

Cisco Aironet Access Point FAQ

Document ID: 8103

Refer to the **Cisco Wireless Software Center** (registered customers only) in order to get Cisco Aironet drivers, firmware and utility software.

Questions

Introduction
Design FAQ
Troubleshoot FAQ
Related Information

Introduction

This document provides answers to the most frequently asked questions (FAQ) about Cisco Aironet Access Points (APs).

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

Design FAQ

Q. What is the default user name and password for Cisco IOS® Software-based APs?

A. Cisco IOS Software-based APs have a default configuration that includes a user name and password combination, both of which are **Cisco** (case sensitive). After you reset to factory defaults, be ready to give Cisco as both the username and password when either the GUI or the command-line interface (CLI) prompts you.

Q. What cable should I use for a console connection?

A. Use a straight-through cable with nine-pin male to nine-pin female connectors in order to connect the COM1 or COM2 port on your computer to the RS-232 port on the AP. Use a terminal emulation program on your computer, such as:

- ◆ Microsoft Windows HyperTerminal
- ◆ Symantec ProComm
- ◆ Minicom

Use these port settings:

Speed:	9600 bits per second (bps)
Data bits:	8
Stop bits:	1
Parity:	None
Flow Control:	Xon/Xoff

Note: If the flow control Xon/Xoff does not work, try using the flow control None.

Q. I have an Aironet 1231 AP. Does Cisco make a 50-foot extension cable so that I can have the AP in one area and the antenna in another?

A. Yes, the part number of the 50-foot cable is AIR-CAB050LL-R. You can use this cable to connect your AP to the antenna.

Q. How do you check the radio type on autonomous AP?

A. You can use the **show controllers** command from the privileged EXEC mode on the AP to get information on the radio type.

Q. How do you set up an IP address on the AP?

A. By default, the AP requests an IP address through DHCP.

Cisco IOS Releases 12.3(2)JA and later change the default behavior of APs requesting an IP address from a DHCP server:

- ◆ When you connect a 1200 or 1230 series AP with a default configuration to your LAN, the AP requests an IP address from your DHCP server. If it does not receive an address, it continues to send requests indefinitely.
- ◆ When you connect an 1100 series AP with a default configuration to your LAN, the 1100 series AP makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for five minutes. During this five minute window, you can browse to the default IP address and configure a static address. If after five minutes the AP is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five minute window for browsing to the AP at 10.0.0.1, you can power-cycle the AP to repeat the process.

You can also manually set the IP address of the AP. On a Microsoft Windows PC that is connected to the Ethernet segment, from the DOS prompt, issue this command:

```
arp -s a.b.c.d 00-12-34-56-78-90
```

Note: The term *a.b.c.d* represents the IP address that is to be set on the AP, and *00-12-34-56-78-90* is the MAC address. This address appears on the panel on the bottom of the AP.

Issue this command in order to verify the address:

```
ping a.b.c.d
```

Note: This procedure does not work if the AP has already been assigned an IP address by another method.

Q. How do you enable HTTPS access on the AP?

A. In order to enable HTTPS, you must add this command to your AP:

```
AP(config)#ip http secure-server
```

When you add the **ip http secure-server** command, you see the RSA keys required for secure communication regenerated on the APs.

Q. How does a client choose an access point (AP) to get associated?

A. Access point (AP) choice is done on the machine radio of the client. Based on the manufacturer, driver, type of card, and so forth, it can use different metrics to make the choice. The most common AP affiliation mechanism used in most clients is based on signal strength received by the client from the APs. The 802.11 standard requires only that the wireless client card reports signal strength with a simple metric called Received Signal Strength Indicator (RSSI). The client then associates with the AP with the strongest signal. It is well known that these algorithms can lead to poor performance. The main reason is due to its lack of knowledge of the load on different APs.

Q. Can a wireless client roam between LWAPP APs and autonomous APs?

A. No, roaming between LAPs and autonomous APs is NOT supported. The reason is that, when connected to LWAPP APs, traffic is passed through an LWAPP tunnel. Since there is no mobility tunnel between the Wireless LAN Controller and the autonomous APs, the roam does not work.

Q. How do you extend the coverage of the AP?

A. There are several ways to extend the coverage area for an AP. These are the most important methods:

- ◆ Use APs in repeater mode.
- ◆ Use a secondary AP in AP mode with nonoverlapping channels.
- ◆ Change the transmitter power level parameter of the existent AP in order to extend the coverage.
- ◆ Position the APs optimally.

Refer to *WLAN Radio Coverage Area Extension Methods* for a complete description of how to implement these methods.

Q. What are the implications if your AP is in repeater mode?

A. The Ethernet port is disabled in repeater mode. The effective throughput is cut in half once for each hop away from the parent AP.

In order to set up repeaters, you must enable Aironet extensions on both the parent (root) access point and the repeater access points. Aironet extensions, which are enabled by default, improve the ability of the access point to understand the capabilities of Cisco Aironet client devices associated with the access point. If you disable Aironet extensions, you can sometimes improve the interoperability between the access point and non-Cisco client devices. Non-Cisco client devices can find communication difficult with repeater access points and the root access point to which repeaters are associated.

The infrastructure SSID must be assigned to the native VLAN. If more than one VLAN is created on an access point or wireless bridge, an infrastructure SSID cannot be assigned to a non-native VLAN. This message appears when the infrastructure SSID is configured on

non-native VLAN:

```
SSID [xxx] must be configured as native-vlan before enabling
infrastructure-ssid
```

Because access points create a virtual interface for each radio interface, repeater access points associate to the root access point twice: once for the actual interface and once for the virtual interface.

Note: You cannot configure multiple VLANs on repeater access points. Repeater access points support only the native VLAN.

Q. What are the features supported by the Aironet Extension option?

A. The Aironet extension is a proprietary feature implemented by Cisco. Aironet extensions contains information elements that support these features.

- ◆ **Load Balancing:** The access point uses Aironet extensions to direct client devices to an access point that provides the best connection to the network based on factors such as the number of users, bit error rates, load and signal strength.

Load balancing is proprietary between devices that understand the Aironet extensions. Load balancing is implemented by extensions in AP beacons and/or probe-responses, which provide information on these:

- ◇ Base-station signal strength
- ◇ Base station loading (% transmitter busy)
- ◇ Number of hops to the backbone
- ◇ Number of client associations

The client evaluates these and associates to the "best" one. Non-Cisco clients do not understand these extensions.

- ◆ **MIC:** Cisco Proprietary Message Integrity Check (MIC) MIC is an additional WEP security feature that prevents attacks on encrypted packets called bit-flip attacks. The MIC is implemented on both the access point and all associated client devices.
- ◆ **Cisco Proprietary Temporal Key Integrity Protocol (CKIP),** also known as WEP key hashing, is an additional WEP security feature that defends against an attack on WEP, in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.
- ◆ In addition to these, Aironet extensions carry more information that include these:

- ◇ Load that the AP currently handles
- ◇ Number of hops from the Wired network
- ◇ Device type, which helps identify the product under the Cisco system for management
- ◇ Device name
- ◇ Number of associated clients
- ◇ Radio type, a feature used to determine certain characteristics about the radio, such as datarate, radio type (1310, 1200, 352 or 342), security type (WEP/802.1x), etc.

Devices that are CCX compatible also can take advantage of some of the Aironet Extension features. Here is a list of the features available with the different versions of Cisco Compatible Extensions:

Cisco Compatible Extensions – Versions and Features

Q. Can you connect two computers together without an AP through wireless interface cards?

A. Yes. From the Aironet Client Utility (ACU), you can configure the clients to run in ad hoc mode. This connection is only a peer-to-peer connection. One PC becomes the parent and controls the connection. The other PCs in ad hoc mode are child stations.

Q. Do you need special hardware to support encryption?

A. The specific hardware model determines the level of encryption for the unit:

- ◆ The 341 and 351 models only support 40-bit encryption.
- ◆ The 342 and 352 models support both 40- and 128-bit encryption.
- ◆ All 1100, 1200, and 1300 series models support both 40- and 128-bit encryption.

Q. Is it possible to view all the APs and their associated clients that belong to that particular network/infrastructure just from a single AP?

A. This is possible from a VxWorks AP. A single VxWorks AP can display all the clients and their APs in a network. This can be achieved if you click **Association > Entire Network > Apply**. In an IOS-based AP, it does not display all the associated clients in that network without the help of a management device, such as WLSE, with one AP as WDS or a controller if the image in AP is an LWAPP image.

Q. I use CCKM in my network, but still the entire authentication process occurs whenever the client device roams. In short, fast secure roaming does not function as expected. Why?

A. This is possibly because of the bug CSCsg10128. This bug is fixed in Version 3.1.03.

Q. Do Cisco Access Points support the UniDirectional Link Detection (UDLD) feature in order to shutdown the Ethernet connection to switches if there is a Layer 1/Layer 2 cable failure?

A. No, Cisco Access Points do not support the UDLD feature.

Q. How do you supply power to an Aironet AP?

A. The power options for your AP depend on the AP model that you have. Refer to Cisco Aironet and WLAN Controller Product Power Options for more information.

Q. I have an AP1010, AP1030, and an AIR-LAP-1232AG. Are they able to use a WS-PWR-PANEL for Power over Ethernet (PoE)?

A. The WS-PWR-PANEL only supports access points with a single radio. Refer to the compatibility matrix available in the *Cisco PoE and Cisco Intelligent Power Management* section of Cisco Aironet Power Over Ethernet Application Note for more information.

Q. How do you save the configuration of the AP?

A. Modifications to the configuration are saved immediately. You can dump the current configuration in a text format from the **Setup** menu. Then, choose **Cisco Services > Manage System Configuration** and download the system configuration.

Q. How do I determine the specific frequency or channel that my AP or bridge uses?

A. Use the **show controllers dot11Radio0** command in order to show the frequency and channel that the AP or bridge is on. This example output shows where to find the information:

```
ap#show controllers dot11Radio0
!
interface Dot11Radio0
Radio AIR-AP1242GA, Base Address 0014.1b58.08f
Version 5.80.12
Serial number: GAM09200992
Number of supported simultaneous BSSID on Dot1
Carrier Set: Americas (US )
DFS Required: No
Current Frequency: 2412 MHzChannel 1
```

Q. How do I make my AP work with other IEEE 802.11b devices?

A. In order to enable the AP to communicate with another 802.11b device, turn off Aironet extensions. Check the **Non-Aironet 802.11** check box in the Express Setup window. Alternatively, you can click the **Use Aironet Extension** radio button in the Advanced AP Radio window.

Q. Which devices can associate with an AP?

- ◆ AP to client
- ◆ AP to AP (in repeater mode)
- ◆ AP (in repeater mode) to base station (in AP mode)
- ◆ AP to workgroup bridge

Q. At what frequency does an AP communicate?

A. In the United States, IEEE 802.11b APs transmit and receive in one of 11 channels within the 2.4 GHz frequency. The IEEE 802.11a APs transmit and receive in one of eight channels in the 5 GHz frequency. The IEEE 802.11g APs transmit and receive in one of 11 channels within the 2.4 GHz frequency. These are public frequency ranges and are unlicensed by the FCC.

Q. How do you secure the data across an AP radio link?

A. There are several methods to secure your data across an AP wireless link. In order to learn more about the different security methods, refer to FAQ on Cisco Aironet Wireless Security.

Q. How many clients can associate to the AP?

A. The AP has the physical capacity to handle 2048 MAC addresses, but, because the AP is a shared medium and acts as a wireless hub, the performance of each user decreases as the

number of users increases on an individual AP. Ideally, not more than 24 clients can associate with the AP because the throughput of the AP is reduced with each client that associates to the AP.

Q. Is there a limitation on the number of MAC address filters that can be configured on the AP?

A. You can use the CLI in order to configure up to 2,048 MAC addresses for filtering, but, with the use of the web-browser interface, you can configure only up to 43 MAC addresses for filtering.

Q. What is the typical range for an AP?

A. The answer to this question depends on many factors, which include these:

- ◆ Data rate (bandwidth) that you desire
- ◆ Antenna type
- ◆ Antenna cable length
- ◆ The device that receives the transmission

In an optimal installation, the range can be up to 300 feet.

Q. What are the available transmit power level settings for a 1200 AP?

A. The transmit power settings are different and depend on the radio that is used. Refer to Cisco Aironet 1200 Series Access Point Data Sheet for the complete list of power setting levels. Because the power settings vary on the basis of the channel, perform a site survey. The site survey is important in order to get accurate information on the setting to use. Refer to Wireless Site Survey FAQ for details on site surveys.

Q. How can I set the AP so that only IEEE 802.11g clients can connect? I do not want the IEEE 802.11b clients to connect and slow down the wireless network. There is a second, parallel 802.11b network for unsecured clients.

A. In order for the AP to receive only 802.11g clients, complete these steps in the GUI:

1. Go to the Network Interfaces section and click **Radio 0–802.11G**.
2. Click the **Settings** tab at the top of the Radio 0–802.11G window.
3. Choose **Disable** for these data rates:
 - ◇ 1.0
 - ◇ 2.0
 - ◇ 5.5
 - ◇ 11.0
4. Choose **Require** for all the other data rates. These are the other data rates:
 - ◇ 6.0
 - ◇ 9.0
 - ◇ 12.0
 - ◇ 18.0
 - ◇ 24.0
 - ◇ 36.0
 - ◇ 48.0
 - ◇ 54.0

5. Click **Apply** at the bottom of the window. This window provides an example:

Data Rates:	Best Range	Best Throughput	Default
1.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
2.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
5.5Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
* 6.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 9.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
11.0Mb/sec	<input type="radio"/> Require	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
* 12.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 18.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 24.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 36.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 48.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable
* 54.0Mb/sec	<input checked="" type="radio"/> Require	<input type="radio"/> Enable	<input type="radio"/> Disable

* OFDM Rates

Q. Is it true that if I only allow IEEE 802.11g clients on a wireless network, they cannot interfere with a parallel IEEE 802.11b network because they use different modulation schemes?

A. No, this is not true. These 802.11g clients can interfere if they use the same frequency. Make sure to use different channels. The three nonoverlapping channels are 1, 6, and 11.

Q. What is the speed of the AP Ethernet port?

A. The AP Ethernet port supports either 10 Mbps or 100 Mbps over an RJ-45 connector, in either half or full duplex. Hard set the speed and duplex to the same settings as your switch or hub.

Q. Is there a mechanism for failover or redundancy for my AP?

A. Yes, you can configure hot standby in order to provide redundancy in the event that the primary AP fails. Refer to the Release Notes for Cisco Aironet Access Points for more information.

Q. What is a WEP key?

A. WEP stands for Wired Equivalent Privacy. You can use WEP to encrypt and decrypt data signals that transmit between wireless LAN (WLAN) devices. WEP is an optional IEEE 802.11 feature that prevents disclosure and modification of packets in transit and also provides access control for the use of the network. WEP makes a WLAN link as secure as a wired link. As the standard specifies, WEP uses the RC4 algorithm with a 40-bit or 10-bit key. RC4 is a symmetric algorithm because RC4 uses the same key for the encryption and the decryption of data. When WEP is enabled, each radio station has a key. The key is used to scramble the data before transmission of the data through the airwaves. If a station receives a packet that is not scrambled with the appropriate key, the station discards the packet and

never delivers such a packet to the host. Refer to Wired Equivalent Privacy (WEP) on Aironet Access Points and Bridges Configuration Example for information on how to configure WEP.

Q. When you use Light Extensible Authentication Protocol (LEAP), what port number do you specify in order to communicate with your Cisco Secure Access Control Server (ACS)?

A. By default, the ACS listens to an authentication request on port 1645 and accounting on port 1646, but you can configure port 1812 for authentication and 1813 for accounting. Confirm that these ports are correctly set on the Authentication Server Setup page on the AP.

Q. In Cisco IOS Software–based APs, can you run static Wired Equivalent Privacy (WEP) keys and Extensible Authentication Protocol (EAP) together on the same AP for authentication? This has worked with VxWorks–based APs.

A. No, you cannot run static WEP keys for encryption and EAP for authentication in the same service set identifier (SSID). VxWorks has allowed this configuration because of software vulnerability, but this ability is not a feature. What you can do is create two SSIDs and two VLANs (one per SSID). Then, configure open authentication with WEP for one SSID and EAP authentication for the other SSID.

Q. Do you really need to have a site survey done?

A. Yes. Because of the sensitive nature of radio frequency (RF) transmissions, you must know the other types of RF traffic that can be in your environment, even without your knowledge of the traffic presence. A site survey enables a better understanding of this invisible threat to the good performance of your wireless devices. The site survey also helps your professional installer ensure the desired RF coverage. Refer to the Wireless Site Survey FAQ.

Q. If you attempt to modify the AP and you are prompted for a username and password, what do you enter?

A. A prompt for username and password indicates that the User Manager has been enabled. Refer to your AP administrator in order to find out the username and password to use. If you are the AP administrator and do not know what these user accounts are, you need to perform a password recovery. Refer to Password Recovery Procedure for the Cisco Aironet Equipment.

Q. Can you use two external antennas in order to cover two radio cells (for example, antenna 1 for cell 1 and antenna 2 for cell 2)?

A. You cannot use two antennas on an AP in order to cover two radio cells. Attempts to use the antennas to cover two radio cells can result in connectivity problems. The purpose of the two antennas is to enhance the coverage of a cell in an effort to overcome issues that arise with multipath distortion and signal nulls. Refer to Multipath and Diversity for more information on diversity and multipath distortions.

Q. What is the use of the `mobility network-id` command on an AP?

A. You use the `mobility network-id` command in order to configure Layer 3 mobility in a wireless network. You use the `mobility network-id ssid` command in order to associate a service set identifier (SSID) to a Layer 3 mobility network ID. With Layer 3 mobility, clients can roam to different APs that reside in different subnets. The roaming clients stay connected to your network and do not change IP addresses.

You must use a wireless LAN (WLAN) services module (WLSM) as your wireless domain services (WDS) device in order to properly configure Layer 3 mobility. Layer 3 mobility is not supported when you use an AP as your WDS device. For more information on Layer 3 mobility, refer to the *Understanding Layer 3 Mobility* section of Configuring WDS, Fast Secure Roaming, and Radio Management.

The command is meant to be used when the AP participates in a WDS infrastructure with a WLSM module (that acts as the WDS device) where there is Layer 3 mobility. If you use this command incorrectly, connectivity problems in the WLAN network result, such as these:

- ◆ Clients do not get IP addresses from the DHCP.
- ◆ In some cases, the clients cannot associate with the AP.
- ◆ Wireless clients cannot associate with the AP.
- ◆ Extensible Authentication Protocol (EAP) authentication does not happen. With the `mobility network-id` command configured, the AP tries to build a generic routing encapsulation (GRE) tunnel for the forwarding of the EAP packets. If no tunnel is established, the packets cannot go anywhere.
- ◆ The AP that is configured as a WDS device does not function as expected, and the WDS configuration does not work.

Q. How many service set identifiers (SSIDs) can you have per VLAN?

A. You can have only one SSID per VLAN. The use of multiple SSIDs over a single VLAN is not supported with Aironet APs.

Q. What is the BSSID value when multiple ESSIDs are assigned to APs?

A. If the AP is running in lightweight mode, then each ESSID on an AP will be handled via a different BSSID (where each BSSID is based upon the radio base MAC, and differs only in the low-order nibble.)

If the AP is running an IOS, then all ESSIDs on the AP will be handled via the same BSSID (unless MBSSID is configured, in which case they will be handled via different BSSIDs).

Q. Is it possible to set up my A radio for bridge and the G radio for AP functionality? If yes, how can I do this?

A. Yes, it is possible to set up each radio in your AP for different functionality. In your scenario, this can be done if you set up different service set identifiers (SSIDs) for the G and A radio. Then, set up the role in a radio network parameter for the G radio to AP and for the A radio to root bridge.

Q. When two clients associate to two different APs that are connected on the same subnet, does the communication happen through the wired network or happen wirelessly?

A. For this scenario, if the two APs are set to root mode, the communication between the two APs is through the wired network. If one of the APs is set to repeater mode and the other AP is set to root mode, the communication between the APs happens wirelessly.

Q. Can you enable routing or Network Address Translation (NAT) on Cisco APs?

A. No, routing and NAT features are not supported on APs.

Q. Is there a way to schedule a time when the Cisco IOS Software-based AP is available? I want to provide time-based access to clients that connect to the AP.

A. You can configure time-based access control lists (ACLs) with use of time ranges. Time-based ACLs help you to make sure that users are able to access the wireless network within a particular time period, for example, 9:00 a.m. to 5:00 p.m. (0900 to 1700). The use of time-based ACLs does not shut down the AP or radio. Time-based ACLs stop the passing of traffic on the AP so that users cannot access the network. For information on how to configure this feature, refer to the *Time-Based ACLs Using Time Ranges* section of Configuring IP Access Lists.

Q. Can APs have multiple DHCP pools across different subnets?

A. When you configure the AP as a DHCP server, IP addresses are assigned to devices that are on the same subnet as the DHCP server. The devices communicate with other devices on the subnet, but do not communicate beyond the subnet. If you need to pass data beyond the subnet, you must assign a default router. The IP address of the default router should be on the same subnet as the AP that you configured as the DHCP server.

Q. What is the dBm measurement? How do I determine the equivalent dBm values for the signal strength (in mW) listed on my Aironet access point (AP)?

A. The unit dB measures the power of a signal as a function of its ratio to another standardized value. This abbreviation dB is often combined with other abbreviations in order to represent the values that are compared. Hence, dBm is the value which results from comparing dB with a standardized reference value of 1 mW.

The formula to calculate this dBm value from the given signal strength in mW is:

$$\text{Power (in dB)} = 10 * \log_{10} (\text{Signal/Reference})$$

This list defines the terms in the formula. log₁₀ is logarithm base 10.

- ◆ Signal is the power of the signal (for example, 50 mW).
- ◆ Reference is the reference power (for example, 1 mW).

Example:

If you want to calculate the power in dB of 50 mW signal strength, apply this formula:

$$\text{Power (in dB)} = 10 * \log_{10} (50/1) = 10 * \log_{10} (50) = 10 * 1.7 = 17 \text{ dBm}$$

This formula results in a common rule that says:

- ◆ For every increase of 3 dB (dBm here), it leads to a double increase in the current transmit power (mW). For every decrease of 3 dB, this reduces the transmit power to half its current value.
- ◆ For every increase of 10 dB (dBm), it leads to a ten times increase in the current transmit power (mW). For every decrease of 10 dB, this reduces the transmit power to ten times its current value.
- ◆ For every increase of 30 dB (dBm), it leads to a 1000 times increase in the current transmit power. For every decrease of 30 dB, this reduces the transmit power to 1000 times its current value.

This table provides approximate dBm to mW values:

dBm	mW
0	1
1	1.25
2	1.56
3	2
4	2.5
5	3.12
6	4
7	5
8	6.25
9	8
10	10
11	12.5
12	16
13	20
14	25
15	32
16	40
17	50
18	64
19	80
20	100
21	128
22	160
23	200
24	256
25	320
26	400
27	512
28	640
29	800
30	1000 or 1 W

Refer to RF Power Values for more information.

Q. How do I change the date and time settings on the Cisco 1231 AP?

A. Go to the web interface (GUI), choose **Services > SNTP**, select **Time Settings** and then change the time.

Q. If CCKM is NOT configured on the client, but is configured on APs, will the client be able to associate with the AP? Can the clients do normal roaming?

A. The behavior depends on the configuration of the AP. If CCKM is NOT configured/supported on the client, the client does not associate with an AP that is set to CCKM "mandatory." If the infrastructure (AP) is set to CCKM "optional," the client does associate and does its non-CCKM handshake.

Dependent upon the clients deployed, it is typically recommended to set CCKM to "optional" on infrastructure that permits the association of all devices but supports fast roaming ONLY for capable/CCKM-associated devices.

Q. What is the difference in memory capacity between AP 1240 and 1230?

A. These are the memory capacities of the AP 1240 and 1230:

- ◆ AP 1240 is a 32-MB platform AP.
- ◆ AP 1230 is a 16-MB platform AP.

Q. I have two AP 1240s that support link role flexibility. I would like to bridge between them with 802.11a, with clients joined on the 802.11b/g bands. Are there any restrictions to do this?

A. Access point link role flexibility provides bridge mode functionality support for access points that have dual-band capability (1200, 1230, and 1240AG Series). In the target configuration, the 802.11a radio runs in bridge mode, while the 802.11g radio is in the access point mode.

The requirement is that when you configure an AP with link role flexibility, one of the radios of the AP must be configured as a root AP, and the second AP that bridges back must be in repeater or WGB mode to the root AP.

Q. How many wireless IP telephony handsets are recommended per AP?

A. IP telephony network sizing is essential to ensure that adequate bandwidth and resources are available to carry mission-critical voice traffic. In addition to the usual IP telephony design guidelines for sizing components, such as PSTN gateway ports, transcoders, WAN bandwidth, and so forth, also consider these 802.11b issues when sizing your wireless IP telephony network:

- ◆ Number of 802.11b devices per AP: Cisco recommends that you have no more than 15 to 25.
- ◆ Number of 802.11b phones per AP

Before any discussion about network plans can take place, it helps to understand the basics of

the overall network capacity. These network capacity guidelines apply to sizing the Wireless IP Telephony network:

- ◆ No more than seven concurrent G.711 calls per AP
- ◆ No more than eight concurrent G.729 calls per AP

Note: These design recommendations assume that Voice Activity Detection (VAD) has been disabled on the Cisco 7920 Wireless IP Phones.

Use of VAD on the Cisco 7920 phones can conserve bandwidth, but Cisco recommends that you disable VAD on all Cisco CallManager servers to provide better overall voice quality. In addition to the determination of how much bandwidth is needed for an 802.11b VoIP call, you must also consider overall radio contention for a particular RF channel. The general rule is that you should not deploy any more than 20 to 25 802.11b endpoints per AP. The more endpoints you add to an AP, the more you reduce the amount of overall bandwidth and potentially increase transmission delays. The maximum number of phones per AP depends on the calling patterns of individual users (based on Erlang ratios). Cisco recommends that no more than seven concurrent calls use G.711 or eight concurrent calls use G.729. Beyond that number of calls, when excessive background data is present, the voice quality of all calls becomes unacceptable. Packetization rates for these recommendations are based on 20–ms sample rates with VAD disabled. This rate generates 50 packets per second (pps) in each direction. A larger sample size (such as 40 ms) can result in a larger number of simultaneous calls, but it also increases the end–to–end delay of the VoIP calls.

The number of 802.11b phones you can deploy per Layer–2 subnet or VLAN depends on these factors:

- ◆ Use no more than seven G.711 or eight G.729 active calls per AP.
- ◆ The calling ratio is used to determine the number of active and non–active calls. This ratio is often determined with Erlang calculators. Based on these factors and normal business–class Erlang ratios (between 3:1 and 5:1), Cisco recommends that you deploy no more than 450 to 600 Cisco 7920 phones per Layer–2 subnet or VLAN.

Refer to the *Network Sizing* section of *Wireless Network Infrastructure*, as well as *Is Your WLAN Ready for Voice?* for more detailed information.

Q. How can I stop an AP 1200 from processing authentication requests after a set number of tries?

A. You can use the maximum retries option on the AAA server to limit the number of times the clients can try to access a network. The value of the maximum retries can be configured manually on the AAA server, or you can use the default number of retries, which depends upon the AAA server that is used.

Q. Where can I find information on the differences in the various platforms of APs and LAPs?

A. Refer to the Cisco Wireless Hardware Frequently Asked Questions. This document contains useful information that compares the different AP and LAP models.

Q. Is Point–to–Point–Protocol over Ethernet (PPPoE) supported in Cisco Aironet Access Points?

A. No, PPPoE is not supported in Cisco Aironet Access Points.

Q. Is VLAN Trunking Protocol (VTP) supported in Cisco Aironet Access Points?

A. No, VTP is not supported in Cisco Aironet Access Points.

Q. Does the Cisco Aironet AP support 802.11f standard Inter-Access Point Protocol (IAPP)?

A. No, the Cisco Aironet AP does not support 802.11f based IAPP. The Cisco Access Points offer their own robust, feature-rich, and proven inter-Access Point protocol.

Q. What is the use of the `bridge-group 1 block-unknown-source` and `bridge-group 1 source-learning` commands in an AP?

A. Use the `bridge-group block-unknown-source` configuration interface command to block traffic from unknown MAC addresses on a specific interface. Use the `no` form of the command to disable unknown source blocking on a specific interface.

In order for STP to function properly, `block-unknown-source` must be disabled for interfaces that participate in STP.

```
bridge-group group block-unknown-source
```

When you enable STP on an interface, `block-unknown-source` is disabled by default.

The `bridge-group 1 source-learning` command makes the AP learn the source address of the client. Use the `no` form of the command to disable AP from learning the source address of the client.

Q. Is there a way to prioritize the traffic that flows through the AP so that traffic from a particular SSID configured on the AP utilizes a higher bandwidth than the other SSIDs on the same AP?

A. This can be achieved with Quality of Service (QoS) implementation on APs.

- ◆ Create QoS policies and apply the policies to the VLANs configured on your access point. These documents explain QoS and how to configure QoS policies on AP.
 - ◇ Wireless Quality-of-Service
 - ◇ Configuring QoS on Aironet Access Points
- ◆ Then, map the SSIDs configured on the AP to individual VLANs mentioned. In this way, if you prioritize the traffic based on VLAN, you can, in turn, prioritize traffic based on SSID.

Q. Is there a way to limit the maximum number of client devices that can connect to a single Autonomous Access point?

A. The default behavior of a Cisco client device is that it connects to the AP that has best signal strength available. But you can limit the clients that can connect to any particular AP through MAC authentication. You need to provide the MAC address of the client to the AP so that the AP can allow only those clients and restrict all the other clients that are not part of the

allowed MAC address list from connecting to that particular AP.

Q. From where can you download the latest software?

A. Cisco Aironet equipment operates best when you load all the components with the most current version of software. Refer to the Cisco Wireless Software Center (registered customers only) in order to download the latest software and drivers.

Q. Is it necessary to shut off all laptops and other wireless devices during an AP upgrade?

A. No, there is no need to shut off the devices. An AP upgrade is a safe process, and everything can remain on. Make sure that you are connected to a TFTP server.

Q. Where can I find instructions on how to upgrade Cisco IOS® on Cisco Aironet APs?

A. Refer to Working with Software images for instructions on how to upgrade the Cisco IOS on the AP.

Note: Use the **force-reload** option with the **archive download-sw** command.

Note: When you upgrade the AP or bridge system software by entering the **archive download-sw** command on the CLI, you must use the **force-reload** option. If the AP or bridge does not reload the flash memory after the upgrade, the pages in the web-browser interface might not reflect the upgrade. This example shows how to upgrade system software by using the **archive download-sw** command:

```
AP#archive download-sw /force-reload /  
overwrite tftp://10.0.0.1/image-name
```

Q. I have an 1100 AP. I want to upgrade the AP radio from IEEE 802.11b to IEEE 802.11g. If I upgrade the radio in the AP, can I use the existing PC cards? Or do I need to upgrade the PC cards as well? The cards are currently 802.11b cards.

A. An upgrade of the 802.11b radio to 802.11g does not result in any performance enhancement if you only use 802.11b clients. An advantage of a radio upgrade to 802.11g is that you can connect 802.11b and 802.11g clients with the AP. With the upgrade, the 802.11b clients connect at 11 Mbps and 802.11g clients connect at 54 Mbps.

Q. How do you set the AP back to its factory default settings?

A. Refer to Password Recovery Procedure for the Cisco Aironet Equipment.

Troubleshoot FAQ

Q. I have made some configuration changes to the AP. When I try to save the changes, I get this message on the AP: "Error writing new config file "flash:/config.txt.new" nv_done: unable to

open "flash:/config.txt.new" nv_done: unable to open "flash:/private-multiple-fs.new" [OK]". What does the message mean?

A. This error message indicates that there is no space in the Flash to store the new configuration. Try to delete any old crash files that exist. Or, if there is more than one Cisco IOS Software version, delete the one that you do not use. This can free some space on the Flash. Issue the **dir flash** command in order to determine if there are any old exception crashinfo files that you can delete or old images that are not in use. Issue the **write memory** command in order to free up space so that you can write the configuration into memory.

Q. I use Aironet Client Utility (ACU) 6.3 and Cisco 1200 Access Points (APs) that run Cisco IOS Software Release 12.3(8)JA. When the wireless client is associated to the AP, the AP name is not displayed on the ACU. Why?

A. AP Name is the hostname for the AP. If Aironet extensions are enabled on the AP, then the AP name is displayed on the ACU.

If you do not wish to see the AP name, you can disable Cisco Aironet extensions to the IEEE 802.11b standard (**no dot11 extensions aironet** under the radio interface). Cisco Aironet extensions are enabled by default in the AP.

If previously disabled, you can enable Cisco Aironet extensions with this command:

```
AP(config-if)#dot11 extension aironet
```

In a beacon, the AP includes an information element that is Cisco–proprietary that contains the AP name. If you turn off Aironet extensions on the AP, the AP does not beacon its name. Refer to Disabling and Enabling Aironet Extensions for more information on Aironet extensions.

Q. My access point (AP) accepts and connects to only one client at a time. What could be the reason?

A. One possible reason could be that the **max–associations** parameter is set to **1** under the service–set identifier (SSID) configuration. Use the **max–associations** SSID configuration mode command in order to configure the maximum number of associations supported by the radio interface (for the specified SSID). Use the **no** form of the command in order to reset the parameter to the default value. This default maximum is 255.

Q. How can you recover forgotten passwords?

A. Refer to Password Recovery Procedure for the Cisco Aironet Equipment.

Q. Serial numbers do not show up on any of the BR350 or AP350s we have by commands. These are VxWorks and have not been converted to IOS. How do I retrieve this information from the devices?

A. The 350 Series APs and Bridges that run VxWorks do not display the serial number in software. The only way to identify the serial number on these units is to physically inspect the

label on the hardware itself.

Q. What are possible sources of interference for the radio frequency (RF) link of the AP?

A. Interference can come from a number of sources, such as:

- ◆ 2.4 GHz cordless phones
- ◆ Improperly shielded microwave ovens
- ◆ Wireless equipment that other companies manufacture

Electrical motors and the moving metal parts of machinery can also cause interference. Refer to these documents for more information:

- ◆ Troubleshooting Problems Affecting Radio Frequency Communication
- ◆ Intermittent Connectivity Issues in Wireless Bridges

Q. I see the error message : %C4K_EBM-4-HOSTFLAPPING:Host [mac-addr] in vlan [num] is flapping between port [num] and port [num] connected to the Access Points. How do we resolve this?

A. This error message occurs when switch learns the same MAC address through multiple ports. This can be due to one of these reasons

1. When a client roams from one AP to another AP, the new AP informs the client of the MAC address to the switch. If both the APs are connected to the same switch, the MAC address of the client is associated to both the switch ports connected to the APs. This creates a duplicate entry for the client and generates this error message until the time that the switch synchronizes its CAM table. This error message is quite normal in a wireless environment, but, if too much roaming occurs, this can overload the CPU of the switch. Check the client driver and firmware. In addition, ensure that coverage is good so that the client does not roam often.
2. When there is a loop, the switch can learn the same MAC address through multiple ports connected to other switches. Ensure that the TP is enabled on the switch.

Q. Why is it that the client card does not associate to the closest AP?

A. If there are multiple APs in your wireless topology, your client maintains an association with the AP with which the client originally associated, until the client loses keepalive beacons from that AP. If contact is lost and if attempts to regain contact with the original AP continue to fail, the client then seeks out another AP. The client attempts to associate to this new AP if the client has sufficient rights and authorization on the new AP.

Q. I have a Cisco AP and Cisco Secure Access Control Server (ACS) 3.2. I have Extensible Authentication Protocol (EAP) implemented in the network. Users are not authenticated by the RADIUS server. When I issue debug commands on the AP, I get this output: "Jun 2

```
15:58:13.553: %RADIUS-4-RADIUS_DEAD: RADIUS server  
10.10.1.172:1645,1646 is not responding. Jun 2  
15:58:13.553: %RADIUS-4-RADIUS_ALIVE: RADIUS server  
10.10.1.172:1645,1646 has returned. Jun 2 15:58:23.664:
```

%DOT11-7-AUTH_FAILED: Station 0040.96a0.3758

Authentication failed." Why do I see these error messages on the AP?

A. One of the reasons why these error messages appear is that the shared secret is not the same in the AP and the ACS. This mistake is common when you configure EAP. If there is a shared-secret mismatch between the AP and the ACS 3.2, EAP does not work. The RADIUS server does not accept packets that the AP forwards. Ensure that the shared secret on the AP matches with that configured on the ACS server. For information on how to debug, refer to Debug Authentications.

Q. When I viewed the logs on the AP, I found this error: "Mar 9 11:05:26.225 Information Group rad_acct: Radius server 10.10.1.172:1645,1646 is responding again (previously dead). Mar 9 11:03:09.361 Error Group rad_acct: No active radius servers found." What is the cause of this error and how can I resolve the problem?

A. It is normal to see this log when the setting **radius-server deadtime** is configured on the AP. It is an information log and not a major problem. Use the **radius-server deadtime** command in order to set an interval during which the AP does not attempt to use servers that do not respond, thus avoiding the wait for a request to time out before trying the next configured server. A server marked as dead is skipped by additional requests for the duration of minutes that you specify, up to 1440 (24 hours).

Q. I have an AP 1230 with Cisco IOS Software Release 12.3(4)JA. When I update the access control list (ACL), I receive this message: "% Warning: Saving this config to nvram may corrupt any network management or security files stored at the end of nvram. Continue? [no]:"

A. This is a warning message and not an error. If you select [no] then it does not save on the access points (APs). The configurations are not saved on the non-volatile RAM (NVRAM), they are saved on the Flash.

Even though it is a warning, you do have a memory issue on this AP. You have numerous .rcore files that take up a lot of space on your memory. This output shows an example:

```
3 -rwx 262144 Mar 3 2002 22:40:04 +00:00 r13_5705_9760_1EA7A81E.rcore
4 -rwx 262144 Mar 1 2002 17:21:44 +00:00 r13_5705_9760_709D16F4.rcore
5 -rwx 262144 Mar 7 2002 20:19:12 +00:00 r13_5705_9760_9D2DE9CD.rcore
6 -rwx 262144 Mar 26 2002 23:42:22 +00:00 r13_5705_9760_AAE78172.rcore
151-rwx 262144 Mar 1 2002 17:22:00 +00:00 r13_5705_9760_7187935C.rcore
```

In order to clean the memory, erase all of the .rcore files from Flash.

This is an example of the command you need to enter in enable mode:

```
ap#delete flash:r13_5705_9760_1EA7A81E.rcore
```

Note: Issue this **delete flash:** command for every .rcore file on your Flash.

Q. I have a Wireless LAN Services Module (WLSM) with Cisco IOS Software Release 12.4(4)T1 installed. Connections to clients are dropping. After I look up logs, I see a number of messages such as "Previous authentication no longer valid" and "Disassociated because sending station is leaving (or has left) BSS". What is the issue?

A. Both of these messages point towards an RF issue. Assign different channels on the AP in order to fix this issue.

Q. The Cisco Aironet APs in my WLAN network do not broadcast the service set identifiers (SSIDs). What could be the reason? Do I need to enable a particular feature on the AP?

A. As long as you do not enable Guest mode under the SSID Manager, the AP does not broadcast the SSID in its beacons. You can verify with a client and scan for SSIDs in order to make sure it is not listed.

In order to enable guest mode on an SSID, type this command on the AP in global configuration mode:

```
Ap<config>#dot11 ssid ssid-string  
Ap<config-ssid>#guest-mode
```

Q. I have my AIR-AP1231G-A-K9 AP. Why do I not see an option to turn on the A radio on this AP and am only able to see the option for G radios? Am I not able to associate 802.11b clients with it?

A. The AIR-AP1231G-A-K9 AP has a G radio. The part number AP1231G implies it has only G radio with it. G radios are backwards compatible with B radios because they work on the same frequency. There is no A radio on this unit and that is why you cannot turn it on. You might need to add the A radio module. The A radio works on a different frequency (at 5 GHZ) than radios G and B (at 2.4 GHZ).

Q. I have a Cisco Wireless IP Phone 7920 that is connected to a Cisco AP. I see that the 7920 is associated with the AP, but no IP address is assigned. I use Extensible Authentication Protocol (EAP). I see the message "Info Station [SEP001121ceb9a4]001121ceb9a4 Authenticated", which is followed by "Info Station [SEP001121ceb9a4]001121ceb9a4 Reassociated" and "Warning EAP retry limit reached for Station [SEP001121ceb9a4]001121ceb9a4". Then I see "Info Deauthenticating [SEP001121ceb9a4]001121ceb9a4, reason 'Previous Authentication No Longer Valid' ". What is the problem?

A. The reason that you get these messages is that the shared secret in the AP is different than the shared secret from the RADIUS server. Make sure that the shared-secret keys for EAP are identical on both. You must retype the shared-secret key in both the AP and the RADIUS server.

Q. I have a problem with my AP. It continues to send too many RTS messages in bursts which cause the unexpected disassociation of associated clients. These clients were associated with this AP at a signal level between -91 and -95 dBm. What is the reason for this unexpected disassociation? Is this an expected behavior of the AP?

A. Yes, this is an expected behavior. Your client is at the very edge of the 1 Mbps cell. Since you see it at -91 to -95 dBm, the erratic behavior is expected.

Install more APs in order to address this issue. Or, if your desired coverage is in a focused area rather than omni-directional, use directional antennas.

RTS is caused by the retry mechanisms kicking in. The client should respond to an RTS with a CTS, but if the client sees them in a sniffer as a group of around eight RTS frames with no corresponding CTS, then the client does not hear the AP, or the client is so far away that the AP cannot hear it. Both devices have to hear each other, not just your AP hearing the client. So, if the antenna on the client is not of great design (probable), or their transmitter does not transmit at 100 mW (very probable), or their receiver is nowhere near -90 to -95 dBm sensitivity (almost guaranteed if it is not a Cisco client), then you get the operation that you describe.

Q. We use Cisco LWAPP Wireless APs. Although I have seen many TCP retransmissions and duplicate ACKs at clients, I do not see those in our wired environment. Is that normal for wireless?

A. Corrupted packets and retransmitted packets are two of the fundamental metrics of an 802.11 WLAN. Analysis of corrupted and retransmitted packets in 802.11 differs from analysis in a wired LAN for three reasons:

- ◆ First, 802.11 WLANs typically have many more corrupted packets than do wired LANs, so the importance of corrupted frames in an 802.11 WLAN is enhanced.
- ◆ Second, 802.11 defines a reliable data-link layer, which means that every corrupted packet must result in a retransmission. Wired LANs typically do not define a reliable data-link layer, so a retransmission only occurs if a reliable upper-layer protocol is in use.
- ◆ Finally, upper-layer reliability is typically end-to-end, which means that a corrupted packet anywhere between the source and destination causes a retransmission. An 802.11 retransmission, since it occurs at layer 2, is implemented between wireless interfaces, so an 802.11 retransmission can only be caused by corruption on the local "segment." This makes it much easier to identify the location of corruption in an 802.11 WLAN than in a traditional wired LAN. Let us explore the implications of these differences.

One of the challenges of a wireless environment is that it is difficult to determine whether the analyzer sees the same things as do the clients. Differences between the analyzer and the client different radios, antennae, or physical locations can cause the analyzer to see different things than does the client. For example, if the analyzer is far from the AP, but the wireless client is close to the AP, the analyzer can see a corrupted frame, while the station sees an

uncorrupted frame. Since we know that every corrupted frame results in a retransmission, we can use the relative numbers of retransmissions and corrupted frames to evaluate the degree to which the analyzer sees what the station(s) on the network see.

Q. We see this syslog message broadcast on our network. Why does this occur, and how do we stop it?

```
AP:001f.ca26.bfb4: %LWAPP-3-CLIENTERRORLOG: Decode Msg: could not match WLAN <id>
```

A. These messages are warning messages and are seen when WLAN Override is enabled and the particular WLAN ID is not selected or advertised on a slot/radio.

Q. I have problems when I upgrade my AP using the TFTP server. Every time I try to upgrade, it adds a .tar extension to the upgrade image file c1200-k9w7-tar.default, which cause the AP not to recognize the file. I could not find a way to get rid of the additional .tar extension. (I downloaded and tried both solarwind and tftpd32.) What should I do to eliminate this issue?

A. The problem could be that the Operating System is hiding the known file type. Go to **My Computer**. Click **Tools > Folder Options > View**, scroll down until you find the parameter **Hide extensions for known file types**, and uncheck the box. This should eliminate the issue.

Q. My Access Points often encounter a "high CPU utilization" alarm message. In such cases, a hardware reboot gets the Access Point back into working condition. How can I overcome this issue?

A. There are several reasons for Access Points to reach "high CPU utilization."

- ◆ If the Cisco Access Point (AP) is connected to the network through a switch, sometimes "high CPU utilization" is observed on the AP. This is because, by default, all the VLANs are allowed onto the AP from the switch to which the AP is connected. This can create a problem, especially when applied to a huge network. If all the VLANs are allowed onto the AP, it can result in **high CPU utilization**, and the connectivity can be affected. Clients associated to the Access Point face throughput issues, and sometimes high CPU utilization can also bring the Wireless network down.

In order to avoid this problem, prune the VLANs at the switch so that only the VLAN traffic in which the AP is interested is passed through the AP.

- ◆ If the Access Points are configured with loopback interfaces, sometimes "high CPU utilization" is observed on the AP. Although loopback interfaces can be configured on the Cisco AP, they are not supported on the AP, so they must not be configured. It is advised to remove the loopback interfaces if they are configured on the AP.

Note: APs and bridges do not support the interface loopback command.

As a first step in troubleshooting this issue, issue the **show process cpu** command in the AP. This gives you an idea of what processes use the CPU.

Also, if the AP runs a version earlier than 12.3(2)JA2, upgrade it to version 12.3(2)JA2 because there is a known issue in earlier versions where service requests killed the CPU.

Q. The 871W Wi-Fi Router drops wi-fi established sessions so that the user's VPN session needs to be reestablished all the time. What is the reason?

A. There are several possible reasons that can cause this issue. Connect both the antennas to the 871W Router. Change the channel to 1, 6 or 11 and verify which channel receives the best performance. Also, you might have other APs in the neighborhood which can be causing interference. This is just one possible reason.

Related Information

- **Cisco Downloads for Wireless Products (registered customers only)**
 - **Cisco Aironet 1240 AG Series Q&A**
 - **Cisco Aironet 1230 AG Series Q&A**
 - **Cisco Aironet Access Point Software Configuration Guide for VxWorks**
 - **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.2(13)JA**
 - **Cisco Aironet 350 Series Troubleshooting TechNotes**
 - **Wireless Product Support**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2011 – 2012 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2010

Document ID: 8103
