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, first check the LED indicators on the device to quickly assess the device's status.

The LED indicator setup is not the same across all Cisco Aironet series access points. Depending on the series, your access point may have a single Status LED indicator, or three indicators – Ethernet LED, Status LED, and Radio LED. Refer to your access point's *Getting Started Guide* or the *Hardware Installation Guide* (for Outdoor Access Points) for information on its LED indicator setup.

Note There will be small variations in LED color intensity and hue from unit to unit. This is expected and within the normal range of the LED manufacturer's specifications and is not a defect.

Checking Power

You can verify the availability of power to the access point/bridge by checking the power injector's LED indicator:

- Green color indicates input power is being supplied to the bridge.
- Red color indicates an overcurrent or overvoltage error condition—disconnect input power from the power injector, check all coax cable connections for a possible short, wait approximately 1 minute, and reconnect input power to the power injector. If the LED turns red again, contact technical support for assistance.

  Note The power injector requires approximately 50 seconds to recover from an overcurrent or overvoltage condition.

Off indicates input power is not available—verify that the power module is connected to the power injector and that AC power is available or that 12- to 40-VDC input power is connected to the power injector.

Low Power Condition

Access points can be powered from the 48-VDC power module or from an in-line power source.

For full operation, the 1040, 1140, 1260, and 700W series access points require 12.95 W of power. The power module and Cisco Aironet power injectors are capable of supplying the required power for full operation, but some inline power sources are not capable of supplying 12.95 W. Also, some high-power inline power sources, might not be able to provide 12.95 W of power to all ports at the same time.

The 2600, 3600, 2700 and 3700 series access points need 18.5 Watts, and therefore 802.3at or PoE+. However, these access points can also function with 802.3af power, by disabling one of the radio chains on each radio module.

Note An 802.3af compliant switch (Cisco or non-Cisco) is capable of supplying sufficient power for full operation.

Note When an AP 2700 or AP 3700 is running in low power mode with PoE 802.3af power, one of the radios is shutdown. As the saved power from the shut down radio is utilized for the running radio, that radio is reset. During the reset, communication with associated WLAN clients will get disrupted. After the radio comes back online after reset, the WLAN clients will re-associate with it afresh.

On power on, the access points are placed into low power mode (both radios are disabled), Cisco IOS software loads and runs, and power negotiation determines if sufficient power is available. If there is sufficient power then the radios are turned on; otherwise, the access point remains in low power mode with the radios disabled to prevent a possible over-current condition. In low power mode, the access point activates the Status LED low power error indication, displays a low power message on the browser and serial interfaces, and creates an event log entry.

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 SSID as the wireless device. If a client device's SSID does not match the SSID of an wireless device in radio range, the client device will not associate.

WEP Keys

The 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.

Refer to Chapter 10, "Configuring WLAN Authentication and Encryption,"for instructions on setting the wireless device's WEP keys.

Security Settings

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

If your radio clients are using EAP-FAST authentication, you must configure open authentication with EAP. If you do not configure open authentication with EAP, a warning message appears. If you are using the CLI. the following warning appears:

SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.

If you are using the GUI, this warning message appears:

WARNING:
"Network EAP is used for LEAP authentication only. If radio clients are configured to authenticate using EAP-FAST, Open Authentication with EAP should also be configured."

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.

Troubleshooting using Sniffer Mode

You can have the AP operating in sniffer mode to aid troubleshooting. The sniffer mode is strictly for troubleshooting purposes. The sniffer mode passively monitors the surrounding WLAN environment, over a specifically configured channel, and tunnels all the 802.11 WLAN traffic to an end point on your network as configured by you. At that end point you can use a protocol analysis tool, such as Wireshark or Airopeek, to review the packets and diagnose issues.

Starting in global configuration mode, perform the following steps.

	Command	Purpose
Step 1	**int {d0 | d1}**	Entering interface configuration command mode for configuring the radio interfaces.
Step 2	**station-role sniffer**	Changing the station role to sniffer.
Step 3	**channel** *number*	Selecting the channel in which to operate in sniffer mode.
Step 4	**no shut**	Reverses the shutdown of the interface.
Step 5	**exit**	Exits interface configuration command mode.
Step 6	**sniffer ip-address** *destination-ip* **port** *port-number*	Sets the IP address and port number, to which AP will redirect all the packets. You can specify an IP address on any port number between 1024 to 65535.
Step 7	**wireshark enable**	If you are using Wireshark at the end point, this adds a Wireshark header to the packets.

Sample configuration:

```
ap(config)# int d0
ap(config-if)# station-role sniffer
ap(config-if)# channel 11
ap(config-if)# no shut
ap(config-if) # exit
ap(config)# sniffer ip-address 10.126.251.30 port 5555
ap(config)# wireshark enable
```

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. On all access points, you can use the MODE button on the access point or the web-browser interface. On 350 series access points, you can use the web-browser or CLI interfaces.

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 MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the MODE button.

Note To reset the configuration to defaults, intead of using the MODE button, follow the instructions in the "Using the Web Browser Interface" section on page 26-5, or in the "Using the CLI" section on page 26-6.
You cannot use the MODE button to reset the configuration to defaults on 350 series access points.

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the **MODE** button while you reconnect power to the access point.

Step 3 Hold the MODE button until the Status LED turns blue.

Step 4 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP). The default username and password are **Cisco**, which is case-sensitive.

Using the Web Browser Interface

Follow these steps to delete the current configuration and return all wireless device settings to the factory defaults using the web browser interface:

Step 1 Open your Internet browser.

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click **Software** and the System Software screen appears.

Step 6 Click **System Configuration** and the System Configuration screen appears.

Step 7 Click the **Reset to Defaults** or **Reset to Defaults (Except IP)** button.

Note Select **Reset to Defaults (Except IP)** if you want to retain a static IP address.

Step 8 Click **Restart**. The system reboots.

Step 9 After the wireless device reboots, you must reconfigure the wireless device by using the Web-browser interface or the CLI. The default username and password are **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 and reapplying power.

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...
    using  eeprom values
WRDTR,CLKTR: 0x80000800 0x80000000
RQDC ,RFDC : 0x80000033 0x000001cb
    ddr init done
IOS Bootloader - Starting system.
Xmodem file system is available.
DDR values used from system serial eeprom.
WRDTR,CLKTR: 0x80000800, 0x80000000
RQDC, RFDC : 0x80000033, 0x000001cb
```

Step 8 When the access point has finished rebooting the software, establish a new Telnet session to the access point.

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 9 When 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 Access Point Image

If the wireless device has a firmware failure, you must reload the image file using the Web browser interface or on all access points, by pressing and holding the MODE button for around 30 seconds. You can use the browser interface if the wireless device firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image.

Using the MODE button

You can use the MODE button on all access points to reload the access point image file from an active Trivial File Transfer Protocol (TFTP) server on your network or on a PC connected to the access point Ethernet port.

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, security configurations, the wireless device IP address, and SSIDs.

Follow these steps to reload the access point image file:

Step 1 The PC you intend to use must be configured with a static IP address in the range of 10.0.0.2 to 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as such as *ap3g2-k9w7-tar.152-4.JB5.tar*) in the TFTP server folder and that the TFTP server is activated. For additional information, refer to the "Obtaining the Access Point Image File" and "Obtaining TFTP Server Software" sections.

Step 3 Rename the access point image file in the TFTP server folder. For example, if the image file is **ap3g2-k9w7-tar.152-4.JB5.tar**, rename the file to **ap3g2-k9w7-tar.default**.

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Step 7 Hold the **MODE** button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 8 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, you must reconfigure the access point by using the Web-browser interface or the CLI.

Using the Web Browser Interface

You can also use the Web browser interface to reload the wireless device image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your wireless device configuration does not change when you use the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the wireless device image file on your PC and download the image to the wireless device. Follow the instructions below to use the HTTP interface:

Step 1 Open your Internet browser. You must use Microsoft Internet Explorer or Netscape Navigator (version 7.x).

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click **Browse** to find the image file on your PC.

Step 7 Click **Upload**.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the wireless device image file. Follow the instructions below to use a TFTP server:

Step 1 Open your Internet browser.

Step 2 Enter the wireless device's IP address in the browser address line and press **Enter**. An Enter Network Password screen appears.

Step 3 Enter your username in the Username field.

Step 4 Enter the wireless device password in the Password field and press **Enter**. The Summary Status page appears.

Step 5 Click the **Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 6 Click the **TFTP Upgrade** tab.

Step 7 Enter the IP address for the TFTP server in the TFTP Server field.

Step 8 Enter the file name for the image file in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 9 Click **Upload**.

For additional information click the **Help** icon on the Software Upgrade screen.

Using the CLI

Follow the steps below to reload the wireless device image using the CLI. When the wireless device begins to boot, you 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 using 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/ap3g2-k9w7-tar.152-4.JB5.tar flash
```

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

```
extracting info (286 bytes)
ap3g2-k9w7-mx.152-4.JB5/ (directory)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-mx.152-4.JB5 (208427 bytes)
ap3g2-k9w7-mx.152-4.JB5/ap3g2-k9w7-tx.152-4.JB5 (73 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/appsui.js (563 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/back.shtml (512 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/cookies.js (5032 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/forms.js (20125 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/sitewide.js (17089 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stylesheet.css (3220 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/config.js (26330 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/popup_capabilitycodes.shtml.gz (1020 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter.js.gz (1862 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter_vlan.js.gz (1459 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/filter_mac_ether.js.gz (1793 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/security.js.gz (962 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/vlan.js.gz (1121 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ssid.js.gz (4286 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/network-if.js.gz (2084 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/dot1x.js.gz (988 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/stp.js.gz (957 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_assoc.shtml.gz (5653 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_event-log.shtml.gz (3907 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_home.shtml.gz (7071 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_network-if.shtml.gz (3565 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_network-map.shtml.gz (3880 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_services.shtml.gz (3697 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_system-sw.shtml.gz (2888 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/ap_contextmgr.shtml.gz (3834 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/ (directory)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/ap_title_appname.gif (2092 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/2600_title_appname.gif (2100 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button.gif (1211 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_1st.gif (1171 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_cbottom.gif (318 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_current.gif (1206 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_endcap.gif (878 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_encap_last.gif (333 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_last.gif (386 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_button_nth.gif (1177 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_dkgreen.gif (869 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_green.gif (879 bytes)
ap3g2-k9w7-mx.152-4.JB5/html/level/1/images/apps_leftnav_upright.gif (64 bytes)
.../...
```

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:/ap3g2-k9w7-tar.152-4.JB5/ap3g2-k9w7-tar.152-4.JB5
```

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

```
ap: set
BOOT=flash:/ap3g2-k9w7-tar.152-4.JB5/ap3g2-k9w7-tar.152-4.JB5
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 Access Point Image File

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

Step 1 Use your Internet browser to access the Download Software page for wireless products, at the following URL:

http://software.cisco.com/download/navigator.html?mdfid=278875243&i=!h

Step 2 Login to the Cisco.com site.
Click **Log In** at the top right corner of the page and enter your CCO login and password.

Step 3 In Select a Product area, from the right-most column click **Access Points**.

Step 4 Click the appropriate access point.

Step 5 Click the appropriate access point version.

Step 6 Click **Autonomous AP IOS Software**.
A list of available software versions appear.

Step 7 Choose the version you wish to download.
The download page for the version you chose appears.

Step 8 Click **Download**. The Software Download Rules page appears.

Step 9 Read the Software Download Rules carefully and click **Agree**.

Step 10 Save the file to your hard drive.

Obtaining TFTP Server Software

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

http://tftpd32.jounin.net

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

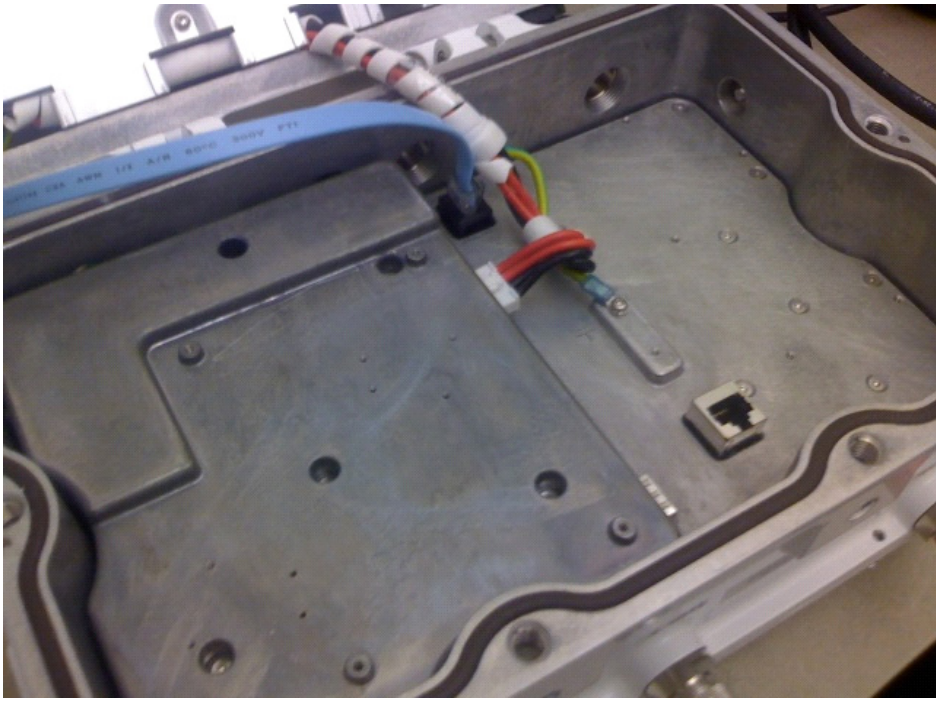
Image Recovery on the 1520 Access Point

The process for image recovery on an 1520 access point is similar to the process for any IOS access point with a console port.

To perform image recovery on the 1520 access point, follow these steps:

Step 1 With the access point powered off, connect an RJ45 console cable to the console port (). The console port is the black plastic RJ45 jack inside the unit.

Figure 26-1 Connecting an RJ45 Console Cable to the Console Port



Step 2 Configure the terminal emulator for 8 databits, no parity, no flow control, 9600 bps.

Step 3 Apply power to the access point.

Step 4 When the bootloader displays “Base Ethernet MAC Address”, hit the <esc> key to break to the **ap:** prompt:

```
IOS Bootloader - Starting system.
Xmodem file system is available.
flashfs[0]: 13 files, 2 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 31868928
flashfs[0]: Bytes used: 9721344
flashfs[0]: Bytes available: 22147584
flashfs[0]: flashfs fsck took 20 seconds.
Reading cookie from flash parameter block...done.
Base Ethernet MAC address: 00:1f:27:75:db:00

The system boot has been aborted.  The following
commands will finish loading the operating system
software:
    ether_init
    tftp_init
    boot
ap:
```

Note If the **ENABLE_BREAK=no environmental** variable is set, you will not be able to escape to the bootloader.

Step 5 Cable the 1520 access point's LAN port ("PoE In") to a TFTP server. For example, a Windows PC with tftpd32 installed.

Step 6 Install a good copy of the **k9w7** IOS image on the TFTP server.

Step 7 Configure the TFTP server's LAN interface with a static IP address. For example, 10.1.1.1.

Step 8 On the access point enter:

```
ap: dir flash:
```

Verify there is enough free space on flash to hold the new code (or if the flash file system is corrupt), then enter:

```
ap: format flash:
```

Step 9 Copy the image using TFTP to the 1520 access point's flash.