Fixing a Broken Wireless LAN Connection

Document ID: 30218

Contents

Introduction

This document provides information to help identify and troubleshoot common problems in a wireless LAN in which there is at least one access point (AP) and one or more wireless clients.

Prerequisites

Requirements

Cisco recommends that you have this knowledge:

- A basic understanding of Ethernet, TCP/IP, and LAN connectivity
- Familiarity with and the ability to access the management pages for the device, either through console connection or a web browser

Components Used

The information in this document is based on Cisco Aironet equipment.

Cisco Aironet equipment operates best when you load all the components with the most current version of software. Upgrade to the latest versions of the software early within the troubleshooting process.

Note: You can download the latest software and drivers from Cisco Wireless Downloads.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Problem Definition

A clear understanding of any problem is the first step to find a solution. This applies to networking issues. Networks consist of many pieces that work together to achieve a common goal interconnection. You must understand the contribution that each piece makes to interconnection and the faults that each piece can encounter.

A common approach to troubleshooting is also important. One methodology that this document follows is the Open System Interconnection (OSI) model. This method works layer by layer to locate and resolve the problem and does not skip layers or jump to immediate conclusions.

This document takes a step back in troubleshooting. The document does not simply look at the radio frequency (RF) connections, but also examines the appropriate network components that work together as a whole.

This document looks at two cases of connectivity problems:

- Connectivity Problems AP to Wired LAN
- Connectivity Problems Wireless Client to AP/Base Station (Radio Link)

What Changed?

In order to troubleshoot a wireless LAN that was operational and then stopped, step back and ask, "What changed?"

- Did the firmware in the AP or Base Station Ethernet (BSE) change?
- Did the client drivers change?
- Did you change the firmware or client utilities?

If you upgrade any one part of the client software, such as the Aironet Client Utility (ACU), network driver interface specification (NDIS) driver, or radio firmware, upgrade the other two parts to the revision that was released at the same time. Refer to Cisco Wireless Downloads for the latest software releases.

Connectivity Problems AP to Wired LAN

This document presents this topic on AP−to−wired LAN connectivity problems first because of the hierarchy of the network. Often, RF connectivity between the AP and the client can indeed be fine, but in reality, traffic flows from the client, through the AP, and out to the rest of the network. If there is a problem between the AP and the rest of the LAN, the problem can go unrecognized until clients try to pass traffic through the AP, and not just to the AP.

Filters

If there are any filters that are configured on either the Ethernet side or the radio side of the AP, disable them temporarily, until you resolve the connectivity issue. This disablement helps to determine if the filters contribute to the problem. You can disable filters from the interfaces while the filters remain a part of the configuration. If the filters are long or complex, reenable them in phases in order to isolate the condition that causes the problem. For information about how to enable filters in APs, refer to the Configuring Filters section of Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.

IP Addressing

Although IP addressing is a basic issue, the subject requires comment. If the AP or wireless clients are statically addressed, be sure that the static address is indeed in the same network as the rest of the LAN. The AP communicates with rest of the network through the IP address assigned to the BVI interface. You must be sure that the IP address is numbered similarly and has the same subnet mask. The AP is not a router and does not perform any routing functions. Therefore, never consider the AP the default gateway of a network. Do not configure the IP address of the AP on any device as the default gateway of that device.

In most cases, the AP and clients obtain the IP address through DHCP. If the AP is configured to recieve the IP address through DHCP but does not receive a valid response from the DHCP server, the AP does this:

- Uses a default address of 10.0.0.1
- Reuses the last address that the DHCP server assigned the AP

Thoroughly investigate a failure to receive a dynamic address. Be sure to check:

- That the DHCP server service runs
- That the DHCP scope has not been exhausted
- That other wired clients on the same segment can be successfully addressed dynamically
- The characteristics and configuration of the port on the hub or switch to which the AP is connected
- The cabling between the AP and the switch
- The configuration of the Ethernet interface on the AP
- The Ethernet statistics on the transmit and receive sides of both of these:
    - ♦ The AP
    - ♦ The port on the hub or switch to which the AP connects

  Note: See the Statistical Analysis section of this document for information on how to analyze the Ethernet statistics.

Root Versus Repeater Configuration

In the context of IEEE 802.11 networking and APs, as well as the relevant subset standards, a root device is one that is physically connected to the wired LAN. If an AP is configured to be a repeater, the Ethernet interface on that AP is disabled. This is by design and functions in accordance with standards. If inline power is used, the power connections of the Ethernet interface are not disabled. You can see the status of the

Ethernet port from the Summary Status window of the AP browser interface. When you investigate problems with the connection of an AP to a wired LAN, be sure that the AP is configured with the proper mode, either root or repeater.

An AP that is configured as a root device has these characteristics:

- Accepts association and communicates only with clients and repeaters
- Does not communicate with other root devices
- Can be one of many root devices per RF system

An AP that is configured as a nonroot or repeater device has these characteristics:

- Associates and communicates to a root or another nonroot that is associated to a root
- Accepts association and communicates only with clients and repeaters, if the AP is registered to a root

In the current software versions, the APs configured in Bridge mode also can associate wireless clients. But for normal wireless connectivity, the AP must be configured in Root mode. For more information refer to the Configuring Radio Settings section of Cisco IOS Software Configuration Guide .

Device Configuration

Make sure the switch port to which the AP is connected is configured appropriately. If multiple VLANs are configured on the AP, configure the switch port as a *Trunk port*. If all the wireless clients belong to the same VLAN, you can configure the switch port as an *Access port*. Ensure that the wireless VLANs are allowed on the trunk ports or else the traffic for the VLAN will be not be allowed through the switch. For more information on how to configure the switch, refer to Using VLANs with Cisco Aironet Wireless Equipment.

Port Consideration

Try to match the speed and duplex capabilities as closely as possible. Hard−set values for speed and duplex tend to work better than autonegotiated ones. Give equal attention to the port to which the AP is connected and to the AP Ethernet port. When you hard set the AP to a particular speed and duplex value, hard set the port on the switch or hub to which the AP connects as well. Be cautious when you use unmanageable devices like 10/100−Mbps autosensing hubs. Problems can occur when you mix these two rates in the same hub. The Statistical Analysis section of this document describes conditions in which the port on the hub or switch can be suspect. A change of ports or swap out of the hubs, switches, or cables can be necessary in an effort to isolate the problem.

Physical Connectivity

Physical connectivity is often the point at which to start. Be sure that an AP is connected to a hub or switch with a straight−through cable. If the AP is plugged in to an uplink port or connected directly to an end PC, a cross−over cable is necessary. Use a cable that is at least 1 meter (m) (about 3 feet [ft]) in length. Do not exceed the Ethernet cable−length recommendations in this table:

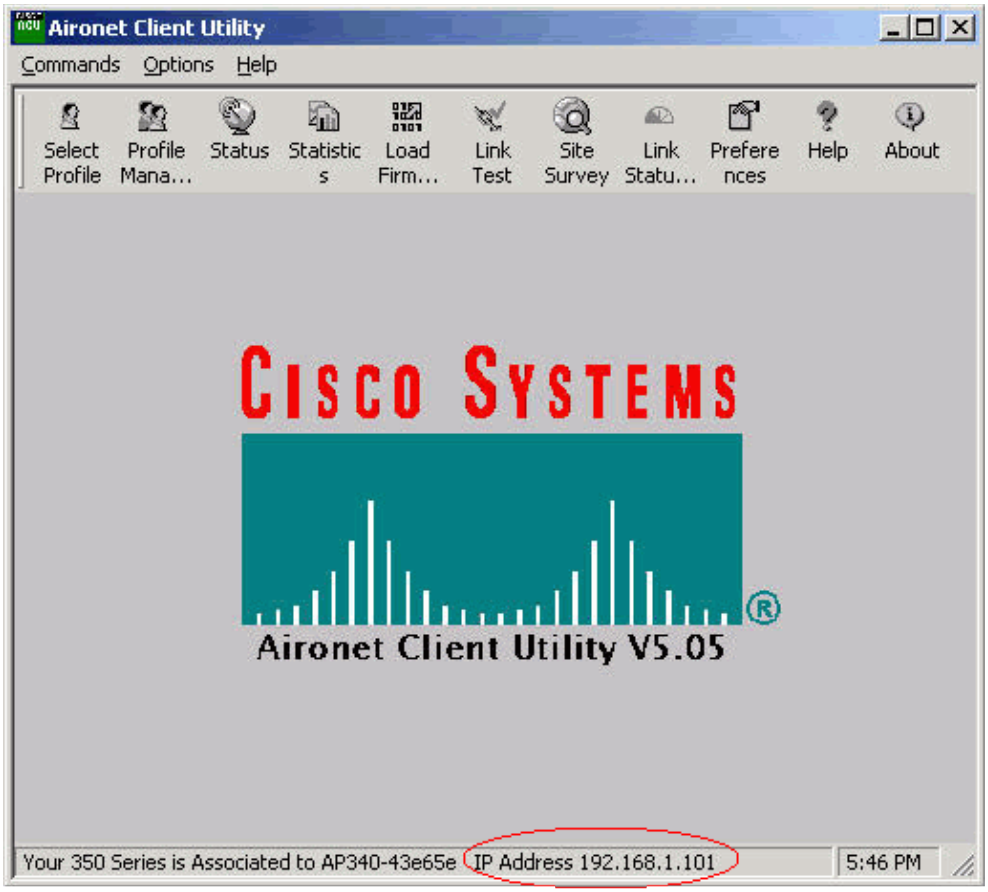
Cable Type	Length
Coax 10BASE−2	185 m/607 ft
Category 5 10BASE−T	100 m/328 ft

Connectivity Problems Wireless Client to AP/Base Station (Radio Link)

When you troubleshoot problems with clients, you must isolate whether the symptom is displayed on a single client or all clients. If the symptoms are the same with all clients, the problem can be the AP configuration or its connection to the wired LAN, rather than the client. If the AP connection to the wired LAN is suspect, you can resolve the problem faster if you spend some time with the Connectivity Problems AP to Wired LAN section of this document.

Association

Determine if the radio link works. The easiest and most common way to make this determination is to open either the ACU, ADU, Base Station Client Utility, or AP management page and see if there is an association to an IP address. This example shows what the ACU looks like:



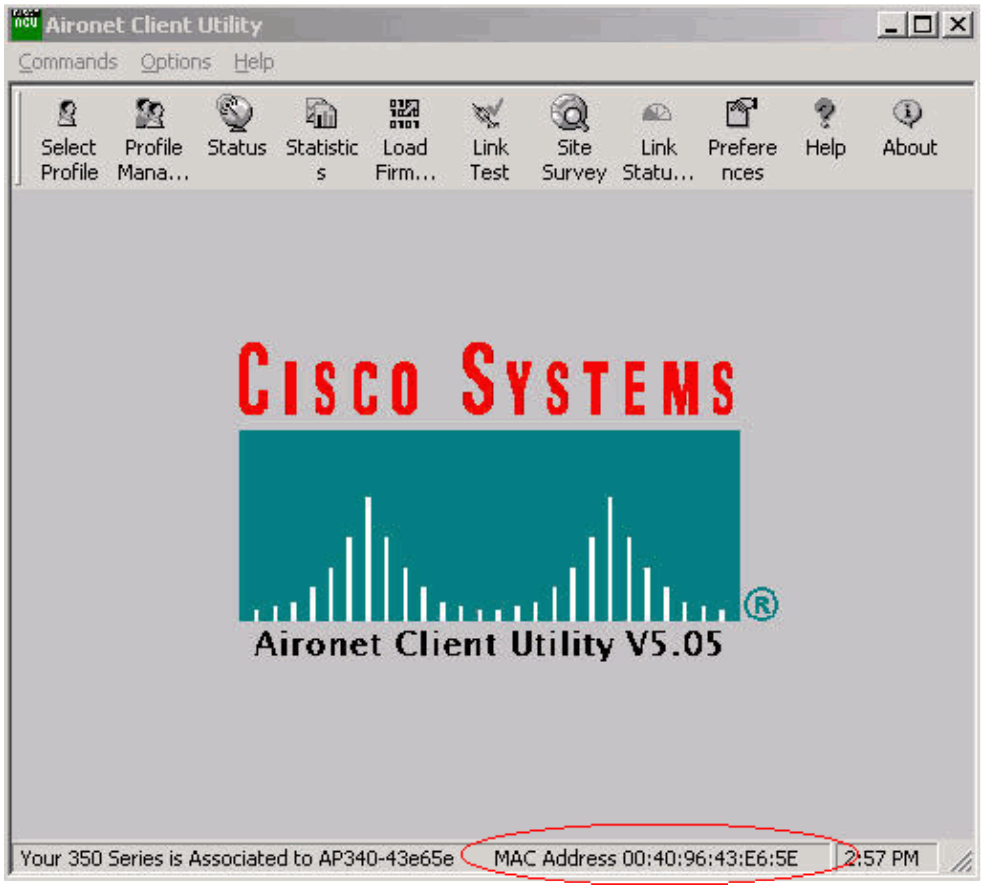
If the client is associated to a MAC address but not an IP address, the most common problem is a mismatch in Wired Equivalent Privacy (WEP) keys. Reconfigure the WEP on both the AP/base station and the client card. Ensure that these match:

- Key value and length
- Key entry method

  The key entry method is either hexadecimal or ASCII.
- Authentication

  Whether open, shared, or Extensible Authentication Protocol (EAP), authentication must be the same.

This is an example of a client that is associated to a MAC address but not an IP address:



Note: For some non−Cisco APs, this window can show the AP as associated to a MAC address. In this case, double check the configuration and move on to perform the IP address check. See the IP Addressing section of this document for the IP address check procedure.

If the client is not associated, be sure to check:

- Any entries in the AP log

  The entries can indicate why the client does not associate.
- Check the signal strength at the client. Good signal strength is essential for proper communication. For good signal strength, you can increase the power level at the AP or change the client location to get associated.

  Note: Too much power on the AP extends the coverage outside the desired area which causes a potential risk of an exposed network.
- That the service set identifier (SSID) that is configured in the client matches the SSID that is configured in the AP

  Check the Express Setup page of the AP browser interface.

Temporarily disable WEP/Light EAP (LEAP)/EAP until you have resolved the connectivity problem. The disablement helps to determine if some portion of authentication contributes to the problem. You can disable authentication from the AP and the client while they remain a part of the configuration. If the authentication is complex, reenable it in phases in order to isolate the aspect of authentication that causes the problem.

RF Issues

A site survey is necessary in order to install a wireless network. Perform the site survey on the actual site under normal operating conditions with all inventory present. Such a survey is critical because the RF behavior varies with the physical properties of the site. You cannot accurately predict the behavior without doing a site survey. You may face intermittent connectivity in certain locations or during certain environmental conditions for example, when a wooden roof is wet after a rain. The intermittent connectivity can indicate that a site survey was not performed or that the site survey did not consider these factors. In order to learn more about site surveys, refer to Wireless Site Survey FAQ.

If a client adapter on a PC with the ACU is used to check the signal strength, run the Site Survey option in ACU at the point of interest.

IP Addressing

Clients can be either statically addressed or dynamically addressed via DHCP. A base station acts as a DHCP server for the wireless network if the base station is in cable, digital subscriber line (DSL), or PPP over Ethernet (PPPoE) mode. The AP does pass DHCP packets from the Ethernet side to the wireless side by default.

If you have a WEP key mismatch, DHCP does not work. See the Connectivity Problems Wireless Client to AP/Base Station (Radio Link) section of this document.

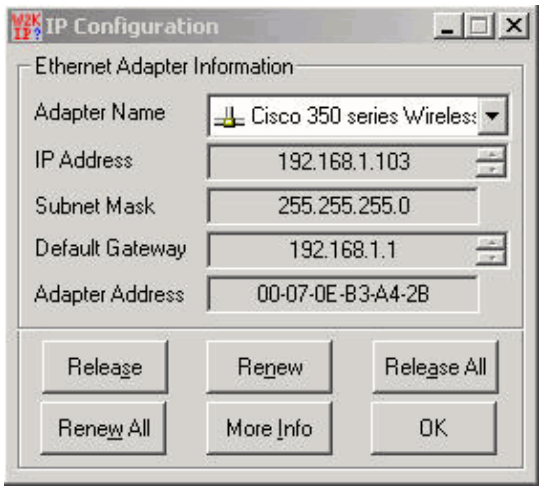
Complete these steps in order to check the IP address on a PC with a Microsoft Windows operating system:

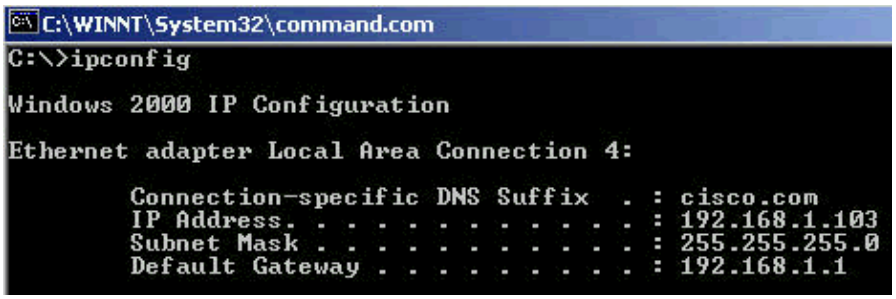
1. Choose **Start > Run** in order to open a command window.
2. Issue the appropriate command (as listed in this step) and click **OK**.

    - Windows ME, Windows 2000, Windows NT, and Windows XP **cmd**
    - Windows 98 and Windows 95 **command**
3. Issue the appropriate command (as listed in this step) in the command window in order to display the IP address.

    - Windows ME, Windows 2000, Windows NT, and Windows XP **ipconfig**
    - Windows 98 and Windows 95 **winipcfg**

    The display that results looks like one of these two examples:





When you have output that is similar to these examples, perform these steps in order to confirm connectivity:

1. Verify that all the fields are complete.

   If not all fields are complete, you can have a problem with your DHCP server. Or if you use a static configuration, there can be something wrong with your IP configuration.
2. Verify that the subnet mask is the same for all the devices on the LAN.
3. Ping the default gateway IP address in order to verify connectivity to your default gateway.

   From the command window, issue the **ping** *x.x.x.x* command.

   Note: In the command, *x.x.x.x* is the IP address of the default gateway.

   If the ping is unsuccessful, see the Connectivity Problems AP to Wired LAN section of this document.
4. Issue the **ping www.cisco.com** command in order to verify connectivity to the Internet.

   If this ping is successful, you have a working connection to the Internet that allows you to browse web pages. If the ping is not successful, there can be a problem with your browser settings. Go on to Step 5.
5. If the ping in step 4 fails, try to ping the IP address 198.133.219.25.

   Note: This is the IP address for Cisco.com.

   If this ping is successful, there is a problem with the Domain Name System (DNS). The most likely problem is that no DNS server is listed. Issue **ipconfig /all** in the command window and verify that at least one DNS server is listed. If no DNS server is listed, check for these items:

   - The DHCP server, if DHCP is used

     The DHCP server should assign a DNS server address.
   - Your Windows IP configuration, if you use a static configuration

If the client does not associate without any authentication configured, analyze the radio statistics on the transmit and receive sides of both the client and the AP. See the Statistical Analysis section of this document for information on analysis of the radio statistics.

Clients do not Receive the IP Address from the DHCP Server

The AP can also be configured as a DHCP server in order to provide the IP addresses to the wireless clients. However, there are times when the AP is configured as a DHCP server that the wireless clients do not get the IP addresses even though the pools of IP addresses are correctly defined. One of the reasons for this is that the interface BVI IP address on the AP and IP address pool defined might not be in the same IP addressing range. If this is the case, use the **ip helper** command on the ethernet interface of the AP in order to point the AP to the DHCP server on the network.

```
ap(config)#interface fastethernet 0
        ap(config-if)ip helper <ip address of the DHCP server>
```

When you configure the AP as a DHCP server, it assigns IP addresses to devices on the subnet. The devices communicate with other devices on the subnet but not beyond it. If data needs to be passed beyond the subnet, you must assign a default router. The IP address of the default router should be on the same subnet as the AP configured as the DHCP server.

Driver and Firmware issues

It is equally important that things are in place on the client side. Complete these checks on the client side:

1. Check if the client is installed properly on the machine. The status of the client card can be checked from the Windows Device Manager screen. Look for the message that reads `This device is working properly`. If it is not present, it indicates that the drivers are not installed properly. Try to uninstall the driver and reinstall the drivers on the machine. In order to uninstall the drivers, right−click the wireless adapter from the Device Manager screen and click Uninstall. For more information on how to reinstall the client adapter, refer to the Installing the Client Adapter section of Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.

   Note: If you use ACU to configure the client card, make sure that the radio is not disabled on the ACU. In addition, check if the status of the card is enabled under Network Connection on the Windows Control Panel.
2. Sometimes the client card is not recognized by the computer. In that case, try the card on a different slot. If it does not work, try it on a different computer. For more information on issues within installation, refer to the Troubleshooting section of Cisco Aironet 340, 350, and CB20A Wireless LAN Client Adapters Installation and Configuration Guide for Windows.
3. If you find connectivity issues only with a single client, upgrade the drivers and firmware of that client. If you find connectivity issues with a majority of the clients and you have ruled out other issues, choose to upgrade the AP.

Indicator LEDs

The indicator lights can sometimes help you determine the status of a device if its integrity is in question. You can check the indicator lights on any of these devices:

- Client adapters
- APs
- Base stations
- Bridges

Refer to the Fixed and Mobile Wireless Solution product documentation for each of the wireless devices in order to find an explanation of the indicator lights.

Statistical Analysis

Refer to Error Statistics on the Cisco Aironet 340 Series Bridge for more details on how to interpret both the wired side and wireless side statistics. Although the title of this document implies otherwise, the interpretation of statistics is the same for either product.

Transmit Statistics

The wired Ethernet side can be full−duplex, but the radio side is not full−duplex. When the radio has a packet to transmit, the radio does not transmit during transmission by another radio on the same channel or same frequency. When this situation occurs, the **HOLDOFFS** statistic counter increments. When the device continues to receive packets in the Ethernet interface but is unable to transmit the packets over the radio interface because of holdoffs, the buffers that are designed to hold the outbound packets fill very quickly. How quickly the buffers fill depends on the traffic flow and volume. When the buffers overflow, the excess packets are discarded, and the **QUEUE FULL DISCARDS** statistic counter increments. Messages can display on the console of the AP or in the error log.

When the radio of a device transmits a packet, the receiving device must send an acknowledgment back to the transmitting device. Then, the transmitting device can move on to the next packet in its transmit queue. If the transmitting device does not receive the acknowledgment, the device transmits that same packet again, until it receives an acknowledgment from the receiving device. When a device transmits the same packet more than once, the **RETRIES** statistic counter increments. When this occurs, you can assume either one of these two cases:

- The receiving device did not send the acknowledgment.
- The receiving device sent the acknowledgment, but the acknowledgment was not received by the transmitting device. Therefore, the transmitter resent the packet.

These statistics do not essentially indicate a failure of the physical hardware.All these statistics indicate a problem with the quality of the RF link between the AP and the client. For more information on how to establish a good RF link refer to the RF Issues section of Troubleshooting Client Issues in the Cisco Unified Wireless Network.

Receive Statistics

When the radio of a device successfully receives a packet, the device sends an acknowledgment back to the transmitting device. Then, the transmitting device can move on to the next packet in its transmit queue. If the transmitting device does not receive the acknowledgment, the device transmits the same packet again, until it receives an acknowledgment from the receiving device. When a device receives the same packet more than once, the **DUPLICATE FRAMES** statistic counter increments. When this occurs, you can assume either one of these two cases:

- The receiving device did not send the acknowledgment.
- The receiving device sent the acknowledgment, but the acknowledgment was not received by the transmitting device. Therefore, the transmitter resent the packet.

After the radio of a device successfully receives a packet and successfully sends the acknowledgment, the device then checks the packet for accuracy. The device calculates a cyclic redundancy check (CRC) value for the packet and compares this CRC value to the CRC value that is contained in the packet. If the calculated value does not match the value that is contained in the packet, the packet is discarded and the **CRC Errors** statistic counter increments. The presence of CRC errors does not necessarily indicate a hardware problem with the device; the device did not corrupt the packet when it simply received it. Most often, a nonmatching CRC value is calculated for one of these reasons:

- The packet becomes corrupt in transit due to interference and noise in the RF environment.
- The originating device miscalculates the CRC value during the initial build of the packet.

In either case, the receiving device simply calculates a CRC value on the packet that the device receives. Refer to Error Statistics on the Cisco Aironet 340 Series Bridge for additional information about what the

error statistics show and how to correct the errors.

Additional Troubleshooting Help

For additional assistance in troubleshooting connectivity problems, create a service request with Cisco Technical Support. Use the TAC Service Request Tool (registered customers only) . You can also contact Cisco Technical Support by telephone at 800 553−2447. Include the information in this list with your online case, or have the information available when you call:

- The serial number of each device that is involved
- The model number of each device that is involved
- The firmware version of each device that is involved
- A brief description of the topology of your wireless LAN

Related Information

- **Wireless Site Survey FAQ**
- **Troubleshooting BR350 Bridges**
- **Intermittent Connectivity Issues in Wireless Bridges**
- **Troubleshooting Client Issues in the Cisco Unified Wireless Network**
- **Wireless Support Page**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 19, 2009 Document ID: 30218