

Upgrading Firmware on the Cisco Aironet 340 Series Bridge

Document ID: 8114

Introduction

Prerequisites

Requirements

Components Used

Conventions

Initial Menu Navigation

Load New Firmware and Configurations

Download with Xmodem Protocol

Download or Upload with the File Transfer Protocol

Download a New Firmware/Configuration File

Upload a New Firmware Version

Upload the Configuration for the Unit

Download with the Internet Boot Protocol

Distribute Firmware or Configuration

Control Which Units the Distribute Affects

Control Which Parts of the Configuration are Distributed

Start the Distribution

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes methods for upgrading firmware on a Cisco Aironet 340 Series Bridge. Perform these procedures when you must increase the functionality and stability that are offered by more current software revisions.

This document also describes how to:

- Upload and retrieve configuration files that are used to back up or restore the configuration of a bridge in case of a failure.
- Distribute firmware that is used to ensure that all bridges run the same firmware versions to other bridges. One Bridge distributes all firmware.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

A Cisco Aironet 340 Series Bridge firmware image is required to upgrade firmware for a bridge. You can download the latest Aironet 340 Series Bridge firmware images at the Cisco Software Center. After you download the file, uncompress the file before you use it and move it to an FTP server.

If you must transfer the file through the console, the file must reside on the PC from which the console connection is made.

You must perform basic configuration by accessing the console serial port when you power up the unit for the first time. To gain access through the serial port, you must connect the bridge to a terminal or a PC running a terminal emulator software, such as HyperTerminal. Set the session to:

- 9600 bits per second (bps)
- no parity
- 8 data bits
- 1 stop bit
- Xon/Xoff flowcontrol

Once the bridge is assigned an IP address, access the console remotely using:

- A Telnet application from a remote host or PC
- An HTML browser from a remote host

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

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Initial Menu Navigation

When you use a Telnet application from a remote host or PC, the main menu displays after you connect the Aironet 340 Series Bridge.

```

                                     Main Menu
      Option          Value          Description
1 - Configuration  [ menu ]      - General configuration
2 - Statistics     [ menu ]      - Display statistics
3 - Association    [ menu ]      - Association table maintenance
4 - Filter         [ menu ]      - Control packet filtering
5 - Logs          [ menu ]      - Alarm and log control
6 - Diagnostics   [ menu ]      - Maintenance and testing commands
7 - Privilege     [ write ]     - Set privilege level
8 - Help          [ write ]     - Introduction

Enter an option number or name
>
```

Note: When you use an HTML browser from a remote host, the main menu display is different. However, the menu options presented are the same.

Use the **Diagnostics** option to access the Diagnostics menu.

```

Diagnostics Menu
Option      Value      Description
1 - Network [ menu ] - Network connection commands
2 - Linktest [ menu ] - Run a link test
3 - Restart          - Equivalent to power-up
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
>_

```

Load New Firmware and Configurations

Use the **Load** option to load new code versions of Aironet 340 Series Bridge firmware or configurations. Load the new code versions into the main memory and program into the flash memory chip inside the unit. The flash memory retains the new version even if the power is disconnected. The unit reboots using the new firmware.

Files that begin with the string, ! CONFIGURATION, are considered text files with lines of commands and are executed as though they are typed at the console.

The new firmware or configuration is downloaded using:

- FTP Load the new file to the unit using the Xmodem or FTP protocols. Use the FTP protocol to upload the file from the local unit to remote units on the infrastructure.
- Distribute Load the new file to the unit using the Xmodem or FTP protocols. Use the Distribute option to simultaneously load all units, with wired or wireless connections, on the infrastructure.
- Bootp Load the new firmware and configuration revisions into the units each time they power up.

Use the **Load** option to access the Diagnostics Load menu.

```

Diagnostics Load Menu                                BR105E_22ef0a
Option      Value      Description
1 - Xmodem          - Xmodem load from serial port
2 - Crc-xmodem     - Xmodem-CRC load from serial port
3 - Ftp            [ menu ] - Load using FTP
4 - Distribute     [ menu ] - Distribute the firmware
5 - Bootp/DHCP    [ on ] - Use BOOTP/DHCP on startup
6 - Class         [BRE105E] - DHCP class id

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

```

Download with Xmodem Protocol

In order to load new firmware versions through the console port, use these options, depending on the communications software program installed.

- Xmodem Terminates packets with a checksum.
- CRC-xmodem Terminates packets with a Cyclic Redundancy Check (CRC).

To load firmware using Xmodem or CRC-xmodem, use these steps:

1. Connect a terminal to the Console Port with a communications software program, such as Procomm™ or Windows™ Terminal.
2. Select the communications software specific option, Xmodem or CRC-xmodem. This message displays:

```
Ready for XMODEM download. Use several ^X's to cancel
```

3. Set the communication program to initiate the file transfer to the unit.
4. The unit begins to download the file. A message similar to this appears:

```
XMODEM: received 160450 bytes in 00:03:36; 800 bytes/s transfer rate
```

After new firmware loaded code validates, the flash memory programs and the unit restarts with the new code.

The firmware consists of the boot block and the application code. During the firmware download, the application code is replaced, but the boot block is not.

When the unit powers up, the boot block checks the integrity of the application code. If it is valid, the boot block executes the new firmware. If it is invalid, the boot block displays an error message on the console and you must reload the firmware.

Note: You receive an invalid application code when the flash memory device fails or the power is interrupted while the flash memory programs.

Download or Upload with the File Transfer Protocol

The Aironet 340 Series Bridge serves as an FTP client or an FTP server and you can use it to download and upload firmware. Initiate a connection from one of these:

- The Aironet 340 Series Bridge console to a remote PC or host and retrieve a new version of the firmware
- The Aironet 340 Series Bridge console to a remote PC or host and send a copy of the running firmware
- One Aironet 340 Series Bridge console to another where units send or receive firmware that runs locally
- A PC or host system to an Aironet 340 Series Bridge and send a new firmware version

Note: Set the IP address on all units involved before you download or upload new code versions.

Use the **FTP** option to access the Diagnostics Load FTP Menu.

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		
>		

Download a New Firmware/Configuration File

Use the **Get** option to download firmware or a configuration file. Once you load the file, the unit checks the first characters of the file. If ! CONFIGURATION is present, the file contains menu configuration commands. Otherwise the file is considered firmware and is loaded into the flash memory and executed.

To download firmware with FTP:

1. Load the file onto the PC, host, or bridge from which the file was retrieved.
2. Select the **Dest** option.

Type the IP address for the:

- ◆ host
- ◆ PC
- ◆ Aironet 340 Series Bridge

3. Select the **Username** option.

Type the username required to access the firmware file.

If you download from another Aironet 340 Series Bridge, the **Username** option must have a value, even though the value is not used by the remote Aironet 340 Series Bridge.

4. Select the **Password** option

Type the password associated with the username.

If you download from another Aironet 340 Series Bridge, the login password value must match the console write privilege password on the remote Aironet 340 Series Bridge.

5. Select the **Filename** option.

- a. Type the name of the firmware file you retrieved, with drive and directory.
- b. Press **Enter**

If you download from another Aironet 340 Series Bridge, the **Filename** option must have a value, even though the value is not used by the remote Aironet 340 Series Bridge.

6. Select the **Get** option.

The unit begins an FTP session to the host PC, retrieves the file, programs the flash memory, and reboots.

This message appears:

```
220 sun host FTP server (SunOS 4.1) ready.
230 UseY 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.
```

Upload a New Firmware Version

Use the **Put** option to upload a copy of the current system firmware to another system. If the system is a:

- PC or host A copy of the firmware is stored on the disk for the system.

- Aironet 340 Series Bridge The remote Aironet 340 Series Bridge flashes the new code and begins to run it immediately. It is possible to use an Aironet 340 Series Bridge to upgrade another Aironet 340 Series Bridge.

To upload firmware with FTP:

1. Select the **Dest** option.

a. Type the IP address for the:

- ◇ host
- ◇ PC
- ◇ Aironet 340 Series Bridge

b. Press **Enter**.

2. Select the **Username** option.

a. Type the username for the:

- ◇ host
 - ◇ remote PC
 - ◇ Aironet 340 Series Bridge
- where the firmware is being uploaded

b. Press **Enter**.

If uploading to another Aironet 340 Series Bridge, the Username option must have a value, even though the value is not used by the remote Aironet 340 Series Bridge.

3. Select the **Password** option.

a. Type the access password for:

- ◇ host
- ◇ remote PC
- ◇ Aironet 340 Series Bridge

b. Press **Enter**.

4. Select the **Filename** option.

a. Type the name of the firmware file uploaded to the:

- ◇ host
- ◇ PC
- ◇ Aironet 340 Series Bridge (including drive and directory)

b. Press **Enter**.

If uploading to another Aironet 340 Series Bridge, the Filename option must have a value even though the value is not used by the remote Aironet 340 Series Bridge.

5. Select the **Put** option. The unit begins an FTP session with the:

- ◆ remote host
- ◆ PC
- ◆ Aironet 340 Series Bridge

Upload the Configuration for the Unit

This option saves the configuration on a remote host or PC in a format suitable for download using FTP or BOOTP.

At the prompt, create a file name for the file on the remote system. Once you enter the file name the transfer begins.

Download with the Internet Boot Protocol

When you power on the Aironet 340 Series Bridge, the Bootp/Dynamic Host Configuration Protocol (DHCP) option is enabled by default. Use this process to download firmware files with the Bootp/DHCP parameter.

1. On power up, the Aironet 340 Series Bridge issues boot protocol requests to see if there are any Bootp or DHCP servers on the infrastructure configured with the unit infrastructure address.
2. If the bridge finds no response, it repeats the request up to 30 times with a four second wait after the first request. It then doubles the time between requests for each additional retry. If there is still no response, the unit gives up.
3. If the unit receives multiple responses, the unit picks a DHCP server over a Bootp server.
4. If the bridge receives a response, the unit compares the IP address assigned to the unit by the server to the configured value. If they are different, the configured value is changed.
5. The bridge exams the downloaded file. If the file is not empty, the bridge assumes it is a configuration file in the format produced by the Configuration Dump menu command. The bridge uses a Trivial File Transfer Protocol (TFTP) dialogue to retrieve the file from the server.
6. The contents of the configuration file are processed as though the commands are entered by the operator at the console. The commands in the file modify the current configuration.

Note: The current configuration is not set back to the defaults before the file is processed. Therefore, it is not necessary for the file contents to be a complete configuration. The file contents only need to contain the items to be changed.

7. Once the configuration is processed, the name stored in the diagnostics load FTP filename parameter is assumed to be the name of the firmware file to download. If the parameter is not empty, the unit uses the TFTP protocol to load the file into RAM.
 - ◆ If the firmware is different from the version that currently runs, the unit programs the flash memory with the new code and restarts it to execute.
 - ◆ If the new firmware is the same, the unit discards the loaded file and continues normal operation.

Use the **Class** option to enter a class ID for a client node. The entered string is placed in the DHCP discover messages sent to the DHCP servers. The server determines how to respond based on the class ID.

Distribute Firmware or Configuration

Diagnostics Load Distribution Menu		
Option	Value	Description
1 - Go		- Start the 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

You can use the **Distribute** option to send the firmware or configuration from one Aironet 340 Series Bridge to all other Aironet 340 Series Bridges on the infrastructure. This is true whether the Aironet 340 Series Bridges are repeaters or are connected to the wired infrastructure. When you use the distribute function, the time needed to perform firmware upgrades or make global changes to the configuration is greatly decreased.

Use the Distribute option to upgrade all other units when you load a new version of the firmware into a single Aironet 340 Series Bridge or you change the configuration.

Control Which Units the Distribute Affects

The **Control** option commands how the remote units respond to a request to upload a configuration or firmware. Values options are:

- **None** The unit never responds and cannot be loaded by another unit with the distribute command.
- **Any** The unit always responds. It is up to the unit that distributes to determine whether to load the local unit.
- **Newer** The unit only responds if the version of firmware that is distributed has a larger version number than the code that currently runs. This selection only applies to firmware downloads. For configuration downloads this is equivalent to "any."
- **None of the Above** This is interpreted as a password that must be entered by the operator of the unit that distributes. The local unit does not respond to any distributions that do not supply this password.

If the distribution is password protected, only those units with the same password configured into the control parameter accept the distribution. This protects units from unwanted loads. Passwords are also used to divide the units into code load groups. When units are divided into code load groups, loads to one group do not affect the other groups.

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

Control Which Parts of the Configuration are Distributed

By default certain parts of the configuration are set as part of the distributable configuration. The distribution always contains all configuration items marked this way.

Each configuration item in the bridge is assigned a unique ID number that never changes over the life of the product. These numbers and the arguments to the configuration commands are distributed to prevent menu changes from affecting the configuration.

Use the **dump** command to display the status of the entire configuration. Each line starts with the ID number for the item and its arguments. In a comment field the string `local` appears if the item is not distributable and `sent` if it is. The current full text for the configuration item is in the comment field.

Use these commands to change an distribute status of an items:

- **add** Asks for a configuration ID and if the item is local or distributed.
- **remove** Asks for a configuration ID or "all" and returns the item to its default state.
- **show** Displays the table of changes. Starting the Distribution

Start the Distribution

Use the Go option to start the distribution. This message appears:

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

When the command executes, the local unit reports the new firmware file with its assigned version number. The unit sends a message to all units on the infrastructure similar to this message:

```
BR105E 004096001d45 has code version 3.2a (checksum 1598)
```

The remote units decide to respond based on the value of their `rcv_distribute` parameter.

When the local unit receives a response to its request, the remote unit is added to a list of units to load. When the response timeout period expires in about 10 seconds, the local unit begins to load all remote units in parallel with a proprietary protocol. A message similar to this displays:

```
Loading 004096001d45  
Loading 004096001d45
```

Any remote units that time out during the load, are removed from the list. Once all units load, the local unit displays a count of the successful loads. A message similar to this displays.

```
Completed loading 004096001d45  
Completed loading 00409610345f  
Loading of 2 Aironet 340 Series Bridges completed
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Wireless
Wireless – Mobility: WLAN Radio Standards
Wireless – Mobility: Security and Network Management
Wireless – Mobility: Getting Started with Wireless
Wireless – Mobility: General

Related Information

- [Wireless Technology](#)
 - [Cisco Aironet Access Point Software Configuration Guide](#)
 - [Technical Support – 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: Oct 15, 2009

Document ID: 8114
