



Configuring Other Settings

This chapter identifies and provides information on how to configure other settings on the bridge, such as servers and association tables.

This chapter contains the following sections:

- [Server Setup, page 7-2](#)
- [Routing Setup, page 7-12](#)
- [Association Table Display Setup, page 7-13](#)
- [Event Notification Setup, page 7-18](#)

Server Setup

This section describes how to configure the server to support bridge features. You use separate management system pages to enter server settings. The server setup pages are described in the following sections:

- [Entering Time Server Settings, page 7-2](#)
- [Entering Boot Server Settings, page 7-4](#)
- [Entering Web Server Settings and Setting Up Bridge Help, page 7-7](#)
- [Entering Name Server Settings, page 7-9](#)



Note

See the “[Enabling EAP on the Bridge](#)” section on page 8-15 for instructions on setting up the authentication server.

Entering Time Server Settings

You use the Time Server Setup page to enter time server settings. [Figure 7-1](#) shows the Time Server Setup page:

Figure 7-1 Time Server Setup Page

Uptime: 3 days, 19:54:03

Map Help

Simple Network Time Protocol (SNTP): Enabled Disabled

Default Time Server:

Current Time Server:

GMT Offset (hr): (GMT - 05:00) Eastern Time (US & canada)

Use Daylight Savings Time: yes no

Manually set date (YYYY/MM/DD):

Manually set time (HH:MM:SS):

Apply OK Cancel Restore Defaults

81749

Follow this link path to reach the Time Server Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Time Server** under Services.

Settings on the Time Server Setup Page

The Time Server Setup page contains the following settings:

- [Simple Network Time Protocol](#)
- [Default Time Server](#)
- [GMT Offset \(hr\)](#)
- [Use Daylight Savings Time](#)
- [Manually Set Date and Time](#)

The page also shows the active time server.

Simple Network Time Protocol

Select **Enabled** or **Disabled** to turn Simple Network Time Protocol (SNTP) on or off. If your network uses SNTP, select **Enabled**.

Default Time Server

If your network has a default time server, enter the server's IP address in the Default Time Server entry field.

The Current Time Server line under the entry field reports the time server the bridge is currently using.



Note

The DHCP or BOOTP server can override the default time server.

GMT Offset (hr)

The GMT Offset drop-down menu lists the world's time zones relative to Greenwich Mean Time (GMT). Select the time zone in which the bridge operates.

Use Daylight Savings Time

Select **yes** or **no** to have the bridge automatically adjust to Daylight Savings Time.

Manually Set Date and Time

Enter the current date and time in the entry fields to override the time server or to set the date and time if no server is available.

When entering the date and time, use forward-slashes to separate the year, month, and day, and use colons to separate the hours, minutes, and seconds. For example, you would enter 2001/02/17 for February 17, 2001, and 18:25:00 for 6:25 pm.

Entering Boot Server Settings

You use the Boot Server Setup page to configure the bridge for your network's BOOTP or DHCP servers for automatic assignment of IP addresses. [Figure 7-2](#) shows the Boot Server Setup page:

Figure 7-2 Boot Server Setup Page

The screenshot shows the 'Boot Server Setup' page with a yellow background. At the top left are 'Map' and 'Help' buttons. At the top right is the 'Uptime: 6 days, 21:54:44'. The main configuration area includes:

- Configuration Server Protocol:** A dropdown menu set to 'DHCP'.
- Use previous Configuration Server settings when no server responds?** Radio buttons for 'yes' (selected) and 'no'.
- Read ".ini" file from file server?** A dropdown menu set to 'if specified by server' and a 'Load Now' button.
- Current Boot Server:** Text field containing '0.0.0.0'.
- Specified ".ini" File Server:** Text field containing '0.0.0.0'.
- BOOTP Server Timeout (sec):** Text field containing '120'.
- DHCP Multiple-Offer Timeout (sec):** Text field containing '5'.
- DHCP Requested Lease Duration (min):** Text field containing '1440'.
- DHCP Minimum Lease Duration (min):** Text field containing '0'.
- DHCP Client Identifier Type:** A dropdown menu set to 'Ethernet (10Mb)'.
- DHCP Client Identifier Value:** Text field containing '004096406fe6'.
- DHCP Class Identifier:** Text field containing 'AP4800E'.

At the bottom right are buttons for 'Apply', 'OK', 'Cancel', and 'Restore Defaults'. A vertical '4800E' label is on the far right edge.

Follow this link path to reach the Boot Server Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Boot Server** under Services.

Settings on the Boot Server Setup Page

The Boot Server Setup page contains the following settings:

- [Configuration Server Protocol](#)
- [Use Previous Configuration Server Settings](#)
- [Read .ini File from File Server](#)
- [BOOTP Server Timeout \(sec\)](#)
- [DHCP Multiple-Offer Timeout \(sec\)](#)
- [DHCP Requested Lease Duration \(min\)](#)
- [DHCP Minimum Lease Duration \(min\)](#)
- [DHCP Client Identifier Type](#)

- [DHCP Client Identifier Value](#)
- [DHCP Class Identifier](#)

The page also shows the IP address of the current boot server and specified “.ini” file server.

Configuration Server Protocol

Use the Configuration Server Protocol drop-down menu to select your network’s method of IP address assignment. The menu contains the following options:

- None—Your network does not have an automatic system for IP address assignment.
- BOOTP—Your network uses Boot Protocol, in which IP addresses are hard-coded based on MAC addresses.
- DHCP—With Dynamic Host Configuration Protocol, IP addresses are leased for a period of time. You can set the lease duration with the settings on this page.

Use Previous Configuration Server Settings

Select **yes** to have the bridge save the boot server’s most recent response. The bridge uses the most recent settings if the boot server is unavailable.

Read .ini File from File Server

Use this setting to have the bridge use configuration settings in an .ini file on the BOOTP or DHCP server or the default file server. Files with .ini extensions usually contain configuration information used during system start-up. The drop-down menu contains the following options:

- Always—The bridge always loads configuration settings from an .ini file on the server.
- Never—The bridge never loads configuration settings from an .ini file on the server.
- If specified by server—The bridge loads configuration settings from an .ini file on the server if the server’s DHCP or BOOTP response specifies that an .ini file is available. This is the default setting.

The Load Now button under the drop-down menu tells the bridge to read an .ini file immediately.

The Current Boot Server line under the drop-down menu lists the server that responded to the bridge’s boot request. If all zeros appear, it means that the bridge is not using BOOTP/DHCP or that no server responded to the BOOTP/DHCP request. The Specified “.ini” File Server line lists the IP address of the server where the .ini file is stored. If all zeroes appear, it means that no file server is set up to provide an .ini file.

BOOTP Server Timeout (sec)

This setting specifies the length of time the bridge waits to receive a response from a single BOOTP server. Enter the number of seconds the bridge should wait. This setting applies only when you select BOOTP from the Configuration Server Protocol drop-down menu.

DHCP Multiple-Offer Timeout (sec)

This setting specifies the length of time the bridge waits to receive a response when there are multiple DHCP servers. Enter the number of seconds the bridge should wait.

DHCP Requested Lease Duration (min)

This setting specifies the length of time the bridge requests for an IP address lease from your DHCP server. Enter the number of minutes the bridge should request.

DHCP Minimum Lease Duration (min)

This setting specifies the shortest amount of time the bridge accepts for an IP address lease. The bridge ignores leases shorter than this period. Enter the minimum number of minutes the bridge should accept for a lease period.

DHCP Client Identifier Type

Use this optional setting to include a class identifier type in the DHCP request packets the bridge sends to your DHCP server. Your DHCP server can be set up to send responses according to class identifier type. If most of the client devices using the bridge are the same device type, you can select that device type to be included in the DHCP request packet.

Use **Ethernet (10Mb)**, the default setting, if you do not intend to set up your DHCP server to send responses according to class identifier type.

If you want to include a unique value in the DHCP Client Identifier Value field (the setting under DHCP Client Identifier Type on the Boot Server Setup page), select **Other - Non Hardware**.

[Table 7-1](#) lists the options in the DHCP Client Identifier Type drop-down menu.

Table 7-1 Options in the DHCP Client Identifier Type Menu

Option	Definition
Ethernet (10Mb)	This is the default setting. Use this setting if you do not need your DHCP server to send responses based on the class identifier in the bridge's DHCP request packets.
Experimental Ethernet	Select one of these specific device types if most of the client devices using the bridge are the same device type. The bridge includes the device type in the DHCP request packets it sends to the DHCP server.
Amateur Radio AX.25	
Proteon ProNET Token Ring	
Chaos	
IEEE 802 Networks	
ARCNET	
Hyperchannel	
Lanstar	
Autonet Short Address	
LocalTalk	
LocalNet	
Other - Non Hardware	Select this option to include a unique value in the DHCP Client Identifier Value field.

DHCP Client Identifier Value

Use this setting to include a unique identifier in the bridge's DHCP request packet. This field contains the bridge's MAC address by default. If you select **Other - Non Hardware** from the DHCP Client Identifier Type drop-down menu, you can enter up to 255 alphanumeric characters. If you select any other option from the DHCP Client Identifier Type drop-down menu, you can enter up to 12 hexadecimal characters. Hexadecimal characters include the numbers 0 through 9 and the letters A through F.

DHCP Class Identifier

Your DHCP server can be set up to send responses according to the group to which a device belongs. Use this field to enter the bridge's group name. The DHCP server uses the group name to determine the response to send to the bridge. The bridge's DHCP class identifier is a vendor class identifier.

Entering Web Server Settings and Setting Up Bridge Help

You use the Web Server Setup page to enable browsing to the web-based management system, specify the location of the bridge Help files, and enter settings for a custom-tailored web system for bridge management. [Figure 7-3](#) shows the Web Server Setup page:

Figure 7-3 Web Server Setup Page

Map Help Uptime: 02:30:58

Allow Non-Console Browsing? yes no

HTTP Port:

Default Help Root URL:

Extra Web Page File: Load Now

Default Web Root URL:

Apply OK Cancel Restore Defaults

49306

Follow this link path to reach the Web Server Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Web Server** under Services.

Settings on the Web Server Setup Page

The Web Server Setup page contains the following settings:

- [Allow Non-Console Browsing](#)
- [HTTP Port](#)
- [Default Help Root URL](#)
- [Extra Web Page File](#)
- [Default Web Root URL](#)

Allow Non-Console Browsing

Select **yes** to allow browsing to the management system. If you select no, the management system is accessible only through the console and Telnet interfaces.

HTTP Port

This setting determines the port through which your bridge provides web access. Your System Administrator should be able to recommend a port setting.

Default Help Root URL

This entry tells the bridge where to look for the Help files. The Help button on each management system page opens a new browser window displaying help for that page. The online help files are provided on the bridge and bridge CD in the Help directory. You can point to the help files in one of four possible locations:

- **Internet**—Cisco maintains up-to-date help for bridges on the Cisco website. While this location requires online access for every occasion of needing online help, it offers the most up-to-date information. If you use this help location, which is the default setting, you don't need to copy the files from the bridge and bridge CD.
- **File Server**—On multi-user networks, the help files can be placed on the network file server. For this location, enter the full directory URL in the Default Help Root URL entry field. Your entry might look like this:
`[system name]\[directory]\wireless\help`
- **Hard Drive**—you can copy the help files to the hard drive of the computer you use to manage the wireless LAN. If you use this location, enter the full directory URL. Your entry might look like this:
`file:/// [drive letter]:\[folder or subdirectory]\wireless\help`

Extra Web Page File

If you need to create an alternative to the bridge's management system, you can create HTML pages and load them into the bridge. You use this entry field to specify the filename for your HTML page stored on the file server.

Click **Load Now** to load the HTML page.

Default Web Root URL

This setting points to the bridge management system's HTML pages. If you create alternative HTML pages, you should change this setting to point to the alternative pages. The default setting is:

mfs0:/StdUI/

Entering Name Server Settings

You use the Name Server Setup page to configure the bridge to work with your network's Domain Name System (DNS) server. [Figure 7-4](#) shows the Name Server Setup page:

Figure 7-4 The Name Server Setup Page

The screenshot shows the Name Server Setup page with the following configuration:

- Domain Name System (DNS): Enabled Disabled
- Default Domain:
- Current Domain: company.com
- Domain Name Servers:

	Default	Current
1.	<input type="text" value="209.165.200.229"/>	209.165.200.229
2.	<input type="text" value="209.165.200.240"/>	209.165.200.240
3.	<input type="text"/>	
- Domain Suffix:

Buttons at the bottom: Apply, OK, Cancel, Restore Defaults. Uptime: 02:32:22. A vertical ID number 490009 is on the right side.

Follow this link path to reach the Name Server Setup page:

- On the Summary Status page, click **Setup**
- On the Setup page, click **Name Server** under Services.

Settings on the Name Server Setup Page

The Name Server Setup page contains the following settings:

- [Domain Name System](#)
- [Default Domain](#)
- [Domain Name Servers](#)
- [Domain Suffix](#)

Domain Name System

If your network uses a Domain Name System (DNS), select **Enabled** to direct the bridge to use the system. If your network does not use DNS, select **Disabled**.

Default Domain

Enter the name of your network's IP domain in the entry field. Your entry might look like this:

mycompany.com

The Current Domain line under the entry field lists the domain that is serving the bridge. The current domain might be different from the domain in the entry field if, on the Boot Server Setup page, you have DHCP or BOOTP set as the Configuration Server Protocol, but you selected No for the setting “Use previous Configuration Server settings when no server responds?”

Domain Name Servers

Enter the IP addresses of up to three domain name servers on your network. The Current lines to the right of the entry fields list the servers the bridge is currently using, which may be specified by the DHCP or BOOTP server.

Domain Suffix

In this entry field, enter the portion of the full domain name that you would like omitted from bridge displays. For example, in the domain “mycompany.com” the full name of a computer might be “mycomputer.mycompany.com.” With domain suffix set to “mycompany.com,” the computer's name would be displayed on management system pages as simply “mycomputer.”

Entering FTP Settings

You use the FTP Setup page to assign File Transfer Protocol settings for the bridge. All non-browser file transfers are governed by the settings on this page.

Figure 7-5 shows the FTP Setup page:

Figure 7-5 The FTP Setup Page

The screenshot shows the FTP Setup page with the following elements:

- Map Help** (top left)
- Uptime: 02:37:33** (top right)
- File Transfer Protocol:** A dropdown menu with **FTP** selected.
- Default File Server:** An empty text input field.
- FTP Directory:** An empty text input field.
- FTP User Name:** A text input field containing **anonymous**.
- FTP User Password:** A text input field containing *********.
- Buttons:** **Apply**, **OK**, **Cancel**, and **Restore Defaults** (bottom right).
- 49918** (vertical text on the right edge)

Follow this link path to reach the FTP Setup page:

- On the Summary Status page, click **Setup**
- On the Setup page, click **FTP** under Services.

Settings on the FTP Setup Page

The FTP Setup page contains the following settings:

- [File Transfer Protocol](#)
- [Default File Server](#)
- [FTP Directory](#)
- [FTP User Name](#)
- [FTP User Password](#)

File Transfer Protocol

Use the drop-down menu to select **FTP** or **TFTP** (Trivial File Transfer Protocol). TFTP is a relatively slow, low-security protocol that requires no username or password.

Default File Server

Enter the IP address or DNS name of the file server where the bridge should look for FTP files.

FTP Directory

Enter the file server directory that contains the firmware image files.

FTP User Name

Enter the username assigned to your FTP server. You don't need to enter a name in this field if you select TFTP as the file transfer protocol.

FTP User Password

Enter the password associated with the file server's username. You don't need to enter a password in this field if you select TFTP as the file transfer protocol.

Routing Setup

You use the Routing Setup page to configure the bridge to communicate with the IP network routing system. You use the page settings to specify the default gateway and to build a list of installed network route settings. [Figure 7-6](#) shows the Routing Setup page.

Figure 7-6 Routing Setup Page

The screenshot shows the Routing Setup page with the following elements:

- Buttons: **Map** and **Help** at the top left.
- Uptime: 02:38:32 at the top right.
- Default Gateway:** A text input field containing the IP address 209.165.200.201.
- New Network Route:** A section with three input fields:
 - Dest Network:** An empty text input field.
 - Gateway:** An empty text input field.
 - Subnet Mask:** An empty text input field.
- Installed Network Routes:** A scrollable list box that is currently empty.
- Buttons: **Add** and **Remove** buttons are positioned to the right of the New Network Route and Installed Network Routes sections, respectively.
- Bottom navigation buttons: **Apply**, **OK**, **Cancel**, and **Restore Defaults**.
- A small vertical number 49324 is visible on the right edge of the page.

Follow this link path to reach the Routing Setup page:

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

Entering Routing Settings

The Routing Setup page contains the following settings:

- [Default Gateway](#)
- [New Network Route Settings](#)
- [Installed Network Routes List](#)

Default Gateway

Enter the IP address of your network's default gateway in this entry field. The entry 255.255.255.255 indicates no gateway.

New Network Route Settings

You can define additional network routes for the bridge. To add a route to the installed list, fill in the three entry fields and click **Add**. To remove a route from the list, highlight the route and click **Remove**. The three entry fields include:

- Dest Network—Enter the IP address of the destination network.
- Gateway—Enter the IP address of the gateway used to reach the destination network.
- Subnet Mask—Enter the subnet mask associated with the destination network.

Installed Network Routes List

The list of installed routes provides the destination network IP address, the gateway, and the subnet mask for each installed route.

Association Table Display Setup

You use the Association Table Filters and the Association Table Advanced pages to customize the display of information in the bridge's Association Table.

Association Table Filters Page

Figure 7-7 shows the Association Table Filters page.

Figure 7-7 Association Table Filters Page

Map Help Uptime: 02:39:47

Stations to Show: Client Repeater Bridge AP
 Infra. Host Multicast Entire Network

Fields to Show: System Name IP Address Device Class
 State Parent SW Version

Packets To/From Station: Total Alert
Bytes To/From Station: Total Alert

Primary Sort: Device System Name IP Addr./Name MAC Address Class Parent
Secondary Sort: Device System Name IP Addr./Name MAC Address Class

OK Cancel Restore Defaults 490098

Follow this link path to reach the Association Table Filters page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Display Defaults** under Associations.

You can also reach the Association Table Filters page through the “additional display filters” link on the Association Table page. When you reach the page through the “additional display filters” link, four buttons appear at the bottom of the page that are different from the standard buttons on management system pages. The buttons include:

- **Apply**—Applies your selections to the Association Table and returns you to the Association Table page.
- **Save as Default**—Saves your selections as new default settings and returns you to the Association Table page.
- **Restore Current Defaults**—Applies the currently saved default settings to the Association Table and returns you to the Association Table page.
- **Restore Factory Defaults**—Applies the factory default settings to the Association Table and returns you to the Association Table page.

Settings on the Association Table Filters Page

The Association Table Filters page contains the following settings:

- [Stations to Show](#)
- [Fields to Show](#)
- [Packets To/From Station](#)
- [Bytes To/From Station](#)
- [Primary Sort](#)
- [Secondary Sort](#)

Stations to Show

Select the station types that you want to be displayed in the Association Table. If you select all station types, all stations of these types appear in the bridge’s Association Table.

Fields to Show

The fields you select here are the column headings for the Association Table. Fields include:

- **System Name**—A device’s system name.
- **State**—A device’s operational state. Possible states include:
 - **Assoc**—The station is associated with a bridge.
 - **Unauth**—The station is unauthenticated with any bridge.
 - **Auth**—The station is authenticated with an bridge.
- **IP Address**—A device’s IP address.
- **VlanID**—The VLAN used by the client.
- **SSID**—The client’s SSID.
- **Parent**—A wireless client device’s parent device, which is usually an bridge.
- **Device**—A device’s type, such as a 350 series bridge or a PC Client Card. Non-Aironet devices appear as “Generic 802.11” devices.

- SW Version—The current version of firmware on a device.
- Class—A device’s role in the wireless LAN. Classes include:
 - AP—an access point station.
 - Client or PS Client—a client or power-save client station.
 - Bridge, Bridge R—a bridge or a root bridge.
 - Rptr—a repeater bridge.
 - Mcast—a multicast address.
 - Infra—an infrastructure node, usually a workstation with a wired connection to the Ethernet network.

Packets To/From Station

Use these settings to display packet volume information in the Association Table. Select **Total** to display the total number of packets to and from each station on the network.

Select **Alert** to display the number of alert packets to and from each station on the network for which you have activated alert monitoring. Select the **Alert** checkbox on a device’s Station page to activate alert monitoring for that device. See the [“Using Station Pages” section on page 9-3](#).

The Total and Alert selections both add a column to the Association Table.

Bytes To/From Station

Use these settings to display byte volume information in the Association Table. Select **Total** to display the total number of bytes to and from each station on your wireless network. Select **Alert** to display the number of alert bytes to and from each station on the wireless network. Both selections add a column to the Association Table.

Primary Sort

This setting determines the information that appears in the first column in the Association Table. Choices available are:

- Device
- System Name
- IP Address or domain name
- MAC Address
- VLAN
- SSID
- Class
- Parent

Secondary Sort

This setting determines the information that appears in the second column in the Association Table. All primary sort options, except Parent, are available for the secondary sort.

Association Table Advanced Page

You use the Association Table Advanced page to control the total number of devices the bridge can list in the Association Table and the amount of time the bridge continues to track each device class when a device is inactive. [Figure 7-8](#) shows the Association Table Advanced page.

Figure 7-8 Association Table Advanced Page

Map Help Uptime: 5 days, 00:28:12

Handle Alerts as Severity Level External Information

Maximum number of bytes stored per Alert packet 0

Maximum Number of Forwarding Table Entries: 8192

Rogue AP Alert Timeout (minutes) 30

RFC 1493 802.1D Statistics in MIB (**dot1dTpFdbTable**): Enabled Disabled

Aironet Extended Statistics in MIB (**awcTpFdbTable**): Enabled Disabled

Map Multicast Entries to Broadcast Entry: Enabled Disabled

Block ALL Inter-Client Communications ("PSPF"): Yes No

Default Activity Timeout (seconds) Per Device Class:

Unknown Class 300

Multicast Addresses 28800

Infrastructure Hosts 1800

Client Stations 1800

Repeaters 28800

Access Points 28800

Across-Bridge Hosts 1800

Non-Root Bridges 28800

Root Bridges 28800

Apply OK Cancel Restore Defaults

Follow this link path to reach the Association Table Advanced page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Advanced** under Associations.

Settings on the Association Table Advanced Page

The Association Table Advanced page contains the following settings:

- [Handle Station Alerts as Severity Level](#)
- [Maximum number of bytes stored per Station Alert packet](#)
- [Maximum Number of Forwarding Table Entries](#)
- [Rogue AP Alert Timeout \(minutes\)](#)
- [RFC 1493 802.1D Statistics in MIB \(dot1dTpFdbTable\)](#)

- [Aironet Extended Statistics in MIB \(awcTpFdbTable\)](#)
- [Block ALL Inter-Client Communications \(PSPF\)](#)
- [Map Multicast Entries to Broadcast Entry](#)
- [Default Activity Timeout \(seconds\) Per Device Class](#)

Handle Station Alerts as Severity Level

This setting determines the Severity Level at which Station Alerts are reported in the Event Log. This setting also appears on the Event Handling Setup page. You can choose from four Severity Levels:

- **Fatal Severity Level (System, Protocol, Port)**—Fatal-level events indicate an event that prevents operation of the port or device. For operation to resume, the port or device usually must be reset. Fatal-level events appear in red in the Event Log.
- **Alert Severity Level (System, Protocol, Port, External)**—Alert-level messages indicate that you need to take action to correct the condition and appear in magenta in the Event Log.
- **Warning Severity Level (System, Protocol, Port, External)**—Warning-level messages indicate that an error or failure may have occurred and appear in blue in the Event Log.
- **Information Severity Level (System, Protocol, Port, External)**—Information-level messages notify you of some sort of event, not fatal (that is, the port has been turned off, the rate setting has been changed, etc.) and appear in green in the Event Log.

Maximum number of bytes stored per Station Alert packet

This setting determines the maximum number of bytes the bridge stores for each Station Alert packet when packet tracing is enabled. If you use 0 (the default setting), the bridge does not store bytes for Station Alert packets; it only logs the event. See the [“Event Handling Setup Page” section on page 7-21](#) for instructions on enabling packet tracing.

Maximum Number of Forwarding Table Entries

This setting determines the maximum number of devices that can appear in the Association Table.

Rogue AP Alert Timeout (minutes)

When an bridge detects a rogue bridge, it sends an alert message to the system log. This setting specifies the amount of time in minutes the bridge transmits the alert message. When the timeout is reached, the bridge stops sending the alert message.

RFC 1493 802.1D Statistics in MIB (dot1dTpFdbTable)

Use this setting to enable or disable the storage of detailed RFC 1493 802.1D statistics in access point memory. When you disable extended statistics you conserve memory, and the access point can include more devices in the Association Table.

Aironet Extended Statistics in MIB (awcTpFdbTable)

Use this setting to enable or disable the storage of detailed statistics in bridge memory. When you disable extended statistics you conserve memory, and the bridge can include more devices in the Association Table.

Block ALL Inter-Client Communications (PSPF)

Publicly Secure Packet Forwarding (PSPF) prevents client devices associated to an bridge from inadvertently sharing files with other client devices on the wireless network. It provides Internet access to client devices without providing other capabilities of a LAN. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network. This feature is useful for public wireless networks like those installed in airports or on college campuses.

**Note**

The PSPF feature is available in firmware versions 11.08 and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at <http://www.cisco.com/public/sw-center/sw-wireless.shtml>.

Map Multicast Entries to Broadcast Entry

Use this setting to make the bridge more virus resistant. Some viruses send entire 1000+ blocks of multicast MAC addresses to the network, which overwhelms the access point's forwarding table. Setting this parameter to enabled maps all multicast MAC addresses into the broadcast address (without changing the packet's MAC address). When this parameter is enabled, the bridge is not able to distinguish between multicast and broadcast addresses.

Default Activity Timeout (seconds) Per Device Class

These settings determine the number of seconds the bridge continues to track an inactive device depending on its class. A setting of zero tells the bridge to track a device indefinitely no matter how long it is inactive. A setting of 300 equals 5 minutes; 1800 equals 30 minutes; 28800 equals 8 hours.

Event Notification Setup

You use the Event Display Setup, Event Handling Setup, and Event Notifications Setup pages to customize the display of bridge events (alerts, warnings, and normal activity).

Event Display Setup Page

You use the Event Display Setup page to determine how time should be displayed on the Event Log. In addition, you can determine what severity level is significant enough to display an event. [Figure 7-9](#) shows the Event Display Setup page.

Figure 7-9 The Event Display Setup Page

Map Help Uptime: 02:45:33

How should time generally be displayed? Wall-Clock Time

How should Event Elapsed (non-wall-clock) Time be displayed? Since Boot

Severity Level at which to display events immediately on the console: External Information

Severity Level at which to display events on the console log: External Information

Severity Level at which to display events on the GUI log: External Information

Apply OK Cancel Restore Defaults

Follow this link path to reach the Event Display Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Display Defaults** under Event Log.

Settings on the Event Display Setup Page

The Event Display Setup page contains the following settings:

- [How should time generally be displayed?](#)
- [How should Event Elapsed \(non-wall-clock\) Time be displayed?](#)
- [Severity Level at which to display events](#)

How should time generally be displayed?

You use this drop-down menu to determine whether the events in the Event Log are displayed as system uptime or wall-clock time. If you select system uptime, the events are displayed either since the boot or since the last time the Event Log was displayed. If you select wall-clock time, the events are displayed in a YY:MM:DD HH:MM:SS format. If time has not been set on the bridge (either manually or by a time server), the time display appears as uptime regardless of this selection.

How should Event Elapsed (non-wall-clock) Time be displayed?

Choose to display event time since the last boot-up of the bridge or the time that has elapsed since the event occurred.

Severity Level at which to display events

When an event occurs, it may be displayed immediately on the console, on the console log, or on the GUI log for read purposes only. The event may also be recorded. (You control display and recording of events through the Event Handling Setup page; see the [“Event Handling Setup Page” section on page 7-21](#) for details.) Use the drop-down menus to choose one of the sixteen severity levels for each display area. [Table 7-2](#) lists the severity levels.

Table 7-2 Event Display Severity Levels

Severity Level	Description
silent	The *silent* setting directs the bridge to not display any events immediately on the console, the console log, or the GUI log.
System Fatal Protocol Fatal Port Fatal	The Fatal settings indicate an event that prevents operation of the port or device. For operation to resume, the port or device usually must be reset. <ul style="list-style-type: none"> • System refers to the bridge as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the bridge's Ethernet or radio network interface.
System alert Protocol alert Port alert External alert	The Alert settings indicate events of which an administrator specifically requested to be informed. <ul style="list-style-type: none"> • System refers to the bridge as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the bridge's Ethernet or radio network interface. • External refers to a device on the network other than the bridge.
System warning Protocol warning Port warning External warning	The Warning settings indicate that a failure has occurred. <ul style="list-style-type: none"> • System refers to the bridge as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the bridge's Ethernet or radio network interface. • External refers to a device on the network other than the bridge.
System information Protocol information Port information External information	The Information settings indicate a normal action that isn't fatal (that is, the port has been turned off, the rate setting has been changed, etc.) <ul style="list-style-type: none"> • System refers to the bridge as a whole. • Protocol refers to a specific communications protocol in use, such as HTTP or IP. • Port refers to the bridge's Ethernet or radio network interface. • External refers to a device on the network other than the bridge.

These selections affect display of events only. They are used to filter information, not to remove it from the Event Log. To remove information from the Event Log, click **Purge Log** on the Event Log page.

Event Handling Setup Page

You use the Event Handling Setup page to determine how notification of the fatal, alert, warning, and information events should occur. You can choose to only count the events, display them to the console but not store them, record them after displaying them on the console, or notify someone of the occurrence after displaying and recording the event. [Figure 7-10](#) shows the Event Handling Setup page.

Figure 7-10 The Event Handling Setup Page

The screenshot shows the Event Handling Setup page with the following elements:

- Buttons: [Map](#), [Help](#)
- Uptime: 1 day, 04:43:03
- Table: Disposition of Events (by Severity Level) and Total Events
- Configuration options for Alerts and Detailed Event Trace Buffer.
- Buttons: Clear Alert Statistics, Purge Trace Buffer

Disposition of Events (by Severity Level)	Total Events
System Fatal	0
Protocol Fatal	0
Network Port Fatal	0
System Alert	0
Protocol Alert	0
Network Port Alert	0
External Alert	0
System Warning	0
Protocol Warning	0
Network Port Warning	0
External Warning	0
System Information	0
Protocol Information	0
Network Port Information	87
External Information	0

Handle **Alerts** as Severity Level: External Information

Maximum number of bytes stored per **Alert** packet: 0

Maximum memory reserved for **Detailed Event Trace Buffer** (bytes): 0

Download **Detailed Event Trace Buffer**: [Headers Only](#) [All Data](#)

Buttons: Clear Alert Statistics, Purge Trace Buffer

Follow this link path to reach the Event Handling Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Event Handling** under Event Log.

Settings on the Event Handling Setup Page

The Event Handling Setup page contains the following settings:

- [Disposition of Events](#)
- [Handle Alerts as Severity Level](#)
- [Maximum number of bytes stored per Alert packet](#)
- [Maximum memory reserved for Detailed Event Trace Buffer \(bytes\)](#)
- [Download Detailed Event Trace Buffer](#)
- [Clear Alert Statistics](#)
- [Purge Trace Buffer](#)

Disposition of Events

The event settings control how events are handled by the bridge: counted, displayed in the log, recorded, or announced in a notification. The settings are color coded: red for fatal errors, magenta for alerts, blue for warnings, and green for information. You select an option from each setting's drop-down menu. Each option includes and builds upon the previous option.

- **Count**—Tallies the total events occurring in this category without any form of notification or display.
- **Display Console**—Provides a read-only display of the event but does not record it.
- **Record**—Makes a record of the event in the log and provides a read-only display of the event.
- **Notify**—Makes a record of the event in the log, displays the event, and tells the bridge to notify someone of the occurrence.

Handle Alerts as Severity Level

You use this setting to set a severity level for Station Alerts. Use the drop-down menu to choose one of the sixteen severity levels. [Table 7-2 on page 7-20](#) lists the severity levels in the menu. The *silent* option is not available for station events, however.

Maximum number of bytes stored per Alert packet

Enter the number of bytes the access point should store for each packet. If you want to see the entire contents of each packet, enter **1600**; if you want to see only the packet header, enter **64**.

Maximum memory reserved for Detailed Event Trace Buffer (bytes)

Enter the number of bytes reserved for the Detailed Event Trace Buffer. The Detailed Event Trace Buffer is a tool for tracing the contents of packets between specified stations on your network.

After you reserve space for the trace buffer, browse to a device's Station page and select the **Alert** checkboxes in the To Station and From Station columns. See the [“Browsing to Network Devices” section on page 9-2](#) for instructions on opening a device's Station page.

Download Detailed Event Trace Buffer

Use these links to view Headers Only or All Data in the detailed trace buffer. The number of bytes saved per packet is controlled on the Association Table Advanced Setup page.

If your browser is Netscape Communicator, click the links with your left mouse button to view the trace data. Click the links with your right mouse button and select **Save Link As** to save the data in a file.

Clear Alert Statistics

Click this button to reset the alert tallies to 0.

Purge Trace Buffer

Click this button to delete the packet traces from the Event Trace Buffer.

Event Notifications Setup Page

You use the Event Notifications Setup page to enable and configure notification of fatal, alert, warning, and information events to destinations external to the bridge, such as an SNMP server or a Syslog system.

**Note**

For event notifications to be sent to an external destination, the events must be set to Notify on the Event Handling Setup page. See the [“Event Handling Setup Page”](#) section on page 7-21 for a description of the settings on the Event Handling Setup page.

[Figure 7-11](#) shows the Event Notifications Setup page.

Figure 7-11 Event Notifications Setup Page

Map Help Uptime: 00:16:35

Should Notify-Disposition Events generate SNMP Traps? yes no

SNMP Trap Destination:

SNMP Trap Community:

Should Notify-Disposition Events generate Syslog Messages? yes no

Should Syslog Messages use the Cisco EMBLEM Format? yes no

Syslog Destination Address:

Network Default Syslog Destination: 0.0.0.0

Syslog Facility Number: 16

IEEE SNMP Traps should generate the following notifications:

Client Authentication Failure

Client Deauthentication

Client Disassociation

Apply OK Cancel Restore Defaults 66313

Follow this link path to reach the Event Notifications Setup page:

1. On the Summary Status page, click **Setup**.
2. On the Setup page, click **Notifications** under Event Log.

Settings on the Event Notifications Setup Page

The Event Notifications Setup page contains the following settings:

- [Should Notify-Disposition Events generate SNMP Traps?](#)
- [SNMP Trap Destination](#)
- [SNMP Trap Community](#)
- [Should Notify-Disposition Events generate Syslog Messages?](#)
- [Should Syslog Messages use the Cisco EMBLEM Format](#)
- [Syslog Destination Address](#)
- [Syslog Facility Number](#)
- [IEEE SNMP Traps Should Generate the Following Notifications](#)

The page also displays the IP address of the network default syslog destination.

Should Notify-Disposition Events generate SNMP Traps?

Select **yes** to send event notifications to an SNMP server.

**Note**

For notifications to be sent to an SNMP server, SNMP must be enabled on the SNMP Setup page, and you must set an SNMP trap destination and an SNMP trap community.

SNMP Trap Destination

Type the IP address or the host name of the server running the SNMP Management software. This setting also appears on the SNMP Setup page.

SNMP Trap Community

Type the SNMP community name. This setting also appears on the SNMP Setup page.

Should Notify-Disposition Events generate Syslog Messages?

Select **yes** to send event notifications to a Syslog server.

Should Syslog Messages use the Cisco EMBLEM Format

When this setting is enabled, the bridge generates EMBLEM (Baseline Manageability Specification) standard compliant system log messages:

```
ipaddress Counter: [yyyy mmm dd hh:mm:ss TimeZone +/- hh:mm]: %FACILITY- SEVERITY-MNEMONIC:
Message-text
```

Example without timestamp:

```
192.168.12.83: %APBR-6-STA_ASSOC_OK: [BR350-12] Station [TEST-LPT]000750abcd2a Associated
```

Example with timestamp:

```
192.168.85:2002 SEP 12 13:52:12 PST -08:00: %APBR-6-STA_ASSOC_OK: [BR350-12] Station
[TEST-LPT]000750abcd2a Associated
```

The timestamp is optional and included in the message only when the wall clock time is set on the bridge. The facility code for all messages is APBR.

Syslog Destination Address

Type the IP address or the host name of the server running Syslog.

The Network Default Syslog Destination line under the syslog destination address field lists the syslog destination address provided by the DHCP or BOOTP server. This default syslog destination is only used if the syslog destination address field is blank.

Syslog Facility Number

Type the Syslog Facility number for the notifications. The default setting is 16, which corresponds to the Local0 facility code.

IEEE SNMP Traps Should Generate the Following Notifications

You can designate how the SNMP traps handles the following client events:

- Authentication failure
- Deauthentication
- Disassociation

You can set the following options for each event:

- No Trap nor Event Log—the event is neither trapped nor logged
- Event Log Only—the event is generated and sent to the event log only
- IEEE Trap Only—the event is trapped and sent to an SNMP community
- Both IEEE Trap and Event Log—the event is trapped and sent to the event log