CHAPTER 10

Managing Firmware and Configurations

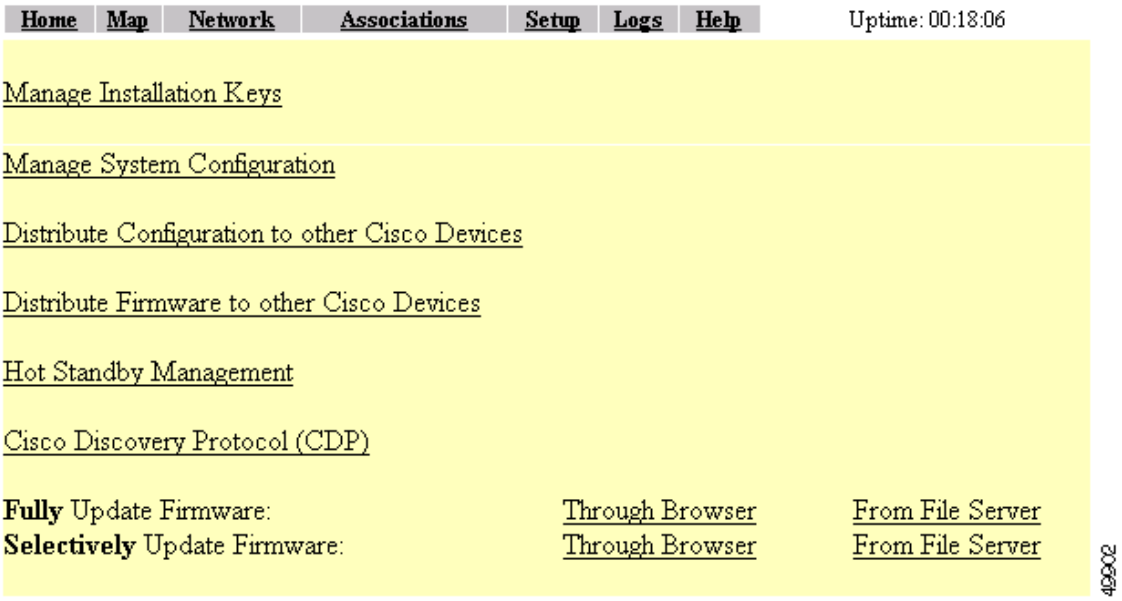
This section describes how to update the firmware version on the bridge, how to distribute firmware to other bridges, how to distribute the bridge's configuration to other bridges, and how to download, upload, and reset the bridge configuration. You use the Cisco Services Setup page as a starting point for all these activities.

This chapter contains the following sections:

Updating Firmware

You use the Cisco Services Setup page to update the bridge's firmware. You can perform the update by browsing to a local drive or by using FTP to update the firmware from a file server. Figure 10-1 shows the Cisco Services Setup page.

Figure 10-1 Cisco Services Setup Page



Follow this link path in the browser interface to reach the Cisco Services Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.

Removing Power During Firmware Update Can Corrupt Radio Firmware

When you update the firmware on the bridge, allow the unit to finish its start-up sequence before removing power. If you update the firmware and remove power before the bridge finishes the start-up sequence, the radio firmware might be corrupted, making the unit inoperable. If the radio firmware is corrupted, the radio indicator (the bottom of the three indicators on top of the unit) lights solid red and the following error message appears when the access point starts up:

```
Failed to start driver for port "awc0" (errno=0x006d0002)
```

If the bridge's radio firmware is corrupted, you must return the unit to Cisco for service.

You can safely remove power after a firmware update when the configuration management pages reappear in the command-line or web-browser interfaces, or when the three status indicators on top of the bridge complete the following pattern:

1. All three indicators light solid green, indicating that the access point is beginning to update the firmware.
2. The middle indicator lights solid green and the top and bottom indicators are not lit, indicating that the access point is updating the radio firmware.

When the middle indicator blinks or the top and bottom indicators blink, you can remove power.

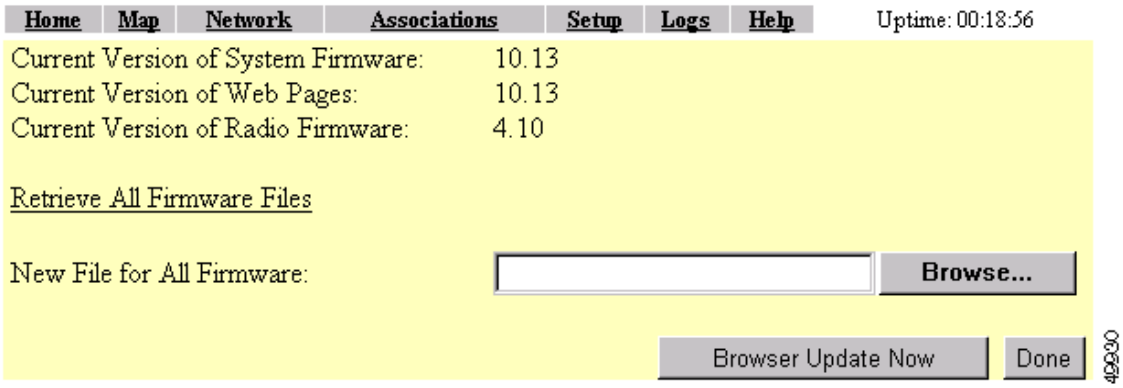
Updating with the Browser from a Local Drive

When you update firmware with your browser, you browse to the drive that contains the new firmware and load the firmware from there. You can update three firmware components individually or you can update all the firmware components at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **Through Browser** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware Through Browser page appears. Figure 10-2 shows the Update All Firmware Through Browser page.

Figure 10-2 Update All Firmware Through Browser Page



Follow these steps to update all three firmware components through the browser:

Step 1 If you know the exact path and filename of the new firmware image file, type it in the New File for All Firmware entry field.

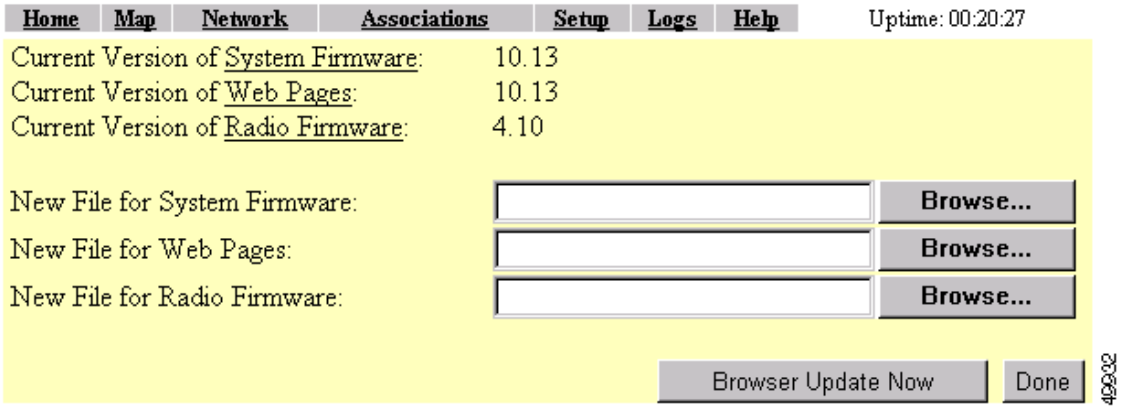
If you aren't sure of the exact path to the new firmware image file, click **Browse...** next to the New File entry field. When the File Upload window appears, go to the directory that contains the firmware image file and select the file. Click **Open**.

Step 2 When the filename for the new firmware appears in the New File entry field, click **Browser Update Now** to load and install the new firmware. When the update is complete, the bridge automatically reboots.

Selective Update of the Firmware Components

To update firmware components individually, click **Through Browser** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware Through Browser page appears. Figure 10-3 shows the Update Firmware Through Browser page.

Figure 10-3 Update Firmware Through Browser Page



Follow these steps to update one of the three firmware components through the browser:

Step 1 If you know the exact path and filename of the new firmware component, type it in the New File for [component] entry field.

If you aren't sure of the exact path to the new component, click **Browse...** next to the component's New File entry field. When the File Upload window appears, go to the directory that contains the component and select the file. Click **Open**.

Step 2 When the filename for the new component appears in the New File entry field, click **Browser Update Now** to load and install the new component. When the update is complete, the bridge automatically reboots.

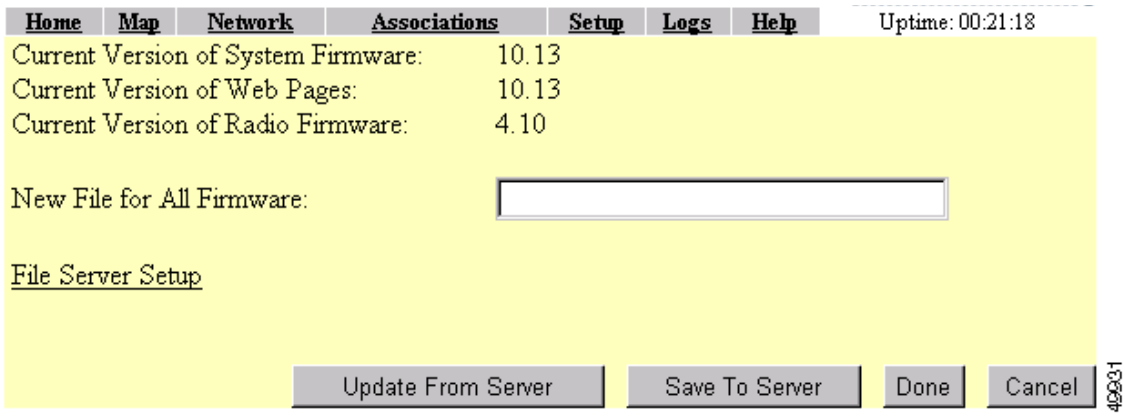
Updating from a File Server

When you update the firmware from a file server, you load new firmware through FTP or TFTP from a file server. You can update the three firmware components—the management system firmware, the firmware web pages, and the radio firmware—individually or all at once. It is simplest to update all the components at once, but in some situations you might want to update them individually.

Full Update of the Firmware Components

To update all the firmware components at the same time, click **From File Server** on the Fully Update Firmware line on the Cisco Services Setup page. The Update All Firmware From File Server page appears. Figure 10-4 shows the Update All Firmware From File Server page.

Figure 10-4 Update All Firmware From File Server Page



Follow these steps to update all three firmware components from a file server:

Step 1 Click the File Server Setup link to enter the FTP settings. The FTP Setup page appears. Figure 10-5 shows the FTP Setup page.

Figure 10-5 FTP Setup Page

Step 2 Enter the FTP settings on the FTP Setup page.

a. Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.

b. In the Default File Server entry field, enter the IP address of the server where the bridge should look for FTP files.

c. In the FTP Directory entry field, enter the directory on the server where FTP files are located.

d. In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.

e. In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.

f. Click **OK**. You return automatically to the Update All Firmware Through File Server page.

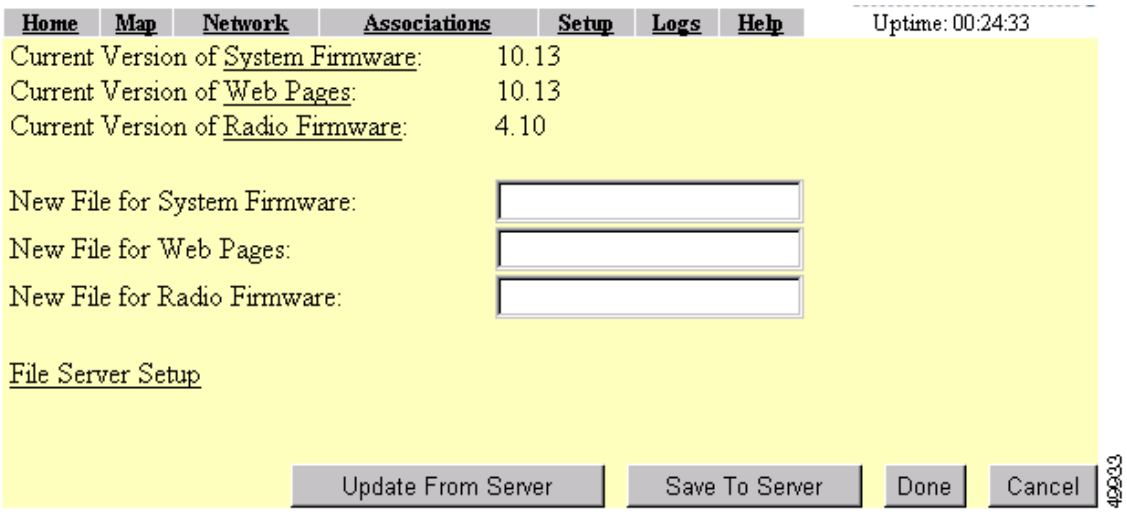
Step 3 On the Update All Firmware Through File Server page, type the filename of the new firmware image file in the New File for All Firmware entry field.

Step 4 Click **Update From Server** to load and install the new firmware. When the update is complete, the bridge automatically reboots.

Selective Update of the Firmware Components

To update firmware components individually, click **From File Server** on the Selectively Update Firmware line on the Cisco Services Setup page. The Update Firmware From File Server page appears. Figure 10-6 shows the Update Firmware From File Server page.

Figure 10-6 Update Firmware From File Server Page



To update one of the three firmware components from the file server, follow the steps listed in the "Full Update of the Firmware Components" section on page 10-4, but in Step 3, type the filenames of the firmware components you want to update in the components' entry fields. Click **Update From Server** to load and install the new firmware. When the update is complete, the bridge automatically reboots.

Distributing Firmware

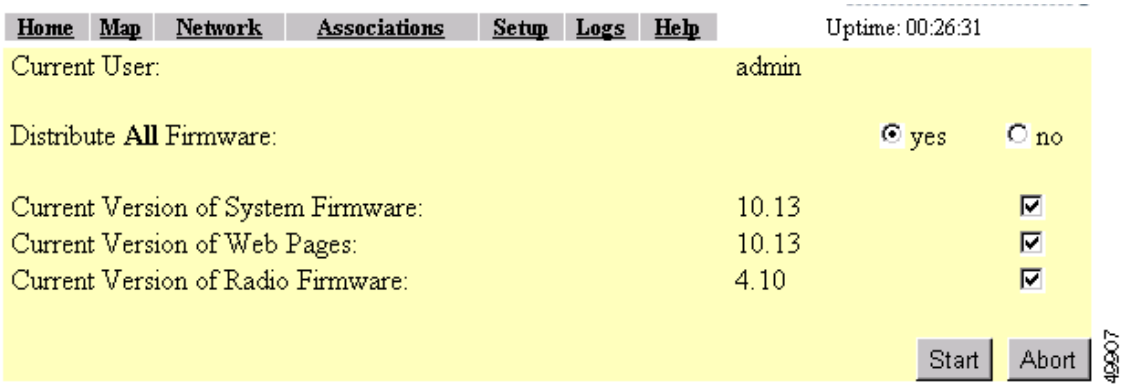
Use the Distribute Firmware page to distribute the bridge's firmware to other Cisco Aironet bridges. Figure 10-7 shows the Distribute Firmware page. The distributing bridge and the bridges that receive the firmware must have a Default Gateway setting other than the default setting, which is 255.255.255.155 (the Default Gateway setting is on the Express Setup and Routing Setup pages).

The bridge sends its firmware to all the bridges on your network that:

- Are running bridge firmware version 10.00 or newer
- Can detect the IP multicast query issued by the distributing bridge (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see Web Server Setup)

- Have the same HTTP port setting as the distributing bridge (the HTTP port setting is on the Web Server Setup page)
- Have a Default Gateway setting other than the default setting, which is 255.255.255.255
- If they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing bridge)

Figure 10-7 Distribute Firmware Page



Follow this link path in the browser interface to reach the Distribute Firmware page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Firmware to other Cisco Devices**.

Follow these steps to distribute firmware to other bridges:

Step 1 Follow the link path to reach the Distribute Firmware page.

Step 2 To distribute all firmware components at once, verify that *yes* is selected for Distribute All Firmware. This is the default setup for the Distribute Firmware page.

To distribute the firmware components individually, select **no** for Distribute All Firmware, and click the checkboxes for the components you want to distribute.

Step 3 Click **Start**. The bridge's firmware is distributed to the bridges on your network. To cancel the distribution, click **Abort**.

When the distribution is complete, the bridges that received the firmware automatically reboot.

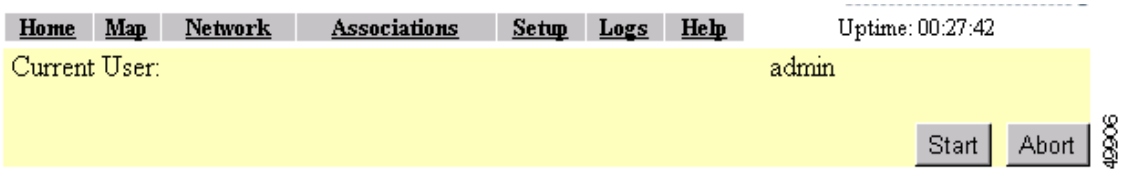
Distributing a Configuration

You use the Distribute Configuration page to distribute the bridge's configuration to other Cisco Aironet bridges. Figure 10-8 shows the Distribute Configuration page. The distributing bridge and the bridges that receive the configuration must have a Default Gateway setting other than the default setting, which is 255.255.255.155 (the Default Gateway setting is on the Express Setup and Routing Setup pages).

The bridge sends its entire system configuration except for its IP identity information and its User List. The configuration is sent and applied to all the bridges on your network that:

- Are running bridge firmware version 10.05 or newer
- Can detect the IP multicast query issued by the distributing bridge (network devices such as routers can block multicast messages)
- Have their web servers enabled for external browsing (see the "Entering Web Server Settings and Setting Up Bridge Help" section on page 7-7)
- Have the same HTTP port setting as the distributing bridge (the HTTP port setting is on the Web Server Setup page)
- Have a Default Gateway setting other than the default setting, which is 255.255.255.255
- If they have User Manager enabled, contain in their User Lists a user with the same user name, password, and capabilities as the user performing the distribution (the person logged in on the distributing bridge)

Figure 10-8 Distribute Configuration Page



Follow this link path in the browser interface to reach the Distribute Configuration page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Distribute Configuration to other Cisco Devices**.

Follow these steps to distribute the bridge's configuration to other bridges:

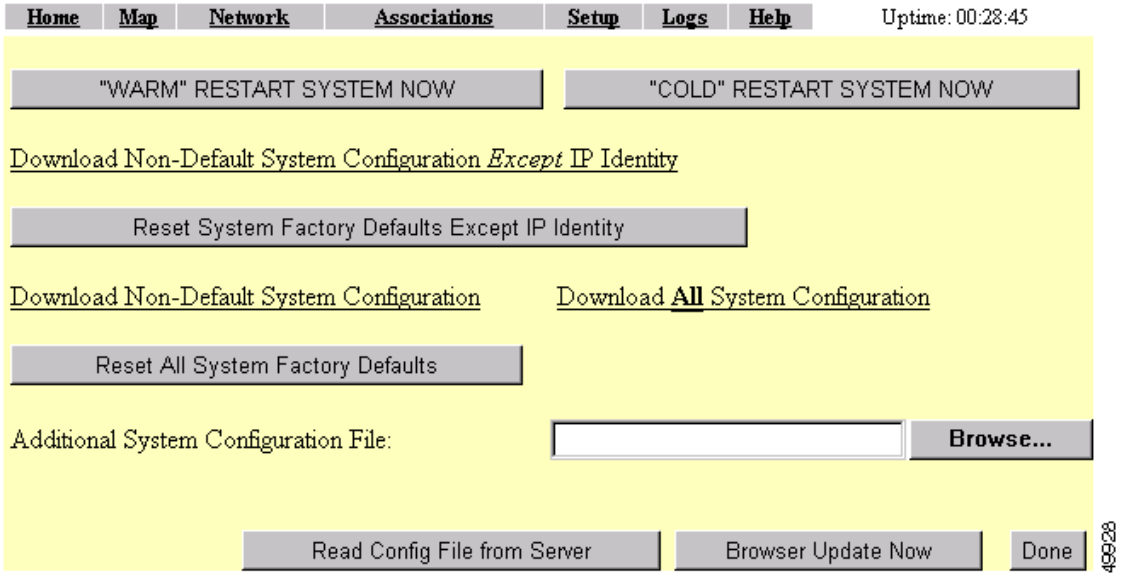
Step 1 Follow the link path to reach the Distribute Configuration page.

Step 2 Click **Start**. The bridge's configuration, except for its IP identity and its User List, is distributed to the bridges on your network. To cancel the distribution, click **Abort**.

Downloading, Uploading, and Resetting the Configuration

You use the System Configuration Setup page to download the current bridge configuration to a local drive, upload a configuration from a local drive or file server, and reset the configuration to default settings. You can also use the System Configuration Setup page to restart the bridge. Figure 10-9 shows the System Configuration Setup page.

Figure 10-9 System Configuration Setup Page



Follow this link path in the browser interface to reach the System Configuration Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Cisco Services Setup**.
3. On the Cisco Services page, click **Manage System Configuration**.

Downloading the Current Configuration

Follow these steps to download the bridge's current configuration to your hard drive or to a mapped network drive:

Step 1 Follow the link path to the System Configuration Setup page.

Step 2 If your web browser is Microsoft Windows Internet Explorer, use the download configuration links to save the configuration file:

- Click **Download System Configuration Except IP Identity** to save an .ini file containing the current configuration except for the bridge's IP address.
- To save the current non-default configuration including the bridge's IP address, click **Download Non-Default System Configuration**.
- To save the current default and non-default configuration including the bridge's IP address, click **Download All System Configuration**.

If your web browser is Netscape Communicator, use your right mouse button to click the download configuration links and select **Save link as** in the pop-up menu. If you click the links with your left mouse button, Netscape Communicator displays the text file but does not open the Save as window.

Step 3 When the Save as window appears, select the drive and directory where you want to save the file, and provide a filename for the configuration file. Click **Save**.

Uploading a Configuration

You can upload a configuration file to the bridge from your hard drive or a mapped network drive, or you can upload a configuration from a file server.

Uploading from a Local Drive

Follow these steps to upload a configuration file from your hard drive or a mapped network drive:

Step 1 Follow the link path in the browser interface to reach the System Configuration Setup page.

Step 2 If you know the exact path and filename of the configuration file, type it in the Additional System Configuration File entry field.

If you aren't sure of the exact path to the configuration file, click **Browse...** next to the entry field. When the File Upload window appears, go to the directory that contains the configuration file and select the file. Click **Open**.

Step 3 When the filename appears in the Additional System Configuration File entry field, click **Browser Update Now**.

The configuration file is loaded and applied in the bridge.

Uploading from a File Server

Follow these steps to upload a configuration file from a file server:

Step 1 Before you load a configuration file from a server, you need to enter FTP settings for the server. If you have already entered the FTP settings, skip to Step 3.

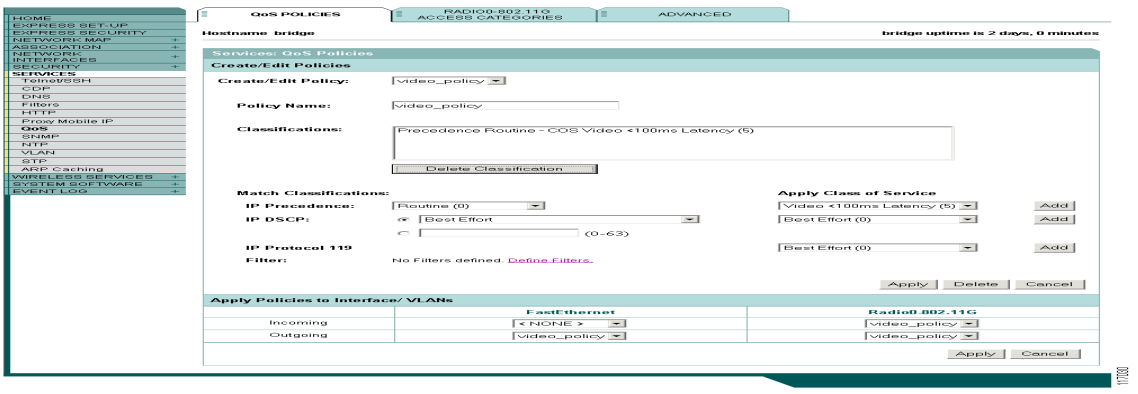
Follow this link path in the browser interface to reach the FTP Setup page:

a. On the Summary Status page, click **Setup**

b. On the Setup page, click **FTP**

The FTP Setup page appears. Figure 10-10 shows the FTP Setup page.

Figure 10-10 FTP Setup Page



Step 2 Enter the FTP settings on the FTP Setup page.

a. Select FTP or TFTP from the File Transfer Protocol pull-down menu. FTP (File Transfer Protocol) is the standard protocol that supports transfers of data between local and remote computers. TFTP (Trivial File Transfer Protocol) is a relatively slow, low-security protocol that requires no user name or password.

b. In the Default File Server entry field, enter the IP address of the server where the bridge should look for FTP files.

c. In the FTP Directory entry field, enter the directory on the server where FTP files are located.

d. In the FTP User Name entry field, enter the user name assigned to the FTP server. If you selected TFTP, you can leave this field blank.

e. In the FTP Password entry field, enter the password associated with the user name. If you selected TFTP, you can leave this field blank.

f. Click **OK**. You return automatically to the Setup page.

Step 3 Follow the link path in the web browser to reach the System Configuration Setup page.

Step 4 Click **Read Config File From Server**. The management system checks the server for several possible configuration filenames while attempting to load the configuration file. If the management system doesn't find the first filename, it continues to the next until it finds the file and loads it. It checks the server for the following names in the following order:

a. [system name].ini

b. [IP address].ini

c. [boot file from DHCP/BOOTP server].ini

d. [boot file from DHCP/BOOTP server].ini by TFTP

Resetting the Configuration

You can reset the bridge configuration to the default settings without resetting the bridge's IP identity, or you can reset the configuration to the default settings including the IP identity. If you reset the bridge's IP identity, however, you might lose your browser connection to the bridge.

Two buttons on the System Configuration Setup page reset the configuration to defaults:

- Reset System Factory Defaults Except IP Identity—this button returns all bridge settings to their factory defaults *except*:
  - The bridge's IP address, subnet mask, default gateway, and boot protocol
  - The users in the User Manager list
  - The SNMP Administrator Community name
- Reset All System Factory Defaults—this button returns all bridge settings to their factory defaults *except*:
  - The users in the User Manager list
  - The SNMP Administrator Community name

Note To completely reset all bridge settings to defaults, follow the steps in the "Resetting to the Default Configuration" section on page 13-31.

Follow these steps to reset the configuration to default settings:

Step 1 Follow the link path to reach the System Configuration Setup page. Figure 10-9 shows the System Configuration Setup page. The link path is listed under Figure 5-9.

Step 2 Click **Reset System Factory Defaults Except IP Identity** to reset the bridge configuration to the default settings without resetting the bridge's IP identity. Click **Reset All System Factory Defaults** to reset the configuration to the default settings including the IP identity.

Note If you reset the bridge's IP identity, you might lose your browser connection to the bridge.

Restarting the Bridge

Use the System Configuration Setup page to restart the bridge.

- Click **"Warm" Restart System Now** to perform a warm restart of the bridge. A warm restart reboots the bridge.
- Click **"Cold" Restart System Now** to perform a cold restart of the bridge. A cold restart is the equivalent of removing and then reapplying power for the bridge.