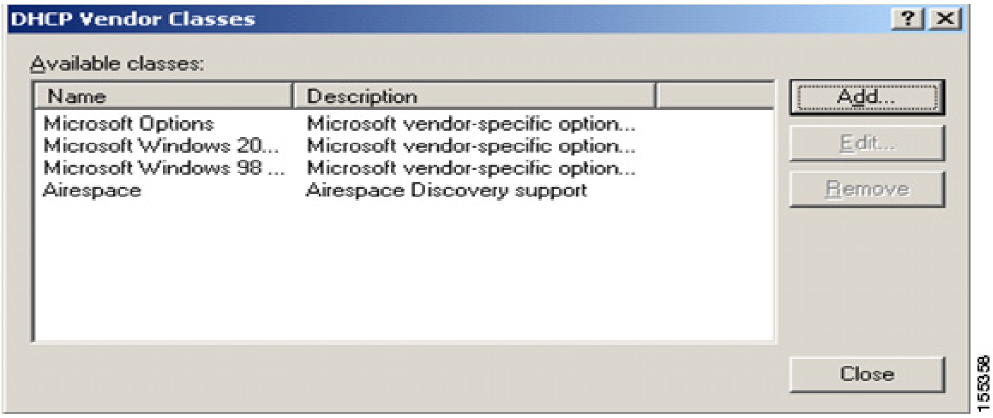
Display name: Airespace

Description: Airespace Discovery support

```
ID:                  Binary:                  ASCII:
0000   41 69 72 65 73 70 61 63   Airespac
0008   65 2E 41 50 31 32 30 30   e.AP1200
0010
```

You should now see that the new class has been created (see Figure 112). Now click **CLOSE**.

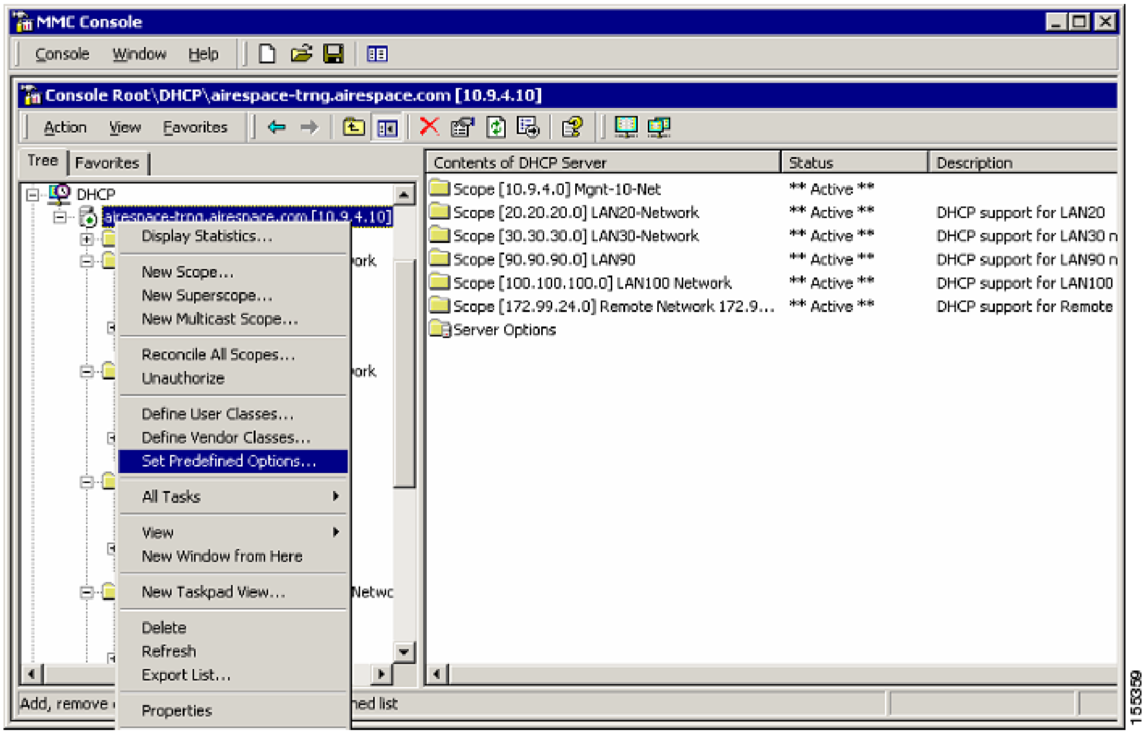
Figure 112 DHCP Vendor Classes Including the Newly Added "Airespace" Class



| Name | Description |
|---|---|
| Microsoft Options | Microsoft vendor-specific option... |
| Microsoft Windows 20... | Microsoft vendor-specific option... |
| Microsoft Windows 98 ... | Microsoft vendor-specific option... |
| Airespace | Airespace Discovery support |

The next step is to add an entry for the WLAN controller sub-option in the "Predefined Options" for the newly created Vendor Class. This will be where you define the sub-option code type and the data format that will be used to deliver the vendor specific information (Option 43) to the access points. To create a Predefined Option, right click on the server icon and choose Select Predefined Options from the list of menu items presented. This is shown in Figure 113:

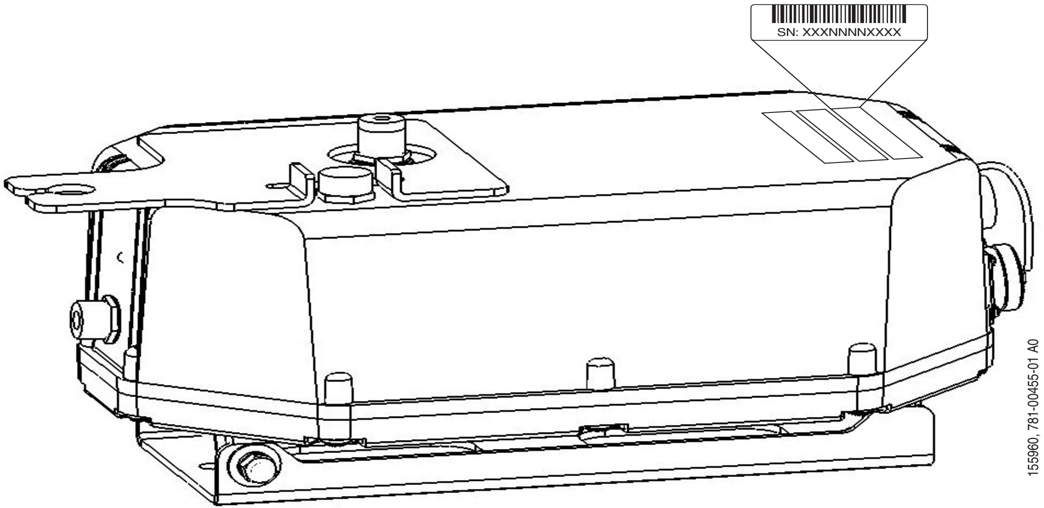
Figure 113 Adding a Predefined Option



| Contents of DHCP Server | Status | Description |
|---|---|---|
| Scope [10.9.4.0] Mgnt-10-Net | ** Active ** | |
| Scope [20.20.20.0] LAN20-Network | ** Active ** | DHCP support for LAN20 |
| Scope [30.30.30.0] LAN30-Network | ** Active ** | DHCP support for LAN30 n |
| Scope [90.90.90.0] LAN90 | ** Active ** | DHCP support for LAN90 n |
| Scope [100.100.100.0] LAN100 Network | ** Active ** | DHCP support for LAN100 |
| Scope [172.99.24.0] Remote Network 172.9... | ** Active ** | DHCP support for Remote |
| Server Options | | |

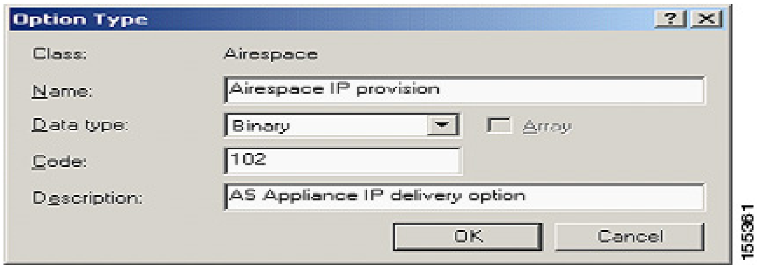
A new window opens where you will set the Option class to the value you previously configured for the vendor class. In our example, we are using vendor class name "Airespace". Click **Add** to define the option code. This is shown in Figure 114:

*Figure 114 Adding a Predefined Option*



An Option Type box will pop-up. In the Name field, enter a descriptive string value-for example, **Airespace IP provision**. Select **Binary**" as the Data Type.  In the **Code** field, enter the sub-option value 102. Enter a **Description**, if desired. Click **OK** . This is shown in Figure 115:

*Figure 115 Defining the Predefined Option*


Option Type

Class: Airespace

Name: Airespace IP provision

Data type: Binary □ Array

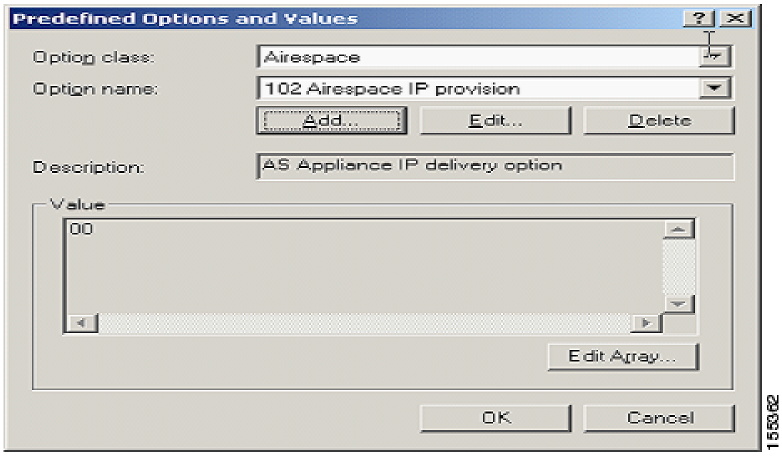
Code: 102

Description: AS Appliance IP delivery option

You should see the new Predefined Option that is associated with the Airespace class (see Figure 116).

Now click **OK** at the bottom of the **Predefined Options** and **Values** box. This is shown in Figure 116:

*Figure 116 Predefined Option Defined for Vendor Class*



Predefined Options and Values

Option class: Airespace

Option name: 102 Airespace IP provision

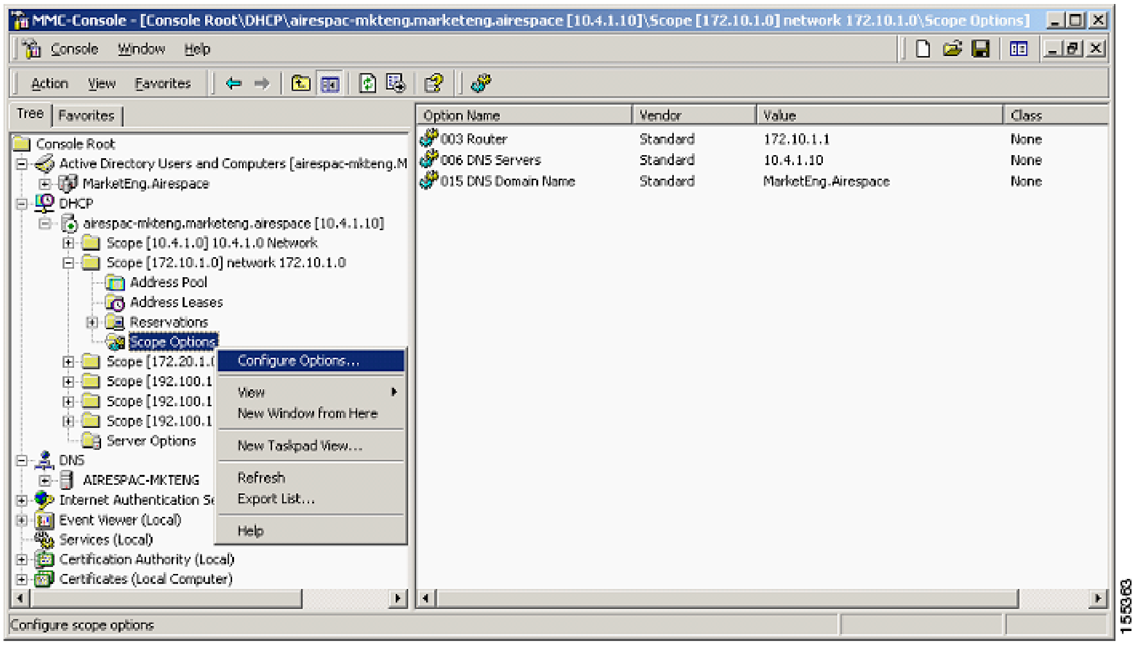
Description: AS Appliance IP delivery option

Value: 00

This completes the creation of the Vendor class and sub-option type needed to support controller discovery.

Next, you use the vendor class and pre-defined option to support controller auto discovery by defining the appropriate value for the DHCP scope the access points will use. Navigate to the appropriate DHCP scope for the access points. Right-click the **Scope Option**s folder under the DHCP scope and select **Configure Options**. This is shown in Figure 117:

*Figure 117 Configuring Vendor Specific Information per DHCP Scope*



MMC-Console - [Console Root\DHCP\airespac-mkteng.marketeng.airespace [10.4.1.10]\Scope [172.10.1.0] network 172.10.1.0\Scope Options]

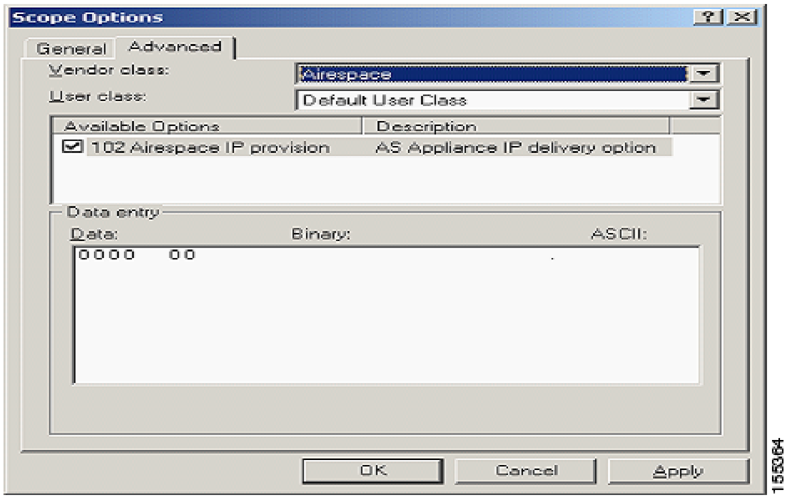
```
Console Root
  Active Directory Users and Computers [airespac-mkteng.M
    MarketEng.Airespace
  DHCP
    airespac-mkteng.marketeng.airespace [10.4.1.10]
      Scope [10.4.1.0] 10.4.1.0 Network
      Scope [172.10.1.0] network 172.10.1.0
        Address Pool
        Address Leases
        Reservations
        Scope Options
      Scope [172.20.1.(
      Scope [192.100.1
      Scope [192.100.1
      Scope [192.100.1
      Server Options
  DNS
    AIRESPAC-MKTENG
  Internet Authentication S(
  Event Viewer (Local)
  Services (Local)
  Certification Authority (Local)
  Certificates (Local Computer)
```

| Option Name | Vendor | Value | Class |
|---|---|---|---|
| 003 Router | Standard | 172.10.1.1 | None |
| 006 DNS Servers | Standard | 10.4.1.10 | None |
| 015 DNS Domain Name | Standard | MarketEng.Airespace | None |

Configure scope options

The Scope Options box will appear. Change to the Advanced tab. Select the Vendor Class that you are going to use-in this case "Airespace". See Figure 118:

*Figure 118 Selecting the Vendor Class and Sub-Option*



Vendor class: Airespace

User class: Default User Class

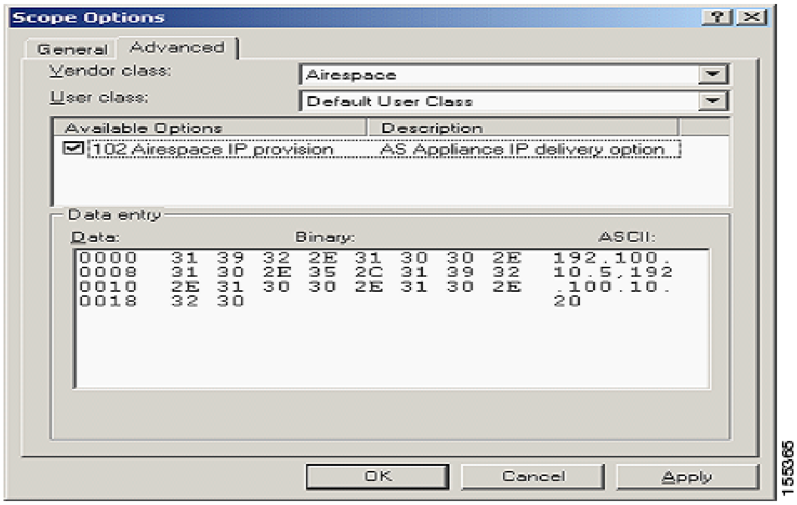
| Available Options | Description |
|---|---|
| ☑ 102 Airespace IP provision | AS Appliance IP delivery option |

Data entry

```
Data:        Binary:                              ASCII:
0000    00                                        .
```

Select the predefined 102 sub-option that you will assign to this scope. In the Data Entry area, enter the controller management IP address(es) that you are going to return to the access points in the **ASCII** section. This is a comma delimited list. Also note that there is a period (.) found in the initial empty Data Entry area. Make sure you remove this period from the list of IP addresses that will be added in the data entry area. See Figure 119:

*Figure 119 Entering WLAN Controller IP Address Values*



Vendor class: Airespace

User class: Default User Class

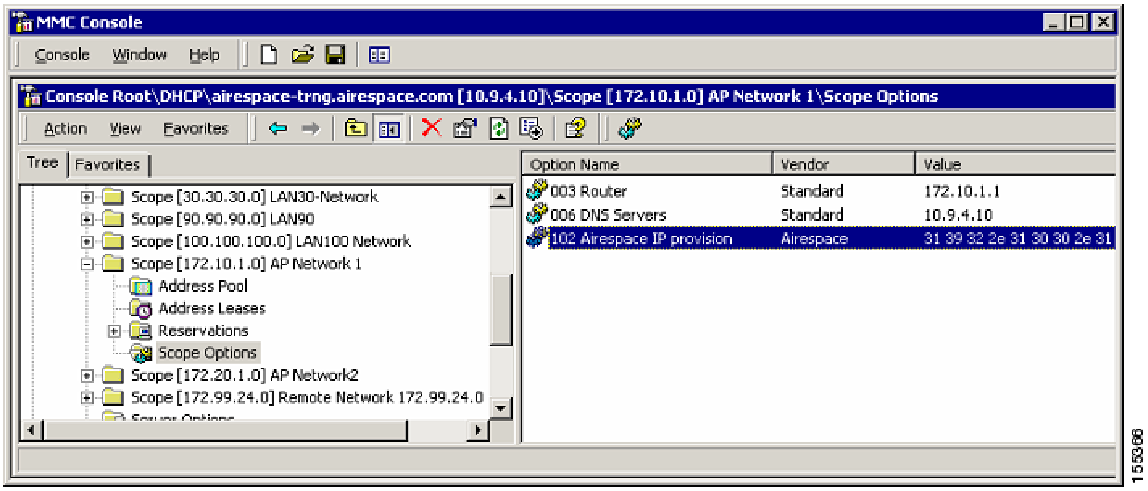
| Available Options | Description |
|---|---|
| ☑ 102 Airespace IP provision | AS Appliance IP delivery option |

Data entry

```
Data:        Binary:                              ASCII:
0000    31 39 32 2E 31 30 30 2E    192.100.
0008    31 30 2E 35 2C 31 39 32    10.5,192
0010    2E 31 30 30 2E 31 30 2E    .100.10.
0018    32 30                      20
```

When finished, your results should look similar to what's shown in Figure 120. Repeat these steps for each DHCP scope.

*Figure 120 Vendor Specific Information for Cisco 1000 Defined for a DHCP Scope*



Console Root\DHCP\airespace-trng.airespace.com [10.9.4.10]\Scope [172.10.1.0] AP Network 1\Scope Options

```
Scope [30.30.30.0] LAN30-Network
Scope [90.90.90.0] LAN90
Scope [100.100.100.0] LAN100 Network
Scope [172.10.1.0] AP Network 1
    Address Pool
    Address Leases
    Reservations
    Scope Options
Scope [172.20.1.0] AP Network2
Scope [172.99.24.0] Remote Network 172.99.24.0
Server Options
```

| Option Name | Vendor | Value |
|---|---|---|
| 003 Router | Standard | 172.10.1.1 |
| 006 DNS Servers | Standard | 10.9.4.10 |
| 102 Airespace IP provision | Airespace | 31 39 32 2e 31 30 30 2e 31 |

## Configuring Vendor-Specific DHCP Options for Lightweight Cisco Aironet Series Access Points (1130, 1240, and 1200 series)

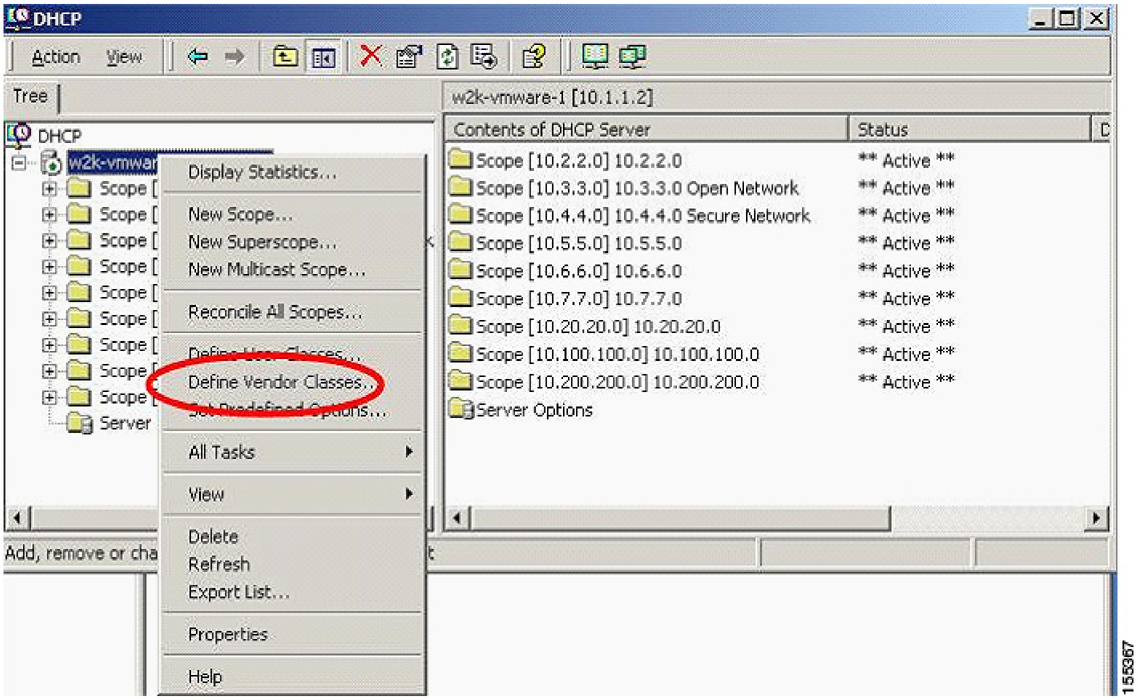
This section describes how the Windows DHCP Server is used to configured to return vendor-specific information to lightweight Cisco Aironet Series access points. Key information you'll need to know are:

- Vendor Class Identifier (VCI)
- Option 43 sub-option code
- Management IP address(es) of wireless LAN controller(s)

From Table 4 in Appendix C, the VCI for a lightweight Cisco Aironet Series access point is specific to each model type. To support more than one access point model, a Vendor Class needs to be created for each model type. As stated in Appendix C, the Option 43 sub-option code for Cisco Aironet Series access points is type 241 (0xf1).

To configure these options in the Windows DHCP Server, open the DHCP Server Administration Tool or MMC console. Right-click the mouse on the DHCP root and then choose **Define Vendor Classes** (see Figure 121):

*Figure 121 Defining the Vendor Class*

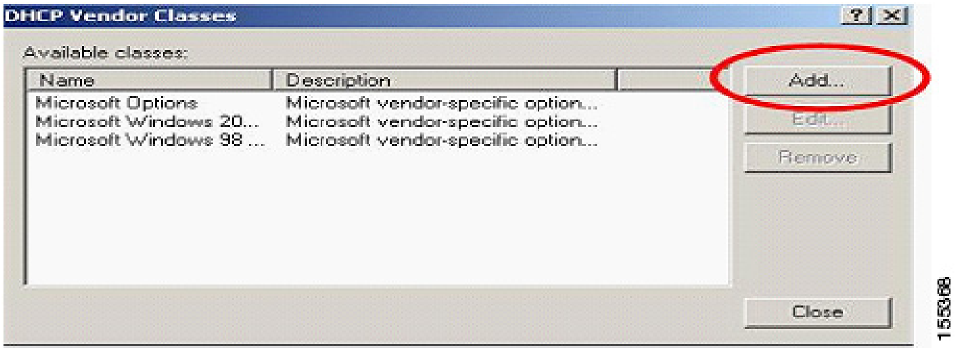


w2k-vmware-1 [10.1.1.2]

| Contents of DHCP Server | Status |
|---|---|
| Scope [10.2.2.0] 10.2.2.0 | ** Active ** |
| Scope [10.3.3.0] 10.3.3.0 Open Network | ** Active ** |
| Scope [10.4.4.0] 10.4.4.0 Secure Network | ** Active ** |
| Scope [10.5.5.0] 10.5.5.0 | ** Active ** |
| Scope [10.6.6.0] 10.6.6.0 | ** Active ** |
| Scope [10.7.7.0] 10.7.7.0 | ** Active ** |
| Scope [10.20.20.0] 10.20.20.0 | ** Active ** |
| Scope [10.100.100.0] 10.100.100.0 | ** Active ** |
| Scope [10.200.200.0] 10.200.200.0 | ** Active ** |
| Server Options | |

The DHCP Vendor Classes utility window appears. Select **Add** (see Figure 123):

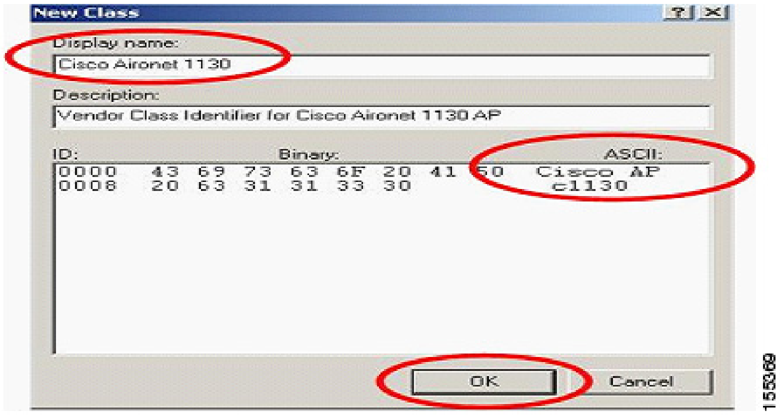
*Figure 122 Defining the Vendor Class*



| Name | Description |
|---|---|
| Microsoft Options | Microsoft vendor-specific option... |
| Microsoft Windows 20... | Microsoft vendor-specific option... |
| Microsoft Windows 98 ... | Microsoft vendor-specific option... |

A New Class configuration box will pop-up. Enter a value for the **Display Name** field—for example, Cisco Aironet 1130 AP—and an appropriate description. Click on the **ASCII Section** and enter the appropriate string value for the **Vendor Class Identifier** (see Table 4). Click **OK** to complete the task (see Figure 123) and then click CLOSE on the DHCP Vendor Classes window (see Figure 123).

*Figure 123 Defining the Vendor Class*



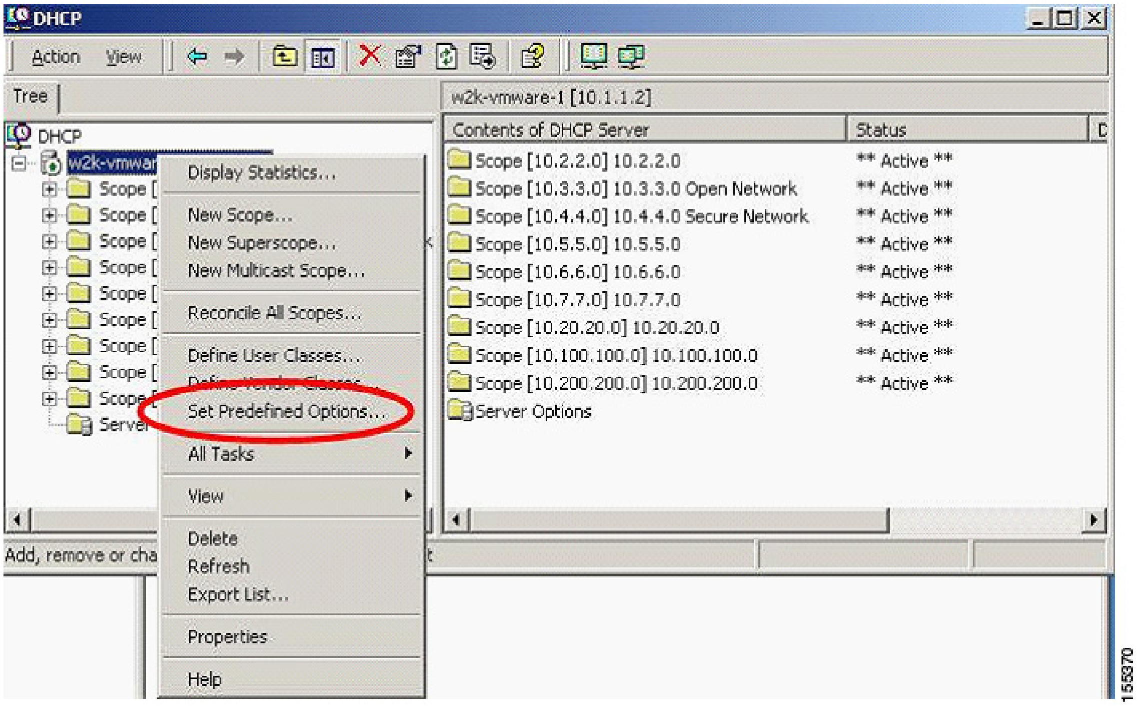
Display name:
Cisco Aironet 1130

Description:
Vendor Class Identifier for Cisco Aironet 1130 AP

```
ID:     Binary:                           ASCII:
0000    43 69 73 63 6F 20 41 50           Cisco AP
0008    20 63 31 31 33 30                 c1130
```

The next step is to add an entry for the wireless LAN controller sub-type as a pre-defined option must be configured for the Vendor Class. Right-click on the DHCP Server Root and then select **Set Predefined Options** (see Figure 124):

*Figure 124 Adding a Pre-defined Option*

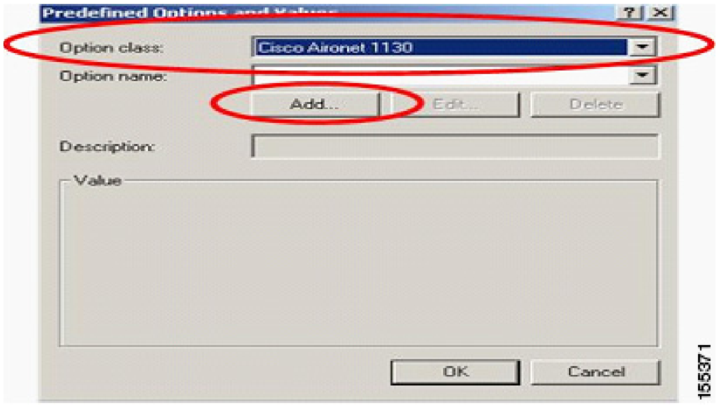


w2k-vmware-1 [10.1.1.2]

| Contents of DHCP Server | Status |
|---|---|
| Scope [10.2.2.0] 10.2.2.0 | ** Active ** |
| Scope [10.3.3.0] 10.3.3.0 Open Network | ** Active ** |
| Scope [10.4.4.0] 10.4.4.0 Secure Network | ** Active ** |
| Scope [10.5.5.0] 10.5.5.0 | ** Active ** |
| Scope [10.6.6.0] 10.6.6.0 | ** Active ** |
| Scope [10.7.7.0] 10.7.7.0 | ** Active ** |
| Scope [10.20.20.0] 10.20.20.0 | ** Active ** |
| Scope [10.100.100.0] 10.100.100.0 | ** Active ** |
| Scope [10.200.200.0] 10.200.200.0 | ** Active ** |
| Server Options | |

Select the newly created Vendor Option Class in the Option Class field, and then click **Add** (see Figure 125):

*Figure 125 Adding a Pre-defined Option*



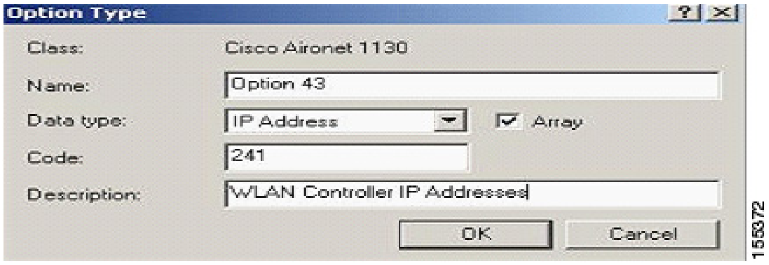
Predefined Options and Values

Option class: Cisco Aironet 1130

Option name:

The Option Type box will appear (see Figure 126). In the Name field, enter a string value-for example, Option 43. Select the **IP Address**" as the Data Type. Click the **Array** check-box. In the **Code** field, enter the sub-option code value 241 (0xf1). Enter a Description if desired. Click **OK** (see Figure 126):

*Figure 126 Defining a Sub-Option*



Option Type

Class: Cisco Aironet 1130

Name: Option 43

Data type: IP Address ☑ Array

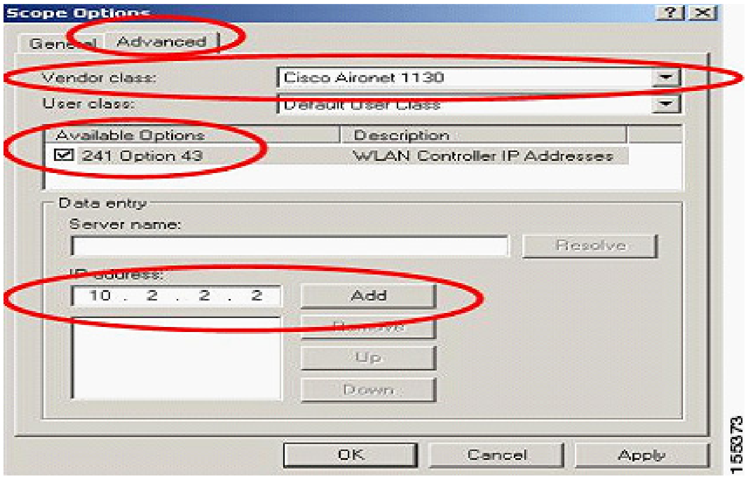
Code: 241

Description: WLAN Controller IP Addresses

The Vendor Class and sub-option are now programmed into the DHCP Server. Now the vendor specific information must be defined for the access point DHCP scope. Select the appropriate DHCP scope. Right-click the mouse on the **Scope Options** and select **Configure Options** (see Figure 117).

Select the **Advanced Tab** (see Figure 127). Select the Vendor Class previously defined. Click the check-box for the value 241, and then enter each WLC management interface IP address. When finished, click **OK**.

*Figure 127 Defining the Vendor Specific Information*



Scope Options

Vendor class: Cisco Aironet 1130

User class: Default User Class

| Available Options | Description |
|---|---|
| ☑ 241 Option 43 | WLAN Controller IP Addresses |

Data entry

Server name:

IP address: 10 . 2 . 2 . 2

A Vendor Class and sub-options must be defined for each type of lightweight Cisco Aironet access point. Vendor specific information must also be defined for each vendor class in each DHCP scope.

# Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/web/about/ac123/ac114/about_cisco_packet_magazine.html

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/web/about/ac123/ac114/about_cisco_packet_magazine.html

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/web/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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