CHAPTER 18

Wireless Device Troubleshooting

This chapter provides troubleshooting procedures for basic problems with the wireless device. For the most up-to-date, detailed troubleshooting information, refer to the Cisco TAC website at the following URL (select **Top Issues** and then select **Wireless Technologies)**:

http://www.cisco.com/tac

Checking the LED Indicators

If your wireless device is not communicating, check the LED indicators to quickly assess the device status. The indicator signals on the wireless device have the following meanings (for additional details refer to Table 18-1):

- The Ethernet indicator signals traffic on the wired LAN. This indicator is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The indicator is off when the Ethernet cable is not connected.
- The status indicator signals operational status. Steady green indicates that the wireless device is associated with at least one wireless client. Blinking green indicates that the wireless device is operating normally but is not associated with any wireless devices.
- The radio indicator blinks green to indicate radio traffic activity. The light is normally off, but it blinks whenever a packet is received or transmitted over the wireless device radio.

Table 18-1 Indicator Signals

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test.
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS software.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the wireless device SSID and WEP settings.

Table 18-1 Indicator Signals (continued)

Message type	Ethernet indicator	Status indicator	Radio indicator	Meaning
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	–	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failures	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
	Blinking red	–	–	Hardware failure. The wireless device must be replaced.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the wireless device does not communicate with client devices, check the areas described in this section.

SSID

Wireless clients attempting to associate with the wireless device must use the same service set identifier (SSID) as the wireless device. If a client device SSID does not match the SSID of an wireless device in radio range, the client device will not associate. The wireless device default SSID is *tsunami*.

WEP Keys

The Wired Equivalent Privacy (WEP) key you use to transmit data must be set up exactly the same on the wireless device and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must set WEP Key 3 on the wireless device to exactly the same value. The wireless device does not need to use Key 3 as its transmit key, however.

Security Settings

Wireless clients attempting to authenticate with the wireless device must support the same security options configured in the wireless device, such as Extensible Authentication Protocol (EAP) or Light Extensible Authentication Protocol (LEAP), MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a wireless client is unable to authenticate with the wireless device, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the wireless device settings.

Note The wireless device MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the wireless device radio.

Resetting to the Default Configuration

If you forget the password that allows you to configure the wireless device, you may need to completely reset the configuration.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID. The default username and password are both **Cisco**, which is case-sensitive.

Using the CLI

Follow the steps below to delete the current configuration and return all wireless device settings to the factory defaults using the CLI.

Step 1 Open the CLI using a Telnet session or a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power from and reapplying power to the router.

Step 3 Let the wireless device boot until the command prompt appears and the wireless device begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...###########################################################################
################################################################################
################################################################################
####################
```

Step 4 At the ap: prompt, enter the **flash_init** command to initialize the flash.

```
ap: flash_init
Initializing Flash...
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
...done initializing Flash.
```

Step 5 Use the **dir flash:** command to display the contents of flash and find the config.txt configuration file.

```
ap: dir flash:
Directory of flash:/
3 .rwx 223 <date> env_vars
4 .rwx 2190 <date> config.txt
5 .rwx 27 <date> private.config
150 drwx 320 <date> c350.k9w7.mx.122.13.JA
4207616 bytes available (3404800 bytes used)
```

Step 6 Use the **rename** command to change the name of the config.txt file to config.old.

```
ap: rename flash:config.txt flash:config.old
```

Step 7 Use the **reset** command to reboot the wireless device.

```
ap: reset
Are you sure you want to reset the system (y/n)?y
System resetting..Xmodem file system is available.
flashfs[0]: 142 files, 6 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 7612416
flashfs[0]: Bytes used: 3407360
flashfs[0]: Bytes available: 4205056
flashfs[0]: flashfs fsck took 0 seconds.
Reading cookie from flash parameter block...done.
Base ethernet MAC Address: 00:40:96:41:e4:df
Loading "flash:/c350.k9w7.mx.122.13.JA/c350.k9w7.mx.122.13.JA"...######## . . .
```

Note The wireless device is configured with factory default values, including the IP address (set to receive an IP address using DHCP) and the default username and password (**Cisco**).

Step 8 When Cisco IOS software is loaded, you can use the **del** privileged EXEC command to delete the config.old file from flash.

```
ap# del flash:config.old
Delete filename [config.old]
Delete flash:config.old [confirm]
ap#
```

Reloading the Image

If the wireless device has a firmware failure, you must reload the image file. If the wireless device experiences a firmware failure or a corrupt firmware image, indicated by three red LED indicators, you must reload the image from a connected TFTP server.

Note This process resets *all* configuration settings to factory defaults, including passwords, WEP keys, the wireless device IP address, and SSIDs.

Using the CLI

Follow the steps below to reload the wireless device image using the CLI. When the wireless device begins to boot, interrupt the boot process and use boot loader commands to load an image from a TFTP server to replace the image in the wireless device.

Note Your wireless device configuration is not changed when using the CLI to reload the image file.

Step 1 Open the CLI by using a Telnet session or a connection to the wireless device console port.

Step 2 Reboot the wireless device by removing power and reapplying power.

Step 3 Let the wireless device boot until it begins to inflate the image. When you see these lines on the CLI, press **Esc**:

```
Loading "flash:/c350-k9w7-mx.v122_13_ja.20031010/c350-k9w7-mx.v122_13_ja.20031010"
...###########################################################################
################################################################################
################################################################################
####################
```

Step 4 When the ap: command prompt appears, enter the **set** command to assign an IP address, subnet mask, and default gateway to the wireless device.

Note You must use upper-case characters when you enter the **IP-ADDR**, **NETMASK**, and **DEFAULT_ROUTER** options with the **set** command.

Your entries might look like this example:

```
ap: set IP_ADDR 192.168.133.160
ap: set NETMASK 255.255.255.0
ap: set DEFAULT_ROUTER 192.168.133.1
```

Step 5 Enter the **tftp_init** command to prepare the wireless device for TFTP.

```
ap: tftp_init
```

Step 6 Enter the **tar** command to load and inflate the new image from your TFTP server. The command must include this information:

- the **-xtract** option, which inflates the image when it is loaded
- the IP address of your TFTP server
- the directory on the TFTP server that contains the image

- the name of the image
- the destination for the image (the wireless device flash)

Your entry might look like this example:

```
ap: tar -xtract tftp://192.168.130.222/images/c350-k9w7-tar.122-13.JA1 flash:
```

Step 7 When the display becomes full, the CLI pauses and displays `--MORE--`. Press the spacebar to continue.

```
extracting info (229 bytes)
c350-k9w7-mx.122-13.JA1/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/ (directory) 0 (bytes)
c350-k9w7-mx.122-13.JA1/html/level1/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/appsui.js (558 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/back.htm (205 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/cookies.js (5027 bytes).
extracting c350-k9w7-mx.122-13.JA1/html/level1/forms.js (15704 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/sitewide.js (14621 bytes)...
extracting c350-k9w7-mx.122-13.JA1/html/level1/config.js (2554 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/stylesheet.css (3215 bytes)
c350-k9w7-mx.122-13.JA1/html/level1/images/ (directory) 0 (bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/ap_title_appname.gif (1422 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_1st.gif (1171 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_cbottom.gif (318 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_current.gif (348 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last.gif (386 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_filler.gif (327
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_last_flat.gif (318
bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_button_nth.gif (1177 bytes)
extracting c350-k9w7-mx.122-13.JA1/html/level1/images/apps_leftnav_dkgreen.gif (869 bytes)
 -- MORE --
```

Note If you do not press the spacebar to continue, the process eventually times out and the wireless device stops inflating the image.

Step 8 Enter the **set BOOT** command to designate the new image as the image that the wireless device uses when it reboots. The wireless device creates a directory for the image that has the same name as the image, and you must include the directory in the command. Your entry might look like this example:

```
ap: set BOOT flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
```

Step 9 Enter the **set** command to check your bootloader entries.

```
ap: set
BOOT=flash:/c350-k9w7-mx.122-13.JA1/c350-k9w7-mx.122-13.JA1
DEFAULT_ROUTER=192.168.133.1
IP_ADDR=192.168.133.160
NETMASK=255.255.255.0
```

Step 10 Enter the **boot** command to reboot the wireless device. When the wireless device reboots, it loads the new image.

```
ap: boot
```

Obtaining the Image Files

You can obtain the wireless device image file from the Cisco.com software center by following these steps:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

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

Step 2 Find the wireless device firmware and utilities section and click on the link for the wireless device.

Step 3 Double-click the latest firmware image file for wireless devices.

Step 4 Download the image file to a directory on your PC hard drive.

Obtaining TFTP Server Software

You can download TFTP server software from several websites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

Reloading the Bootloader Image

Follow this procedure to download the boot loader image to the device:

Step 1 Place the bootloader image in the proper directory on a TFTP server.

Step 2 Connect to the console.

Step 3 Enter the **enable** command to enter privileged mode.

Step 4 Download the new boot loader image from the TFTP server to the boot sector by using the **copy tftp:**//*ip address*/*path*/*imagename* **bs:** command, where ip address is the address of the TFTP server and path is the path to the directory where the boot loader image is located.

Caution The boot sector flash file system is addressed as **bs:**. The WMIC will not boot up and will not recover if a non-bootloader image is downloaded to the boot sector of the flash file system.

Step 5 When the boot loader download is complete, enter the **reset** command at the console prompt to reset the device.

Step 6 When the boot loader upgrade is complete, enter the **boot** command at the console prompt to reboot the device.

Step 7 Enter the **version** command to verify that it boots using the upgraded boot loader.

Example Command Output

```
bridge: copy tftp://223.255.254.253/tftpboot/jrehage/loader_c3202_bs.img bs:
................................................................
File "tftp://223.255.254.253/tftpboot/jrehage/loader_c3202_bs.img" successfully copied to
"bs:"
bridge:reset
Are you sure you want to reset the system (y/n)?y
System resetting...
                   Xmodem file system is available.
flashfs[0]:136 files, 6 directories
flashfs[0]:0 orphaned files, 0 orphaned directories
flashfs[0]:Total bytes:15998976
flashfs[0]:Bytes used:7458304
flashfs[0]:Bytes available:8540672
flashfs[0]:flashfs fsck took 30 seconds.
Base ethernet MAC Address:00:ff:ff:f0:01:4f
Initializing ethernet port 0...
Reset ethernet port 0...
Reset done!
ethernet link up, 100 mbps, full-duplex
Ethernet port 0 initialized:link is up
```

Error and Event Messages

This section lists the CLI error and event messages. Table 18-2 lists the errors and events and provides an explanation and recommended action for each message.

Table 18-2 Error and Event Messages

Message	Explanation	Recommended Action
Software Auto Upgrade Messages		
SW_AUTO_UPGRADE-FATAL: Attempt to upgrade software failed, software on flash may be deleted. Please copy software into flash.	Auto upgrade of the software failed. The software on the flash memory might have been deleted. Copy software into the flash memory.	Copy software before rebooting the unit.
SW_AUTO_UPGRADE-7-FAILURE: dhcp_client_start_stop failed	Auto upgrade of the software failed due to error in starting/stopping DHCP client process.	Copy the error message exactly as it appears and report it to your technical support representative.
SW_AUTO_UPGRADE-7-FAILURE: Failed to obtain ip addr from dhcp server	Auto upgrade of the software failed.	Copy the error message exactly as it appears and report it to your technical support representative.
SW_AUTO_UPGRADE-7-FAILURE: boot_file_pathent creation failed	Auto upgrade of the software failed due to error in creation of pathent (internal data structure).	Copy the error message exactly as it appears and report it to your technical support representative.
Association Management Messages		
DOT11-2-RADIO_HW_RESET: Radio subsystem is under going hardware reset to recover from problem	Radio must be reset due to problem.	None.

Table 18-2 Error and Event Messages (continued)

Message	Explanation	Recommended Action
DOT11-3-BADSTATE: [mac-address] [chars] [chars] -> [chars]	802.11 association and management uses a table-driven state machine to keep track and transition an Association through various states. A state transition occurs when an Association receives one of many possible events. When this error occurs, it means that an Association received an event that it did not expect while in this state.	The system can continue but may lose the Association that generates this error. Copy the message exactly as it appears and report it to your technical service representative.
DOT11-3-RADIO_OVER_ TEMPERATURE: Interface [interface] Radio over temperature	The WMIC detected that the unit has exceeded the radio operating temperature.	Investigate and take steps to cool the unit.
DOT11-3-RADIO_IF_LO: Interface [interface] Radio cannot lock IF freq	The unit cannot lock the intermediate frequency.	None.
DOT11-3-RADIO_RF_LO: Interface [interface] Radio cannot lock RF freq	The unit cannot lock the radio frequency.	None.
DOT11-3-RF_LOOPBACK_FAILURE: Interface [interface] Radio failed to pass RF loopback test	Radio loopback test failed at startup time.	None.
DOT11-3-TX_PWR_OUT_OF_ RANGE: Interface [interface] Radio Tx power control out of range	The unit has detected that the radio transmit power cannot be locked within the operating range.	None.
DOT11-4-MAXERTRIES: Packet to client [mac] reached max retries, remove the client	A packet sent to the client has not been successfully delivered many times, and the max retries limit has been reached. The client is deleted from the association table.	None.
DOT11-6-ASSOC: Interface [interface], Station [char] [mac] Associated	A station associated to a bridge.	None.
DOT11-6-ADD: Interface [interface], Station [mac] Associated to Parent [mac]	A station associated to a bridge.	None.
DOT11-6-DISASSOC: Interface [interface], Deauthenticating Station [mac] [char]	A station disassociated from a bridge.	None.
DOT11-6-ROAMED: Station [mac-address] Roamed to [mac-address]	A station has roamed to a new bridge.	None.
Unzip Messages		
SOAP-4-UNZIP_OVERFLOW: Failed to unzip flash:/c1200-k9w7-mx.122-3.6.JA1/html/level15/ap_xxx.htm.gz, exceeds maximum uncompressed html size	The HTTP server cannot retrieve a compressed file in response to an HTTP GET request because the size of the file is too large for the buffers used in the uncompression process.	Make sure file is a valid HTML page. If so, you'll have to copy an uncompressed version of the file into flash to retrieve it through HTTP.
802.11 Subsystem Messages		

Table 18-2 Error and Event Messages (continued)

Message	Explanation	Recommended Action
DOT11-6-FREQ_INUSE: Radio frequency [int] is in use	When scanning for an unused frequency, the unit recognized another radio using the displayed frequency.	None.
DOT11-6-FREQ_USED: Radio frequency [int] selected	After scanning for an unused frequency, the unit selected the displayed frequency.	None.
DOT11-4-VERSION_MISMATCH: Require radio version [hex].[int], found version [hex].[int]	When starting the radio, the wrong firmware version was found. The radio will be loaded with the required version.	None.
DOT11-2-VERSION_INVALID: Unable to find required radio version [hex].[int]	When trying to re-flash the radio firmware, the device recognized that the radio firmware packaged with the IOS firmware had the incorrect version.	None.
DOT11-4-NO_SSID: No SSIDs configured, radio not started	All SSIDs were deleted from the configuration. At least one must be configured for the radio to run.	Configure at least one SSID on the device.
DOT11-4-FLASHING_RADIO: Flashing the radio firmware ([chars])	The radio has been stopped to load new firmware.	None.
DOT11-2-NO_FIRMWARE: No radio firmware file ([chars]) was found	When trying to flash new firmware into the radio, the file for the radio was not found in the flash file system.	The wrong image has been loaded into the unit. Locate the correct image based on the type of radio used.
DOT11-2-BAD_FIRMWARE: Radio firmware file ([chars]) is invalid	When trying to flash new firmware into the radio, the file was found to be invalid.	Put the correct firmware image file in the place where the unit is looking.
DOT11-4-FLASH_RADIO_DONE: Flashing the radio firmware completed	The radio firmware flash is complete, and the radio will be restarted with the new firmware.	None.
DOT11-4-LINK_DOWN: Radio parent lost: [chars]	The connection to the parent bridge was lost for the displayed reason. The unit will try to find a new parent bridge.	None.
DOT11-4-CANT_ASSOC: Cannot associate: [chars]	The unit could not establish a connection to a parent bridge for the displayed reason.	Check the configuration of both the parent bridge and this unit to make sure the basic settings (SSID, WEP, and others) match.
Inter-Bridge Protocol Messages		
DOT11-6-ROAMED: Station [mac-address] Roamed to [mac-address]	A station has roamed to a new bridge.	None.
DOT11-6-STANDBY_ACTIVE: Standby to Active, Reason = [chars] ([int])	The device is transitioning from standby mode to active mode.	None.
DOT11-6-ROGUE_AP: Rogue AP [mac-address] reported. Reason: [chars]	A station has reported a potential rogue bridge for the stated reason.	None.

Table 18-2 Error and Event Messages (continued)

Message	Explanation	Recommended Action
SCHED-3-UNEXPECTEDMESSAGE: Unknown message [hex] received (ptr arg [hex], num arg [hex]).	A process can register to be notified when various events occur in the router. This message indicates that a process received a message from another process that it does not know how to handle.	Copy the error message exactly as it appears, and report it to your technical support representative.
SCHED-3-UNEXPECTEDEVENT: Process received unknown event (maj [hex], min [hex]).	A process can register to be notified when various events occur in the router. This message indicates that a process received an event that it did not know how to handle.	Copy the error message exactly as it appears, and report it to your technical support representative.
Miscellaneous Messages		
WGB_CLIENT_VLAN: Workgroup Bridge Ethernet client VLAN not configured.	A VLAN configuration is missing for client devices connected to a workgroup bridge.	Use the workgroup-bridge client-vlan command to assign a VLAN to Ethernet client devices connected to the workgroup bridge.
UNDER_VOLTAGE: Under voltage condition detected.	The hardware under voltage detection logic has reported a low voltage condition.	Check the power supply and associated power connections.