



# Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(8)JA2

---

**June 1, 2006**

These release notes describe features, enhancements, and caveats for Cisco IOS Release 12.3(8)JA2. They also provide important information about Cisco Aironet 350, 1100, 1130AG, 1200, 1230AG, 1240AG Series Access Points, and Cisco Aironet 1300 Series Outdoor Access Point/Bridges.

## Contents

These release notes contain the following sections:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New Features, page 6](#)
- [Important Notes, page 9](#)
- [Caveats, page 16](#)
- [Troubleshooting, page 18](#)
- [Documentation Updates, page 18](#)
- [Related Documentation, page 19](#)
- [Obtaining Documentation, page 19](#)
- [Documentation Feedback, page 20](#)
- [Cisco Product Security Overview, page 21](#)
- [Obtaining Technical Assistance, page 22](#)
- [Obtaining Additional Publications and Information, page 23](#)



---

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

© 2006 Cisco Systems, Inc. All rights reserved.

# Introduction

The Cisco Aironet Access Point is a wireless LAN transceiver that acts as the connection point between wireless and wired networks or as the center point of a standalone wireless network. In large installations, the roaming functionality provided by multiple access points enables wireless users to move freely throughout the facility while maintaining uninterrupted access to the network.

You can configure and monitor 350, 1100, 1130AG, 1200, and 1240AG series access points and the 1300 series outdoor access point/bridge using the command-line interface (CLI), the web-browser interface, or Simple Network Management Protocol (SNMP).

## System Requirements

You can install Cisco IOS Release 12.3(8)JA2 on all 350, 1100, 1130AG, 1200, 230AG, 1240AG series access points, and 1300 series outdoor access point/bridges.

**Note**

Software upgrades fail when you use the web-browser interface to install Cisco IOS Release 12.3(8)JA2 on 1200 series access points. The image size exceeds the access point's 4-MB restriction for software upgrades. Use TFTP to upgrade your access point to this release. For complete instructions on using TFTP to upgrade access point software, see the "Working with Software Images" section in the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*. Click this link to browse to that document:

<http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/acsspts/i1232ja/i1232sc/index.htm>

You can also install this release on 350 and 1200 series access points that have been converted to run Cisco IOS software. You can tell whether an access point runs VxWorks or Cisco IOS software by looking at the GUI: the GUI on an access point running VxWorks has a yellow and red color scheme, and the GUI on an access point running Cisco IOS software has a green, light-green, and black color scheme.

Your 350 series access point must run one of these VxWorks versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 11.23T, or 11.21. Your 1200 series access point must run one of these VxWorks versions before you can convert to IOS software: 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T. If your access point runs version 12.04, you must downgrade to a supported VxWorks version before upgrading to IOS software.

The conversion upgrade image for 350 series access points installs Cisco IOS Release 12.2(13)JA1 on your 350 series access point. The conversion upgrade image for 1200 series access points installs Cisco IOS Release 12.2(13)JA2 on your 1200 series access point.

**Note**

Cisco Aironet 340 Series Access Points do not support IOS software. Do not attempt to load an IOS image on 340 series access points or on 350 and 1200 series access points that have not been converted.

## Finding the IOS Software Version

To find the version of IOS software running on your access point, use a Telnet session to log into the access point and enter the **show version** EXEC command. This example shows command output from an access point running Cisco IOS Release 12.2(15)JA:

```
ap1200>show version
Cisco Internetwork Operating System Software
IOS (tm) C1200 Software (C1200-K9W7-M), Version 12.2(15)JA
Copyright (c) 1986-2006 by Cisco Systems, Inc.
```

On access points running IOS software, you can also find the software version on the System Software Version page in the access point's web-browser interface. If your access point does not run IOS software, the software version appears at the top left of most pages in the web-browser interface.

## Upgrading to a New Software Release

For instructions on installing access point software for your access point:

- 
- Step 1** Follow this link to the Cisco home page:  
<http://www.cisco.com>
  - Step 2** Click **Technical Support and Documentation**. The Technical Support and Documentation page appears.
  - Step 3** Click **Wireless**. The Wireless Support Resources page appears.
  - Step 4** Scroll down to the Wireless LAN Access section.
  - Step 5** Select the access point model for which you need the information. The Introduction page for the model you selected appears.
  - Step 6** Under the Configure section, click **Install and Upgrade Guides**. A list of configuration documents appears.
  - Step 7** Click **Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, 12.3(8)JA**.
  - Step 8** Navigate to the Managing Firmware and Software chapter.
- 

For information on Cisco IOS software, click this link to browse to the Cisco IOS Software Center on Cisco.com:

<http://www.cisco.com/public/sw-center/sw-ios.shtml>

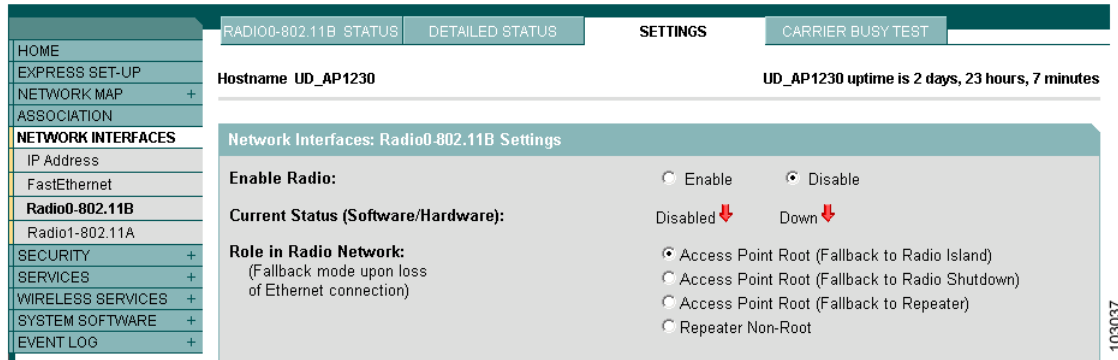
## Disable Radios to Prevent Unexpected Reboot When Upgrading System Software

If your access point runs Cisco IOS Release 12.2(11)JA, 12.2(11)JA1, or 12.2(11)JA2, your access point might unexpectedly reboot after you upgrade to a later Cisco IOS Release. Because of a rare timing condition that affects the radios, the access point sometimes reboots immediately after the upgrade when the radios are enabled. However, after the access point reboots the upgrade is complete and the access point operates normally. To prevent the access point from rebooting unexpectedly, disable the radio interfaces before upgrading software.

Follow these steps to disable the radio interfaces using the web-browser interface:

- Step 1** Browse to the Network Interfaces: Radio Settings page. [Figure 1](#) shows the top portion of the Network Interfaces: Radio Settings page.

**Figure 1** Network Interfaces: Radio Settings Page



- Step 2** Select **Disable** to disable the radio.
- Step 3** Click **Apply** at the bottom of the page.
- Step 4** If your access point has two radios, repeat these steps for the second radio.

Beginning in privileged EXEC mode, follow these steps to disable the access point radios using the CLI:

	Command	Purpose
<b>Step 1</b>	<code>configure terminal</code>	Enter global configuration mode.
<b>Step 2</b>	<code>interface dot11radio {0   1}</code>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
<b>Step 3</b>	<code>shutdown</code>	Disable the radio port.
<b>Step 4</b>	<code>end</code>	Return to privileged EXEC mode.
<b>Step 5</b>	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

If your access point has two radios, repeat these steps for the second radio. Use the **no** form of the **shutdown** command to enable the radio.

## Converting to Cisco IOS Software

If your 350 or 1200 series access point does not run IOS software, you can use the conversion utility or the conversion upgrade image to convert the access point system to IOS software. Use the conversion utility to maintain the current configuration after the conversion, or load the upgrade image to convert to IOS software without saving the current configuration. Your access point must be running one of these VxWorks firmware versions before you can convert to IOS software:

- 350 series access points must be running VxWorks version 12.03T, 12.02T1, 12.01T1, 11.23T, or 11.21

- 1200 series access points must be running VxWorks version 12.03T, 12.02T1, 12.01T1, 12.00T, 11.56, or 11.54T

The conversion upgrade image for 350 series access points installs Cisco IOS Release 12.2(13)JA1 on your 350 series access point. The conversion upgrade image for 1200 series access points installs Cisco IOS Release 12.2(13)JA2 on your 1200 series access point.

**Note**

The upgrade image and the conversion tool do not support VxWorks version 12.04. Access points running version 12.04 must be downgraded to a supported operating system version before you can use the upgrade image or the conversion tool.

**Note**

The upgrade to Cisco IOS software is permanent; you cannot revert to non-IOS software. Product warranties do not cover unintended upgrades.

For complete instructions on using the conversion utility, refer to the *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.0 Administrator Guide for Windows*. Click this link to browse to the Administrator Guide:

[http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_administration\\_guide\\_book09186a008024f246.html](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_administration_guide_book09186a008024f246.html)

To download the conversion utility or the upgrade image, click this link to browse to the Cisco IOS Software Center on Cisco.com:

<http://www.cisco.com/public/sw-center/sw-ios.shtml>

On the Cisco IOS Software Center page, enter your Cisco.com username and password to use the Feature Navigator or the Cisco IOS Upgrade Planner, or click **Wireless Software** to go to the Wireless LAN Software page. Download the conversion utility or the upgrade image for 350 or 1200 series access points. You can also download instructions for using the utility and the image.

## Some Fields Not Updated During Upgrade to IOS Software

When you upgrade an access point to run Cisco IOS software, some fields that are reported in the console messages during the upgrade are blank or are populated with zeros. However, blank or zero fields are normal after a successful upgrade, because 350 and 1200 series access points do not support that information. This example shows fields that might appear blank or populated with zeros:

```
32K bytes of flash-simulated non-volatile configuration memory.
Base Ethernet MAC Address: 00:05:9A:38:42:91
Part Number: 0-0000-00
PCA Assembly Number: 000-00000-00
PCA Revision Number:
PCB Serial Number:
Top Assembly Part Number: 000-00000-00
Top Assembly Serial Number:
Top Revision Number:
Product/Model Number: AIR-AP352-IOS-UPGRD
```

# New Features

Cisco IOS Release 12.3(8)JA2 does not contain new features.

## Installation Notes

This section contains information you should keep in mind when installing 350, 1100, 1130AG, 1200, 1230AG, 1240AG series access points, and 1300 series outdoor access point/bridges.

### Installation in Environmental Air Space

This section provides information on installing 1100 and 1200 series access points in environmental air space, such as above suspended ceilings.

Cisco Aironet 1100, 1130AG, 1200, and 1240AG Series Access Points provide adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the *National Electrical Code* (NEC) and Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.



#### Caution

The power injector does not provide fire resistance and low smoke-producing characteristics and is not intended for use in extremely high or low temperatures or in environmental air spaces such as above suspended ceilings.



#### Note

If you plan to mount a 1200 series access point with a 5-GHz radio in an area subject to environmental air space, Cisco recommends that you mount the access point horizontally so that its antennas point down. Doing so ensures that the access point complies with regulatory requirements for environmental air space with the 5-GHz radio installed.

## Power Considerations

This section describes issues you should consider before applying power to an access point.



#### Caution

The operational voltage range for 1100 series access points is 35 to 57 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.



#### Caution

The nominal voltage for 1200 series access points is 48 VDC, and the access point is operational up to 60 VDC. Voltage higher than 60 VDC can damage the equipment.



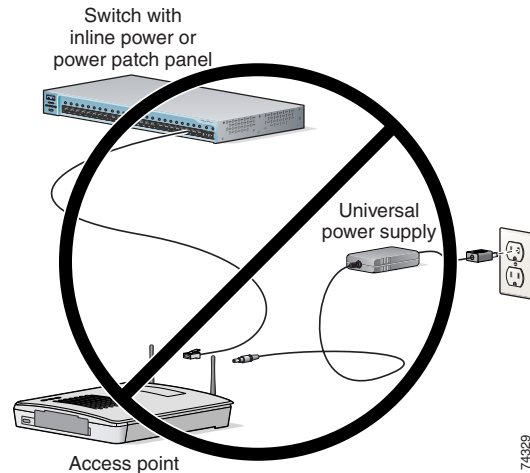
#### Caution

Cisco Aironet power injectors are designed for use with Cisco Aironet access points and bridges only. *Do not use the power injector with any other Ethernet-ready device.* Using the power injector with other Ethernet-ready devices can damage the equipment.

## Use Only One Power Option

You cannot provide redundant power to 1100, 1130AG, and 1200 series access points with both DC power to its power port and inline power from a patch panel or powered switch to the access point's Ethernet port. If you apply power to the access point from both sources, the switch or power patch panel might shut down the port to which the access point is connected. [Figure 2](#) shows the power configuration that can shut down the port on the patch panel or powered switch.

**Figure 2** *Improper Power Configuration Using Two Power Sources*



## Configuring Power for 1130AG and 1240AG Access Points

The 1130AG and 1240AG access points disable the radio interfaces when the unit senses that the power source to which it is connected does not provide enough power. Depending on your power source, you might need to enter the power source type in the access point configuration. Use the System Software: System Configuration page on the web-browser interface to select a power option. [Figure 3](#) shows the System Power Settings section of the System Configuration page.

**Figure 3** *Power Options on the System Software: System Configuration Page*

System Power Settings	
Power State:	FULL POWER
Power Source:	AC_ADAPTOR
Power Settings:	<input type="radio"/> Power Negotiation <input checked="" type="radio"/> Pre-standard Compatibility
Power Injector:	<input type="checkbox"/> Installed on Port with MAC Address: <input type="text" value="DISABLED"/> (HHHH.HHHH.HHHH)
<input type="button" value="Apply"/>	

121655

### Using the AC Power Adapter

If you use the AC power adapter to provide power to the access point, you do not need to adjust the access point configuration.

## Using a Switch Capable of IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the access point and the switch supports the IEEE 802.3af power negotiation standard, select **Power Negotiation** on the System Software: System Configuration page.

## Using a Switch That Does Not Support IEEE 802.3af Power Negotiation

If you use a switch to provide Power over Ethernet (PoE) to the access point and the switch does not support the IEEE 802.3af power negotiation standard, select **Pre-Standard Compatibility** on the System Software: System Configuration page.

## Using a Power Injector

If you use a power injector to provide power to the access point, select **Power Injector** on the System Software: System Configuration page and enter the MAC address of the switch port to which the access point is connected.

## Operating 5-GHz Radio Requires Power Injector, Power Module, or Catalyst 3550-24 PWR Switch

The 1200 series power injector and the 1200 series power module support operation of the 5-GHz radio in the access point. Currently, the Catalyst 3550-24 PWR switch supports power for both the 2.4-GHz radio and the 5-GHz radio. Other switches and power patch panels might not provide enough power for the 5-GHz radio.

## Access Point Requires 1200 Series Universal Power Supply and Power Injector

The 350 series universal power supply and power injector are not compatible with the 1200 series access point. If you use a power injector or a power module to provide power to a 1200 series access point, you must use a 1200 series universal power supply. If you need to use a power injector to inject power into the access point's Ethernet port, you must use a 1200 series power injector.

## Unpowered 1100 Series Access Points Cause Loopback When Connected to Switches Without Loopback Detection

When you connect an unpowered 1100 series access point to a switch without loopback detection, the access point causes a loopback. To avoid this problem, make sure loopback detection is enabled on the switch to which the access point is connected. If your switch does not have loopback detection, disconnect the access point from the switch when the access point power is off.

## Antenna Installation

For instructions on the proper installation and grounding of external antennas for 1200 and 1240AG series access points, refer to the National Fire Protection Association's *NFPA 70, National Electrical Code*, Article 810, and the Canadian Standards Association's *Canadian Electrical Code*, Section 54.



### Warning

**Do not install the antenna near overhead power lines or other electric light or power circuits, or where it can come into contact with such circuits. When installing the antenna, take extreme care not to come into contact with such circuits, as they may cause serious injury or death.**

## Important Notes

This section describes important information about the access point.

### Change to Default IP Address Behavior

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

- When you connect a 350, 1130AG, 1200, 1230AG, 1240AG series access point or a 1300 series outdoor access point/bridge with a default configuration to your LAN, the access point requests an IP address from your DHCP server and, if it does not receive an address, continues to send requests indefinitely.
- When you connect an 1100 series access point with a default configuration to your LAN, the 1100 series access point 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 access point 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 access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

### Save Interface Level Configuration Before Upgrading to Release 12.3(8)JA

If the access points have SSIDs configured at the interface level (rather than at the global level), before upgrading to Cisco IOS Release 12.3(8)JA and later, upgrade to Cisco IOS Release 12.3(4)JA, save the configurations and then upgrade to Release 12.3(8)JA or later. This procedure must be followed to make sure that the SSID configurations are converted from the interface level to global level.

### Changes to the Default Configuration—Radios Disabled and No Default SSID

In this release, the radio or radios are disabled by default, and there is no default SSID. You must create an SSID and enable the radio or radios before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points.

### Clients Using WPA/WPA2 and Power Save May Fail to Authenticate

Certain clients using WPA/WPA2 key management and power save may take many attempts to authenticate or, in some cases, fail to authenticate. Any SSID defined to use authentication key-management wpa, coupled with clients using power save mode and authenticating using WPA/WPA2 may experience this problem.

A hidden configure level command, **dot11 wpa handshake timeout**, can be used to increase the timeout between sending the WPA key packets from the default value (100 ms) to a value between 101 and 2000 ms. The command stores its value in the configuration across device reloads.

## Default Username and Password Are *Cisco*

When you open the access point interface, you must enter a username and password. The default username for administrator login is *Cisco*, and the default password is *Cisco*. Both the username and password are case sensitive.

## Some Client Devices Cannot Associate When QoS Is Configured

Some wireless client devices, including Dell Axim handhelds and Hewlett-Packard iPaq HX4700 handhelds, cannot associate to an access point when the access point is configured for QoS. To allow these clients to associate, disable QoS on the access point. You can use the QoS Policies page on the access point GUI to disable QoS, or enter this command on the CLI:

```
ap(config-if)#no dot11 qos mode
```

## Some Devices Disassociate When Multiple BSSIDs Are Added or Deleted

Devices on your wireless LAN that are configured to associate to a specific access point based on the access point MAC address (such as client devices, repeaters, hot standby units, or workgroup bridges) might lose their association when you add or delete a multiple BSSID. When you add or delete a multiple BSSID, check the association status of devices configured to associate to a specific access point. If necessary, reconfigure the disassociated device to use the BSSID's new MAC address.

## Enabling MBSSIDs Without VLANs Disables Radio Interface

If you use the mbssid configuration interface command to enable multiple BSSIDs on a specific radio interface but VLANs are not configured on the access point, the access point disables the radio interface. To re-enable the radio, you must shut down the radio, disable multiple BSSIDs, and re-enable the radio. This example shows the commands you use to re-enable the radio:

```
AP1134(config)# interface d1
AP1134(config-if)# shut
AP1134(config-if)# no mbssid
AP1134(config-if)# no shut
```

After you re-enable the radio, you can enable VLANs on the access point and enable multiple BSSIDs.

## Cannot Set Channel on DFS-Enabled Radios

Access points with 5-GHz radios configured at the factory for use in Europe, Singapore, Korea, Japan, Taiwan, and Israel now comply with regulations that require radio devices to use Dynamic Frequency Selection (DFS) to detect radar signals and avoid interfering with them. You cannot manually set the channel on DFS-enabled radios.

## Cisco 7920 Phones Require Firmware Version 1.09 or Later When Multiple BSSIDs Are Enabled

When multiple BSSIDs are configured on the access point, Cisco 7920 wireless IP phones must run firmware version 1.09 or later.

## AIR-RM21A/AIR-RM22A Radio Modules Usually Set to Max Transmit Power

AIR-RM21A and AIR-RM22A radio modules measure transmit power in decibels per milliwatt (dBm), but earlier versions of 802.11a radios in Cisco Aironet access points measure power in milliwatts (mW). Because power settings in mW do not translate directly to settings in dBm, the access point usually uses the default power setting of maximum when you install a new AIR-RM21A or AIR-RM22A radio module.

**Table 1** lists 802.11a transmit power settings in mW and the power settings that the access point assigns to a new radio module.

**Table 1** *Transmit Power Settings Assigned to New Radio Modules*

Power Settings in mW	Power Setting Assigned to New Radio Module
5	5 dBm (approximately 3 mW)
10	maximum (17 dBm)
20	maximum
40	maximum

## GRE Tunnelling Through WLSM Sometimes Requires MTU Setting Adjustments

If client devices on your wireless LAN cannot use certain network applications or cannot browse to Internet sites, you might need to adjust the MTU setting on the client devices or other network devices. For more information, refer to the Tech Note at this URL:

[http://www.cisco.com/en/US/tech/tk827/tk369/technologies\\_tech\\_note09186a0080093f1f.shtml](http://www.cisco.com/en/US/tech/tk827/tk369/technologies_tech_note09186a0080093f1f.shtml)

## TACACS+ and DHCP IP Address Sometimes Locks Out Administrators

When you configure an access point for TACACS+ administration and to receive an IP address from the DHCP server, administrators might be locked out of the access point after it reboots if the administrator does not have a local username and password configured on the access point. This issue does not affect access points configured with a static IP address. Administrators who have been locked out must regain access by using the to reset the unit to default settings.

## Access Points Do Not Support Loopback Interface

You must not configure a loopback interface on the access point.



---

Configuring a loopback interface might generate an IAPP GENINFO storm on your network and disrupt network traffic.

---

## Non-Cisco Aironet 802.11g Clients Might Require Firmware Upgrade

Some non-Cisco Aironet 802.11g client devices require a firmware upgrade before they can associate to the 802.11g radio in the access point. If your non-Cisco Aironet 802.11g client device does not associate to the access point, download and install the latest client firmware from the manufacturer's website.

## Throughput Option for 802.11g Radio Blocks Association by 802.11b Clients

When you configure the 802.11g access point radio for **best throughput**, the access point sets all data rates to basic (required). This setting blocks association from 802.11b client devices. The **best throughput** option appears on the web-browser interface Express Setup and Radio Settings pages and in the **speed** CLI configuration interface command.

## Transmit Power Set to Maximum When You Install 802.11g Radio

When you replace the 802.11b radio in a 1200 series access point with an 802.11g radio, the 802.11g radio is set to the maximum transmit power allowed in your regulatory domain regardless of the power setting configured on the 802.11b radio. After you install the 802.11g radio and the access point reboots, configure the 802.11g radio to the preferred transmit power.

## Use Auto for Ethernet Duplex and Speed Settings

Cisco recommends that you use **auto**, the default setting, for both the speed and duplex settings on the access point Ethernet port. When your access point receives inline power from a switch, any change in the speed or duplex settings that resets the Ethernet link reboots the access point. If the switch port to which the access point is connected is not set to **auto**, you can change the access point port to **half** or **full** to correct a duplex mismatch and the Ethernet link is not reset. However, if you change from **half** or **full** back to **auto**, the link is reset and, if your access point receives inline power from a switch, the access point reboots.



---

**Note** The speed and duplex settings on the access point Ethernet port must match the Ethernet settings on the port to which the access point is connected. If you change the settings on the port to which the access point is connected, change the settings on the access point Ethernet port to match.

---

## Use force-reload Option with archive download-sw Command

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

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

## Radio MAC Address Appears in ACU

When a Cisco Aironet client device associates to an access point running IOS software, the access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

## Radio MAC Address Appears in Access Point Event Log

When a client device roams from an access point (such as access point *alpha*) to another access point (access point *bravo*), a message appears in the event log on access point alpha stating that the client roamed to access point bravo. The MAC address that appears in the event message is the MAC address for the radio in access point bravo. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

## Mask Field on IP Filters Page Behaves the Same As in CLI

In Cisco IOS Release 12.2(8)JA and later, the mask that you enter in the Mask field on the IP Filters page in the access point GUI behaves the same way as a mask that you enter in the CLI. If you enter 255.255.255.255 as the mask, the access point accepts any IP address. If you enter 0.0.0.0, the access point looks for an exact match with the IP address that you entered in the IP Address field.

## Repeater Access Points Running IOS Software Cannot Associate to Parent Access Points Running VxWorks

Repeater access points running Cisco IOS software cannot associate to parent access points that do not run IOS software (all 340 series access points, and 350 and 1200 series access points that have not been converted to run IOS software).

## Repeater Access Points Cannot Be Configured as WDS Access Points

Repeater access points can participate in WDS but cannot serve as the main WDS access point. You cannot configure a repeater access point as the main WDS access point, and if a root access point becomes a repeater in fallback mode, it cannot provide WDS.

## Crossover Cable Sometimes Needed When Ethernet Speed and Duplex Set to Fixed on 1100 Series Access Points

If you change the speed and duplex settings from auto to fixed on an 1100 series access point's Ethernet port, the auto-MDIX feature on the port is disabled. When auto-MDIX is disabled, you must determine whether to use a straight-through or a crossover cable to connect the access point Ethernet port to another device. If the Ethernet link goes down after you set the speed and duplex to fixed, try changing the Ethernet cable from crossover to straight-through or from straight-through to crossover.

## Cannot Perform Link Tests on Non-Cisco Aironet Client Devices and on Cisco Aironet 802.11g Client Devices

The link test feature on the web-browser interface does not support non-Cisco Aironet client devices nor Cisco Aironet 802.11g client devices.

## System Software Upgrade Sometimes Fails Using Microsoft Internet Explorer 5.01 SP2

A system software upgrade sometimes fails when you use Microsoft Internet Explorer 5.01 SP2 to upgrade system software using the TFTP Upgrade page in the web-browser interface. Use a later version of Microsoft Internet Explorer to perform HTTP system software upgrades, or use TFTP to upgrade system software. Click this URL to browse to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for complete instructions on performing software upgrades:

[http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/wireless/ps4570/prod_configuration_guides_list.html)

## 1100 Series Access Points with Boot Loader Version 12.2(4)JA Boot into Monitor Mode

When the Ethernet port is disabled on an 1100 series access point running boot loader version 12.2(4)JA, the access point boots into monitor mode when it reboots. To avoid this problem, connect the access point Ethernet port to one of the following:

- a wired LAN
- the Ethernet port on a PC

Remove power from the access point and reapply power to reboot the unit. When the access point senses an Ethernet connection, it boots normally.

## Corrupt EAP Packet Sometimes Causes Error Message

During client authentication, the access point sometimes receives a corrupt EAP packet and displays this error message:

```
Oct 1 09:00:51.642 R: %SYS-2-GETBUF: Bad getbuffer, bytes= 28165
-Process= "Dot11 Dot1x process", ipl= 0, pid= 32
-Traceback= A2F98 3C441C 3C7184 3C604C 3C5E14 3C5430 124DDC
```

You can ignore these messages.

## When Cipher Is TKIP Only, Key Management Must Be Enabled

When you configure TKIP-only cipher encryption (not TKIP + WEP 128 or TKIP + WEP 40) on any radio interface or VLAN, every SSID on that radio or VLAN must be set to use WPA or CCKM key management. If you configure TKIP on a radio or VLAN but you do not configure key management on the SSIDs, client authentication fails on the SSIDs.

## Non-Cisco Aironet Clients Sometimes Fail 802.1x Authentication

Some non-Cisco Aironet client adapters do not perform 802.1x authentication to the access point unless you configure **Open authentication with EAP**. To allow both Cisco Aironet clients using LEAP and non-Cisco Aironet clients using LEAP to associate using the same SSID, you might need to configure the SSID for both **Network EAP** authentication and **Open authentication with EAP**.

## Pings and Link Tests Sometimes Fail to Clients with Both Wired and Wireless Network Connections

When you ping or run a link test from an access point to a client device installed in a PC running Microsoft Windows 2000, the ping or link test sometimes fails when the client has both wired and wireless connections to the LAN. Microsoft does not recommend this configuration. For more information, refer to Microsoft Knowledge Base article 157025 at this URL:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;157025&Product=win2000>

## Layer 3 Mobility Not Supported on Repeaters and Workgroup Bridges

Repeater access points and workgroup bridges cannot associate to an SSID configured for Layer 3 mobility. Layer 3 mobility is not supported on repeaters and workgroup bridges.

## WLSM Required for Layer 3 Mobility

You must use a Wireless LAN Services Module (WLSM) as your WDS device in order to properly configure Layer 3 mobility. If you enable Layer 3 mobility for an SSID and your WDS device does not support Layer 3 mobility, client devices cannot associate using that SSID.

# Caveats

This section lists open and resolved caveats for access points.

## Open Caveats

These caveats are open in Cisco IOS Release 12.3(8)JA2:

- CSCsb00606—350 series access points reload every two weeks
- CSCsb80462—When network topology changes, the 1300 series outdoor access point/bridge fails to forward traffic of certain wired clients even though STP has converged.

**Workaround:** None. In general this problem does not happen to a stable network with a limited amount of flooding traffic. The switch that connecting to the power injector of the 1300 will not flood packets to the 1300 if both source and destination devices are on ports other than the 1300 port.

The power injector of the 1300 functions like a switch and does source learning. It has a 5 minute aging timeout before any learned entry is purged from the forwarding table. If the network topology changes during the aging timeout period, and the both the source and destination device mac-addresses had been learned at the power injector input, the power injector will not forward the packet to the 1300 it services until the table entry is purged.

- CSCsb84696—WLSE access point radio scan shows occasional SNMP timeouts

An access point radio scan on an 1100 series access point running Cisco IOS Release 12.3(4)JA may occasionally fail because the WLSE is not able to set the **Dot11RadioDiagTempTxPowerLevel** on the AP. The request times out with an “ERROR: AP not SNMP accessible” error.

**Workaround:** none.

- CSCsd77950—Intel Pro Wireless 2200BG adapter crashes

Laptop clients with Intel Pro Wireless 2200BG adapters associated to an access point running Cisco IOS Release 12.3(8)JA or later sometimes reboot under these conditions:

- **dot11 phone** is configured on the access point
- The client device has these Intel drivers installed: 8.0.12.20000 (3/8/2004) or 8.0.12.90000 (1/2/2004)

**Workaround:** Disable the **dot11 phone** command on the access point or install Intel driver 9.0.3.9.

- CSCse02766—Client devices associated to a repeater access point sometimes fail to receive an IP address from the DHCP server and do not appear in the root access point’s association table.

**Workaround:** None.

- CSCse34644—Shared authentication sometimes fails on non-native VLANs.

**Workaround:** Configure VLANs and SSIDs, save the configuration, and reload the access point. When the access point reboots, shared authentication clients are able to authenticate.

## Resolved Caveats

These caveats are resolved in Cisco IOS Release 12.3(8)JA2:

- CSCek26492

Symptoms: A router may crash if it receives a packet with a specific crafted IP option as detailed in Cisco Security Advisory: Crafted IP Option Vulnerability:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

Conditions: This DDTS resolves a symptom of CSCec71950. Cisco IOS with this specific DDTS are not at risk of crash if CSCec71950 has been resolved in the software.

Workaround: Cisco IOS versions with the fix for CSCec71950 are not at risk for this issue and no workaround is required. If CSCec71950 is not resolved, see the following Cisco Security Advisory: Crafted IP Option Vulnerability for workaround information:

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-ip-option.shtml>

- CSCek37177

The Cisco IOS Transmission Control Protocol (TCP) listener in certain versions of Cisco IOS software is vulnerable to a remotely-exploitable memory leak that may lead to a denial of service condition.

This vulnerability only applies to traffic destined to the Cisco IOS device. Traffic transiting the Cisco IOS device will not trigger this vulnerability.

Cisco has made free software available to address this vulnerability for affected customers.

This issue is documented as Cisco bug ID [CSCek37177](#).

There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at

<http://www.cisco.com/warp/public/707/cisco-sa-20070124-crafted-tcp.shtml>

- CSCed32369—Disabling SNMPv3 now removes the **snmp server-host** command from the configuration.
- CSCei18359—Access points no longer run low on memory when performing posture validation over an extended period of time.
- CSCin99605—Access points no longer reboot when you configure a TACACS server.
- CSCsc02981—Access points no longer fail when **mac-authen filter-cache** is enabled.
- CSCsc79121—Radio interfaces are now operational after an upgrade.
- CSCsc83665—Access points no longer reboot unexpectedly when the configuration contains the **dot11 network-map** command.
- CSCsc88624—Devices in non-root bridge mode no longer modify VTP packets from SNAP format to DIX format.
- CSCsc97727—Access points no longer reboot unexpectedly when you use the CLI to add or remove a TACACS server.
- CSCsd00738—Access points no longer reboot unexpectedly when you log into the CLI as an administrator.
- CSCsd40250—Access points no longer leak memory when AES is configured.
- CSCsd60670—Access points no longer reboot unexpectedly when several client devices attempt to authenticate at the same time.

- CSCsd67403—The Local User List option on the User Admin page in the access point GUI now functions correctly.
- CSCsd69160—Access points no longer reboot when you override a running configuration with a configuration from access point Flash.
- CSCsd77228—The IGMP snooping feature no longer generates large amounts of multicast traffic.
- CSCsd78200—Access points now clear the PMK cache at the end of each reauthentication period.
- CSCsd82624—WPA client devices that are authenticated can now reauthenticate when the card is restarted.
- CSCsd84198—802.11b radios are now operational after upgrade.
- CSCsd90136—Configuring 802.1q trunking on the access point no longer causes a change to the DHCP configuration.
- CSCsd91009—1200 series access points now track Aeroscout RFID tags.
- CSCsd98387—You can now select a specific 5-GHz channel 30 minutes after a dynamic frequency selection (DFS) event.

## If You Need More Information

If you need information about a specific caveat that does not appear in these release notes, you can use the Cisco Bug Toolkit to find select caveats of any severity. Click this URL to browse to the Bug Toolkit:

[http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl)

(If you request a defect that cannot be displayed, the defect number might not exist, the defect might not yet have a customer-visible description, or the defect might be marked Cisco Confidential.)

## Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. Click **Technology Support**, choose **Wireless** from the menu on the left, and click **Wireless LAN**.

## Documentation Updates

This section lists changes, errors, and omissions from user documentation for access points.

### Omissions

The command **dot11 extension power native** was omitted from the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points 12.3(8)JA* and *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges 12.3(8)JA*.

When enabled, the **dot11 extension power native** shifts the power tables the radio uses from the IEEE 802.11 tables to the native power tables. The radio derives the values for this table from the NativePowerTable and NativePowerSupportedTable of the CISCO-DOT11-1F-MIB. The Native Power tables were designed specifically to configure powers as low as -1dBm for Cisco Aironet radios that support these levels.

## Related Documentation

This section lists documents related to Cisco IOS Release 12.3(8)JA and to 350, 1100, 1130AG, 1200, 1240AG series access points, and 1300 series outdoor access point/bridges.

- *Cisco Aironet Conversion Tool for Cisco IOS Software, 2.0 Administrator Guide for Windows*
- *Quick Start Guide: Cisco Aironet 350 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1100 Series Access Points*
- *Quick Start Guide: Cisco Aironet 1130AG Series Access Points*
- *Quick Start Guide: Cisco Aironet 1200 Series Access Points Running Cisco IOS Software*
- *Quick Start Guide: Cisco Aironet 1240AG Series Access Points*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *Hardware Installation Guide for Cisco Aironet 350 Series Access Points Running Cisco IOS Software*
- *Cisco Aironet 1100 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1200 Series Access Point Hardware Installation Guide*
- *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*
- *Installation Instructions for Cisco Aironet Power Injectors*

## Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

### Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

<http://www.cisco.com/go/marketplace/>

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Cisco will continue to support documentation orders using the Ordering tool:

- Registered Cisco.com users (Cisco direct customers) can order documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/>
- Instructions for ordering documentation using the Ordering tool are at this URL:  
[http://www.cisco.com/univercd/cc/td/doc/es\\_inpck/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm)
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

## Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—[security-alert@cisco.com](mailto:security-alert@cisco.com)

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—[psirt@cisco.com](mailto:psirt@cisco.com)

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



### Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.htm](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm)

The link on this page has the current PGP key ID in use.

# Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

## Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

<http://tools.cisco.com/RPF/register/register.do>

**Note**

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:  
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

<http://www.cisco.com/go/iqmagazine>

or view the digital edition at this URL:

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:  
<http://www.cisco.com/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:  
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:  
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:  
<http://www.cisco.com/en/US/learning/index.html>

---

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)