# Network Management

This section describes how to use the web-browser management system to browse to other devices on your network, how to use Cisco Discovery Protocol with your wireless networking equipment, how to set up Spanning Tree Protocol, how to assign a specific network port to a MAC address, and how to enable wireless network accounting.

This chapter contains the following sections:

**Note**     You can use the Association Table page with the console and Telnet interfaces. The Network Map window is available only through a Java-enabled web-browser interface.

# Using the Association Table

The management system's Association Table page lists all the devices, both wireless and wired to the root LAN, of which the bridge is aware. Figure 9-1 shows an example of the Association Table page.

*Figure 9-1    Association Table Page*
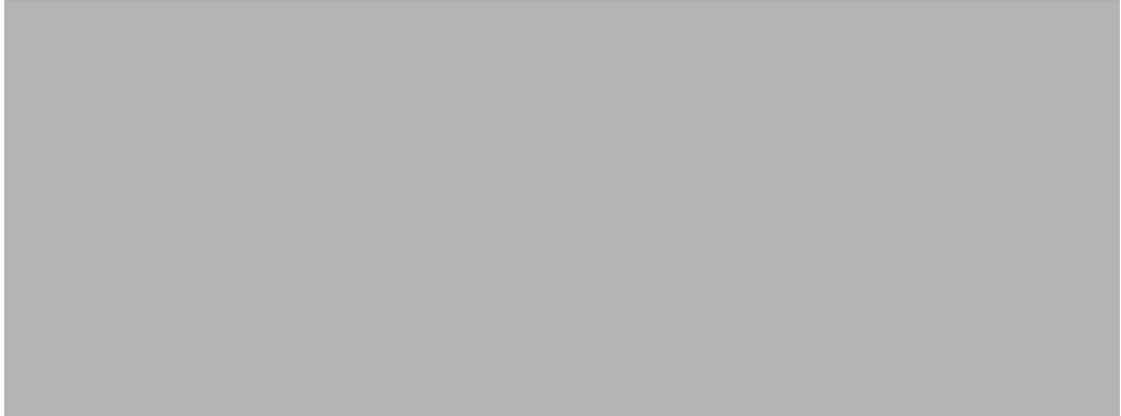


Click the **Association** link at the top of any main management system page to go to the Association Table.

# Browsing to Network Devices

To browse to a device's web-browser interface, click the device's IP address in the IP Addr. column. The home page of the device's management system appears. Cisco Aironet bridges, access points, and workgroup bridges have web-browser interfaces, and many servers and printers have them, also.

If the device does not have a web-browser interface, click the device's MAC address in the MAC Addr. column. A Station page appears for the device, displaying the information the bridge knows about the device, including the device's identity and statistics on traffic to and from the device. Some devices, such as PC card client adapters, do not have web-browser interfaces.

# Setting the Display Options

You use the display options to select the device types to be listed in the table. The default selections list only the bridge and any devices with which it is associated. To change the selections, click a display option and then click **Apply**.

To modify the table further, click **additional display filters**, which is a link to the Association Table Filters page. You use the Association Table Filters page to select the columns of information that appear in the Association Table and the order in which devices are listed.

For more information on customizing the Association Table display, read the "Association Table Display Setup" section on page 7-13.

# Using Station Pages

Click a device's MAC address in the Association Table's MAC Addr. column to display a Station page for the device.

Station pages provide an overview of a network device's status and data traffic history. The information on a Station page depends on the device type; a Station page for an access point, for example, contains different information than the Station page for a PC card client adapter.

You can also use the Station page to perform pings and link tests for network devices. Figure 9-2 shows a sample Station page for a PC card client adapter.

*Figure 9-2    Station Page*

# Information on Station Pages

## Station Identification and Status

The yellow table at the top of the Station page lists the following information:

- System Name—The name assigned to the device.
- Device—The type and model number of the device.
- MAC Address—A unique identifier assigned by the manufacturer.
- IP Address—The device's IP address.

    When you click the IP address link, the browser attempts to display the device's home page. Cisco Aironet bridges, access points, and workgroup bridges have web-browser interfaces, and many servers and printers have them also.

- VLAN ID—The identification number of configured VLANs.
- Policy Grp.—A group of filters specifically designed to allow or deny certain types of traffic from entering or leaving the access point.
- State—Displays the operational state of the wireless station. Possible states include:
    - Assoc—The station is associated with an access point or bridge. Client stations associated with this bridge will also show an Association Identifier (AID) value that is an index into a table of stations associated with this bridge. Maximum AID count is 2007.
    - Unauth—The station is not authenticated with any access point or bridge.
    - Auth—The station is authenticated with an access point or bridge.
    - Local Auth—The station has authenticated at least once with this bridge.
- Class—This field displays the type of station. Station types include:
    - AP—An access point.
    - Client, PS Client—A client or power-save client station.
    - Bridge, Bridge R—A bridge or a root bridge.
    - Rptr—A repeater.
    - Mcast—A multicast address.
    - Infra—An infrastructure node, typically a workstation with a wired connection to the Ethernet network.
- Status—This field indicates the device's operating status. Possible statuses include:
    - OK—The device is operating properly.
    - EAP Pending
    - EAP Authenticated
    - IP Forwarding Agent
    - BootP/DHCP Client—The device is using BOOTP or DHCP protocol
    - ARP Proxy Server
    - IP Virtual Router
    - WEP—WEP is enabled on the device.

## To Station Information

Fields in the To Station column in the second table on the Station page contain the following information:

- Alert—Click this box if you want detailed packet trace information captured for the Association Table page. This option is only available to users with Administrator capability.

- Packets OK—Reports the number of good packets coming to the station.

- Total Bytes OK—Reports the number of good bytes coming to the station.

- Total Errors—Reports the total number of packet errors coming to the station.

- Max. Retry Pkts.—Reports the number of times data packets have reached the maximum long or short retry number. Set the maximum RTS value on the Root Radio Hardware page; see the "Entering Radio Hardware Information" section on page 3-12 for instructions.

- RTS (Short) Retries—Reports the number of times the RTS packet had to be retried.

- Data (Long) Retries—Reports the number of times the data packet had to be retried.

## From Station Information

Fields in the To Station column contain the following information:

- Alert—Click this box if you want detailed packet trace information captured for the Association Table page. This option is only available to users with Administrator capability.

- Packets OK—Reports the number of good packets sent from the station.

- Total Bytes OK—Reports the number of good bytes sent from the station.

- Total Errors—Reports the total number of packet errors sent from the station.

- WEP Errors—Reports the number of encryption errors sent from the station.

## Rate, Signal, and Status Information

The table under the To and From Station table lists rate, signal, and status information for the device.

Data rate and signal quality information appears on Station pages for client devices. On Station pages for access points and bridges, this area shows network information such as system uptime.

- Parent—Displays the system name of the device to which the client, bridge or repeater is associated. The entry [self] indicates that the device is associated with this bridge.

- Current Rate—Reports the current data transmission rate. If the station is having difficulty communicating with the bridge, this might not be the highest operational rate.

- Latest Retries—Tally of short and long data retries.

- Next Hop—If repeater bridges are used on the network, this field names the next bridge or access point in the repeater chain.

- Operational Rates—The data transmission rates in common between the bridge and the station.

- Latest Signal Strength—Displays the current index of radio signal quality.

The following four fields appear only on the Station page for a bridge or access point:

- Stations Associated—Displays, by number and class, all stations associated with the bridge.

- Uptime—Displays the cumulative time the device has been operating since the last reset.

- Software Version—Displays the version level of Cisco software on the device.

- Announcement Packets—Total number of Announcement packets since the device was last reset.

### Hops and Timing Information

The table at the bottom of the Station page lists information on the chain of devices, if any, between the device and the wired LAN, on the monitoring timeout for the device, and on the time of the most recent system activity.

- Hops to Infra.—The number of devices between this station and the network infrastructure.

- Activity Timeout—Total time that can elapse after the bridge's last data receipt before the bridge presumes the device has been turned off. See the "Association Table Advanced Page" section on page 7-16 for information on setting timeouts for each device class.

- Communication Over Interface—The network port over which the access point or bridge is communicating with the device.

- Echo Packets—The link test sequence number; it lists the total number of link test packets sent to this station.

- Latest Activity—Elapsed time in hours, minutes, and seconds since the station and the bridge last communicated. All zeros means there is current communication.

## Performing Pings and Link Tests

Use the ping and link test buttons to perform pings and link tests on the device. If the device is associated to the bridge through which you reached the Station page, the link test button and packet fields appear. If the device is not associated with the bridge, only the ping button and packet fields appear.

### Performing a Ping

Follow these steps to ping the device described on the Station page:

**Step 1**   To customize the size and number of packets sent during the ping, enter the number of packets and size of the packets in the Number of Pkts. and Pkt. Size fields.

**Step 2**   Click **Ping**.

The ping runs using the values in the Number of Pkts. and Pkt. Size fields, and a ping window appears listing the test results. To run the ping again, click **Test Again**. Figure 9-3 shows a ping window.

*Figure 9-3    Ping Window*

```
PING 161.44.236.219: 56 data bytes
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=2. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=3. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=4. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=5. time<19 msec
64 bytes from dhcp-akron-236-219.cisco.com (161.44.236.219): icmp_seq=6. time<19 msec
----161.44.236.219 PING Statistics----
7 packets transmitted, 5 packets received, 28% packet loss
round-trip (ms)  min/avg/max = 0/0/0
```

Test Again

49923

## Performing a Link Test

Follow these steps to perform a link test between the bridge and the device described on the Station page:

**Step 1**  To customize the size and number of packets sent during the link test, enter the number of packets and size of the packets in the Number of Pkts. and Pkt. Size fields.

**Step 2**  Click **Link Test**.

The link test runs using the values in the Number of Pkts. and Pkt. Size fields.

✎

**Note**    If you need to stop the link test before the test is complete, click **Stop Test**.

A results window appears listing the test results. To run the test again, click **Test Again**. To run a continuous link test, click **Continuous Test**. Figure 9-4 shows a link test results window.

*Figure 9-4    Link Test Results Window*

| Pkts. Attempted | 100 | Pkts. Requested | 100 |
|---|---|---|---|
| Pkts. Successful | 100 | Payload Size | 500 |
| Avg. Delay | 19.2 msec | [Min, Max] Delay | [19.2, 19.2] msec |
| Transmit Rates | 100 at 11.0B | | |

| To the Station | | From the Station | |
|---|---|---|---|
| Avg. Signal Strength | 96% | Avg. Signal Strength | 84% |
| [Min, Max] Strength | [80%, 100%] | [Min, Max] Strength | [70%, 100%] |
| Pkts. No Retries | 95 | Pkts. No Retries | 96 |
| Pkts. 1 Retry | 5 | Pkts. 1 Retry | 4 |
| Pkts. Mult. Retries | 0 | Pkts. Mult. Retries | 0 |
| Pkts. Max. Retries | 0 | | |
| Pkts. Lost | 0 | Pkts. Lost | 0 |
| Duplicate Pkts. | 0 | Duplicate Pkts. | 0 |
| RTS Retries | 0 | RTS Retries | 0 |
| Data Retries | 5 | Data Retries | 4 |

Test Again    Continuous Test

## Clearing and Updating Statistics

Use the Clear Stats and Refresh buttons to clear and update the Station page statistics.

- Clear Stats—Clears all packet, octet and error counts and resets the counters to 0.
- Refresh—Updates the counts to their latest accumulated values, and saves the Alert selections.

## Deauthenticating and Disassociating Client Devices

Use the Deauthenticate and Disassociate buttons to deauthenticate and disassociate the device from the bridge. These buttons appear only on Station pages for devices that are associated with the bridge, and only users with administrator capability can operate them.

- Deauthenticate—Forces a device to re-authenticate with the bridge.

- Disassociate—Allows a device to break its current association, re-evaluate the currently associated access point or bridge and determine which of the surrounding access points or bridges has the best signal quality to associate with.

# Using the Network Map Window

To open the Network Map window, click **Map** at the top of any management system page. (See the "Navigating with the Map Windows" section on page 2-3 for information about the Map page.) When the Map window appears, click **Network Map**.

You use the Network Map window to open a new browser window displaying information for any device on your wireless network. Unlike the Association Table, the Network Map window does not list wired devices on your LAN. Figure 9-5 shows the Network Map window.

**Note**   Your web browser must have Java enabled to use the map windows.

*Figure 9-5    Network Map Window*

Click the name of a wireless device to open a new browser window displaying a Station page displaying the bridge's local information for that device. Click **Go** beside the device name to open a new browser window displaying that device's home page, if available. Some devices, such as PC card clients, do not have web-browser interfaces.

Click **show clients** to display all the wireless client devices on your network. The client names appear under the access point or bridge with which they are associated. If clients are displayed, click **hide clients** to display only non-client devices.

# Using Cisco Discovery Protocol

Cisco Discovery Protocol (CDP) is a device-discovery protocol that runs on all Cisco network equipment. Each device sends identifying messages to a multicast address, and each device monitors the messages sent by other devices. Information in CDP packets is used in network management software such as CiscoWorks2000.

Use the CDP Setup page to adjust the bridge's CDP settings. CDP is enabled by default. Figure 9-6 shows the CDP Setup page.

*Figure 9-6    CDP Setup Page*



Follow this link path to reach the CDP Setup page:

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

2. On the Setup page, click **Cisco Services**.

3. On the Cisco Services Setup page, click **Cisco Discovery Protocol** (CDP).

## Settings on the CDP Setup Page

The CDP Setup page contains the following settings:

- Enabled/Disabled—Select **Disabled** to disable CDP on the bridge; select **Enabled** to enable CDP on the bridge. CDP is enabled by default.

- Packet hold time—The number of seconds other CDP-enabled devices should consider the bridge's CDP information valid. If other devices do not receive another CDP packet from the bridge before this time elapses they should assume that the bridge has gone offline. The default value is 180. The packet hold time should always be greater than the value in the "Packets sent every" field.

- Packets sent every—The number of seconds between each CDP packet the bridge sends. The default value is 60. This value should always be less than the packet hold time.

- Individual Interface Enable: Ethernet—When selected, the bridge sends CDP packets through its Ethernet port and monitors the Ethernet for CDP packets from other devices.

- Individual Interface Enable: Root Radio—When selected, the bridge sends CDP packets through its radio port and monitors the radio for CDP packets from other devices.

## MIB for CDP

A MIB file is available for use with CDP. The filename is CISCO-CDP-MIB.my, and you can download the MIB at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

# Setting Up Spanning Tree Protocol

Bridges use Spanning-Tree Protocol (STP) to eliminate loops in an extended network. Bridges exchange bridge protocol data unit (BPDU) messages with other bridges to detect loops, and the bridges shut down selected ports to stop the loops. Bridges also monitor BPDU messages to detect a failure in the network and change their port status to keep the network intact.

**Note**    If you use the bridge as an access point or if your network contains only two bridges (in other words, the network has no potential for a loop), you do not need to set up STP. However, if your network uses several bridges and loops are possible, you should set up STP.

Figure 9-7 shows a network that relies on STP to prevent a loop. Each bridge uses BPDU messages to determine whether its ports should forward or block data. In this example, bridge 3 determines that it should shut down its radio port to create only one active path for data between LAN segments A and B.

*Figure 9-7    Bridges Using STP*
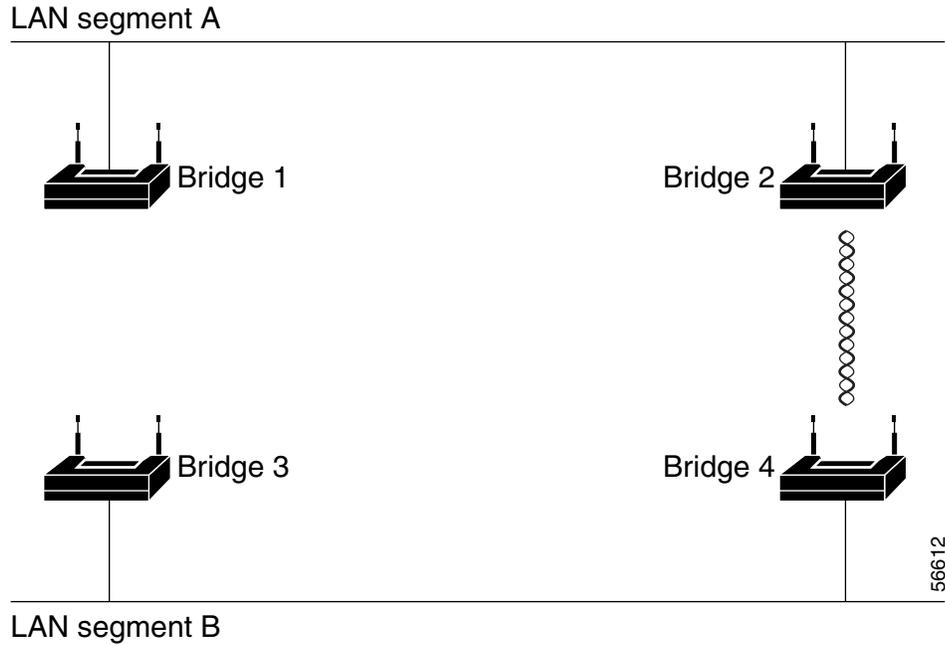


You can configure STP to customize the spanning tree used by your bridges or you can use the STP defaults. The bridges on your network will exchange BDPU messages to build a spanning tree using default values.

For a thorough overview of STP, consult *Cisco CCNA Exam #640-507 Certification Guide*, available from CiscoPress.com. Use the following URL to browse to CiscoPress.com:

http://www.ciscopress.com/

# Entering STP Values

Use the Spanning Tree Setup page to enter STP values. Figure 9-8 shows the Spanning Tree Setup page.

*Figure 9-8    Spanning Tree Setup Page*



Follow this link path to reach the Spanning Tree Setup page:

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

**2.** On the Setup page, click **Spanning Tree** in the Association section near the top of the page.

# Settings on the STP Setup Page

## STP Enabled/Disabled

Use this setting to enable or disable STP on the bridge. This setting is directly linked to the Role in radio network setting on the Express Setup page. If you select **Root Access Point** or **Repeater Access Point** from the Role in radio network pull-down menu, the STP Enabled/Disabled setting switches to Disabled automatically. If you select **Disabled** for this setting, the Role in radio network setting automatically switches to Root Access Point.

To maintain a bridge link with STP disabled, you also must select **yes** for the *Always unblock Ethernet when STP is disabled* setting. Follow these steps to disable STP while maintaining a bridge link:

**Step 1**    Follow this link path to reach the Spanning Tree Setup page:

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

b.    On the Setup page, click **Spanning Tree** in the Association section near the top of the page.

**Step 2**    On the Spanning Tree Setup page, select **yes** for the *Always unblock Ethernet when STP is disabled* setting and click **Apply**.

**Step 3**    Select **Disabled** for the Spanning Tree Protocol setting and click **Apply**.

The bridge's Role in Radio Network setting on the Express Setup page changes to reflect the bridge's STP status. If the bridge is set to Non-Root Bridge w/Clients before you disable STP, the Role in Radio Network setting changes to **Non-Root w/Clients, no STP**. If the bridge is set to Non-Root Bridge w/o Clients before you disable STP, the Role in Radio Network setting changes to **Non-Root Bridge w/o Clients, no STP**. The bridge maintains a bridge link with STP disabled in both of these roles.

If a bridge loop occurs, the bridge automatically shuts down its Ethernet port to avoid disabling your network.

**Note**    When STP is disabled and the Ethernet port is unblocked, the bridge appears as a workgroup bridge in the association tables of other Cisco Aironet access points and bridges. Bridges with STP disabled use the workgroup bridge protocol, which is reported in the Association Table's Device column.

## Always Unblock Ethernet When STP is Disabled

Select yes for this setting to maintain a bridge link when STP is disabled. Follow the steps in the "STP Enabled/Disabled" section on page 9-13 to disable STP and maintain a bridge link.

## Root Configuration Settings

Use the Root Configuration settings to influence which bridge is the root bridge in the spanning tree.

**Note**    Spanning tree discussions use the term *root* to describe two concepts: the bridge on the network that serves as a central point in the spanning tree is called the *root bridge*, and the port on each bridge that provides the most efficient path to the root bridge is called the *root port*. These meanings are separate from the Role in radio network setting that includes root and non-root options. A bridge whose Role in radio network setting is Root Bridge does not necessarily become the root bridge in the spanning tree.

- Priority (0 – 65535)

    Use the priority setting to influence which bridge is designated the root bridge in the spanning tree. When bridges have the same priority setting, STP uses the bridges' MAC addresses as a tiebreaker. The bridge with the lowest priority setting is likely to be designated the root bridge in the tree. Enter a value from 0 to 65535.

- Max Age (6 – 40 seconds)

    This setting determines how long the bridge waits before deciding the network has changed and the spanning tree needs to be rebuilt. For example, with Max Age set to 20, the bridge attempts to rebuild the spanning tree if it does not receive a hello BDPU from the root bridge in the spanning tree within 20 seconds.

    When you select a Max Age setting, consider the amount of time required for a hello BPDU to traverse the network and allow for a few hello BPDUs to be lost before the bridge reacts and attempts to change the spanning tree. Enter a value from 6 to 40 seconds.

- Hello Time (1 – 10 seconds)

    This setting determines how often the root bridge in the spanning tree sends out a hello BPDU telling the other bridges that the network topology has not changed and that the spanning tree should remain the same. Enter a value from 1 to 10 seconds.

- Forward Delay (4 – 30 seconds)

    This setting determines how long the bridge's ports should stay in the listening and learning transition states if there is a change in the spanning tree. For example, before changing a port to forwarding, the bridge puts the port into listening state for the duration of the Forward Delay, and no packets are forwarded; when the Forward Delay has elapsed, the bridge puts the port into learning state for the duration of the Forward Delay, and no packets are forwarded. After the listening and learning periods, the bridge changes the port to forwarding. The listening and learning periods help prevent loops during spanning tree changes. Enter a value from 4 to 30 seconds.

## Port Configuration Settings

These settings apply to individual ports on the bridge. Use these settings to adjust the status of individual ports on the bridge.

- Path Cost (1 – 65535)

    The path cost indicates the relative efficiency of a port's network link. A port with a high path cost is less likely to become a bridge's root port. Enter a value from 1 to 65535.

    **Note**    If a bridge is used as a standby bridge, you may need to set the path cost for the radio higher than the path cost for the Ethernet port so that the Spanning Tree Protocol blocks the radio port instead of the Ethernet port. Even though the radio port is blocked, the hot standby feature still maintains association with the root, which is required for standby monitoring.

- Priority (0 – 255)

    Use the priority setting to influence whether STP designates a port as a bridge's root port. A port with a low priority setting is more likely to become a bridge's root port. Enter a value from 0 to 255.

- Enable

    This setting determines whether the port participates in STP. A port set to disabled does not forward traffic and does not participate in STP. A port set to enabled participates in STP, and STP determines whether the port blocks or forwards traffic.

# Assigning Network Ports

Use the Port Assignments page to assign a specific network port to a non-root bridge or to a repeater access point. When you assign specific ports, your network topology remains constant even when devices reboot. Figure 9-9 shows the Port Assignments page.

*Figure 9-9    Port Assignments Page*



Follow this link path to reach the Port Assignments page:

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

2.  On the Setup page, click **Port Assignments** in the Association section near the top of the page.

## Settings on the Port Assignments Page

The port assignments page (see Figure 9-9) displays the following parameters:

- ifIndex—Lists the port's designator in the Standard MIB-II (RFC1213-MIB.my) interface index.

- dot1dBasePort—Lists the port's designator in the Bridge MIB (RFC1493; BRIDGE-MIB.my) interface index.

- AID—Lists the port's 802.11 radio drivers association identifier.

- Station—Enter the MAC address of the device to which you want to assign the port in the port's Station entry field. When you click **Apply** or **OK**, the port is reserved for that MAC address.

# Enabling Wireless Network Accounting

You can enable accounting on the bridge to send network accounting information about wireless client devices to a RADIUS server on your network. Cisco Secure ACS writes accounting records to a log file or to a database daily. Consult the *Cisco Secure ACS 2.6 for Windows 2000/NT Servers User Guide* for instructions on viewing and downloading the log or database:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/tsd_products_support_series_home.html

If you have a UNIX server, use this URL to browse to the *CiscoSecure ACS 2.3 for UNIX User Guide*:

http://www.cisco.com/en/US/products/sw/secursw/ps4911/products_user_guide_book09186a00800eb438.html

**Note**    RADIUS accounting is available in firmware versions 11.10T and later, which are available on Cisco.com. You can download Cisco Aironet firmware releases at http://www.cisco.com/cisco/software/navigator.html.

Use the Accounting Setup page to enable and set up accounting on the bridge. Figure 9-10 shows the Accounting Setup page.

*Figure 9-10   Accounting Setup Page*



Follow this link path to reach the Accounting Setup page:

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

2.  On the Setup page, click **Accounting** under Services.

# Settings on the Accounting Setup Page

The Accounting Setup page contains these settings:

-   Enable accounting—Select Enabled to turn on accounting for your wireless network.

-   Enable delaying to report stop—Select this option to delay sending a stop report to the server when a client device disassociates from the bridge. The delay reduces accounting activity for client devices that disassociate from the bridge and then quickly reassociate.

-   Minimum delay time to report stop (sec.)—Enter the number of seconds the bridge waits before sending a stop report to the server when a client device disassociates from the bridge. The delay reduces accounting activity for client devices that disassociate from the bridge and then quickly reassociate.

-   Server Name/IP—Enter the name or IP address of the server to which the bridge sends accounting data.

-   Server Type—Select the server type from the pull-down menu. RADIUS is the only menu option; additional types will be added in future software releases.

- Port—The communication port setting used by the bridge and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and bridges and for Cisco secure ACS.

- Shared Secret—Enter the shared secret used by your RADIUS server. The shared secret on the device must match the shared secret on the RADIUS server.

- Retran Int (sec.)—Enter the number of seconds the bridge should wait before ceasing to contact the server. If the server does not respond within this time, the bridge tries to contact the next accounting server in the list if one is specified. The bridge uses backup servers in list order when the previous server times out.

- Max Retran—Enter the number of times the bridge should attempt to contact the server before giving up. If the server does not respond after these retries, the bridge tries to contact the next accounting server in the list if one is specified. The bridge uses backup servers in list order when the previous server times out.

- Enable Update—Click the Enable Update checkbox to enable accounting update messages for wireless clients. With updates enabled, the bridge sends an accounting start message when a wireless client associates to the bridge, sends updates at regular intervals while the wireless client is associated to the bridge, and sends an accounting stop message when the client disassociates from the bridge. With updates disabled, the bridge sends only accounting start and accounting stop messages to the server.

- Update Delay—Enter the update interval in seconds. If you use 360, the default setting, the bridge sends an accounting update message for each associated client device every 6 minutes.

- Use accounting server for—Select the authentication types for which you want to collect accounting data. When you select **EAP authentication**, the bridge sends accounting data to the server for client devices that authenticate using Cisco Aironet LEAP, EAP-TLS, or EAP-MD5. When you select **non-EAP authentication**, the bridge sends data to the server for client devices using authentication types other than EAP, such as open, shared key, or MAC-based authentication.

Table 9-1 lists the accounting attributes.

*Table 9-1    Accounting Attributes*

| Attribute | Definition |
|---|---|
| Acct-Status-Type | The client device's current accounting status; possible statuses include ACCT_START, ACCT_STOP, and ACCT_UPDATE. The bridge sends an ACCT_START frame to the accounting server when a client device successfully authenticates on a RADIUS server through the bridge; the bridge sends an ACCT_STOP frame to the server when a client device disassociates from the bridge; and the bridge sends an ACCT_UPDATE frame to the server periodically while the authenticated client device is associated to the bridge. |
| Acct-Session-ID | A unique accounting identifier for each connection activity that is bounded by ACCT_START and ACCT_STOP. The bridge sends this attribute to the server with all three status types. |
| User-Name | The username with which the client device's authenticated to the network. The bridge sends this attribute to the server with all three status types. |

*Table 9-1    Accounting Attributes  (continued)*

| Attribute | Definition |
|---|---|
| NAS-Port | The port number used for the client device's connection. The bridge sends this attribute to the server with all three status types. |
| Acct-Authentic | The method with which the client device is authenticated to the network. This value is always 1, which represents RADIUS authentication. The bridge sends this attribute to the server with all three status types. |
| NAS-Identifier | The network access server (NAS) sending the accounting data; for wireless networks, the name of the bridge sending the accounting information. The bridge sends this attribute to the server with all three status types. |
| Acct-Session-Time | The elapsed time in seconds that the client device has been associated to the bridge. The bridge sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types. |
| Acct-Input-Octets | The number of octets received on the wireless network through the bridge since the client device associated to the bridge. The bridge sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types. |
| Acct-Output-Octets | The number of octets sent on the wireless network through the bridge since the client device associated to the bridge. The bridge sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types. |
| Acct-Input-Packets | The number of packets received on the wireless network through the bridge since the client device associated to the bridge. The bridge sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types. |
| Acct-Output-Packets | The number of packets sent on the wireless network through the bridge since the client device associated to the bridge. The bridge sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types. |
| Acct-Terminate-Cause | How the client device's session was terminated. This attribute lists the same cause for every disassociated client device: Loss of service. The bridge sends this attribute only with the ACCT_STOP status type. |
| Acct-Delay-Time | The delay between the time the event occurred and the time that the attribute was sent to the server. The bridge sends this attribute to the server with all three status types. |
| RADIUS_IPADR | The IP address of the bridge sending the accounting information. The bridge sends this attribute to the server with all three status types. |