

# Wireless LAN Controller (WLC) FAQ

Document ID: 69561

## Questions

**Introduction** **General FAQ** **Troubleshoot FAQ**  
**NetPro Discussion Forums – Featured Conversations**  
**Related Information**

## Introduction

This document provides information on the most frequently asked questions (FAQ) about the Cisco Wireless LAN Controllers (WLCs).

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

## General FAQ

### Q. What is a Wireless LAN Controller (WLC)?

A. Wireless networks have become a necessity today. Currently, we find that corporate environments require deployment of wireless networks on a large scale. Cisco has come up with the concept of the Cisco Unified Wireless Network (CUWN) solution, which helps make it easier to manage such large-scale deployments. WLC is a device that assumes a central role in the CUWN. Traditional roles of access points (APs), such as association or authentication of wireless clients, are done by the WLC. APs, called lightweight access points (LAPs) in the unified environment, register themselves with a WLC and tunnel all of the management and data packets to the WLCs, which then switch the packets between wireless clients and the wired portion of the network. All of the configurations are done on the WLC. LAPs download the entire configuration from WLCs and act as a wireless interface to the clients. For more information on how a LAP registers with a WLC, refer to the document Lightweight AP (LAP) Registration to a Wireless LAN Controller.

### Q. Where can I find more information about the initial configuration of WLCs in my WLAN network?

A. In order to configure the WLC for basic operation, refer to the document Wireless LAN Controller and Lightweight Access Point Basic Configuration Example.

### Q. What are the various options available to access the WLC?

A. This is the list of options available to access the WLC:

- GUI access with HTTP or HTTPS
- Command-line interface (CLI) access with Telnet, SSH, or console access
- Access through service port

For more information on how to enable these modes, refer to the Using the Web-Browser and CLI Interfaces section of the document Cisco Wireless LAN Controller Configuration Guide, Release 5.1. Usually, the management interface IP address is used for GUI and CLI access. Wireless clients can access the WLC only when the option **Enable Controller Management to be accessible from Wireless Clients** is checked. In order to enable this option, click the **Management** menu of the WLC, and click **Mgmt via Wireless** on the left-hand side. WLC can also be accessed with one of its dynamic interface IP addresses. Use the **config network mgmt-via-dynamic-interface** command to enable this feature. Wired computers can have only CLI access with the dynamic interface of the WLC. Wireless clients have both CLI and GUI access with the dynamic interface.

## Q. How does a WLC switch packets?

A. All of the client (802.11) packets are encapsulated in a Lightweight Access Point Protocol (LWAPP) packet by the LAP and sent to the WLC. WLC decapsulates the LWAPP packet and acts based on the destination IP address in the 802.11 packet. If the destination is one of the wireless clients associated to the WLC, it encapsulates the packet again with the LWAPP and sends it to the LAP of the client, where it is decapsulated and sent to the wireless client. If the destination is on the wired side of the network, it removes the 802.11 header, adds the Ethernet header, and forwards the packet to the connected switch, from where it is sent to the wired client. When a packet comes from the wired side, WLC removes the Ethernet header, adds the 802.11 header, encapsulates it with LWAPP, and sends it to the LAP, where it is decapsulated, and the 802.11 packet is delivered to the wireless client. For more information, refer to the LWAPP Fundamentals section of the document WLC Deployment Guide.

## Q. Does the 4400 WLC route packets between VLANs?

A. The 4400 WLC is an appliance that attaches to your network but does not function like a router. There must be a Layer 3 device to route packets between VLANs. The WLC maps the Service Set Identifier (SSID) of the clients to the VLAN subnet and puts them back out on the management interface for the upstream routers to route packets.

## Q. How do I configure WLAN on a WLC?

A. WLAN is similar to that of SSID in the APs. It is required for a client to associate with its wireless network. In order to configure a WLAN on a WLC, refer to the sample configuration in the document Guest WLAN and Internal WLAN using WLCs Configuration Example.

## Q. How does DHCP work with the WLC?

A. The WLC is designed to act as a DHCP relay agent to the external DHCP server and acts like a DHCP server to the client. This is the sequence of events that occurs:

1. Generally, WLAN is tied to an interface that is configured with a DHCP server.
2. When the WLC receives a DHCP request from the client on a WLAN, it relays the request to the DHCP server with its management IP address.
3. The WLC shows its Virtual IP address, which must be a nonroutable address, usually configured as 1.1.1.1, as the DHCP server to the client.
4. The WLC forwards the DHCP reply from the DHCP server to the wireless client with its Virtual IP address.

**Note:** You can also configure the WLC to act as a DHCP server. For more information on how to configure a WLC as a DHCP server, refer to the Configuring DHCP Scopes section of the document Cisco Wireless LAN Controller Configuration Guide Release 5.1.

## Q. What are all of the authentication mechanisms supported by WLC?

A. WLC supports various Layer 2 and Layer 3 client authentication mechanisms. Layer 2 authentication mechanisms include Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and 802.1x. Layer 3 authentications are commonly web authentication and web pass-through. For more information on how to configure the WLC for various authentication mechanisms, refer to the document Authentication on Wireless LAN Controllers Configuration Examples.

## Q. How do I change power and channels for a LAP?

A. Once a LAP registers to a WLC, all of the configuration for a LAP is done on the WLC. There is a built-in feature in WLC called Radio Resource Management (RRM), wherein the WLC internally runs an algorithm and automatically adjusts the channel and power settings as per the deployment of LAPs. RRM is turned on by default on the WLC. You need not change the channel and power settings for a LAP, but you can override the RRM feature and statically assign power and channel settings for a LAP. For more information on how to manually configure the channel and power settings, refer to the Statically Assigning Channel and Transmit Power Settings to Access Point Radios section of the document Cisco Wireless LAN Controller Configuration Guide, Release 5.1.

## Q. I have multiple WLCs in my network. Is there any device or software available to manage multiple WLCs in my network?

A. Yes, the Cisco Wireless Control System (WCS) is a server software that can manage multiple WLCs on the network. It manages the WLCs, their associated APs, and clients. For more information on the WCS, refer to Cisco Wireless Control System Configuration Guide, Release 5.0.

## Q. Can a WLC push configurations to other WLCs and manage them without a wireless control system (WCS)?

A. No, WLCs do not have the ability to push configurations to other WLCs or manage them.

## Q. How do I find the version of code that runs on the WLC?

A. From the Wireless LAN Controller GUI, click **Monitor > Summary**. In the Summary page, the **Software Version** field shows the version of firmware that runs on the Wireless LAN Controller.

In order to find the version of firmware that runs on the WLC through the WLC CLI, use the command **show run-config**.

```
(Cisco Controller) >show run-config
```

```
Press Enter to continue...
```

```
System Inventory Burned-in MAC Address.....  
00:0B:85:33:52:80
```

Press Enter to continue Or <Ctl Z> to abort

```
System Information Manufacturer's Name.....
Cisco Systems Inc. Product Name.....
Cisco Controller
Product Version..... 4.0.217.0
RTOS Version..... 4.0.217.0
Bootloader Version..... 4.0.217.0
Build Type..... DATA + WPS
Compact Flash Size..... 256 MB
```

In order to view the active boot image, use the command **show boot**.

```
(Cisco Controller) >show boot Primary Boot
Image..... 4.0.217.0 (active) Backup Boot
Image..... 4.0.155.5
```

## **Q. What is the procedure to upgrade the operating system software on a Cisco WLC?**

A. Refer to the document Wireless LAN Controller (WLC) Software Upgrade to provide the procedure for a software upgrade on your WLC.

## **Q. Can I upgrade the WLC from one major version to another directly?**

A. You can upgrade or downgrade the WLC software only between two releases. In order to upgrade or downgrade beyond two releases, you must first install an intermediate release. For example, if your WLC runs a 4.2 or 5.0 release, you can upgrade your WLC directly to Software Release 5.1.151.0. If your WLC runs a 3.2, 4.0, or 4.1 release, you must upgrade your WLC to an intermediate release prior to the upgrade to 5.1.151.0. In order to know the upgrade path that you must follow before you download Software Release 5.1.151.0, refer to the Special Rules for Upgrading to Controller Software Release 5.1.151.0 section of the document Release Notes for Cisco Wireless LAN Controllers and Lightweight Access Points for Release 5.1.151.0. In order to know the upgrade path for any WLC version, refer to the Release Notes of the corresponding release.

## **Q. What happens to the wireless network when I perform a software upgrade? Do *all* of the APs registered to a WLC go down until they are upgraded, or are they upgraded one at a time so that the wireless network can remain up (except for the specific APs that undergo the upgrade)?**

A. Once the WLC is upgraded, it must be rebooted for the changes to take effect. Within this time, connectivity to the WLC is lost. LAPs registered to a WLC lose their association to the WLC, so service to the wireless clients is interrupted. Once the WLC is upgraded, new code is pushed simultaneously to all the LAPs registered to the WLC.

## **Q. Can a Cisco IOS Software-based AP that has been converted to lightweight mode register with Cisco 4100 Series WLCs?**

A. No, Cisco IOS Software-based APs that are converted to lightweight mode cannot register with the Cisco 40xx, 41xx, or 3500 WLCs. These LAPs can register only with the Cisco 4400 and the 2000 series WLCs. For information on the restrictions of APs that are converted to lightweight mode, refer to the *Restrictions* section of Upgrading Autonomous Cisco Aironet

access points to Lightweight Mode.

## **Q. What is the maximum number of APs supported on the 4402 and 4404 WLCs?**

A. The limitation on the number of supported APs is based on the hardware that you have. The 4402 WLC with two gigabit Ethernet ports comes in configurations that support 12, 25, and 50 APs. The 4404 WLC with four gigabit Ethernet ports supports 100 APs.

## **Q. How does roaming occur in a WLC environment?**

A. Roaming is a process where the client can retain uninterrupted application sessions on its move. When a wireless client associates and authenticates to a WLC, it places an entry for that client in its client database. This entry includes the MAC and IP addresses of the client, security context and associations, quality of service (QoS) contexts, the WLAN, and the associated LAP. When a client roams to another LAP associated to the same WLC, it just updates the client database with the new LAP information so that the data can be forwarded appropriately to the client. When a client roams to a LAP associated with a different WLC, either in same or different subnets, it sends the information in the client database to the new WLC. This helps the client to retain its IP address across roams and maintain uninterrupted TCP sessions. For more information on roaming in the WLC environment, refer to the Configuring Mobility Groups section of the document Cisco Wireless LAN Controller Configuration Guide, Release 5.1.

## **Q. How are guest users handled by WLC?**

A. Guest users are third-party network users who need limited access to the network resources and Internet connectivity. WLC provides wireless and wired guest access using the existing wireless network infrastructure. Usually a separate SSID is provided for wireless guest users. Guest users on both the wired and wireless networks are assigned separate VLANs, which provides isolation of guest traffic from the rest of the data traffic. This provides better control over the guest traffic and greater network security. Guest users are usually authenticated through web authentication. For more information on guest access, refer to the document Wireless Guest Access FAQ.

## **Q. How do I configure a local database on the WLC? What are the special characters that can be used for the local net user username and passwords?**

A. The local user database stores the credentials (username and password) of all the local network users. These credentials are then used to authenticate the users. You can configure local network users either through the GUI or the CLI. You can enter up to 24 alphanumeric characters. All of the special characters can be used when you configure usernames and passwords through CLI, but the single-quote character cannot be used when you configure a username and password through GUI.

From the CLI, use these commands to create a local net user:

```
◆ config netuser add <username> <password> wlan <wlan_id> userType  
permanent description <description> ◆ Adds a permanent user to the local user  
database on the WLC.
```

◆ **config netuser add <username> <password> {wlan | guestlan} {wlan\_id | guest\_lan\_id} userType guest lifetime seconds description <description>**◆ Adds a guest user on a WLAN or wired guest LAN to the local user database on the WLC. From the GUI, you can configure local net users from the **Security > AAA > Local Net Users** page.

## **Q. Is it possible to automatically delete the local net user on the WLC?**

**A.** Local Net users are not automatically deleted. You have to delete them manually. In order to delete the user, go to the **Security > AAA > Local Net Users** page. **To remove a user, place the mouse** over the icon  and click **Remove**. If a local net user is configured as a guest user, you must specify the life time, after which the user is automatically deleted. The configurable range is between 60 seconds and 2,592,000 seconds

## **Q. What is a mobility group?**

**A.** Mobility group is a group of WLCs configured with the same mobility group name. The client can roam seamlessly between the WLCs in the same mobility group. WLCs in a mobility group provide for redundancy among themselves. For more information on mobility groups, refer to the document Wireless LAN Controller (WLC) Mobility Groups FAQ.

## **Q. How many WLCs can I have in the same mobility group?**

**A.** You can place up to 24 regular WLCs (Cisco 2000, 4100, and 4400 series) in a single mobility group. You can configure up to 12 Wireless Services Module (WiSM) blades in one mobility group. Therefore, up to a maximum of 3600 APs are supported in a single mobility group.

**Note:** With WLC release 5.1, there can be up to 72 WLCs in a mobility group.

## **Q. Does the Cisco 4400 Series WLC support Internetwork Packet Exchange (IPX) protocol? Does any Cisco Aireospace product support IPX protocol?**

**A.** No, IPX protocol is not supported on any platforms of the Cisco WLC.

## **Q. What are the prerequisites to access the GUI of the WLC?**

**A.** The WLC GUI requires this operating system and web browser:

- Windows XP Service Pack 1 (SP1) or later, or Windows 2000 SP4 or later
- Internet Explorer 6.0 SP1 or later

## **Q. Is the WLC GUI supported on Mozilla browsers?**

**A.** No, WLC GUI is not supported on Mozilla browsers.

## Q. How do I retrieve Cisco WLC MIBs on the web?

A. You can download the Cisco WLC MIBs from the Wireless Downloads (registered customers only) page.

Complete these steps in order to download the WLC MIBs:

1. From the Wireless Downloads page, click **Wireless LAN Controller** and select the WLC platform for which you need the MIBs.
2. The Software Download page for the WLC appears. This page contains all of the files for the WLC, including the MIBs.
3. Choose a software version and download the standard MIBs and the MIBs that are specific to Cisco. These two files should be downloaded and contain the MIBs. The filenames look similar to this example:

`Standard-MIBS-Cisco-WLC4400-2000-XXXXXX.zip`

`Cisco-WLC-MIBS-XXXX.zip`

## Q. In guest tunneling, how many Ethernet over IP (EoIP) tunnels can be formed between a single-anchor WLC to different internal WLCs?

A. A single-anchor WLC supports up to 40 EoIP tunnels with one tunnel per internal WLC. These WLCs can be of different mobility groups.

## Q. What are the functional differences between the 2100 Series WLCs and the 4400 WLCs?

A. The major differences between the 2100 and 4400 Series WLCs are in the features they support.

This hardware feature is not supported on 2100 series WLCs:

- Service port (separate out-of-band management 10/100-Mb/s Ethernet interface)

These software features are not supported on 2100 Series WLCs:

- VPN termination (such as IPSec and L2TP)
- Fortress
- External web authentication web server list
- Layer 2 LWAPP
- Spanning tree
- Port mirroring
- AppleTalk

IPv6 pass-through A 4400 Series WLC supports all of the aforementioned hardware and software features.

## Q. Which LAPs do the 4100 Series WLCs support?

A. Only the AireSPACE 1200 and 1250, the Cisco 1000 Series, and the Cisco 1500 Series LAPs work with the 4100 Series WLCs.

**Q. Can I use this ASA/PIX as a DHCP server instead of windows DHCP server in order to assign IP addresses to my Wireless Clients?**

A. Yes, you can use ASA/PIX as a DHCP server for wireless clients. Ensure that the interface of the WLAN to which the client belongs is on the same subnet as the ASA/PIX interface on which the server is enabled. However, you cannot assign default gateway to the clients. PIX/ASA declares itself as the default gateway to the clients. For more information on how to configure ASA as a DHCP server, see PIX/ASA as a DHCP Server and Client Configuration Example.

**Q. Is it possible to go back and make corrections in the WLC configuration wizard at the time of the initial configuration?**

A. Yes, this can be done with the - (hyphen) key. Use this key to re-enter the previous parameter value.

You use the WLC configuration wizard in order to configure the WLC from the onset.

For example, instead of entering the username as **admin**, you accidentally enter it as **adminn**. In order to correct this mistake, enter - (hyphen key) at the next prompt, then click **Enter**. The system returns to the previous parameter.

```
(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool Use the
'-' character to backup System Name [Cisco_e8:38:c0]:
adminnEnter Administrative User Name (24 characters max) :
-

System Name [Cisco_e8:38:c0] (31 characters max) :
```

**Q. In accordance to RFC 1907 for Simple Network Management Protocol (SNMP), the SNMP location field should support a size from 1–255. However, I am unable to enter more than 31 characters in the SNMP location field. Why?**

A. This is due to Cisco bug ID CSCsh58468 (registered customers only). A user can enter only 31 characters. Currently there is no workaround for this issue.

**Q. With the Management via Wireless feature enabled on WLCs in a mobility group, I can access only one WLC from that mobility group. Why?**

A. This is an expected behavior. When enabled, the Management via Wireless feature allows a wireless client to reach or manage only the WLC to which its associated AP is registered. The client cannot manage other WLCs, even though these WLCs are in the same mobility groups. This restriction is implemented for security and was recently reduced to just the one WLC in order to limit exposure.

The Cisco WLAN Solution Management over Wireless feature allows Cisco WLAN Solution

operators to monitor and configure local WLCs using a wireless client. This feature is supported for all management tasks except for uploads to and downloads from (transfers to and from) the WLC.

This can be enabled through the WLC CLI with the **config network mgmt-via-wireless enable** command.

On the GUI, click **Management**; from the left-hand side, click **Mgmt Via Wireless**, and check the box **Enable Controller Management to be accessible from Wireless Clients**.

**Note:** When you enable this option, you can expose the data. Ensure that you have enabled a proper authentication and encryption scheme.

### **Q. Is it possible to assign an integrated controller in a Cisco Catalyst 3750 Switch and a 4400 WLC within the same mobility group?**

**A.** Yes, it is possible to create a mobility group between a Catalyst 3750 Switch with an integrated controller and a 4400 WLC.

### **Q. Are there any basic requirements to maintain when I use the mobility anchor feature in order to configure WLCs for guest access?**

**A.** These are the two basic requirements that need to be maintained when you use mobility anchor in order to configure WLCs for guest access.

- The mobility anchor of the local WLC must point to the anchor WLC, and the mobility anchor of the anchor WLC must point only to itself.

**Note:** You can configure redundant anchor WLCs. Local WLC uses them in the order that the WLCs are configured.

- Make sure that you configure the same security policy for the SSID on both the local and anchor WLCs. For example, if the SSID is "guest" and you turn on web authentication on the local WLC, make sure the same SSID and security policy is also configured on the anchor WLC.
- For the mobility anchor feature to work well, make sure that the anchor WLC and the local WLC use the same IOS version.

### **Q. What are some of the options that can be configured on a Cisco WLC to improve its interoperability with devices that are not manufactured by Cisco?**

**A.** The interoperability of a WLC can be improved through these options:

- Proprietary features reduce the chance of interoperability between third-party devices. These are the proprietary features of Cisco:
  - ◇ Aironet IE – Aironet IE contains information, such as the AP name, load, number of associated clients, and so on sent out by the access point in the beacon and probe responses of the WLAN. Cisco Compatible Extensions clients use this information to choose the best AP with which to associate.

◇ MFP: Management Frame Protection is a feature introduced to protect the management frames, such as deauthentication, disassociation, beacons, and probes wherein the AP adds a Message Integrity Check Information Element (MIC IE) to each of the management frames. Any discrepancy in the MIC IE generates an alert.

These features are enabled by default for any WLAN that is created on the WLC. In order to disable these features, click the WLANs menu in the WLC. A list of WLANs configured on the WLC displays. Click the WLAN to which the client wants to associate. Under the Advanced Tab of WLANs > Edit page, uncheck the boxes that correspond to Aironet IE and MFP.

- Short Preamble ◇ A short preamble improves the throughput performance and is enabled by default. Certain devices, such as SpectraLink Phones, can work only with long preambles. In such cases, it helps in association to uncheck short preambles. In order to disable the short preamble, click the **Wireless** menu of the WLC GUI. Then click the **802.11b/g** > network menu on the left-hand side. Uncheck the **Short Preamble** box.
- Enable the broadcast SSID on the WLAN ◇ With the broadcast SSID enabled, the WLAN/SSID information is sent in the beacons. This also helps the clients that perform passive scans (those that do not transmit probe requests), as well as clients configured without an SSID to associate with the WLC through this WLAN.

**Note:** Make sure that you have strong authentication mechanisms in place, since unintended clients can associate to your wireless network.

- Disable aggressive load balancing globally on the WLC.

## **Q. Can a WLC be managed by CiscoWorks, which is used to manage routers and switches?**

A. No, CiscoWorks cannot manage a WLC. A WCS is needed to manage the WLC.

## **Q. What is the maximum number of rogue APs per WLC?**

A. The maximum number of rogue APs is 100 per 2006 WLC and 500 for all other platforms.

## **Q. Can the WLC send e-mail notifications to the administrator when a critical event occurs?**

A. The WLC does not send e-mail, but it can send traps to the network management stations (NMSs), such as HP OpenView (HPOV). HPOV can perform things such as running scripts to send e-mail on receipt of particular traps.

HPOV is a Hewlett Packard product range that consists of an extensive portfolio of network and systems management products. HPOV is most commonly described as a suite of software applications that allows large-scale system and network management of an organization's IT assets. HPOV includes hundreds of optional modules from HP as well as thousands of third parties that connect within the well-defined framework and communicate with one another.

**Q. If the WLCs in the same mobility group are separated by Network Address Translation (NAT) boundaries, can they communicate mobility messages with each other?**

A. No, the WLC drops mobility traffic on port 16666 if it passes through a NAT/PAT gateway and is NAT translated. This is because mobility message payloads carry IP address information about the source WLC. This is the original management IP address of the WLC. This IP address is validated with the source IP address (NAT translated IP address) of the IP header. This behavior poses a problem when a NAT device is introduced in the network, because it changes the source IP address in the IP header. When you configure the mobility group in a network where NAT is enabled, enter the IP address sent to the WLC from the NAT in the page device of the mobility group member rather than the original management interface IP address of the WLC.

**Q. The physical ports on the WLC are currently set to operate at 1000 mb/s speed. Is it possible to change this port speed to 100 mb/s?**

A. No, the port speed on the WLC cannot be changed. These are set at 1000 mb/s, full duplex speed only.

**Q. Is there any standard procedure that can be performed in order to copy a configuration from one WLC to a second unit?**

A. Complete these steps in order to copy a configuration from one WLC to another:

1. Go to **Management > Upload** on the WLC from where you need to copy the configuration. Then, upload a copy of the configuration to a TFTP server.
2. On the WLC to which you want to copy the configuration, go to **Management > Download** and pull the configuration to it from the TFTP server. Keep in mind that the configuration file has information of the original WLC, which includes IP address, hostname, and so on.
3. After the configuration is copied to the intended WLC, you need to change the hostname, IP addressing information, RADIUS shared secret keys (possibly) and mobility group lists information. Change the mobility group member, which is listed as <Local> under the Controller > Mobility Management page.

**Q. I have set the Radio Resource Management (RRM) to the default settings on my WLC. However, I cannot find my RRM to automatically adjust the channel and power levels. Why?**

A. RRM possibly does not work for any of these reasons

- The RRM works only if an AP hears RF signals from at least three nearby APs, with a third neighbor that transmits a signal strength greater than -65dbm. If any of these conditions fail, the RRM does not work.
- The auto RRM feature includes channel adjustment, power adjustment, and coverage hole detection. These features do not work if they are disabled or the method of assignment is chosen as manual.

While a fresh AP boots up, it initially keeps power at the default value of 1 (highest). When it sees three or more APs with power levels greater than -65 dBm (in the same RF-Mobility-Domain and same channel), it attempts RRM first (change channels). If not

successful because the channels are manually fixed or there are more APs than channels available, the AP drops its power level.

Refer to Radio Resource Management: Concepts for more information on how RRM works.

### **Q. Does the WLC locally support EAP–PEAP authentication?**

**A.** Through version 4.1, Protected Extensible Authentication Protocol (PEAP) is not supported locally on the WLC. You need an external RADIUS server. With WLC version 4.2 and later versions, local Extensible Authentication Protocol (EAP) now supports PEAPv0/MSCHAPv2 and PEAPv1/GTC authentication.

### **Q. Can we place the LAP under NAT? Does the LWAPP from AP to WLC work through NAT boundaries?**

**A.** Yes, you can place the LAP under NAT. On the AP side, you can have any type of NAT configured, but on the WLC side, you can have only 1:1 (Static NAT) configured. PAT cannot be configured on the WLC side because LAPs cannot respond to WLCs if the ports are translated to ports other than 12222 or 12223, which are meant for data and control messages.

### **Q. Is it possible to set a limit to the number of clients that connect to the AP on the AP itself?**

**A.** In general, there is no way on the AP to limit the number of clients that connect. But you can load balance between APs once they exceed the profile threshold value, which by default is 12 users. There is another feature called aggressive load balancing, which load balances the clients. Aggressive load balancing sets this threshold value at three users.

**Note:** Ultimately, it is the decision of the client to abide by aggressive load balancing or not. The client can again try to associate to the same AP, in which case the AP has to accept client association.

Refer to Aggressive Load Balancing on Wireless LAN Controllers (WLCs) for more information.

## **Troubleshoot FAQ**

### **Q. We have finished our initial deployment of LAPs. When our clients move from one end of the building to the other, they stay associated with the AP to which they were closest. The clients do not appear to be handed off to the next-closest AP until the signal strength from the initial AP is completely depleted. Why?**

**A.** Coverage area of an AP is entirely controlled by the WLC. The WLC talks between its APs and manages their signal strength on the basis of how each AP senses other APs. However, the client movement from one AP to another is entirely controlled by the client. The radio within the client determines when the client wants to move from one AP to the other. No setting on the WLC, AP, or the rest of your network can influence the client's decision to roam to a different AP.

**Q. I changed my WLC to Master Controller mode and saved the configuration. Later, when I rebooted the WLC, I could not see WLC retaining the Master Controller mode. Why? Is this an issue or a normal behavior?**

A. This is the expected behavior. Master Controller mode is normally used only while new APs are added to the Cisco WLAN Solution. When no more APs are added to the network, Cisco WLAN Solution recommends that you disable the master controller mode. Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or operating system code upgrade.

**Q. Is there any way to recover my password for WLC?**

A. No, there is no way to recover the password on your WLC. If you use the Cisco WCS in order to manage the WLC, Wireless LAN Controller Module (WLCM) or WiSM, you should be able to access the WLC from the WCS and create a new admin user without logging into the WLC itself. Or, if you did not save the configuration on the WLC after you deleted the user, then a reboot (power cycling) of the WLC should bring it back up with the deleted user still in the system. If you do not have the default admin account or another user account with which you can log in, your only option is to default the WLC to factory settings and reconfigure it from scratch.

**Q. I changed the LAP mode of my 1030 AP from Local to Bridge mode, and the 2006 WLC no longer detects it. How can I restore the 1030 AP back to its Local AP mode?**

A. In order to configure the bridge in Local Mode, complete these steps:

1. Go to the WLC GUI and choose **Wireless >**. **It displays the list of APs that are currently registered to the WLC. Click on the AP for which you need to change the mode.**

**Note:** Check to see if the AP supports REAP mode. This must be **YES** for indoor bridging APs.

2. Check the option AP mode. If it says Bridge, then change it back to **Local**. This changes the Bridge AP to Normal AP. For more information on how to configure the bridging mode, see the Ethernet Bridging in Point-Point Wireless Mesh Network Configuration Example.

**Q. I have set up a guest WLAN, and the WLC is physically separated from my internal LAN. I decided to use the internal DHCP feature of this WLC, but my wireless clients do not get IP addresses from the WLC. How do the wireless guest users get IP addresses from the WLC when they are connected on a physically separate network?**

- Check to see if the DHCP scope is enabled on the WLC. In order to check this, click the **Controller** menu and click **Internal DHCP server** on the left-hand side.
- Generally, the DHCP server is specified on the interface, which maps to the WLAN. Make sure that the management interface address of the WLC is specified as the

DHCP server on the interface that maps to the guest user WLAN. Alternatively, you can enable the DHCP server override option on the **WLANs > Edit** page and specify the management interface address of the WLC in the **DHCP server IP Addr** field.

**Q. I have a 4400 Series WLC and LAPs registered to the WLC. I have configured WLANs for the clients to connect on the WLC. The problem is that the WLC does not broadcast the SSIDs that I configured for the WLANs. Why?**

**A.** The Admin Status and the Broadcast SSID parameters are disabled by default. Complete these steps in order to enable Admin Status and Broadcast SSID:

1. Go to the WLC GUI and choose **Controller > WLANs**. The WLANs page appears. This page lists the WLANs that are configured.
2. Select the WLAN for which you want to enable broadcasting of the SSID and click **Edit**.
3. In the WLAN > Edit page, check **Admin Status** in order to enable the WLAN. Also check **Broadcast SSID** in order to ensure that the SSID is broadcast in the beacon messages sent by the AP.

**Q. Does the Cisco Unified Wireless solution support redundant WLCs in the demilitarized zone (DMZ) for guest tunneling?**

**A.** Yes, WLCs in the DMZ support redundant WLCs in the DMZ for guest tunneling. For more information on how to configure redundant WLCs, refer to the Configuring Auto-Anchored Mobility section of the document Cisco Wireless LAN Controller Configuration Guide, Release 5.1.

**Q. Wireless LAN clients associated with the LAPs are not able to get IP addresses from the DHCP server. How do I proceed?**

**A.** The DHCP server for a client is usually marked on the interface, which maps to the WLAN. Check if the interface is configured appropriately. For more information on how to troubleshoot DHCP-related issues, refer to the IP Address Issues section of the document Troubleshooting Client Issues in the Cisco Unified Wireless Network.

**Q. My 1131 LAP does not register with my 4402 WLC. What can be the possible reason for this?**

**A.** One common reason is that the LWAPP Transport Mode is configured on the WLC. A 4402 WLC can operate in both Layer 2 and Layer 3 LWAPP mode. Whereas, an 1131 LAP can only operate in Layer 3 mode. Layer 2 mode is not supported on the 1131 LAP. So, if the WLC is configured with the LWAPP Transport Mode of Layer 2, then your LAP does not join the WLC. In order to overcome this problem, change the LWAPP Transport Mode of the WLC from Layer 2 to Layer 3.

In order to change the LWAPP Transport Mode using the GUI, go to the WLC page and locate the second selection in the main field which is LWAPP Transport Mode. Change this to Layer 3 and reboot the WLC. Now, your LAP is able to register with the WLC. For more information on issues related to LAP registration, refer to the document Troubleshoot a Lightweight Access Point Not Joining a Wireless LAN Controller.

**Q. No traps are generated by the WLC for ad hoc rogues, and the SNMP debugs on the WLC do not show any traps from the WLC for ad hoc even though the WLC GUI reported the ad hoc rogues. The WLC runs firmware version 3.2.116.21. Why does this happen?**

A. This issue is due to Cisco bug ID CSCse14889 (registered customers only). The WLC consistently sends traps for detected rogue APs but not for detected ad hoc rogues. This bug is fixed in WLC firmware versions 3.2.171.5 and later.

**Q. What is a rogue AP? Can the rogue APs in my wireless network be automatically blocked?**

A. APs that are not part of your wireless deployment are called rogue APs. It can be either an autonomous AP or LAP that happens to be in the range of authorized APs. Rogue APs cannot be automatically blocked. This must be done manually. The reason for this is that when a rogue AP is found, the finding AP disassociates the clients of the rogue AP, which causes denial of service (DoS) to the clients. This can cause legal issues if the AP of the neighbor is detected as a rogue, and their clients are denied service. For more information on how rogue APs are detected by the WLC, refer to the document Rogue Detection under Unified Wireless Networks.

**Q. We have an enterprise Cisco Airespace WLAN infrastructure. WLAN clients are unable to browse a Microsoft Active Directory domain. This issue is seen in one of our buildings. Other buildings do not have the problem. We do not use any access control lists (ACLs) internally. Also, when a failed client is hard-wired, they can immediately browse the Microsoft Active Directory domain. What could be the problem?**

A. One of the reasons can be that multicast mode is disabled on the WLC. Enable multicast mode on the WLC and see if you are able to access the Microsoft Active Directory domain.

**Q. Does Layer 3 mobility work with an AP group VLAN configuration?**

A. Yes, Layer 3 mobility works with an AP group VLAN configuration. Currently, traffic sources from a Layer 3 roamed wireless client is put on the dynamic interface assigned on the WLAN or the interface of the AP group VLAN.

**Q. Why are our APs that are registered to other WLCs that are in the same RF group shown as rogues?**

A. This can be due to Cisco bug ID CSCse87066 (registered customers only). LWAPP APs in the same RF group are seen as rogue APs by another WLC for one of these reasons:

- The AP sees more than 24 neighbors. The neighbor list size is 24, so the 25th AP is reported as a rogue.
- AP1 can hear the client that communicates to AP2, but AP2 cannot be heard.

Therefore, it cannot be validated as a neighbor. The workaround is to manually set the APs to known internal on the WLC or WCS. Complete these steps on the WLC in order to manually set the APs to known internal:

1. Go to the WLC GUI and choose **Wireless**.
2. Click **Rogue Aps** on the left-hand menu.
3. From the Rogue-AP list, choose the specific AP and click **Edit**.
4. From the Update Status menu, choose **Known internal**.
5. Click **Apply**. This bug is fixed in version 4.0.179.11.

**Q. I have a 1200 LAP to be registered with my WLC. I have configured my DHCP server with option 43. How can I verify whether DHCP option 43 is functioning properly?**

**A.** With DHCP option 43, the DHCP server provides the IP address of the WLCs along with the IP address provided through DHCP. This can be verified from the LAP if the AP is a Cisco IOS-based LWAPP AP, such as the 1242 or 1131AG LAP. In these cases, issue the **debug dhcp detail** command on the AP side to see if the AP successfully receives the option 43 information and what it receives.

**Q. My 2006 WLC shows that different channels have been assigned to the registered APs. However, when I scan with Aironet Desktop Utility (ADU) or Netstumbler, all of the APs are in the same channel (1). What is the reason?**

**A.** This problem occurs when these registered APs are in close proximity with each other. You might be hitting Cisco bug ID CSCsg03420 (registered customers only).

**Q. When I issue the ipconfig/all command at the command prompt of my PC, a different DHCP server address shows. It shows 1.1.1.1 as the DHCP server IP address. This is the virtual interface IP address of the WLC and not the DHCP server address. Why is this shown as the DHCP server?**

**A.** This is because the 1.1.1.1 virtual interface address acts as a DHCP proxy for the original DHCP server. If you want to see the original DHCP server address at the output of the **ipconfig/all** command, then disable the DHCP proxy feature in the WLC to which the client is associated. This can be disabled with the **config dhcp proxy disable** command.

This command will replace the 1.1.1.1 virtual interface address, which shows up itself as the DHCP server, with the actual DHCP server IP address that you defined on the interface or in the override option of the WLAN.

**Q. We have a couple of Access Control Servers (ACSs) that authenticate the wireless clients associated to WLCs. One ACS acts as a primary authenticating server and the other as a failover server. If the primary server fails, the WLC falls back to secondary for authenticating the wireless clients. Once the primary server comes back up, the WLC does not fall back to the primary server. Why?**

A. This is an expected behavior. These steps occur when a client is authenticated through the WLC in multiple ACS deployments:

1. Upon boot up, the WLC determines the active ACS.
2. When this active ACS does not respond to the RADIUS request from the WLC, the WLC searches and makes a failover to the secondary ACS.
3. Even when the primary ACS comes back up, the WLC does not fall back to it until the ACS to which the WLC is currently authenticating fails. In such cases, reboot the WLC in order for the WLC to identify the primary ACS again and fall back to it. This fallback does not occur immediately after reboot. It might take some time.

**Q. I am not able to Secure Shell (SSH) into the WLC when I use SecureCRT SSH v2 SH client software. My WLC runs version 4.0.179.8.**

A. SecureCRT works only with WLCs that run version 4.0.206.0 or later. Upgrade your WLC to this version. Then you can use SecureCRT SH client in order to SSH into the WLC.

**Q. How do I encrypt the configuration files on the WLC?**

A. Encryption of configuration files is already available in WLCs. If you choose from the WLC GUI, **Commands > Upload File**, you see the **Configuration File Encryption** checkbox.

You can force the file to be encrypted through WCS in this way:

- From the WCS GUI, choose **Configure controller**. It displays the list of WLCs that are configured in the WCS. Click on a WLC.
- In the left-hand side, click the **commands** option. You receive a list of controller commands.
- Under **Upload/Download Commands**, choose **download config** from the drop-down menu. At this time, you see this message: **Note: Configuration file encryption key is not set. Downloading configuration file will fail if encryption key is needed. Please click here to setup encryption.**

Basically, you can force the WCS to always set an encryption key for WLC configurations. Encryption is not enabled by default, but it can be enabled both in WLC and WCS, as needed.

## **NetPro Discussion Forums – Featured Conversations**

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

Wireless – Mobility: WLAN Radio Standards

Wireless – Mobility: Security and Network Management

Wireless – Mobility: Getting Started with Wireless

Wireless – Mobility: General

## **Related Information**

- **Cisco Wireless LAN Controller Module Q&A**
- **Cisco Wireless LAN Controllers Q&A**
- **Cisco Wireless LAN Controller Configuration Guide, Release 3.2**
- **Wireless Support Page**
- **Technical Support & Documentation – Cisco Systems**