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 (WLAN) Controllers (WLCs).

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

General FAQ

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

A. Refer to these documents:

- Cisco Wireless LAN Controller Module Q&A
- Cisco Wireless LAN Controllers Q&A

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

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 (OS) software on a Cisco WLC?

A. The Wireless LAN Controller (WLC) Software Upgrade to Versions 3.2, 4.0, and 4.1 document provides the procedure for a software upgrade on your WLC.

Q. Can I upgrade directly from Version 3.1.105 to Version 3.2.78, or do I need to upgrade to Version 3.1.111 before I upgrade to Version 3.2.78?

A. Yes, you can upgrade directly to 3.2.78.0 from 3.1.105.0. After you set up a TFTP server, you can choose **Commands > Download File**, and then choose **Code** from the File Type menu to download the software to the WLC. Reboot the WLC after the file transfer for the new code to take effect.

For instructions on how to perform the upgrade, refer to Wireless LAN Controller (WLC) Software Upgrade to Versions 3.2, 4.0, and 4.1.

Q. Can an Airespace controller that runs Code Version 3.2 be upgraded to Controller Version 4.0? If so, can it be directly upgraded or does it have to be upgraded in increments?

A. All Airespace controllers run up to 3.2 code. Only the Cisco Controllers can run 4.0 and later.

Q. Does the 4400 WLC route the VLANs that are configured on it like a router?

A. The 4400 WLC is an appliance that attaches to your network but does not function like a router. There should be a Layer 2 or Layer 3 device to provide the routing for the VLANs. The WLC maps the SSID of the clients to the VLAN subnet and puts them back out the management interface for the upstream routers to distribute/ACL, etc.

Q. What happens to the wireless network when I perform a software upgrade? Do *all* the access points (APs) 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. The upgrade is done on the WLC, as well as on *all* the lightweight APs (LAPs).

Note: A LAP always has the same version as the WLC.

You must reboot the WLC in order for the new software to take effect, so there is a period of network downtime. Be sure to schedule a maintenance window for the upgrade.

Q. Can a Cisco IOS Software−based access point (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 lightweight APs (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 Wireless LAN Controllers (WLCs)?

A. The limitation on the number of supported access points 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 access points. The 4404 WLC with four gigabit Ethernet ports supports 100 access points.

Q. How do I configure a local database on the Wireless LAN Controller (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 through either the GUI or the CLI. You can enter up to 24 alphanumeric characters. All the special characters with the exception of the quote character can be used for the username and passwords.

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

- **config netuser add <username> <password> wlan <wlan_id> userType permanent description <description>** Adds a permanent user to the local user database on the controller.
- **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 controller.

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 controller?

A. You can give the local net user configured on the controller a lifetime which automatically deletes the username after the allotted lifetime.

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 access points (APs) are supported in a single mobility group.

Q. How does DHCP work with the WLC?

A. The WLC acts as a DHCP relay device. The WLC does the DHCP relay through the virtual interface. Typically, the 1.1.1.1 address is assigned to the virtual interface. This address can be any address. However, it *must not* be a routable address.

These are the events that occur:

1. The WLAN client sees the administration−defined virtual address as the DHCP server address. The recommended address is usually 1.1.1.1 because this address is not normally a routable network address.
2. The WLC shows the virtual address to the WLAN clients and the management interface address upstream.
3. The WLC acts as a DHCP relay (Bootstrap Protocol [BOOTP] relay) device.

Note: When the internal DHCP server is used, the lightweight access point (AP) should be directly connected to the WLC. Also, you cannot share a DHCP scope between two or more WLCs.

Q. Does the Cisco 4400 Series WLC support Internetwork Packet Exchange (IPX) protocol? Does any Airespace 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 graphical user interface (GUI) of the Wireless LAN Controller (WLC)?

A. The controller 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

Note: Internet Explorer 6.0 SP1 or later is the only browser supported to access the controller GUI and to use WebAuth.

Q. Is the Wireless LAN Controller (WLC) GUI supported on Mozilla browsers?

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

Q. How do I retrieve Cisco Wireless LAN Controller (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 on **Wireless LAN Controller** and select the controller platform for which you need the MIBs.
2. The Software Download page for the controller appears. This page contains all the files for the WLC including the MIBs.
3. Download the standard MIBs and the Cisco specific MIBs. 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. Can a controller push configurations to other controllers and manage them, without a wireless control system (WCS)?

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

Q. In a WLC version 4.0, what is the maximum number of supported controllers per mobility group and per radio frequency (RF) domain? Also, in guest tunneling, how many Ethernet over IP (EoIP) tunnels can be formed between a single anchor controller to different internal controllers?

A. The latest WLCs support up to 20 WLCs per RF domain and 24 WLCs per mobility group. Also, a single anchor controller 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 2000 Series Controllers and the 4400 Controllers?

A. The major differences between the 2000 and 4400 Series Controllers are in the features they support.

A 2000 Series Controller does not support these hardware features:

- Power over Ethernet (PoE)
- Service port (separate out−of−band management 10/100−Mbps Ethernet interface)

These software features are not supported on 2000 Series Controllers:

- 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 Controller supports all the forementioned hardware and software features.

Q. Which lightweight access points (LAPs) do the 4100 Series Controllers support?

A. Only the Airespace 1200, 1250, the Cisco 1000 Series, and the Cisco 1500 Series LAPs work with the earlier 4100 Series Controllers.

Q. I have a Cisco Adaptive Security Appliance (ASA) device. Can I use this ASA as a DHCP server instead of windows DHCP server in order to assign IP addresses to my lightweight access points (LAPs)?

A. No, it is not possible to use an ASA as a DHCP server for LAPs. This is because the DHCP requests from the LAPs are forwarded to the external DHCP server through the WLC. Therefore, a WLC acts as a DHCP relay agent to forward the request from the LAP. However, ASA does not support DHCP requests from a DHCP relay agent.

If ASA is configured as a DHCP server, you cannot configure DHCP relay services on an interface on which the server is enabled. Additionally, DHCP clients must be directly connected to the interface on which the server is enabled. Refer to PIX/ASA as a DHCP Server and Client Configuration Example for more information.

The Cisco ASA combines the functions of a firewall, Virtual Private Network (VPN), and intrusion prevention system (IPS) in a single appliance. The ASA is managed by an easy−to−use Adaptive Security Device Manager (ASDM).

Q. Is it possible to go back and make corrections in the wireless LAN controller (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.

For example, you use the WLC configuration wizard in order to configure the WLC from scratch.

Instead of entering the username as **admin**, you enter it as **adminn**. In order to correct this, 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]: adminn
Enter 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) . As of the latest controller version 4.0.206.0, a user can enter only 31 characters. Currently, there is no workaround for this.

Q. With the Management via Wireless feature enabled on wireless LAN controllers (WLCs) in a mobility group, I can only access one WLC from that mobility group, but not all. 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 access point is registered. The client cannot manage other WLCs, even though these WLCs are in same mobility groups. This is implemented for security, and recently was tightened down 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 controllers using a wireless client. This feature is supported for all management tasks, except uploads to and downloads from (transfers to and from) the controller.

This feature allows wireless clients to manage only the Cisco WLC associated with the client and the associated lightweight access point. This means that clients cannot manage another Cisco WLC to which they are not associated.

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

Q. Is it possible to assign an integrated controller in a 3750 Switch and a 4400 Wireless LAN Controller 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 Controller.

Q. Are there any basic requirements to maintain when I use the mobility anchor feature in order to configure wireless LAN controllers (WLCs) for guest access?

A. These are the 2 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 controller must point to the anchor controller, and the mobility anchor of the anchor controller must point to itself.
- Make sure you configure the same security policy for the service set identifier (SSID) on both the local and anchor controllers. For example, if the SSID is "guest" and you turn on web authentication on the local controller, make sure the same SSID and security policy is also configured on the anchor controller.

Q. What are some of the options that can be configured on a Cisco Wireless LAN Controller (WLC) to improve its interoperability?

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

- Enable broadcast service set identifier (SSID) per WLAN With broadcast SSID enabled, the WLAN/SSID information is sent in the beacons. This also helps clients that perform passive scanning (those that do not transmit probe request) as well as clients configured without an SSID to associate with the controller through this WLAN.
- Disable Aironet extensions (if enabled) per WLAN Cisco−proprietary Aironet extensions detect the capabilities of Cisco Aironet client devices and support features that require specific interaction between the Cisco Access Point (AP) (hence the controller) and associated client devices. Non−Cisco clients do not always support the Aironet extensions. With Aironet Extensions disabled on a particular WLAN, interoperability with the non−Cisco devices can be improved. Therefore, a controller can interoperate with a non−Cisco client device that associates through this WLAN.
- Disable client exclusions per WLAN.
- Disable Management Frame Protection (MFP) signature generation (if enabled) per WLAN Refer to Infrastructure Management Frame Protection (MFP) with WLC and LAP Configuration Example for more information on MFP.
- Disable aggressive load balancing globally on the controller.
- From the controller GUI, disable client exclusion policies under Security > wireless protection policies.
- From the controller GUI, set AP authentication/MFP to off under Security > wireless protection policies.
- Disable short preamble The radio preamble, which is sometimes called a header, is a section of data at the head of a packet that contains information that wireless devices need when sending and receiving packets. You can set the radio preambles to long or short.
    - Short A short preamble improves throughput performance and is enabled by default. Cisco Aironet Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles. However, some wireless devices, such as SpectraLink NetLink phones, require long preambles. In such cases, unchecking short preamble enables long preamble to achieve interoperability with Spectralink Netlink phones. Refer to Using the GUI to Enable Long Preambles for information on how to disable short preamble.
    - Long A long preamble ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your access points, you should use short preambles.

Q. Can a Wireless LAN Controller (WLC) be managed by CiscoWorks, which is used to manage routers and switches?

A. No, CiscoWorks cannot manage a WLC. A Wireless Control System (WCS) is needed to manage the WLC.

Q. What is the maximum number of rogue access points (APs) per controller?

A. The maximum number of rogue APs is 100 per 2006 Wireless LAN Controller, and 500 for all other platforms.

Q. Can the Wireless LAN Controller (WLC) send email notifications to the administrator when a critical event occurs?

A. The WLC does not send email, but it can send traps to the Network Management System (NMS) stations, such as HP OpenView (HPOV). HPOV can perform things such as running scripts to send email 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 which allow 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 which connect within the well−defined framework and communicate with one another.

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

A. No, the controller drops mobility traffic on port 16666 if it passes through a NAT/PAT gateway and is NAT translated. This is because the receiving controller verifies the remote controller's IP address inside the data portion of the packet against the source IP address of the packet.

This is related to Cisco bug ID CSCsb87921 (registered customers only) , which also explains the associated workaround.

NAT is designed for IP address simplification and conservation. It enables private IP inter−networks that use non−registered IP addresses to connect to the Internet. NAT operates on a router, usually connecting two networks together, and translates the private (not globally unique) addresses in the internal network into legal addresses before packets are forwarded onto another network. As part of this functionality, NAT can be configured to advertise only one or a very few addresses for the entire network to the outside world. This provides additional security and effectively hides the entire internal network from the world behind that address. NAT has the dual functionality of security and address conservation, and is typically implemented in remote access environments.

Q. The physical ports on the controller are currently set to operate at 1000 mbps speed. Is it possible to change this port speed to 100 mbps?

A. No, the port speed on the controller cannot be changed. These are set at 1000 mbps, full duplex speed only.

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

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

1. Go to **Management** > **Upload** on the controller from where you need to copy the configuration. Then, upload a copy of the configuration to a TFTP server.
2. On the controller 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 controller to which you copy the configuration will have the same information, which includes IP address, hostname, etc. Therefore, you should copy the

configuration to the backup controller off the production network.
3. After the configuration is copied to the backup controller, 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 one is listed as <Local>.
4. Transfer this modified configuration from the backup controller to the intended controller in the production network.

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

A. You need at least 4 access points (APs) nearby. The APs need to see each other and one has to be on the same channels as its neighbor in order to test auto RRM. Then, at every 600s (10 min) intervals, the WLC decides if a channel/power (RRM) adjustment is necessary by changing the AP to a different channel (Dynamic Channel Selection Algorithm) or by reducing the power (Transmit Power Control Algorithm).

While a fresh AP boots up, it initially keeps power at the default value of 1 (highest). When it sees 3 or more APs (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, and the power level of the neighboring APs are greater than −65 dBm, the AP drops its power level.

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

Q. Does the local user database of the Wireless LAN Controller (WLC) support EAP−PEAP authentication?

A. No, the internal user database on the current versions of WLC cannot be used for PEAP. You need an external RADIUS server.

Q. Can we place the lightweight access point (LAP) under Network Address Translation (NAT)? Does the Lightweight Access Point Protocol (LWAPP) from access point (AP) to controller work through NAT boundaries?

A. Yes, you can place the LAP under NAT. LWAPP and NAT only play well together when you are NATing on the AP side and you perform 1:1 NAT (so you can forward LWAPP ports to the right internal address).

However, make sure that your WLC is not NATed. When the WLC is placed under NAT, the APs cannot join the WLC. This is because it tries to send a join request to the AP−manager private IP address after it receives that IP address in the discovery response from the WLC. The only way for you to make this work is to provide the WLC AP−manager interface with a public "reachable" IP address. This is what occurs when the WLC is placed behind NAT:

1. The AP sends a discovery request to the WLC.
2. The WLC sends a discovery response to the AP that contains the internal IP address of AP−manager interface.
3. The AP sends a join request to the WLC on the internal Interface IP address. However, it never reaches the WLC because this is a private address.

Q. Is it possible to set a limit to the number of clients that connect to the access point (AP) on the AP itself?

A. In general, there is no way on the AP to limit the number of clients that connect. The clients actually load balance between APs once they exceed the profile threshold value, which by default is 12 users. If you enable aggressive load balancing, the WLCs might disassociate some clients. Aggressive load balancing sets this threshold value at 3 users.

Radio Resource Management (RRM) load balances new clients across grouped lightweight access points (LAPs) that report to each controller. The controller provides a centralized view of client loads on all APs. This information can be used to influence where new clients attach to the network or to direct existing clients to new APs in order to improve wireless LAN performance. The result is an even distribution of capacity across an entire wireless network.

Note: Client load balancing works only for a single controller. It does not operate in a multi−controller environment.

Refer to Radio Resource Management (RRM) for more information.

Troubleshoot FAQ

Q. We have finished our initial deployment of lightweight access points (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. The client movement from AP coverage area to a different AP zone 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 the others. The client movement from AP to AP is entirely controlled by the client itself. The radio within the client determines when the client wants to make the jump from one AP to the other. No setting on the WLC, AP, or the rest of your network can make the client move before it wants 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 access points are added to the Cisco Wireless LAN Solution (Cisco WLAN Solution). When no more access points are added to the network, Cisco WLAN Solution recommends that you disable the master controller. Because the master controller is normally not used in a deployed network, the master controller setting is automatically disabled upon reboot or OS code upgrade.

Q. Is there any way to recover my 2006 WLC password?

A. No, there is no way to recover the password on your WLC. If you use the Cisco Wireless Control System (WCS) in order to manage the WLC, Wireless LAN Controller Module

(WLCM) or Wireless Services Module (WiSM), you should be able to access the controller from the WCS and create a new admin user without logging into the controller itself. Or, if you did not save the configuration on the controller after you deleted the user, then a reboot (power cycling) of the controller 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 controller to factory settings and reconfigure it from scratch.

Q. I changed the lightweight access point (LAP) mode of my 1030 access point (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. There are considerations and required steps before you place an LAP into Bridge mode that must be followed in order, or you can cause the LAP to not join the controller. The AP that is directly associated to the controller is the Bridge roof−top access point (RAP), and Remote mode LAPs are pole−top access points (PAPs). Complete these steps in order to enable bridging on the controller, and to prepare LAPs for use as RAP/PAPs.

Begin with the LAPs joined to the Layer 2 Lightweight Access Point Protocol (LWAPP) mode controller, in Local mode.

1. From the GUI, go to the Wireless page and make a note of the intended Bridge AP MAC addresses.
2. Click **Bridging**.
3. Check **Enable Zero Touch Configuration**.
4. Enter an ASCII or HEX Bridging Shared Secret Key that is used to verify LAP identities.
5. Go to the Security page, and click **MAC Filtering** located under AAA on the left. Add the MAC addresses of the intended Bridge APs, and specify the WLAN and the associated Interface.
6. Go to the Wireless page. Bridge capable LAPs show Bridging Information in addition to Detail in order to help identify them. Click **Detail** on one of your intended Bridge APs. Under Inventory Information on the right side, verify the LAP model and if REAP mode is supported.
7. Check **AP Static IP**, and enter an IP address, Netmask, and Gateway in the subnet of the interface that is used. Ensure these IPs are not in the DHCP scopes that are given to clients.

You are now prepared to configure the AP mode, change the role of the AP from Local to Bridge AP, and click **Apply**.

If the setup does not work as expected, follow the recovery process outlined here.

1. From the controller GUI, choose **Wireless > Bridging** and check **Enable Zero Touch Configuration**.
2. From the controller GUI, choose **Security > MAC Filtering** and add a new MAC filter with AP MAC address.
3. Go to the controller CLI and issue the **config network allow−old−bridge−aps enable** command.

This allows the APs to join. Complete these steps once they join.

1. Go to the controller GUI and choose **Wireless > Cisco APs > Detail**.
2. Check if the AP supports REAP mode. This should be **YES** for indoor bridging APs.
3. Check the AP mode. If it says Bridge, then change it back to **Local**. This changes the

Bridge AP to Normal AP.

Q. I recently set up the 4402 Wireless LAN Controller (WLC) to manage the new Cisco lightweight access points (LAPs). I run PIX 501 version 6.3(5) and also use the PIX as a DHCP server for the clients. However, whenever the PIX gets a request from the controller for the wireless clients, it drops the request and the clients do not get an IP address. Why does this happen?

A. The PIX can act as a relay agent. However, in this case the WLC is a relay agent for the client. The PIX does not support DHCP requests from a relay agent. It ignores these requests. Clients must be directly connected to the PIX Firewall and cannot send requests through another relay agent or a router. The PIX has limited functionality in the context of DHCP. It can work as a simple DHCP server for internal hosts that are directly connected to it, so it can maintain its table based on the MAC addresses that are directly connected and that it can see. That is why an attempt to assign addresses from a DHCP relay are not available and the packets are discarded.

Refer to Using DHCP Relay for more information on how to use PIX in order to provide DHCP services.

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

A. One possible solution is to put a DHCP server override on the WLAN settings page for the SSID in question (in this case, it is guest SSID). Then point this DHCP server override to the IP address of the port on the controller to which this guest WLAN is associated.

Q. I have a 4400 Series Wireless LAN Controller (WLC) and lightweight access points (LAPs) registered to the WLC. I have configured WLANs for the clients to connect to on the WLC. The problem is that the WLC does not broadcast the service set identifiers (SSIDs) that I configured for the WLANs. Why?

A. In order for the WLCs to be able to broadcast SSIDs, the Admin Status and the Broadcast SSID parameter must be enabled for the WLANs. Complete these steps in order to enable Admin Status and Broadcast SSID:

1. Go to the controller 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 Staus** 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 DMZ for guest tunneling?

A. Presently there is no support for redundant WLCs in the DMZ for guest tunneling. This is why the client does not automatically connect to the other controller in the DMZ.

Q. Wireless LAN Clients associated with the lightweight access points are not able to get IP addresses from the DHCP server. How do I proceed?

A. The common reason for this problem might be that the WLC and the DHCP server reside on different subnets. The WLC does not do routing and it depends on a Layer 3 device for routing between these different subnets.

The possible workaround is to configure the DHCP server on the same subnet as the WLC. If the DHCP server is on a different subnet, then either a router must be in place in order to route between the WLAN and the DHCP server or you can configure the internal DHCP server on the WLC with a scope for the WLAN.

Q. My 1131 lightweight access point (LAP) does not register with my 4402 Wireless LAN Controller (WLC). What can be the possible reason for this?

A. One common reason is that the Lightweight Access Point Protocol (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 controller. Now, your LAP is able to register with the controller.

Q. I run Version 4.0.206.0 on the WLC. The LAPs frequently deregister from the WLCs. After some time, the LAPs automatically register back to the controller. Why ?

A. This can be due to bug CSCsh50966. Because of this bug, there can be sporadic interruptions in connectivity at ARP refresh time, which possibly result in the periodic loss of associations for LAPs associated through AP managers other than the first (AP−manager). Also, access points associated to a controller that run software release 4.0.206 sometimes reboot when LWAPP traffic drops. This is especially likely if the default router runs an IOS version that is subject to CSCec40253. Use this workaround. On the system that issues the unicast ARP request, configure a static ARP entry for the AP−manager2 (and up) interface(s). For example, if the deficient ARP unicasts are issued by an IOS router, use a command such as this

```
router(config)#arp 10.1.1.1 0000.0102.abcd arpa
```

where 10.1.1.1 is the IP address of the AP−manager<n> interface, and 0000.0102.abcd is its

MAC address.

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 is due to Cisco bug ID CSCse14889 (registered customers only) . The WLC consistently sends traps for detected rogue access points (APs) but not for detected Ad−Hoc rogues. This bug is fixed in WLC firmware versions 3.2.171.5 and later.

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

A. One of the reasons can be that multicast mode is disabled on the controller. Enable multicast mode on the controller and check if you are able to access the Microsoft AD domain.

Q. Does Layer 3 mobility work with an access point (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.

This is how WLCs handle Layer 3 roaming:

1. When a wireless client roams to a new WLC (for example, WLC1), WLC1 sends mobility packets to all WLCs in the same mobility group.
2. The old WLC (for example, WLC2) sends a mobility packet to WLC1 and lets WLC1 know the IP address of the wireless client.
3. From then, WLC1 puts traffic from the wireless client to the local interface on WLC1. It is not the same interface on WLC2.
4. Any traffic to the wireless client is sent to WLC2. WLC2 forwards the packet using Ethernet over IP (EoIP) to WLC1, which in turn sends the traffic to the wireless client via a Lightweight Access Point Protocol (LWAPP) tunnel.

Q. Why are access points (APs) that are on other controllers in the same mobility group shown as rogues?

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

- The AP sees more than 24 neighbors. The neighbor list size is 24, so any other ones are reported as rogues.

- 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 and/or WCS. Complete these steps on the controller in order to manually set the APs to known internal:

1. Go to the WLC GUI and choose **Wireless**.
2. Click **Rogue Aps** in the left side menu.
3. From the Rogue−AP list, choose **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 configured my Wireless LAN Controller using the CLI wizard. I mistyped the system name and am not able to correct it. Should I reconfigure using the CLI wizard? Is there a command to change the system name after completing the CLI wizard?

A. Yes. You can change the system name later. If the system name is mistyped while you configure the WLC using the CLI wizard, you can change it later with the **config sysname <x>** command. You do not have to re−do the CLI wizard in order to correct the system name.

Q. I have a 1200 Lightweight Access Point (LAP) to be registered with my Wireless LAN Controller (WLC). I have configured my DHCP server with option 43. How can I verify whether DHCP option 43 is functioning properly?

A. This can be verified from the LAP if the AP is a Cisco IOS based Lightweight Access Point Protocol (LWAPP) AP, such as the 1242 or 1131AG LAP. In these cases, issue the **debug dhcp detail** command on the AP side in order to see if the AP successfully receives the option 43 information and what it receives.

Q. My 2006 controller shows that different channels have been assigned to the registered access points (APs). However, when I scan with Aironet Desktop Utility (ADU) or Netstumbler, all 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 controller 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 controller 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 (ACS) that authenticate the wireless clients associated to wireless LAN controllers (WLCs). One ACS acts as a primary authenticating server and the other as a failover server. If the primary server fails, the controller falls back to secondary for authenticating the wireless clients. Once the primary server comes back up, the controller does not fallback 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 controller is currently authenticating fails.

In such cases, reboot the WLC in order for the WLC to identify the primary ACS again and fallback 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 wireless LAN controller (WLC) when I use SecureCRT SSH v2 SH client software. My controller runs version 4.0.179.8.

A. This is because of Cisco bug ID CSCsc98897 (registered customers only) . SecureCRT works only with controllers that run version 4.0.206.0. Upgrade your controller to this version. Then, you can use SecureCRT SH client in order to SSH into the controller.

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

A. Encryption of configuration files is already available in controllers. If you choose from the controller 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 > commands > Upload/Download Commands> download config** from the controller. 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 controller 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.

NetPro Discussion Forums − Featured Conversations for Wireless

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**

Updated: Feb 15, 2008 Document ID: 69561