



## Performing Diagnostics

---

This chapter describes how to use the Diagnostics menu to maintain the bridge.

Here's what you'll find in this chapter:

- [Using the Diagnostics Menu](#), page 11-2
- [Using the Network Menu \(Network\)](#), page 11-2
- [Running a Link Test \(Linktests\)](#), page 11-3
- [Restarting the Bridge \(Restart\)](#), page 11-3
- [Returning the Bridge to the Default Configuration \(Defaults/Reset\)](#), page 11-4
- [Loading New Code Versions \(Load\)](#), page 11-4

## Using the Diagnostics Menu

Use the Diagnostics menu to analyze system problems.

**Navigation:** Choose **Main > Diagnostics**

Diagnostics Menu		
Option	Value	Description
1 - Network	[ menu ]	- Network connection commands
2 - Linktests	[ menu ]	- Test the radio link
3 - Restart		- Restart the unit
4 - Defaults		- Return to default configuration
5 - Reset		- Default parts of the configuration
6 - Load	[ menu ]	- Load new version of firmware

Enter an option number or name, "=" main menu, <ESC> previous menu  
> █

44785

## Using the Network Menu (Network)

The Network menu provides several network diagnostics tools.

**Navigation:** Choose **Main > Diagnostics > Network**

Diagnostics Network Menu		
Option	Value	Description
1 - Connect		- Start telnet session
2 - Escape	[ "^X^Y^Z" ]	- Connection escape sequence
3 - Ping		- Send an IP PING packet
4 - Find	[ off ]	- Flash LEDs to find unit

Enter an option number or name, "=" main menu, <ESC> previous menu  
> █

44784

## Starting a Telnet Session (Connect)

The *Connect* option starts a Telnet session with a remote bridge on the infrastructure to access its console menu. The *Connect* option can also be used to access any remote node (PC or server) that supports Telnet access.

Start this connection using the remote node's IP address. The connection is completely routable and the destination can be anywhere in the Internet.

If the connection is to be made to another bridge that has not been assigned an IP address, start the connection using the MAC level infrastructure address of the bridge. This connection uses a proprietary protocol that is not routable. The destination must lie on the local LAN. The MAC level address connection is useful when assigning IP addresses to a large number of bridges.

When starting a Telnet session with the *Connect* option, the remote node's privilege level is set to the highest level that does not have a password.

While the bridge is attempting to connect to the remote node, terminate the connection by pressing **Ctrl-C**. This may be required if the incorrect address was typed.

After connecting, you can close a Telnet session and return to the local console by:

- Entering the escape sequence of characters as defined by the *Escape* option in the Diagnostics menu. See “Changing the Escape Sequence” below.
- If the remote node is a Cisco Aironet node, choose the *Close* option which is accessible on the Main menu during a Telnet session only.
- Using the remote node’s logout command.

## Changing the Escape Sequence (Escape)

The *Escape* option changes the sequence of characters that are assigned to close a Telnet session to a remote destination. Typically, you would change the sequence if the current sequence has meaning to the remote system.

The sequence may be up to 10 characters. To enter nonprinting characters in the sequence you may:

- Use the two-character combination of caret (^) and the alphabetic character corresponding to the control character. For example, to type **Ctrl-Z**, use the string **^Z**.
- Use a backslash (\) followed by three octal numbers.
- Use a dollar sign (\$) followed by two hexadecimal numbers.

## Sending a Ping Packet (Ping)

The *Ping* option tests infrastructure connectivity from the bridge to other IP nodes. The *Ping* option sends an ICMP echo\_request packet to a user-specified remote node. If the remote node receives the packet it also responds with an ICMP echo\_response packet.

The bridge sends the echo\_response packet and waits 3 seconds for a response. If there is no response, the client sends another echo\_response packet. If a response is received and a message is displayed, the command disappears from the screen. Enter **Ctrl-C** to stop the command.

## Physically Locating a Bridge (Find)

The *Find* option physically locates a bridge if you are unsure of its exact location. Invoking the option causes the bridge’s amber LEDs blink on and off. Once you locate the bridge, use the *Find* option again to return the LEDs to normal operation.

## Running a Link Test (Linktests)

The *Linktests* option tests the quality of the radio transmission between the bridge and other nodes on the radio network. See Chapter 4, “Configuring the Radio Network.”

## Restarting the Bridge (Restart)

The *Restart* option reboots the bridge. All associations are lost and the bridge reacts as though it had just been powered on.

## Returning the Bridge to the Default Configuration (Defaults/Reset)

The *Defaults* option returns the bridge configuration to its default factory settings. The bridge erases the currently saved configuration and executes a restart command.

The *Reset* option returns the bridge configuration to only part of the default configuration. There are three entry options:

- **ident\_save**: all parts of the configuration except the IP address are defaulted.
- **radio\_default**: only the radio configuration is defaulted.
- **filter\_default**: only the filter information is defaulted.

## Loading New Code Versions (Load)

The bridge code is stored in a Flash memory chip inside the bridge. Use the *Load* option to load new code versions of the bridge's firmware and save it to Flash memory.

To load new versions of the firmware, the code must be loaded into main memory first, then programmed into the Flash memory. The bridge reboots using the new firmware. The Flash memory retains the new version even if the power is disconnected.

The new firmware can be downloaded into the bridge using:

- **FTP**: load the new firmware into a single bridge using File Transfer Protocol (FTP). Then use FTP to upload (send) the code running in the local bridge to other remote bridges on the infrastructure.
- **Distribute**: load the new firmware into a single bridge using FTP. Then use the *Distribute* option to simultaneously load all of the other bridges on the infrastructure. When you select the *Load* option, the Diagnostics Load menu appears:

**Navigation:** Choose **Main > Diagnostics > Load**

Diagnostics Load Menu		
Option	Value	Description
1 - Ftp	[ menu ]	- Load using FTP
2 - Distribute	[ menu ]	- Distribute the firmware
Enter an option number or name, "=" main menu, <ESC> previous menu		
> █		

44783

## Downloading or Uploading Firmware Using FTP (Ftp)

Use the *Ftp* option to download or upload firmware. The bridge can be an FTP client or FTP server.

To upload or download firmware you can initiate a connection from:

- The bridge console to a remote PC or host and retrieve a new version of the firmware.
- The bridge console to a remote PC or host and send a copy of the running firmware.
- One bridge console to another allowing bridges to send or receive firmware running locally.
- A PC or host system to the bridge and send a new firmware version.



### Note

Before you download or upload new code versions, make sure you have set the IP address on all bridges involved.

When you select the *Ftp* option, the Diagnostics Load FTP menu appears:

**Navigation:** Choose **Main > Diagnostics > Load > Ftp**

Diagnostics Load Ftp Menu		
Option	Value	Description
1 - Get		- Load a firmware/config file
2 - Put		- Send a firmware file
3 - Config		- Send a configuration file
4 - Dest	[ 000.000.000.000 ]	- Host IP address
5 - Username	[ "" ]	- Host username
6 - Password	[ "" ]	- Host password
7 - Filename	[ "" ]	- Host filename

Enter an option number or name, "=" main menu, <ESC> previous menu  
> █

44782

### Downloading a New Firmware or Configuration File (Get)

Use the *Get* option to download (retrieve) firmware or a configuration file. After the file loads, the bridge checks the first characters of the file. If *!CONFIGURATION* is present, the file contains menu configuration commands. Otherwise, the file is considered to be firmware and is loaded in Flash memory and executed. Follow these steps:

- 
- Step 1** Load the file onto the PC, host, or bridge from which you will retrieve the firmware.
- Step 2** Choose the **Dest** option and enter the IP address of the host PC or bridge.
- Step 3** Choose the **Username** option and enter the username required to access the firmware file.  
If downloading from another Cisco Aironet bridge, the *Username* option must have a value even though the value is not used by the remote bridge.
- Step 4** Choose the **Password** option and enter the password associated with the username.  
If downloading from another Cisco Aironet bridge, the login password value must match the console write privilege password on the remote bridge.
- Step 5** Choose the **Filename** option and enter the name of the firmware file you are retrieving (including drive and directory), then press **Enter**.  
If downloading from another Cisco Aironet bridge, the *Filename* option must have a value even though the value is not used by the remote bridge.
- Step 6** Choose the **Get** option.  
The bridge begins an FTP session to the host PC, retrieves the file, programs the Flash memory and reboots. A message similar to the following is displayed.

```
220 sun_host FTP server (SunOS 4.1) ready.
230 User sysop logged in.
200 Type set to I.
200 PORT command successful.
150 Binary data connection for apv33.img (163056 bytes).
226 Binary Transfer complete.
221 Goodbye.
FTP: received 161056 bytes in 00:00:10; 15 Kbytes/s transfer rate
rebooting unit.
```

### Uploading a New Firmware Version (Put)

Use the *Put* option to upload (send) a copy of the currently running firmware to another system. If the system is a PC or host, a copy of the firmware is stored on the system's disk, possibly for downloading to other bridges later.

If the system is a Cisco bridge, the remote bridge flashes the new code and begins running it immediately. You can use one bridge to upgrade another bridge. Follow these steps:

- 
- Step 1** Choose the **Dest** option and enter the IP address of the remote PC, host, or bridge you are sending to and press **Enter**.
- Step 2** Choose the **Username** option and enter the username for the remote PC, host, or bridge you are sending to and Press **Enter**.
- If you are uploading to another Cisco bridge, the *Username* option must have a value even though the value is not used by the remote bridge.
- Step 3** Choose the **Password** option and enter the access password for the remote PC, host, or console. Press **Enter**.
- Step 4** Choose the **Filename** option and enter the name of the firmware file you are sending to the PC, host, or bridge (including drive and directory) and press **Enter**.
- If uploading to another Cisco bridge, the *Filename* option must have a value even though the value is not used by the remote bridge.
- Step 5** Choose the **Put** option. The bridge begins an FTP session to the remote PC host or bridge.
- 

### Uploading the Bridge's Configuration (Config)

The *Config* option saves the configuration on a remote host or PC in a format suitable for later downloading using FTP or BOOTP.

You are first prompted for the name of the file to be created on the remote system. You are then prompted to choose *All*, *Non-default*, or the *Distributable* configuration options:

- **All**: sends every configuration item.
- **Non-default**: sends only those configuration items that have been modified from their default values.
- **Distributable**: sends the configuration items that can be distributed to other bridges.

The file transfer begins after you choose the configuration file type.

## Distributing Firmware or Configuration (Distribute)

**Navigation:** Choose **Main > Diagnostics > Load > Distribute**

Diagnostics Load Distribute Menu		
Option	Value	Description
1 - Go		- Start a distribution
2 - Type	[ firmware ]	- What to distribute
3 - Control	[ newer ]	- How to control distributions
4 - Add		- Change distributable configuration
5 - Remove		- Remove change
6 - Show		- Show changes
7 - Dump		- Show Configuration

Enter an option number or name, "=" main menu, <ESC> previous menu  
> █

44781

The Diagnostics Load Distribute menu provides a range of options for distributing firmware or configuration from one bridge to all other bridges on the infrastructure. These options reduce the time needed to perform firmware upgrades or make global changes to the configuration.

If you are distributing a configuration, examine the parts of the bridge's configuration that will be distributed by choosing **Main > Configuration > Dump > Distributable > Standard**.

The *Go* option starts the distribution. The following message appears:

```
Finding the other units ....
```

When the command executes, the local bridge sends a special broadcast message to all other bridges in the radio infrastructure. The message reports that the bridge has a new firmware file with its assigned version number or a configuration file.

The remote bridges then determine whether to respond based on the value of their control parameter. Any responses are displayed on the local bridge similar to the following message.

```
AIR-WGB340 004096285e73 has code version 8.36 (checksum 1829)
```

When the local bridge receives a response to its request, the remote bridge is added to a list of bridges to be loaded. When the response time-out period has expired, the local bridge begins loading all remote bridges in parallel using a proprietary protocol. A message similar to the following is displayed.

```
Loading 004096001d45
Loading 00409610345f
```

If any remote bridges timeout during the load, they are removed from the list. After all bridges finish loading, the local bridge displays a count of the successful loads. A message similar to the following is displayed.

```
Completed loading 004096001d45
Completed loading 00409610345f
Loading of 2 Workgroup Bridges completed
```

The *Type* option selects the file type to be distributed. Choices are *firmware* or *configuration*.

The *Control* option controls how the remote bridges respond to a request to send a configuration or firmware. You can choose from the following options:

- **None:** the bridge never responds and cannot be loaded by another bridge using the distribute command.
- **Newer:** the bridge only responds if the version of firmware being distributed has a larger version number than the code currently running. This selection applies only to firmware downloads.
- **Any:** the bridge always responds. It is up to the distributing bridge to determine whether to load the local bridge.
- **A password of at most 8 characters:** a password that must be typed by the operator of the bridge doing the distribution. The local bridge will not respond to any distributions that do not supply this password.

If the distribution is password protected, only those bridges that have the same password configured in the control parameter accept the distribution. Therefore, the bridges can be protected from unwanted loads. The password may also be used to divide the bridges into code load groups such that the loads to one group do not affect the other groups.

If the distribution is done without a password, the load is ignored by remote bridges with a configured password. If a remote bridge does not have a password and firmware is being distributed, it only accepts the load based on the version number and code checksum.

The *Add* option changes the distributable configuration. Each line of the configuration carries a designation either *send* or *local*. After typing the encoded configuration ID, type either **send** or **local** to change the assigned designation and press **Enter** twice to apply the change.

The *Remove* option reverses the most recent change. You can choose between reversing the change made to a single encoded configuration ID or typing *all* to reverse all designations.

The *Show* option lists the changes made to configuration items.

The *Dump* option displays the complete configuration.