

Troubleshooting Connectivity in a Wireless LAN Network

Document ID: 8117

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

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Basic Connectivity Issues

- Console Connection
- Cable
- Radio Power Optimization
- Radio Interference
- IP Address Assignment
- Effect of Loopback Interfaces on APs
- No Image in AP Flash
- Booting Issues with the AP
- Power Issue with the AP
- Use of Nonoverlapping Channels
- IOS Upgrade

Client Adapter

- Resource Conflict
- Indicator LEDs
- Verify Client Communications

Access Points

- Root Mode
- Indicator LEDs
- SSID
- VLAN in a Multi-SSID Configuration
- WEP Keys
- Reset
- Firewall Is Enabled on the Client
- Configuration of Data Rates on the AP Radio
- Configuration of Radio Preambles
- Antenna Settings

Bridge

- Indicator LEDs
- SSID
- WEP Keys
- Line of Sight and Fresnel Zone
- Spanning Tree Protocol

Related Information

Introduction

This document helps identify and troubleshoot common connectivity problems in configuration, interference, and cable in a wireless network.

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

You can download the latest software and drivers from the Cisco Wireless Software Center (registered customers only) .

This document complements the information in Fixing a Broken Wireless LAN Connection.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

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

Basic Connectivity Issues

Console Connection

Use a straight-through DB-9 male/female cable for console connection.

In a terminal program like Microsoft HyperTerminal, set the session to:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit
- Xon/Xoff flow control

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

Cable

If you have intermittent connectivity or connectivity with errors, there is a possibility that the cable length is greater than the recommended Ethernet segment length. Do not exceed the Ethernet cable length that is recommended in this table:

| Cable Type | Length |
|------------|--------|
|------------|--------|

| | |
|---------------------|---------------------|
| Coax 10BASE-2 | 185 meters/607 feet |
| Category 5 10BASE-T | 100 meters/328 feet |

If the distance from the switch exceeds the recommended segment length, use a fiber or a wireless hop, such as a repeater.

Interference occurs when you run a network cable near high-power equipment. This interference is especially common when you run the cables in warehouses and factories.

When you have interference because of cable length, and a cable tester shows a positive result, use the cable tester only to find a break in the cable. In order to verify the presence of a cable problem, test the connection to the access point (AP) or bridge with a shorter cable. Then, verify if the problem is still there.

Radio Power Optimization

When you install the AP and the clients associated to it are too close, sometimes the clients disconnect from the AP. This problem can be solved by these two methods:

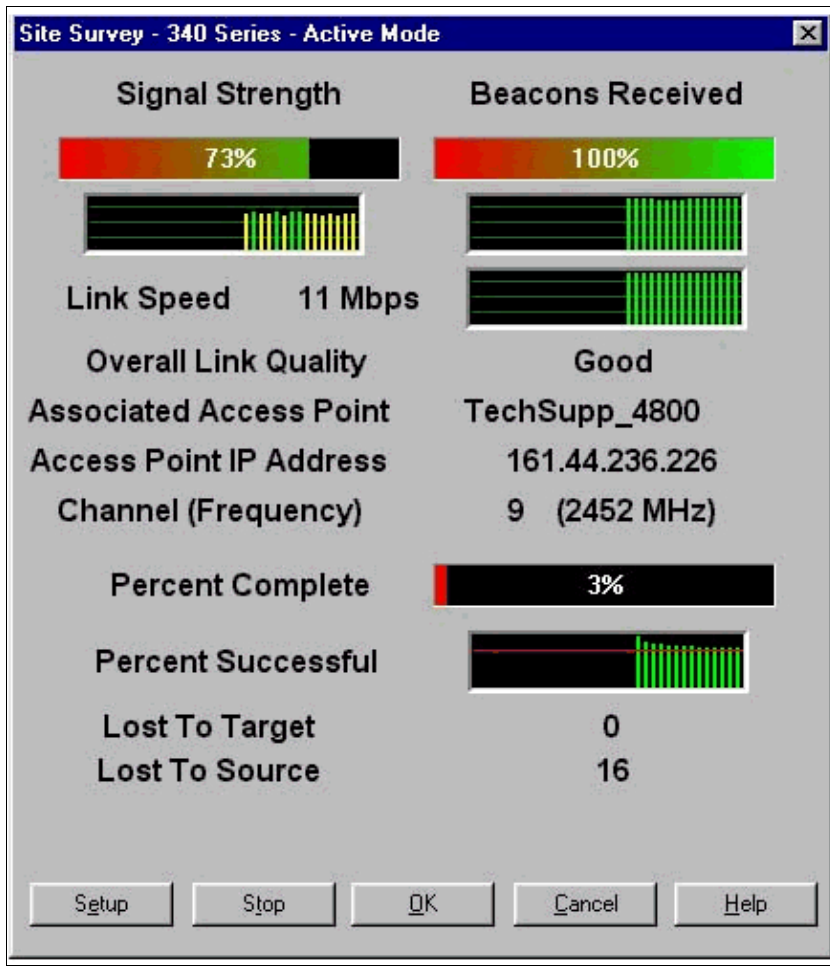
- Keep the clients away from the AP.
- Reduce the power of the AP.

Radio Interference

You must conduct a site survey in order to install a wireless network. Conduct the site survey on the actual site under normal operating conditions with all inventory present. Such a survey is critical because the radio frequency (RF) behavior varies with the physical properties of the site, and you cannot predict the behavior accurately without a site survey. You can face intermittent connectivity at certain areas and during certain environmental conditions. An example is when a wooden roof is wet after a rain. In this case, perhaps a site survey was not done, or a bad site survey did not consider these factors.

If you use a client adapter on a PC with the Aironet Client Utility (ACU) or the Aironet Desktop Utility (ADU), in order to check the signal strength, run the Site Survey option in ACU. Remember that construction materials, such as steel and wood, absorb RF energy as do objects with water content. Consider interference from devices such as microwave ovens and cordless phones when you place the APs.

This window is an example of the signal strength test:



Perform the carrier test in order to see activity in the RF spectrum. The carrier test is available on bridges. The test enables you to view the radio spectrum. This example shows the carrier test on the BR500:

```
Aironet BR500E V8.24          CARRIER BUSY / FREQUENCY
TechSupp_4800

*
*
*  *
*  *  *
*  *  *
*  *  *
*  *  *  *
*  *  *  *
*  *  *  *  *
*  *  *  *  *  *
*  *  *  *  *  *  *
1 1 2 2 3 3 4 4 5 5 6
2 7 2 7 2 7 2 7 2 7 2

Highest point = 35% utilization

Enter space to redisplay, q[uit] ::
```

The numbers 12, 17, and so on represent the 11 frequencies that the bridge uses. For example, 12 represents the frequency 2412 MHz. The asterisks (*) indicate the activity on each frequency. Whenever possible, choose the frequency with the least activity in order to reduce chances of interference.

IP Address Assignment

If you cannot ping the AP or the bridge, check the IP addresses that are assigned to the AP, bridge, and client adapter. Make sure that they are in the same subnet.

For example, if the IP address of the AP is 10.12.60.5 with a mask of 255.255.255.0, verify that the IP address of the client adapter is similar to 10.12.60.X with a mask of 255.255.255.0. Remember that the AP and the bridge are Layer 2 devices. If you need two or more networks, make sure you have a router on the network.

Refer to the IP Subnet Calculator (registered customers only) tool for more help with IP addresses and the design of subnets.

Effect of Loopback Interfaces on APs

Aironet APs and bridges do not support the configuration of loopback interfaces. Even though the command-line interface (CLI) allows you to create a loopback interface, avoid the configuration of loopback interfaces on APs and bridges. The reason is that a loopback interface configuration can generate an Inter-AP Protocol General Information (IAPP GENINFO) storm on your network, which can result in high CPU utilization on the AP. This can slow down the performance of the AP drastically and, in some cases, disrupt network traffic completely. The configuration of loopback interfaces on APs or bridges can also cause memory allocation failures.

Refer to the *Access Points Do Not Support Loopback Interface* section of Release Notes for Cisco Aironet Access Points for Cisco IOS Release 12.3(7)JA2 for more information.

No Image in AP Flash

In some instances, if the AP flash is completely erased, the AP does not have a Cisco IOS® image to boot and gets stuck in **ap:** prompt mode. In order to recover the AP in this situation, reload a new Cisco IOS image on the AP. Refer to the instructions in the *Using the CLI* section of Troubleshooting (Cisco IOS Software Configuration Guide for Aironet APs 12.3(7)JA).

Booting Issues with the AP

In some cases, the AP fails to boot completely. This failure can happen if the firmware on the AP is corrupt. In order to resolve this issue, reinstall the firmware on the AP. You can reload the AP image in order to reinstall the firmware. Refer to the instructions in the *Using the CLI* section of Troubleshooting (Cisco IOS Software Configuration Guide for Aironet APs 12.3(7)JA) in order to reload the firmware.

Power Issue with the AP

When an AP uses a power injector as the power source, in some cases, the AP displays this error message:

```
%CDP_PD-2-POWER_LOW: All radios disabled - LOW_POWER_CLASSIC inline
```

This message indicates that the AP is in low-power mode with all radios disabled and detects a Cisco switch that is unable to supply sufficient power to the AP. Even though the power injector, which can provide sufficient power, is connected with the AP, the AP still displays a LOW POWER error message and disables the radios. Therefore, the AP remains in low-power mode.

One possible reason for this issue might be that the AP supports the Intelligent Power Management feature. The Intelligent Power Management feature uses Cisco Discovery Protocol (CDP) to allow powered devices, such as an AP, to negotiate with a Cisco switch for sufficient power. The AP supports the Intelligent Power

Management feature. As a result of the power negotiations, the AP either enters full-power mode or remains in low-power mode with the radios disabled.

In this case, the AP might be connected to a switch which cannot provide the necessary power to the AP. Therefore, even though the power injector is connected to the AP that uses this Intelligent Power management feature, it gives priority to the CDP information to identify whether or not the switch can provide the power. Once the AP knows, via CDP message, that the switch does not provide sufficient power, it disables the radios and remains in low-power mode.

The workaround to this issue is to tell the AP to ignore the CDP information for power. You can perform this by telnetting into the APs. Issue these commands to enable the APs to use the power injector:

- **power inline negotiation prestandard source**
- **power inline negotiation injector H.H.H**

The **power inline negotiation** command configures the Cisco Aironet 1130AG or 1240AG Series AP to operate with a later version of switch software that does not support Cisco Intelligent Power Management power negotiations.

The **prestandard source** portion of the command specifies that the Cisco switch runs a later version of software that does not support Intelligent Power Management negotiations, but is able to supply sufficient power to the AP.

The **injector H.H.H** portion of the command specifies that a power injector supplies power to the AP, and that the AP connects to a new switch port with the indicated MAC address (H.H.H). Enter the MAC address (in xxxx.xxxx.xxxx hexadecimal format) of the new switch port where the power injector is connected.

Note: This command should only be used when you move an AP and power injector to a different switch port.

The AP can be powered from the 48-VDC power module or from an inline power source. The AP supports these features for inline power sources:

- IEEE 802.3af power standard
- Cisco prestandard Power over Ethernet (PoE) protocol
- Cisco Intelligent Power Management

For full operation, the AP requires 12.95 W of power. The power module and Aironet power injectors are able to supply the required power for full operation, but some inline power sources are not able to supply 12.95 W. Also, some high-power inline power sources cannot provide 12.95 W of power to all ports at the same time.

Use of Nonoverlapping Channels

When you have multiple APs in a wireless LAN (WLAN), ensure that the channels that the adjacent APs use are nonoverlapping. Nonoverlapping channels are frequency bands that do not have a frequency that is common to the other channels. For example, in the 2.4-GHz range, there are three channels that do not overlap (channels 1, 6, and 11). Therefore, when you deploy a secondary AP in order to extend the radio coverage, you can use:

- Channel 1 for the first AP
- Channel 6 for the next adjacent AP
- Channel 11 for the third AP

Then you can start with channel 1.

If you use channels that overlap, RF interference can occur. This leads to connectivity issues and results in poor throughput. Refer to Troubleshooting Problems Affecting Radio Frequency Communication for more information on RF interference.

IOS Upgrade

When you upgrade Cisco IOS on an AP from a previous version to 12.3(7)JA3, the most common problem is that the client does not authenticate properly. This is because the service set identifier (SSID) is no longer on the radio interface. The first step is to reconfigure the SSID, then remove the Encryption. If it still does not work, then reconfigure the AP from scratch. Complete these steps:

1. Choose **SECURITY > Encryption Manager**.
2. Click **None** and then **Apply**.
3. Go to the SSID Manager, highlight the SSID **SSID_Name** and choose **<NO ADDITION>**.
4. From the Open Authentication menu, scroll down and click **Apply**.

Once you have applied these changes, you can test with the client adapter. If the problem still exists, then it is better to start from scratch.

5. Complete these steps in order to reset the AP back to default:
 - a. Choose **System Software > System Configuration**.
 - b. Click **Reset to Defaults** (Except IP).

Once it reboots, you can reconfigure it again and test with the client adapter.

Client Adapter

Resource Conflict

If the client adapter card does not communicate, determine if there are any resource conflicts with other devices. Make sure that the card is set at interrupt request (IRQ) levels that other devices do not use. Microsoft Windows 95, 98, ME, and 2000 are plug and play, therefore no resource conflicts should exist.

If a conflict does exist, go to the Windows Device Manager Properties window and uncheck the **Use Automatic Settings** check box. Enter the IRQ and I/O address manually. If there is a resource conflict, you must manually set Windows NT, as the procedure in this section explains.

Note: You can also choose to disable the IR port with use of the Windows Device Manager.

Complete these steps in order to identify the free resource in Windows NT:

1. Choose **Start > Programs > Administrative Tools (Common) > Windows NT Diagnostics**.
2. Click the **Resources** tab in the Windows NT Diagnostics window.
3. Note the IRQ column and check which IRQ numbers are not listed in the Resources window.
4. Choose **I/O Port** in the Resources window.
5. Note the Address column and make note of several different open addresses in the Resources window.

The card needs 64 contiguous I/O addresses, for example, 0100 through 013f hexadecimal.

Complete these steps in order to set the correct values in Windows NT:

1. Choose **Start > Settings > Control Panel**.
2. Double-click the **Network** icon in the Control Panel window.

3. Click the **Adapters** tab in the Network window.
4. Choose **Aironet Adapter** in the Adapters panel.
5. Click **Properties**.
6. Choose **Interrupt** in the Property column panel in the Adapter Setup window.

In the Value column, select an IRQ value that is not listed in the Resources tab of the Windows NT Diagnostics window.

7. Choose the **I/O Base Address** in the Property column panel in the Adapter Setup window.

In the Value column, select an I/O address that is not listed in the Resources window of the Windows NT Diagnostics window.

8. Click **OK** in the Adapter Setup window, click **OK** in the Network window, and then close all open windows and do an orderly shutdown of Windows.

If the client adapter still shows errors, try another I/O address. Windows NT 4.0 does not always report used resources. It can report that a resource is available when it is not.

Indicator LEDs

Check the status of the Aironet 340 Series Client Adapter LED in order to verify if it matches the device configuration.

The client adapter shows messages and error conditions through two LEDs:

- **Link Integrity/Power LED (green)** This LED lights when the client adapter receives power and blinks slowly when the adapter is linked with the network.
- **Link Activity LED (amber)** This LED blinks when the client adapter receives or transmits data and blinks quickly to indicate an error condition.

Refer to this table in order to determine the condition that a specific LED message indicates:

| Green LED | Amber LED | Condition |
|----------------------------------|----------------|---|
| Off | Off | Client adapter does not receive power or an error occurs. |
| Blinks quickly | Blinks quickly | Power is on, self test is OK, and client adapter scans for a network. |
| Blinks slowly | Blinks quickly | Client adapter associates to an AP. |
| Continuously on or blinks slowly | Blinks | Client adapter transmits or receives data while it associates to an AP. |
| Off | Blinks quickly | Client adapter is in power save mode. |
| On | Blinks quickly | Client adapter is in ad-hoc mode. |
| Off | On | Driver is installed incorrectly. |

| | | |
|-----|---------------------|-------------------------------|
| Off | Blinks in a pattern | Indicates an error condition. |
|-----|---------------------|-------------------------------|

Verify Client Communications

Use these methods in order to verify that the card communicates with the AP:

- Check the AP Association table through the console window.
- Use the ACU diagnostic and configuration utility in order to verify that the card associates with the AP.



If the card associates with an AP but does not talk to the network, check the Ethernet side to see if the AP talks properly to the LAN. Use the ping option in the AP to ping the device on the LAN.

Note: There is a possibility that the problem is an outdated driver. Refer to *Upgrading VxWorks Firmware from the Console (Aironet 340 Series)* for more information.

Access Points

Root Mode

Check the root mode in order to verify that it is set appropriately on the AP.

An AP that is configured as a *root* device:

- 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:

- Associates and communicates to a root or another nonroot that is associated to a root.
- Accepts association and communicates only with clients and repeaters, as long as it is registered to a root.

Indicator LEDs

The indicator lights of the Aironet 340 Series AP have these purposes:

- The Ethernet indicator signals traffic on the wired LAN or Ethernet infrastructure. This indicator blinks green when a packet is received or transmitted over the Ethernet infrastructure.
- The status indicator signals operational status. This indicator blinks green in order to indicate that the AP operates normally but does not associate with any wireless devices. Steady green indicates that the AP associates with a wireless client.

A repeater AP that blinks 50 percent on and 50 percent off indicates that it does not associate with the root AP. A repeater AP that blinks 7/8 on and 1/8 off indicates that it associates with the root AP, but no client devices associate with the repeater. A repeater AP that blinks green steadily indicates that it associates with the root AP, and that client devices associate with that repeater.

- The radio indicator blinks green in order to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the AP radio.

This table helps you determine the condition that a specific LED message indicates:

| Message Type | Radio | Status | Infrastructure | Meaning |
|--------------------|--------------|--------------|----------------|---|
| Association status | Indicator | Indicator | Indicator | At least one wireless client device associates with the unit. |
| | | Blinks green | | |
| Operational | Blinks green | Steady green | | No client devices associate. Check the SSID ¹ and WEP ² settings of the unit. |
| | | Steady green | Blinks green | Transmits/receives packets over Ethernet. |
| | Blinks amber | Steady green | | Maximum retries or buffer full occur on the radio. |
| Error/warning | | Steady green | Blinks amber | There are transmit/receive errors. |
| | | | Blinks red | Ethernet cable disconnects. |
| | | Blinks amber | | This is a general warning. |
| Failure | Steady red | Steady red | Steady red | Indicates a firmware failure. Disconnect power from the unit and |

| | | | | |
|------------------|--|--------|--|------------------------------|
| | | | | reapply power. |
| Firmware upgrade | | Steady | | The unit loads new firmware. |

¹ SSID = service set identifier.

² WEP = Wired Equivalent Privacy.

SSID

Wireless clients that attempt to associate with the AP must use the same SSID as the AP. The default SSID is *tsunami*.

Allow "Broadcast" SSID to Associate?

The Allow "Broadcast" SSID to Associate? setting allows you to choose whether devices that do not specify an SSID are allowed to associate with the AP. Devices that do not specify an SSID "broadcast" in search of an AP with which to associate.

- **Yes** This is the default setting. It allows devices that do not specify an SSID to associate with the AP.
- **No** Devices that do not specify an SSID are not allowed to associate with the AP. The SSID that the client device uses must match the SSID of the AP.

If you have communication problems and the device is set to **No**, change the setting to **Yes** and see if the device can communicate. Leave the setting as **Yes** for the duration of this troubleshoot.

Usage of the mobility network-id Command

Connectivity problems in a WLAN network can occur if you use the **mobility network-id** command incorrectly. You use the **mobility network-id** command in order to configure Layer 3 mobility in a wireless network. This command is meant to be used when the AP participates in a wireless domain services (WDS) infrastructure with a WLAN services module (WLSM) (that acts as the WDS device) where there is Layer 3 mobility.

Therefore, when an AP is configured as a WDS device, do not use the **mobility network-id** command.

If you use this command incorrectly, connectivity problems in the WLAN network result, such as:

- Clients do not get IP addresses from the DHCP.
- Clients cannot associate with the AP.
- A wireless phone cannot be authenticated when you have a voice-over WLAN deployment.

VLAN in a Multi-SSID Configuration

In some cases, when you configure VLANs in a multi-SSID setup, the interfaces on the AP and switch show that trunking is up and running. However, the Layer 3 interface on the switch cannot ping the AP. Also, the AP cannot ping the switch interface. In order to resolve this issue, issue the **bridge-group 1** command under the radio interface and the Fast Ethernet interface. This command ties the native VLAN to the **bvi** interface. Then, issue the **bridge 1 router ip** command in the global configuration mode.

WEP Keys

You must set up the WEP key that you use to transmit data in exactly the same way on your AP and on any wireless devices that the AP associates.

For example, if you set WEP Key 3 on your WLAN adapter to 0987654321 and select this key as the transmit key, you must also set WEP Key 3 on the AP to the same value. However, the AP does not need to use Key 3 as the transmit key. Check the WEP key.

These are some points to remember about WEP keys:

- Open authentication allows authorization and associations with or without a WEP key.
- If a WEP key is used, both the client and the AP must have WEP keys that match.
- If one of these devices does not have a WEP key that matches, data traffic cannot be passed because the data is encrypted.

Do not use the WEP key to verify that the problem persists. Leave the WEP key inactive until you identify the connectivity problem.

Reset

Sometimes the problem with misconfigured SSIDs or WEP keys is difficult to identify. For example, the WEP key can have one digit that is mistyped. In order to overcome such problems, note the configurations and reenter them after a reset.

Firewall Is Enabled on the Client

If you try to access the AP via a PC client with a firewall enabled, you might have to disable the firewall. Otherwise, you cannot log in to the AP.

Configuration of Data Rates on the AP Radio

The data rate setting on the AP radio defines the rate at which the AP transmits information. Radio data rates are expressed in Mbps.

On APs, you can set the data rates to any one of these three states:

- **Basic** This allows transmission at this rate for all packets, both unicast and multicast. You must set the data rates of at least one of the wireless devices to Basic. In the GUI, this state is called **Require**.
- **Enabled** The wireless device transmits only unicast packets at this rate. Multicast packets are sent at one of the data rates that are set to Basic.
- **Disabled** The wireless device does not transmit data at this rate.

The wireless device always attempts to transmit at the highest data rate that is set to Basic. If there are obstacles or interference, the wireless device steps down to the highest rate that allows data transmission.

These data rates are supported on an IEEE 802.11b, 2.4 GHz radio:

- 1 Mbps
- 2 Mbps
- 5.5 Mbps
- 11 Mbps

These data rates are supported on an IEEE 802.11g, 2.4 GHz radio:

- 1 Mbps
- 2 Mbps
- 5.5 Mbps
- 6 Mbps
- 9 Mbps
- 11 Mbps
- 12 Mbps
- 18 Mbps
- 24 Mbps
- 36 Mbps
- 48 Mbps
- 54 Mbps

These data rates are supported on an IEEE 802.11a, 5 GHz radio:

- 6 Mbps
- 9 Mbps
- 12 Mbps
- 18 Mbps
- 24 Mbps
- 36 Mbps
- 48 Mbps
- 54 Mbps

When you configure the AP radio, you must consider the type of clients that are present in the wireless network. If the AP has an 802.11g radio and the WLAN has only 802.11g clients, you can set one or more data rates to Basic and all other data rates to Enabled.

However, if you have a mixed environment of both 802.11b and 802.11g clients in a WLAN network, you must ensure that only the rates that 802.11b supports are set to Basic (or Require in GUI). If data rates that the 802.11b radio does not support (such as 12 Mbps) are set to Basic on the AP radio, the 802.11b clients are not able to associate to the AP.

Alternatively, you can configure the AP radio to select data rates on the basis of range or throughput. When you configure the AP radio to select data rates for range, the AP sets the lowest data rate to Basic and the other rates to Enabled. In this way, the AP can cover a wider area. However, the data rate comes down as the distance from the AP to the client increases. If you configure the AP radio for throughput, the AP sets all data rates to Basic. This configuration ensures a consistent throughput throughout the coverage area.

Refer to the *Configuring Radio Data Rates* section of *Configuring Radio Settings* for more information on how to configure the data rates on the AP radio.

Configuration of Radio Preambles

The radio preamble, which is sometimes called a header, is a section of data at the head of a packet that contains information that the wireless devices (which include wireless clients) need when they send and receive packets. Radio preambles can be either short preambles or long preambles.

If you configure the radio preambles incorrectly, the client is not able to associate with the wireless AP. The radio preamble configuration is dependent on the client cards that are used in the wireless network. Aironet WLAN Client Adapters support short preambles. Early models of the Aironet WLAN Adapter (PC4800 and PC4800A) require long preambles. If these client devices do not associate to the wireless devices, you should

not use short preambles.

Refer to the *Disabling and Enabling Short Radio Preambles* section of Configuring Radio Settings for information on how to configure the radio preambles on the AP.

Antenna Settings

The dual antenna ports on the AP are used for diversity. You only need to connect an antenna to the primary (right) port for radio operations. The left port is not used independently of the primary port. Once you connect the external antenna to either the right or left antenna port of the AP, you must configure the AP to transmit and receive on that specific port. The default is for antenna diversity. This helps the radio compensate for errors due to RF interference. Any antenna adapters used must have the matching impedance of the antenna cable and the AP.

Bridge

There can only be one bridge with the root on in an RF network. Set all other bridges to root off.

Indicator LEDs

The indicator lights of an Aironet 340 Series Bridge have these purposes:

- The Ethernet indicator signals traffic on the wired LAN or Ethernet infrastructure. This indicator blinks green when a packet is received or transmitted over the Ethernet infrastructure.
- The status indicator signals operational status. This indicator blinks green in order to indicate that the bridge operates normally but does not communicate with an AP. Steady green indicates that the bridge communicates with an AP.
- The radio indicator blinks green in order to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the bridge radio.

This table helps you determine the condition that a specific LED message indicates:

| Message Type | Radio | Status | Infrastructure | Meaning |
|--------------------|--------------|------------------------|----------------|---|
| Association status | Indicator | Indicator Steady green | Indicator | Linked to the WLAN. |
| | | Blinks green | | Not linked to the WLAN. Check the SSID and WEP settings of the unit. |
| Operational | Blinks green | Steady green | | Transmits/receives radio packets. |
| | | Steady green | Blinks green | Transmits/receives packets. |
| | Blinks amber | Steady green | | Maximum retries or buffer full occur on the radio. The AP with which the bridge |

| | | | | |
|------------------|------------|--------------|--------------|---|
| | | | | communicates might be overloaded, or radio reception might be poor. Change the SSID of the bridge in order to communicate with another AP, or reposition the bridge in order to improve connectivity. |
| Error/warning | | Steady green | Blinks amber | There are transmit/receive errors. |
| | | | Blinks red | Ethernet cable disconnects. |
| | | Blinks amber | | This is a general warning. |
| Failure | Steady red | Steady red | Steady red | Indicates a firmware failure. Disconnect power from the unit and reapply power. |
| Firmware upgrade | | Steady red | | The unit loads new firmware. |

SSID

The SSID of the bridge must match the SSID of an Aironet AP on your WLAN. The AP must be within radio range of the bridge.

WEP Keys

You must set up the WEP key that you use to transmit data in exactly the same way on your AP and on your bridge.

For example, if you set WEP Key 3 on your bridge to 0987654321 and choose this key as the transmit key, you must also set WEP Key 3 on the AP to exactly the same value.

Line of Sight and Fresnel Zone

For long-distance communications, consider the Fresnel zone in addition to line of sight (LOS). The Fresnel zone is an elliptical area that immediately surrounds the visual path. This area varies depending on the length of the signal path and the frequency of the signal. Take into account the Fresnel zone calculating property when you design a wireless link. You overcome the Fresnel effect when you raise the antenna height. The distance calculation spreadsheet gives the height of the antenna for the given radio distance and with no obstruction. You can calculate the maximum radio distance for a given antenna and cable length with the

Antenna Calculation Spreadsheet (in Microsoft Excel format).

Spanning Tree Protocol

Verify if Spanning Tree Protocol (STP) blocks the bridge. There can be a leased line or an alternate path between the points that is bridged by the RF network. There is a possibility that STP put one of the links in the block mode in order to avoid loops.

Related Information

- [Cisco Wireless Software Center \(registered customers only\)](#)
 - [Fixing a Broken Wireless LAN Connection](#)
 - [Cisco Wireless LAN](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

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

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jul 11, 2007

Document ID: 8117
