



# Release Notes for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges Running Firmware Version 12.00T

---

**October 25, 2002**

These release notes describe features and caveats for Cisco Aironet 340 and 350 Series Access Points and 350 Series Bridges running firmware version 12.00T.

## Contents

- [Introduction, page 2](#)
- [New Features, page 2](#)
- [Installation Notes, page 6](#)
- [Limitations and Restrictions, page 8](#)
- [Important Notes, page 10](#)
- [Caveats, page 11](#)
- [Troubleshooting, page 13](#)
- [Obtaining Documentation, page 13](#)
- [Obtaining Technical Assistance, page 14](#)



---

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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

# Introduction

A Cisco Aironet Access Point is a wireless LAN transceiver that can act as the connection point between wireless and wired networks or as the center point of a standalone wireless network. Cisco Aironet Bridges are wireless LAN transceivers that connect two or more remote networks into a single LAN.

The access point and bridge use a browser-based management system. The system settings are on web pages in the system firmware. You use your Internet browser to view and adjust the system settings.

## New Features

Firmware version 12.00T includes these new software features:

- [Multiple SSID and VLAN Support](#)
- [Quality of Service Support](#)
- [Centralized Administrator Authentication](#)
- [Better Handling of Lost Ethernet](#)
- [Improved Authentication Server Management](#)
- [Secure Shell Support](#)
- [Reporting Access Points That Fail Authentication With LEAP](#)

## Multiple SSID and VLAN Support

Version 12.00T supports multiple SSIDs and VLANs. The multiple SSID feature is active only when VLANs are enabled. You can use multiple SSIDs to create different levels of network access and to access virtual LANs (VLANs). You can configure up to 16 separate SSID-to-VLAN pairs on your network.

### What Is a VLAN?

When a switched network is segmented logically by functions, project, teams, or applications, rather than on a physical or geographical basis, then each logical network segment is called a VLAN. For example, all workstations and servers used by a particular workgroup team can be connected to the same VLAN regardless of their physical connections to the network or the fact that they might be intermingled with other teams. When you logically segment a network into VLANs, you can reconfigure the network through software rather than physically unplugging and moving devices or wires.

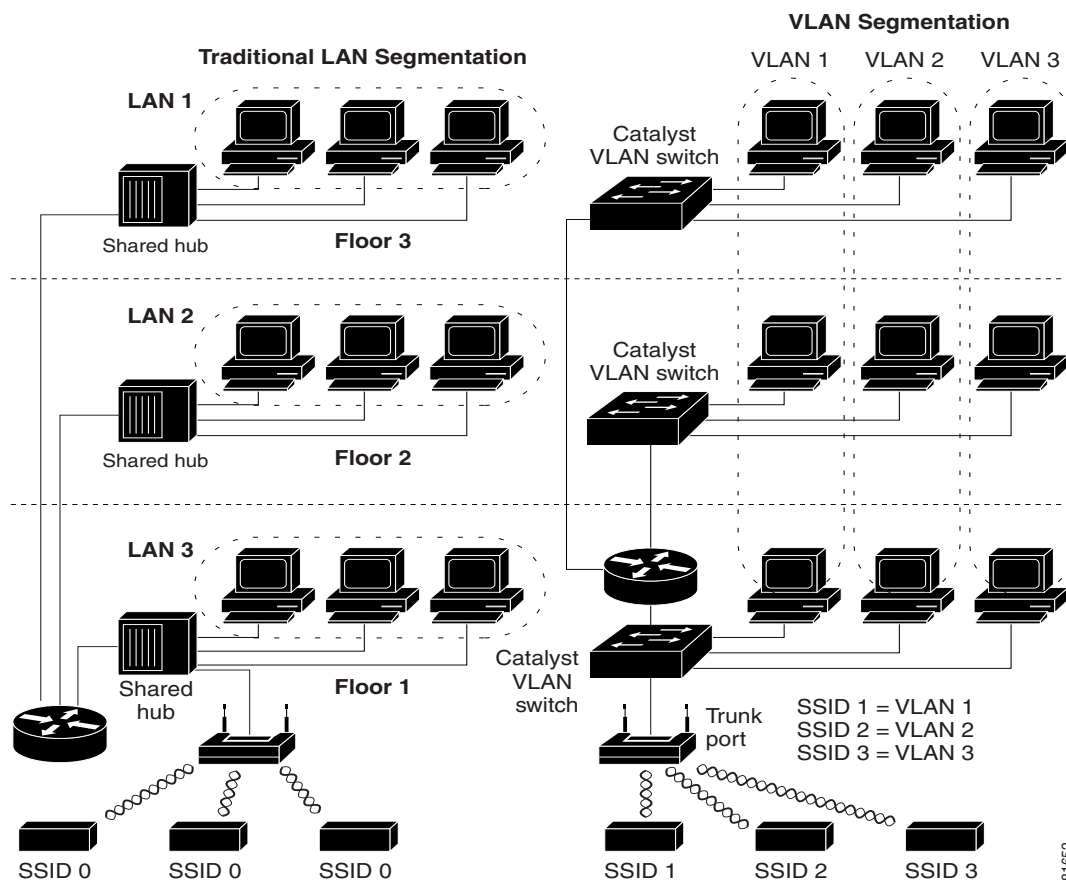
A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment; for example, LAN switches that operate bridging protocols between them with a separate group for each VLAN.

VLANs provide the segmentation services traditionally provided by routers in LAN configurations. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic-flow management. None of the switches within the defined group bridge any frames, not even broadcast frames, between two VLANs.

VLANs are extended into the wireless realm by adding IEEE 802.1Q tag awareness to the access point. Frames destined for different VLANs are transmitted by the access point wirelessly on different SSIDs. When a client is associated to an SSID that is linked to a particular VLAN, then the client receives packets that were 802.1Q tagged for that VLAN. When a client associated to a VLAN-linked SSID sends a packet to the access point, the access point tags the packet with an 802.1Q tag for the VLAN before forwarding the packet onto the wired network.

Figure 1 illustrates the difference between traditional physical LAN segmentation and logical VLAN segmentation with wireless devices connected.

Figure 1 LAN Segmentation and VLAN Segmentation with Wireless Components



## Quality of Service Support

The access point now supports QoS, primarily in the area of interactive VoIP telephones from Spectralink and Symbol Technologies Corporation. The access point also provides priority classification, prioritized queuing, and prioritized channel access for other downlink IEEE 802.11 traffic such as streaming audio or video traffic.

With this software release, the access point does not include any QoS enhancements in Cisco IEEE 802.11 client software.

## What Is QoS?

QoS refers to the ability of a network to provide improved service to selected network traffic over various underlying technologies including Ethernet and IEEE 802.11 wireless LANs. In particular, QoS features provide improved and more predictable network service that:

- Supports dedicated bandwidth
- Improves loss characteristics
- Avoids and manages network congestion
- Shapes network traffic
- Sets traffic priorities across the network

## Limitations and Restrictions

The QoS implementation on the access point has the following limitations and restrictions:

- Provides only prioritized QoS for downlink traffic on IEEE 802.11 links.
- Does not support a general-purpose QoS signalling protocol, uniform admission control, guaranteed bandwidth, and other features that are generally associated with parametrized QoS.
- Supports rudimentary admission control mechanisms for Cisco and Symbol VoIP phones.
- Does not provide a method for prioritizing uplink traffic on IEEE 802.11 links.
- Requires a small DTIM beacon period to support jitter-sensitive streaming multicast audio and video applications.
- Supports IEEE 802.11e EDCF-like channel access prioritization but does not support IEEE 802.11e QoS frame formats.

## Centralized Administrator Authentication

This feature allows the use of an AAA server to authenticate clients if the user manager functionality is enabled on the access point. At the end of a successful login, the AAA server verifies the user login and passes back the appropriate privileges for the user or an administrator. The following points are pertinent to this feature:

- The access point can use either RADIUS or TACACS for user authentication.
- The access point tries to authenticate to the user locally first. If the user is not found locally, the access point authenticates to the remote AAA server.
- By default, the access point is configured to perform only local administrative authentication.
- User privileges are Write, SNMP, Ident, Firmware, and Admin. They are locally cached on the access point. A time-out timer flushes the information every 5 minutes.
- Authentication server configuration:
  - RADIUS protocol: send request on port 1812 or 1615

TACACS protocol: send request on port 49

## Better Handling of Lost Ethernet

This feature allows a number of user-configurable actions to execute when an access point loses backbone connectivity:

- No action—the access point continues to maintain associations with clients and manages traffic between them, but traffic to the backbone is not passed. When the backbone is restored, the access point begins passing traffic to and from the wired network.
- Switch to repeater mode—the access point tries to connect to a root access point using any of the configured SSIDs. If it cannot connect, all clients are disassociated and the access point removes itself from the wireless network until connectivity is restored.
- Shut the radio off—all clients are disassociated and the access point removes itself from the wireless network until backbone connectivity is restored.
- Restrict client access to a specific SSID—the access point allows association using a restricted SSID (for administrator troubleshooting and diagnosis purposes).

## Improved Authentication Server Management

Authentication server management functions are improved with the addition of two new features:

- Display of active authentication servers—For each authentication type: 802.1x/EAP, MAC, or Admin Authentication (if enabled), the active server is identified by a green color.
- Automatic return to primary authentication server—If the selected RADIUS server (primary) is not reachable after a predetermined period of time-out and retries, the access point uses the next server listed. With this parameter set, when the primary server becomes reachable, the access point automatically returns to it.

## Secure Shell Support

Secure Shell (SSH) is an alternative to or a replacement for Telnet that is considered the standard protocol for remote logins. SSH runs in the Application Layer of the TCP/IP stack. SSH clients make SSH relatively easy to use and are available on most computers including those that run Windows or a type of UNIX. SSH clients are also available on some handheld devices.

SSH provides a secure connection over the Internet providing strong user authentication. SSH protects the privacy of transmitted data (such as passwords, binary data, and administrative commands) by encrypting it. The following details are pertinent:

- A maximum of one Telnet connection to the access point is allowed at one time.
- A Telnet SSH request can preempt an active serial SSH connection.

Implementing an SSH connection involves the following:

- SSH server on the access point listens to TCP port 22 for requests.
- When a request from a client is received, the access point sends a password-only public key to the client.
- The client generates a double-encrypted session key and requests authentication

When authentication is successful, all management traffic between the access point and client is encrypted using the session key

## Reporting Access Points That Fail Authentication With LEAP

This feature is part of version 12.00T, but is not functional unless the client is running firmware version 5.02.01 or greater, which will be released at a later date.

An access point running version 12.00T records a message in the system log when a client discovers and reports another access point in the WLAN that fails LEAP authentication.



### Note

---

This feature is client dependent. Version 12.00T provides a method by which the access point or bridge processes the information it receives from a client.

---

The process takes place as follows:

1. A client with a LEAP profile attempts to associate to a access point A.
2. Access point A does not handle LEAP authentication successfully, perhaps because the access point does not understand LEAP or cannot communicate to a trusted LEAP authentication server.
3. The client records the MAC address for access point A and the reason why the association failed.
4. The client associates successfully to access point B.
5. The client sends the MAC address of access point A and the reason code for the failure to access point B.
6. Access point B logs the failure in the system log.

## Installation Notes

You can find the latest release of access point and bridge firmware at this URL:

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

## Installation in Environmental Air Space

Cisco Aironet 350 Series Bridges and metal-case access points are suitable for use in environmental air space in accordance with Section 300-22(c) of the *National Electrical Code*.



### Caution

---

The Cisco Aironet Power Injector has a smaller operating temperature range (32 to 104°F; 0 to 40°C) than the 350 series bridge and metal-case access point. The power injector is not intended for use in extremely high or low temperatures or in environmental air spaces, such as above suspended ceilings.

---

## Antenna Installation

For instructions on the proper installation and grounding of external antennas, 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 locate 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.

## Power Considerations

**Caution**

The operational voltage range for 350 series access points and bridges is 24 to 60 VDC, and the nominal voltage is 48 VDC. Voltage higher than 60 VDC can damage the equipment.

**Caution**

Cisco Aironet power injectors are designed for use with 350 series access points and 350 series 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.

## System Requirements

You must have a 340 or 350 series access point or a 350 series bridge to install firmware version 12.00T.

## Version Supported

Your access point must be running firmware version 10.x or later to install firmware version 12.00T.  
Your bridge must be running version 11.07 or later to install firmware version 12.00T.

## Upgrading to a New Firmware Release

### Determining the Firmware Version

The firmware version number is in the upper-left corner of most management screens in the web-browser interface and at the top of the home (Summary Status) page in the command-line interface.

### Upgrade Procedure

For instructions on installing access point and bridge firmware:

1. Follow this link to the Cisco Aironet documentation home page:  
<http://www.cisco.com/univercd/cc/td/doc/product/wireless/index.htm>
2. Follow this path to the product, document, and chapter:  
**Aironet 350 Series Wireless LAN Products > Cisco Aironet 350 Series Access Points > Cisco Aironet Access Point Software Configuration Guide > Managing Firmware Configurations > Updating Firmware**
3. Follow this link to the Software Center on Cisco.com and download firmware version 12.00T:  
<http://www.cisco.com/public/sw-center/sw-wireless.shtml>

**Note**

To upgrade firmware from a file server, you must enter settings on the access point's or bridge's FTP Server Setup page. Refer to chapter 6 in the *Cisco Aironet Access Point Software Configuration Guide* for more information.

## Limitations and Restrictions

This section describes limitations and restrictions for 340 and 350 series access points and 350 series bridges.

### Cisco Aironet 350 Series Bridges Incompatible with 340 Series Bridges

Cisco Aironet 340 and 350 Series Bridges can be connected to the same LAN segments, but they cannot communicate wirelessly. Although you can disable STP on non-root 350 series bridges, 350 and 340 series bridges are not designed to interoperate. If you use both 340 and 350 series bridges on your network, make sure the 340 series bridges have radio bridge links only to other 340 series bridges, and that 350 series bridges have radio bridge links only to other 350 series bridges.

### Removing Power During Firmware Update Can Corrupt Radio Firmware

When you update the firmware on an access point or bridge, allow the unit to finish its start-up sequence before removing power. If you update the firmware and remove power before the unit finishes the start-up sequence, the radio firmware might be corrupted, making the unit inoperable. If the radio firmware is corrupted, the radio indicator (the bottom of the three indicators on top of the access point or bridge) lights steady red, and the following error message appears when the access point or bridge starts up:

```
Failed to start driver for port "awc0" (errno=0x006d0002)
```

If the radio firmware is corrupted, you should try to reset the unit to factory defaults using the **:resetall** command in the CLI; see chapter 9 of the *Cisco Aironet Access Point Software Configuration Guide* for instructions on resetting the access point. If the unit cannot be reset to defaults, you must return the unit to Cisco for service.

You can safely remove power after a firmware update when the configuration management pages reappear in the command-line or web-browser interfaces, or when the three status indicators on top of the unit complete the following pattern:

1. All three indicators are steady green, meaning that the access point is beginning to update the firmware.
2. The middle indicator is steady green and the top and bottom indicators are off, indicating that the access point or bridge is updating the radio firmware.

When the middle indicator blinks or the top and bottom indicators blink, you can remove power.

## EAP Authentication Requires Matching 802.1x Protocol Drafts


**Note**

This section applies to wireless networks set up to use LEAP. If you do not use LEAP on your wireless network, you can skip this section.

Wireless client devices use Extensible Authentication Protocol (EAP) to log onto a network and generate a dynamic, client-specific WEP key for the current logon session. If your wireless network uses WEP without EAP, client devices use the static WEP keys entered in the Aironet Client Utilities.

If you use Network-EAP authentication on your wireless network, your client devices and access points must use the same 802.1x protocol draft. For example, if the radio firmware on the client devices that will associate with an access point is 4.16, the access point should be configured to use Draft 8 of the 802.1x protocol. [Table 1](#) lists firmware versions for Cisco Aironet products and the draft with which they comply.

**Table 1** 802.1x Protocol Drafts and Compliant Client Firmware

Firmware Version	Draft 7	Draft 8	Draft 10 <sup>1</sup>
PC/PCI cards 4.13	—	x	—
PC/PCI cards 4.16	—	x	—
PC/PCI cards 4.23	—	x	—
PC/PCI cards 4.25 and later	—	—	x
WGB34x/352 8.58	—	x	—
WGB34x/352 8.61 or later	—	—	x
AP34x/35x 11.05 and earlier	—	x	—
AP34x/35x 11.06 and later <sup>2</sup>	—	x	x
AP34x/35x 11.07 and later	—	x	x
AP34x/35x and BR35x 11.21 through 12.00T	—	x	x

1. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.
2. The default draft setting in access point and bridge firmware version 11.06 and later is Draft 10.


**Note**

Draft standard 8 is the default setting in firmware version 11.05 and earlier, and it might remain in effect when you upgrade the firmware to version 11.06 or later. Check the setting on the Authenticator Configuration page in the management system to make sure the best draft standard for your network is selected.

Use the Authenticator Configuration page in firmware version 11.06 or later to select the draft of the 802.1x protocol the access point or bridge radio should use. Follow these steps to set the draft for your access point or bridge:

- 
- Step 1** Browse to the Authenticator Configuration page in the access point management system:
- On the Summary Status page, click **Setup**.
  - On the Setup page, click **Security**.
  - On the Security Setup page, click **Authentication Server**.
- Step 2** Use the 802.1x Protocol Version (for EAP authentication) pull-down menu to select the draft of the 802.1x protocol the access point or bridge radio should use. Menu options include:
- Draft 7—No radio firmware versions compliant with Draft 7 have LEAP capability, so you should not need to select this setting.
  - Draft 8—Select this option if LEAP-enabled client devices that associate with this access point or bridge use radio firmware versions 4.13, 4.16, or 4.23.
  - Draft 10—This is the default setting in firmware versions 11.06 and later. Select this option if client devices that associate with this access point or bridge use Microsoft Windows XP EAP authentication or if LEAP-enabled client devices that associate with this access point or bridge use radio firmware version 4.25 or later. The functionality in Draft 10 is equivalent to the functionality in Draft 11, the ratified draft of the 802.1x standard.
- Step 3** Click **Apply** or **OK** to apply the setting. The access point or bridge reboots.
- 

## Select WEP Key 1 as Transmit Key for EAP Authentication

If you use Network-EAP as the authentication type on your wireless network, you must select key 1 as the transmit key on the access point or bridge AP Radio Data Encryption page. The access point or bridge uses the WEP key you enter in key slot 1 to encrypt multicast and broadcast data signals that it sends to EAP-enabled client devices. Because the access point or bridge transmits the WEP key used for multicast messages to the EAP-enabled client device during the EAP authentication process, that key does not have to appear in the EAP-enabled device's WEP key list. The access point or bridge uses a dynamic WEP key to encrypt unicast messages to EAP-enabled clients. When you set up a non-root bridge or repeater access point to authenticate as a LEAP client, the bridge or repeater derives a dynamic WEP key and uses it to communicate with the root bridge or access point. Bridges and repeaters not set up for LEAP authentication use static WEP keys when communicating with other bridges and access points.



### Note

If you do not use EAP authentication on your wireless network, you can select any WEP key as the transmit key. If you use EAP authentication and you enable broadcast key rotation, you can enable WEP without entering WEP keys.

---

## Important Notes

This section lists important information about access points and bridges running firmware version 12.00T.

## Reboot of Workgroup Bridges Required When Allowing More Than 20

With firmware version 12.00T, you can select **no** for the *Classify Workgroup Bridges as Network Infrastructure* setting on the AP/Root Radio Advanced page to allow up to 50 workgroup bridges to associate to the access point or bridge. After selecting **no** for this setting, you must reboot workgroup bridges associated to the access point or bridge.

## Cisco Discovery Protocol Re-Enabled for Individual Interfaces on Reboot

The Cisco Discovery Protocol (CDP) feature is enabled by default, and CDP is enabled for each of the access point's or bridge's individual interfaces by default. However, if you disable CDP for one of the individual interfaces, the access point or bridge re-enables CDP for that interface when it reboots. If you disable CDP completely, the access point or bridge does not re-enable CDP on reboot.

## Caveats

This section lists open and resolved software issues in firmware version 12.00T.

## Getting Bug Information on Cisco.com

If you are a registered Cisco user, you can use the Cisco TAC Software Bug Toolkit, which consists of three tools (Bug Navigator, Bug Watcher, and Search by Bug ID Number) that help you identify existing bugs (or caveats) in Cisco software products.

Access the TAC Software Bug Toolkit at <http://www.cisco.com/support/bugtools/>.

## Open Caveats

The following caveats have not been resolved for firmware version 12.00T:

- CSCdz04708—Early 340 series access points are incompatible with VLAN tagging  
 Early versions of the 340 series access point are able to set up VLANs, but clients on non-native VLANs will be unable to transmit and receive large packets. The reason for this is because early 340 series access points were limited to a maximum packet data length of 1500 bytes.  
 You can identify an affected access point by browsing to the Ethernet Identification page and checking the Maximum Packet Data Length parameter. If it is 1500, the failure will occur.  
 Possible workaround—If you have an early 340 series access point on your network, you can eliminate the problem by setting the Maximum Packet Data Length parameter for all other devices to 1400 bytes.
- CSCdz05691—Clients are unable to ping on the same VLAN  
 Clients associated to the same access point that are on the same encrypted VLAN (using LEAP) are unable to ping each other regardless of how the Public Secure Packet Forwarding (PSPF) parameter is set.  
 Workaround—Browse to the **Setup>Security>Radio Data Encryption (WEP)** page and set the Use of Data Encryption field to **Full Encryption**.

- CSCin18914**—IP release or renew not occurring with EAP-TLS+MIC+KH+BWR

When a client associates with EAP-TLS + 40/128 bit broadcast key + MIC +Keyhash + Broadcast WEP key rotation (10sec), and IP ipconfig release or renew commands are issued, the client releases the IP address, never receives it again, and remains EAP authenticated. A ping from the AP to the client reaches the client, but doesn't reveal an IP address. The access point association table shows the IP address for the client as 0.0.0.0.
- CSCdy29556**—Symbol IP phone continuously associates and authenticates to an access point configured with multiple VLANs

When a Symbol IP phone is associated to a VoiP VLAN (Symbol extensions enabled), the phone associates to the access point and is authenticated approximately every 2 seconds. The Symbol phone shows a “No Network” error every 1 to 2 minutes.

It also appears that Symbol phones do not work well when using a non-primary SSID. It is possible that the phone does not perform an active Probe and therefore does not hear information about the SSID it associated with in the beacon, causing it to reassociate and re authenticate.

There is no workaround for this caveat.
- CSCdy79715**—WEP enable issue for 340 series access points

In an AP340 without WEP, the radio gives an error (Fatal) : Failed to start driver for port "awc0" (errno=0x006d0002). The radio in the AP will not start. A symptom of this condition is a fatal error message: Failed to start driver for port "awc0" (errno=0x006d0002).is seen after upgrade of AP firmware.

There is no workaround for this caveat.
- CSCdx81372**—Access point does not accept version 11.21-generated .ini file

If you download the full configuration .ini from an access point running 11.21, upgrade to version 12.00T, and then attempt to download the .ini file from an FTP server, the following error message displays:

```
*** No Such MIB Variable as Specified on Initialization File Line xxx! for the
following variables:
awcAaaServerAccountingEnabled.x,
awcVoIPVlanId, awcVoIPVlanEnabled,
awcPublicVlanId.
*** Bad Value for MIB Variable awcVlanEncapMode Specified on Initialization File Line
xxx (error 13)!
```

Workaround—When producing .ini files, dump a non-default configuration for version 11.21 instead of a full configuration.
- CSCdw89705**—All Ethernet devices behind a client bridge show up as roamed

When a non-root bridge roams from one root bridge to another, messages might appear in the logs of the root bridges stating that Ethernet devices connected to the non-root bridge and wireless client devices associated to the non-root bridge have roamed.

You can ignore these messages.

## Resolved Caveats

The following caveats have been resolved in firmware version 12.00T:

- Resolved: CSCdy13290—Nested repeaters now work with static WEP.
- Resolved: CSCdx22660—Hot Standby now works with LEAP enabled.

# Troubleshooting

For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at <http://www.cisco.com/tac>. In the Tools and Utilities section, Select **Wireless Troubleshooting Center**. The Wireless Troubleshooting Center page appears. Choose the link that best suits your troubleshooting needs.

## Related Documentation

Use the following documents with this document:

- *Quick Start Guide: Cisco Aironet Access Points*
- *Cisco Aironet Access Point Hardware Installation Guide*
- *Cisco Aironet Access Point Software Configuration Guide*
- *Quick Start Guide: Cisco Aironet 350 Series Bridges*
- *Cisco Aironet 350 Series Bridge Hardware Installation Guide*
- *Cisco Aironet 350 Series Bridge Software Configuration Guide*
- *Cisco IOS Solutions Configuration Guide, Version xx.x*
- *Cisco IOS Quality of Service Solutions Command Reference, Version xx.x*
- *Cisco IOS Switching Services Configuration Guide*.
- *Cisco Internetworking Design Guide*.
- *Cisco Internetworking Technology Handbook*
- *Cisco Internetworking Troubleshooting Guide*

## Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

### World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com>

Translated documentation is available at this URL:

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

### Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

## Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:  
[http://www.cisco.com/cgi-bin/order/order\\_root.pl](http://www.cisco.com/cgi-bin/order/order_root.pl)
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:  
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the “Leave Feedback” section at the bottom of the page.

You can e-mail your comments to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

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

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

We appreciate your comments.

## Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages

- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

<http://www.cisco.com>

## Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

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

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

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

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, 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, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, 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. (0705R)

Copyright © 2002, Cisco Systems, Inc.  
All rights reserved.