GETTING STARTED GUIDE

Cisco Aironet 701E Access Points

First Published: August, 2014. Available for India only

1 About this Guide

This guide provides instructions on how to install and configure Cisco Aironet 701E Access Points. This guide also provides mounting instructions and limited troubleshooting procedures.

Note Cisco Aironet 701E access points are available only for India.

2 Safety Instructions

Translated versions of the following safety warnings are provided in the translated safety warnings document that is shipped with your access point. The translated warnings are also in the *Translated Safety Warnings for Cisco Aironet Access Points*, which is available on Cisco.com.

Warning **IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

Warning **This product must be connected to an IEC60950 compliant limited power source or an IEEE 802.3af compliant power source:** Statement CS-0404

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20A.** Statement 1005

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.** Statement 332

Caution Do not use plastic wall anchors to mount the access point on a ceiling because they will not support the weight of the access point. The fasteners used must be capable of maintaining a minimum pullout force of 20 lbs (9 kg).

Caution This product and all interconnected equipment must be installed indoors within the same building, including the associated LAN connections as defined by Environment A of the IEEE 802.af Standard.

Note Use only with listed ITE equipment.

Note Cisco Aironet 701E access points are designed for indoor use. If you install the access points in an enclosure, make sure the enclosure is designed to maintain an operating temperature between 32 and 104 degrees F (0 and 40 degrees C) and a humidity range between 10% and 90% (noncondensing). Failure to maintain these temperature and humidity ranges can cause the unit to fail and void your warranty.

3 Unpacking

Follow these steps:

Step 1 Unpack and remove the access point from the shipping box.

Step 2 Return any packing material to the shipping container and save it for future use.

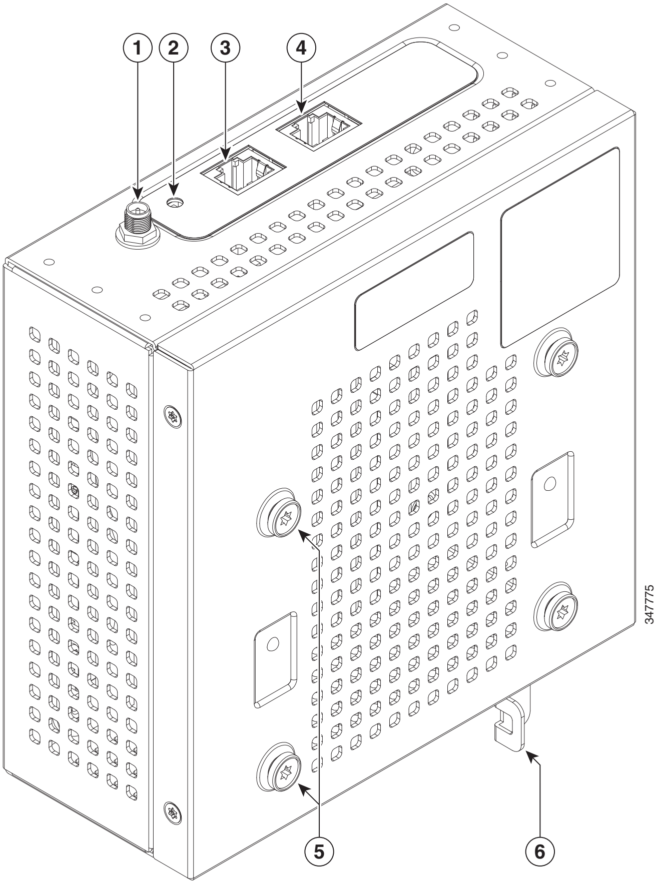
Step 3 Verify that you have received the items listed below. If any item is missing or damaged, contact your Cisco representative or reseller for instructions.

- Access point
- Mounting bracket (optional; might be packaged separately if purchased)
- Adjustable ceiling-rail clip (optional; might be packaged separately if purchased)

4 Overview

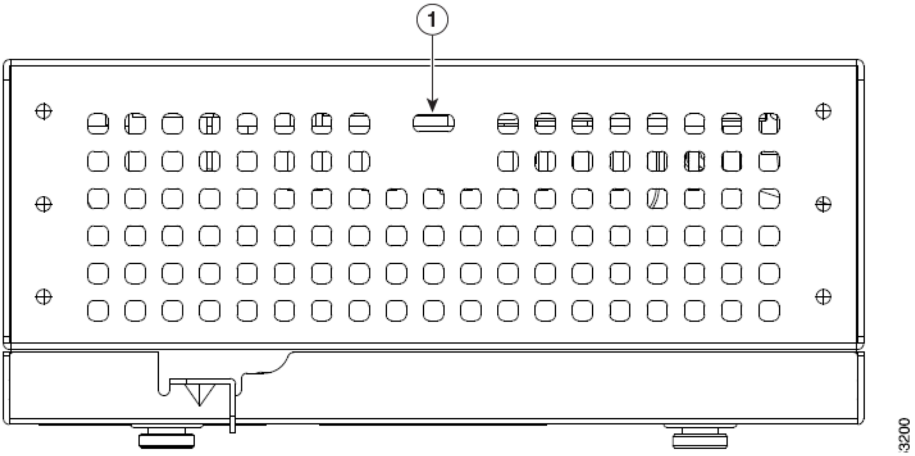
The following illustrations show the access point connections and features. Figure 1 shows the single-radio AIR-701E access point, Figure 2 shows the location of the Kensington lock slot on both models.

Figure 1 AP-701E Access Point Ports and Connections



1	RP-SMA antenna connector	**4**	Ethernet port
2	Mode button	**5**	Mounting bracket pins
3	Console port	**6**	Security hasp

Figure 2 *AP-701E Kensington Lock Slot Location*



1	Kensington Lock Slot		

5 Preparing the Access Point

Before you mount and deploy your access point, we recommend that you perform a site survey (or use the site planning tool) to determine the best location to install your access point.

You should have the following information about your wireless network available:

- Access point locations.
- Access point mounting options: below a suspended ceiling or on a flat horizontal surface.
- Access point power options: power supplied by the recommended external power supply (Cisco AIR-PWRINJ5=), PoE from a network device, or a PoE power injector/hub (usually located in a wiring closet).

Cisco recommends that you make a site map showing access point locations so that you can record the device MAC addresses from each location and return them to the person who is planning or managing your wireless network.

Installing the access point involves these operations:

- Performing a pre-installation configuration (optional)
- Mounting the access point
- Configuring and Deploying the access point on the wireless network

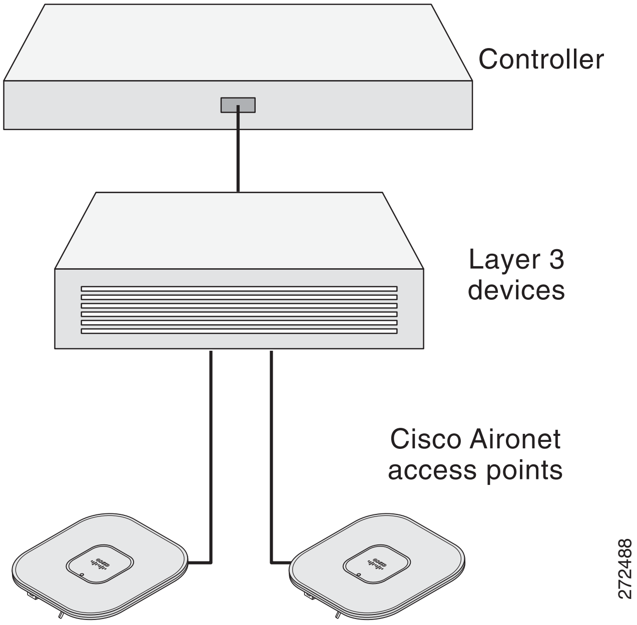
6 Performing a Pre-Installation Configuration

The following procedures ensure that your access point installation and initial operation go as expected. A pre-installation configuration is also known as *priming the access point*. This procedure is optional.

Note Performing a pre-installation configuration is an optional procedure. If your network controller is properly configured, you can install your access point in its final location and connect it to the network from there. See the "Configuring and Deploying the Access Point on the Wireless Network" section on page 10 for details.

Figure 3 shows the pre-installation configuration setup.

Figure 3 Pre-Installation Configuration Setup



Follow these steps to perform the pre-installation configuration.

Step 1 Make sure that the Cisco wireless LAN controller DS port is connected to the network. Use the CLI, web-browser interface, or Cisco Prime Infrastructure procedures as described in the appropriate Cisco wireless LAN controller guide.

a. Make sure that access points have Layer 3 connectivity to the Cisco wireless LAN controller Management and AP-Manager Interface.

b. Configure the switch to which your access point is to attach. See the *Cisco Wireless LAN Controller Configuration Guide* for additional information.

c. Set the Cisco wireless LAN controller as the master so that new access points always join with it.

d. Make sure DHCP is enabled on the network. The access point must receive its IP address through DHCP.

e. CAPWAP UDP ports (UDP 5246/5247) must not be blocked in the network.

f. The access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the "Using DHCP Option 43" section on page 13 for more information.

Step 2 Apply power to the access point:

a. The AP-701E access point is 802.3af (15.4 W) compliant and can be powered by any 802.3af-compliant device. The recommended external power supply for the access point is the Cisco AIR-PWRINJ5= power supply.

Note The access point requires a Fast Ethernet link to prevent the Ethernet port from becoming a bottleneck for traffic because wireless traffic speeds exceed transmit speeds of a 10Mbps Ethernet port.

b. As the access point attempts to connect to the controller, the LEDs cycle through a green, red, and amber sequence, which can take up to 5 minutes.

Note If the access point remains in this mode for more than five minutes, the access point is unable to find the Master Cisco wireless LAN controller. Check the connection between the access point and the Cisco wireless LAN controller and be sure that they are on the same subnet.

c. If the access point shuts down, check the power source.

d. After the access point finds the Cisco wireless LAN controller, it attempts to download the new operating system code if the access point code version differs from the Cisco wireless LAN controller code version. While this is happening, the Status LED blinks dark blue.

e. If the operating system download is successful, the access point reboots.

Step 3 Configure the access point if required. Use the controller CLI, controller GUI, Cisco Prime Infrastructure, Cisco NCS, or Cisco Prime Infrastructure to customize the access-point-specific network settings.

Step 4 If the pre-installation configuration is successful, the Status LED is green indicating normal operation. Disconnect the access point and mount it at the location at which you intend to deploy it on the wireless network.

Step 5 If your access point does not indicate normal operation, turn it off and repeat the pre-installation configuration.

Note When you are installing a Layer 3 access point on a different subnet than the Cisco wireless LAN controller, be sure that a DHCP server is reachable from the subnet on which you will be installing the access point, and that the subnet has a route back to the Cisco wireless LAN controller. Also be sure that the route back to the Cisco wireless LAN controller has destination UDP ports 5246 and 5247 open for CAPWAP communications. Ensure that the route back to the primary, secondary, and tertiary wireless LAN controller allows IP packet fragments. Finally, be sure that if address translation is used, that the access point and the Cisco wireless LAN controller have a static 1-to-1 NAT to an outside address. (Port Address Translation is not supported.)

7 Mounting the Access Point

Cisco Aironet 701E access point can be mounted in several configurations, including on a suspended ceiling, on a hard ceiling or wall, or on an electrical or network box. Mounting equipment is sold separately.

The AP-701E is compatible with the AIR-AP-BRACKET-7=. If this bracket is used then the following can also be used: AIR-AP-T-RAIL-F=, AIR-AP-T-RAIL-R= and AIR-AP-CHNL-ADAPTER=. Mounting accessories are sold separately. For more information on brackets available of use, go to the URL www.cisco.com/go/bracket.

Note Cisco Aironet AP-701E access points are designed for indoor use. If you install the access points in an enclosure, make sure the enclosure is designed to maintain an operating temperature between 32 and 104 degrees F (0 and 40 degrees C) and a humidity range between 10% and 90% (noncondensing). Failure to maintain these temperature and humidity ranges can cause the unit to fail and void your warranty.

8 Configuring and Deploying the Access Point on the Wireless Network

Controller Discovery Process

The configuration process takes place on the Wireless LAN Controller. See the *Cisco Wireless LAN Controller Configuration Guide* for additional information. This guide is available on Cisco.com at the following URL:

http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/configuration-guide/b_cg80.html

The access point uses the IETF standard Control and Provisioning of Wireless Access Points Protocol (CAPWAP) to communicate between the controller and other wireless access points on the network. CAPWAP is a standard, interoperable protocol which enables an access controller to manage a collection of wireless termination points. The discovery process using CAPWAP is identical to the Lightweight Access Point Protocol (LWAPP) used with previous Cisco Aironet access points. LWAPP-enabled access points are compatible with CAPWAP and conversion to a CAPWAP controller is seamless. Deployments can combine CAPWAP and LWAPP software on the controllers.

The functionality provided by the controller does not change except for customers who have Layer 2 deployments, which CAPWAP does not support.

In a CAPWAP environment, a wireless access point discovers a controller by using CAPWAP discovery mechanisms and then sends it a CAPWAP join request. The controller sends the access point a CAPWAP join response allowing the access point to join the controller. When the access point joins the controller, the controller manages its configuration, firmware, control transactions, and data transactions.

Note For additional information about the discovery process and CAPWAP, see the *Cisco Wireless LAN Controller Software Configuration Guide*. This document is available on Cisco.com.

Note You cannot edit or query any access point using the controller CLI if the name of the access point contains a space.

Note Make sure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.

Access points must be discovered by a controller before they can become an active part of the network. The access point supports these controller discovery processes:

- **Layer 3 CAPWAP discovery**—Can occur on different subnets than the access point and uses IP addresses and UDP packets rather than MAC addresses used by Layer 2 discovery.
- **Locally stored controller IP address discovery**—If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's non-volatile memory. This process of storing controller IP addresses on an access point for later deployment is called *priming the access point*. For more information about priming, see the "Performing a Pre-Installation Configuration" section on page 7.
- **DHCP server discovery**—This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the "Configuring DHCP Option 43 and DHCP Option 60" section on page 18.
- **DNS discovery**—The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-LWAPP-CONTROLLER.*localdomain*, where *localdomain* is the access point domain name. Configuring the CISCO-LWAPP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-LWAPP-CONTROLLER.*localdomain*. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

Deploying the Access Point

After you have mounted the access point, follow these steps to deploy it on the wireless network.

Step 1 Connect and power up the access point.

Step 2 Observe the access point LED.

a. When you power up the access point, it begins a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks sequentially green, red, and off. When the access point has joined a controller, the LED is green if no clients are associated or blue if one or more clients are associated.

b. If the LED is not on, the access point is most likely not receiving power.

c. If the LED blinks sequentially for more than 5 minutes, the access point is unable to find its primary, secondary, and tertiary Cisco wireless LAN controller. Check the connection between the access point and the Cisco wireless LAN controller, and be sure the access point and the Cisco wireless LAN controller are either on the same subnet or that the access point has a route back to its primary, secondary, and tertiary Cisco wireless LAN controller. Also, if the access point is not on the same subnet as the Cisco wireless LAN controller, be sure that there is a properly configured DHCP server on the same subnet as the access point, or that DNS resolution is available. See the "Configuring DHCP Option 43 and DHCP Option 60" section on page 18 for additional information.

Tip Use the **ip helper address** command to forward DHCP requests to a DHCP server on a different subnet. Click this URL for more information on the **ip helper address** command: http://www.cisco.com/en/US/docs/ios/12_3t/ip_addr/command/reference/ip1_i1gt.html

Step 3 Reconfigure the Cisco wireless LAN controller so that it is not the Master.

Note A Master Cisco wireless LAN controller should be used only for configuring access points and not in a working network.

9 Troubleshooting

If you experience difficulty getting your access point installed and running, look for a solution to your problem in this guide or in additional access point documentation. These, and other documents, are available on Cisco.com.

Guidelines for Using Cisco Aironet Lightweight Access Points

Keep these guidelines in mind when you use a 701E access point:

- The access point can only communicate with Cisco wireless LAN controllers.
- The access point does not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point joins it.
- CAPWAP does not support Layer 2. The access point must get an IP address and discover the controller using Layer 3, DHCP, DNS, or IP subnet broadcast.
- The access point console port is enabled for monitoring and debug purposes. All configuration commands are disabled when the access point is connected to a controller.

Using DHCP Option 43

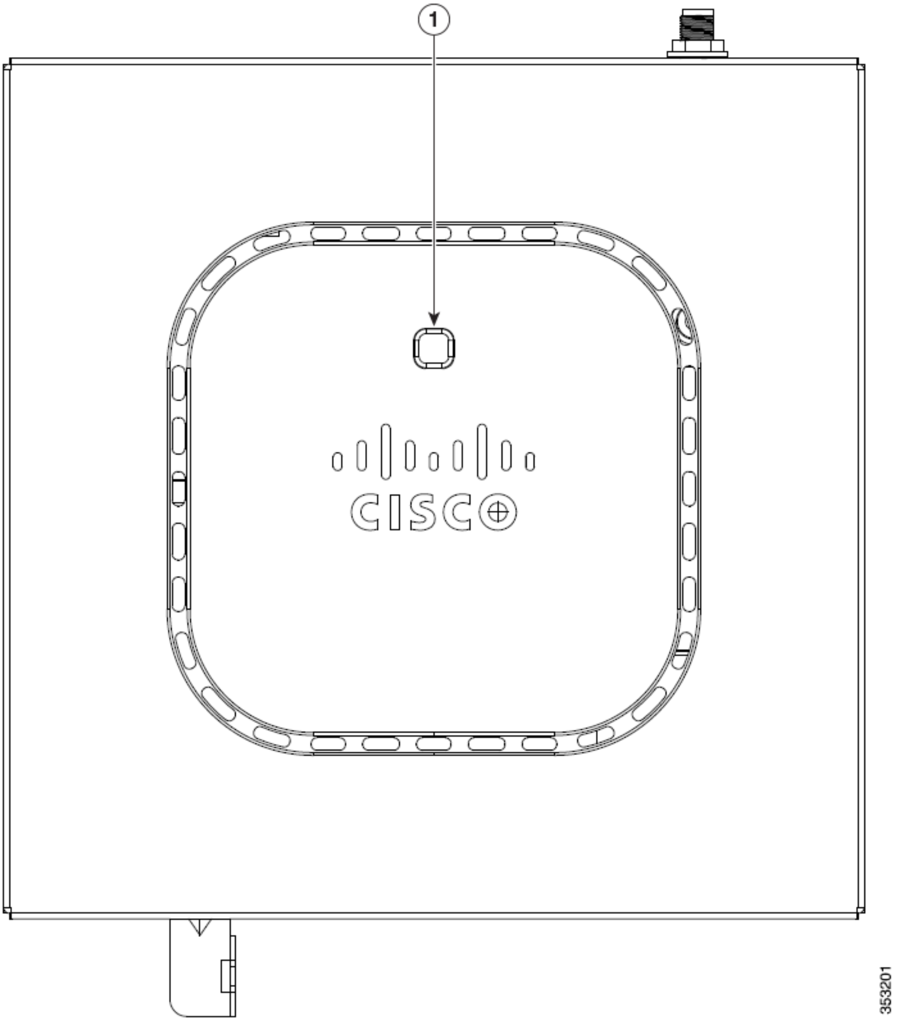
You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling them to find and join a controller. For additional information, refer to the "Configuring DHCP Option 43 and DHCP Option 60" section on page 18.

Checking the Access Point LED

Figure 4 shows the location of the access point Status LED.

Note Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect.

Figure 4 Access Point LED Location



1	Status LED	

Table 1 shows the access point Status LED indications for various conditions.

Table 1 LED Status Indications

Message Type	Status LED	Message Meaning
Boot loader status sequence	Blinking green	DRAM memory test in progress
		DRAM memory test OK
		Board initialization in progress
		Initializing FLASH file system
		FLASH memory test OK
		Initializing Ethernet
		Ethernet OK
		Starting Cisco IOS
		Initialization successful
Association status	Chirping Green	Normal operating condition, but no wireless client associated
	Green	Normal operating condition, at least one wireless client association
Operating status	Blinking amber	Software upgrade in progress
	Cycling through green, red, and amber	Discovery/join process in progress
	Rapidly cycling through red, green, and amber	Access point location command invoked
	Blinking red	Ethernet link not operational
Boot loader warnings	Blinking amber	Configuration recovery in progress (MODE button pushed for 2 to 3 seconds)
	Red	Ethernet failure or image recovery (MODE button pushed for 20 to 30 seconds)
	Blinking green	Image recovery in progress (MODE button released)

Table 1 LED Status Indications (continued)

Message Type	Status LED	Message Meaning
Boot loader errors	Red	DRAM memory test failure
	Blinking red and amber	FLASH file system failure
	Blinking red and off	Environment variable failure
		Bad MAC address
		Ethernet failure during image recovery
		Boot environment failure
		No Cisco image file
		Boot failure
Cisco IOS errors	Red	Software failure; try disconnecting and reconnecting unit power
	Cycling through red, green, amber, and off	General warning; insufficient inline power

Troubleshooting the Access Point Join Process

Access points can fail to join a controller for many reasons: a RADIUS authorization is pending; self-signed certificates are not enabled on the controller; the access point's and controller's regulatory domains don't match, and so on.

Controller software enables you to configure the access points to send all CAPWAP-related errors to a syslog server. You do not need to enable any debug commands on the controller because all of the CAPWAP error messages can be viewed from the syslog server itself.

The state of the access point is not maintained on the controller until it receives a CAPWAP join request from the access point. Therefore, it can be difficult to determine why the CAPWAP discovery request from a certain access point was rejected. In order to troubleshoot such joining problems without enabling CAPWAP debug commands on the controller, the controller collects information for all access points that send a discovery message to it and maintains information for any access points that have successfully joined it.

The controller collects all join-related information for each access point that sends a CAPWAP discovery request to the controller. Collection begins with the first discovery message received from the access point and ends with the last configuration payload sent from the controller to the access point.

When the controller is maintaining join-related information for the maximum number of access points, it does not collect information for any more access points.

An access point sends all syslog messages to IP address 255.255.255.255 by default when any of the following conditions are met:

- An access point running software release 8.0 or later has been newly deployed.
- An existing access point running software release 8.0 or later has been reset after clearing the configuration.

If any of these conditions are met and the access point has not yet joined a controller, you can also configure a DHCP server to return a syslog server IP address to the access point using option 7 on the server. The access point then starts sending all syslog messages to this IP address.

When the access point joins a controller for the first time, the controller sends the global syslog server IP address (the default is 255.255.255.255) to the access point. After that, the access point sends all syslog messages to this IP address until it is overridden by one of the following scenarios:

- The access point is still connected to the same controller, and the global syslog server IP address configuration on the controller has been changed using the **config ap syslog host global syslog_server_IP_address** command. In this case, the controller sends the new global syslog server IP address to the access point.
- The access point is still connected to the same controller, and a specific syslog server IP address has been configured for the access point on the controller using the **config ap syslog host specific Cisco_AP syslog_server_IP_address** command. In this case, the controller sends the new specific syslog server IP address to the access point.
- The access point is disconnected from the controller and joins another controller. In this case, the new controller sends its global syslog server IP address to the access point.
- Whenever a new syslog server IP address overrides the existing syslog server IP address, the old address is erased from persistent storage, and the new address is stored in its place. The access point also starts sending all syslog messages to the new IP address provided the access point can reach the syslog server IP address.

You can configure the syslog server for access points and view the access point join information only from the controller CLI.

A detailed explanation of the join process is on Cisco.com at the following URL:

http://www.Cisco.com/en/US/products/ps6366/products_tech_note09186a00808f8599.shtml

10 Declarations of Conformity and Regulatory Information

All the Declaration of Conformity statements related to this product can be found at the following location: http://www.ciscofax.com

11 Configuring DHCP Option 43 and DHCP Option 60

This section contains a DHCP Option 43 configuration example on a Windows 2003 Enterprise DHCP server for use with Cisco Aironet lightweight access points. For other DHCP server implementations, consult product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

The access point uses the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI string for 701E access points is:

Cisco AP c702

Note If your access point was ordered with the Service Provider Option (AIR-OPT60-DHCP) selected in the ordering tool, the VCI string for the access point contains *ServiceProvider*. For example, a 701E with this option will return this VCI string:
Cisco AP c702-ServiceProvider

The format of the TLV block is listed below:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

To configure DHCP Option 43 in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

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

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

Where:
<pool name> is the name of the DHCP pool, such as AP702
<IP Network> is the network IP address where the controller resides, such as
10.0.15.1
<Netmask> is the subnet mask, such as 255.255.255.0
```

```
<Default router> is the IP address of the default router, such as 10.0.0.1
<DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

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

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

```
For the VCI string, "Cisco AP c702". The quotation marks must be included.
```

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

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

The *hex string* is assembled by concatenating the TLV values shown below:

Type + *Length* + *Value*

Type is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is **option 43 hex f1080a7e7e020a7f7f02**.

12 Access Point Specifications

Table 2 lists the technical specifications for 701E access points.

Table 2 Access Point Specifications

Category	Specification
Dimensions (LxWxD)	6 x 6 x 2.5 in. (15 x 15 x 6.4 cm)
Weight	AP-701E: 1.85 lbs (0.84 kg)
Operating temperature	AP-701E: 32 to 104 degrees F (0 to 40 degrees C)
Storage temperature	–22 to 185 degrees F (–30 to 85 degrees C)
Humidity	10% to 90% (noncondensing)
Antenna	External, 1x RP-SMA (antenna not provided)

Table 2 Access Point Specifications (continued)

Category	Specification
Compliance	India — G.S.R 45(E)
Maximum power and channel settings	Maximum power and the channels allowed in your regulatory domain, refer to *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points*. This document is available on Cisco.com.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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