



Network Management

This section describes how to browse to other devices on your network, how to use Cisco Discovery Protocol with your wireless networking equipment, how to assign a specific network port to a MAC address, and how to enable wireless network accounting.

This chapter contains the following sections:

- [Using the Association Table, page 9-2](#)
- [Using the Network Map Window, page 9-8](#)
- [Using Cisco Discovery Protocol, page 9-8](#)
- [Assigning Network Ports, page 9-9](#)
- [Enabling Wireless Network Accounting, page 9-11](#)

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 access point is aware. Figure 9-1 shows an example of the Association Table page.

Figure 9-1 Association Table Page

Association Table additional display filters					
Device	Name	IP Addr.	MAC Addr.	State	Parent
AP4800-E	MChmura	172.16.0.25	00409642c104	Assoc	[self]
	Petro's AP	172.16.0.48	00409633b4b7		
PC4800B Client	Brian Devney	172.16.0.77	00409636ace0	Assoc	[self]
PC4800B Client	freda_laptop	172.16.0.28	00409630f88c	Assoc	[self]
PC4800B Client	gregs_laptop	172.16.0.10	00409629074c	Assoc	[self]

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



Note

You can also use the Association Table page in the command-line interface.

Browsing to Network Devices

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

If the device does not have a browser-based interface, click the device's MAC address in the MAC Addr. column. A Station page appears for the device, displaying the information the access point 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 browser-based 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 access point 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

Home	Map	Network	Associations	Setup	Logs	Help	Uptime: 18 days, 16:47:59
System Name	AP350-478916			Device	350 Series AP		
MAC Address	[Aironet]00:40:96:47:89:16						
IP Address	 192.168.147.47						
VLAN ID	0			Policy Grp.	0		
State	[self]			Class	Access Point		
Status	OK						
				<input type="button" value="Clear Stats"/>	<input type="button" value="Refresh"/>		
				Number of Pkts.	<input type="text" value="5"/>	Pkt. Size	<input type="text" value="64"/>
				<input type="button" value="Ping"/>			
To Station				<i>Alert</i>	From Station		
				<input type="checkbox"/>			
Packets OK	49476			Packets OK	185183		
Total Bytes OK	8811286			Total Bytes OK	18884748		
Total Errors	0			Total Errors	0		
Max. Retry Pkts.	0						
Short Retries	0			WEP Errors	0		
Long Retries	0						
Stations Associated	0 Clients, 0 Repeaters, 0 Bridges						
Load	0			Software Version	12.00		
Uptime	18 days, 16:47:55			Announcement Pkts.	107710		
Hops to Infra.	0			Echo Packets	0		
Activity Timeout	never			Latest Activity	00:00:00		
Communication Over Interface: Ethernet fec0							

49526

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 access points, bridges, and workgroup bridges have browser-based 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 to or from the access point.
- State—Displays the operational state of the wireless station. Possible states include:
 - Assoc—The station is associated with an access point. Client stations associated with this access point will also show an Association Identifier (AID) value that is an index into a table of stations associated with this access point. Maximum AID count is 2007.
 - Unauth—The station is not authenticated with any access point.
 - Auth—The station is authenticated with an access point.
 - Local Auth—The station has authenticated at least once with this access point.
- 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 Autenticated
 - 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 AP Radio Hardware page; see the [“Entering Radio Hardware Information”](#) section on page 3-9 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, 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 access point.
- Current Rate—Reports the current data transmission rate. If the station is having difficulty communicating with the access point, this might not be the highest operational rate.
- Latest Retries—Tally of short and long data retries.
- Next Hop—If repeater access points are used on the network, this field names the next access point in the repeater chain.
- Operational Rates—The data transmission rates in common between the access point 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 an access point:

- Stations Associated—Displays, by number and class, all stations associated with the access point.
- 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 access point’s last data receipt before the access point presumes the client device has been turned off. See the [“Using the Association Table” section on page 9-2](#) 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 access point 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 access point through which you reached the Station page, the link test button and packet fields appear. If the device is not associated with the access point, 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

499923

Performing a Link Test

Follow these steps to perform a link test between the access point 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**

49920

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 client device from the access point. These buttons appear only on Station pages for devices that are associated with the access point, and only users with administrator capability can operate them.

- Deauthenticate—Forces a client to re-authenticate with the access point.
- Disassociate—Allows a client to break its current association, re-evaluate the currently associated access point and determine which of the surrounding access points 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 “Using the Network Map Window” section on page 9-8 for information about the Map page.) When the Map window appears, click **Network Map**.

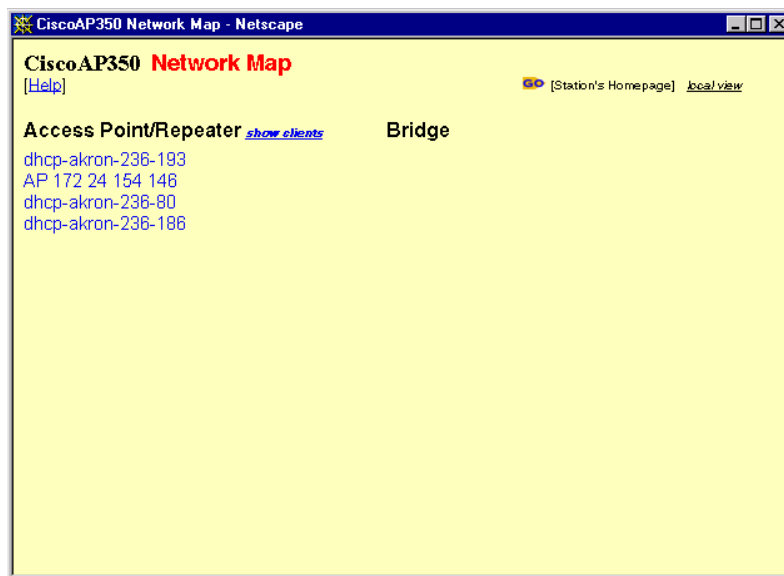
You use the Network Map window to open a new browser window displaying information for any device on your wireless network. Unlike the Association Table, the Network Map window does not list wired devices on your LAN. Figure 9-5 shows the Network Map window.



Note

Your Internet 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 access point’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 browser-based 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 access point’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 access point; select **Enabled** to enable CDP on the access point. CDP is enabled by default.
- Packet hold time—The number of seconds other CDP-enabled devices should consider the access point's CDP information valid. If other devices do not receive another CDP packet from the access point before this time elapses they should assume that the access point 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 access point sends. The default value is 60. This value should always be less than the packet hold time.
- Individual Interface Enable: Ethernet—When selected, the access point sends CDP packets through its Ethernet port and monitors the Ethernet 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/mibs>

Assigning Network Ports

Use the Port Assignments page to assign a specific network port to a repeater access point or to a non-root bridge. When you assign specific ports, your network topology remains constant even when devices reboot. [Figure 9-7](#) shows the Port Assignments page.

Figure 9-7 Port Assignments Page

2001/07/16 14:09:02

[Map](#) [Help](#)

ifIndex	dot1dBasePort	AID	Station
10	6	2	00:00:00:00:00:00
11	7	3	00:00:00:00:00:00
12	8	4	00:00:00:00:00:00
13	9	5	00:00:00:00:00:00
14	10	6	00:00:00:00:00:00
15	11	7	00:00:00:00:00:00
16	12	8	00:00:00:00:00:00
17	13	9	00:00:00:00:00:00
18	14	10	00:00:00:00:00:00
19	15	11	00:00:00:00:00:00
20	16	12	00:00:00:00:00:00
21	17	13	00:00:00:00:00:00
22	18	14	00:00:00:00:00:00
23	19	15	00:00:00:00:00:00
24	20	16	00:00:00:00:00:00
25	21	17	00:00:00:00:00:00
26	22	18	00:00:00:00:00:00
27	23	19	00:00:00:00:00:00
28	24	20	00:00:00:00:00:00
29	25	21	00:00:00:00:00:00
30	26	22	00:00:00:00:00:00
31	27	23	00:00:00:00:00:00
32	28	24	00:00:00:00:00:00
33	29	25	00:00:00:00:00:00
34	30	26	00:00:00:00:00:00
35	31	27	00:00:00:00:00:00
36	32	28	00:00:00:00:00:00

Apply OK Cancel Restore Defaults

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 displays the following information:

- 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 access point 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/univercd/cc/td/doc/product/access/acs_soft/csacs4nt/csnt26/index.htm

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/univercd/cc/td/doc/product/access/acs_soft/cs_unx/csu23ug/index.htm

Use the Accounting Setup page to enable and set up accounting on the access point. Figure 9-8 shows the Accounting Setup page.

Figure 9-8 Accounting Setup Page

The screenshot shows the Accounting Setup page with the following configuration:

- Uptime: 1 day, 22:30:15
- Enable accounting: Enabled Disabled
- Enable delaying to report STOP: Enabled Disabled
- Minimum delay time to report STOP (sec):

Server Name/IP	Server Type	Port	Shared Secret	Retran Int (sec)	Max Retran	Enable Update	Update Delay (sec)
<input type="text"/>	RADIUS	1813	<input type="text"/>	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
<input type="text"/>	RADIUS	1813	<input type="text"/>	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
<input type="text"/>	RADIUS	1813	<input type="text"/>	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							
<input type="text"/>	RADIUS	1813	<input type="text"/>	5	3	<input checked="" type="checkbox"/>	600
Use accounting server for: <input type="checkbox"/> EAP authentication <input type="checkbox"/> non-EAP authentication							

Buttons: Apply, OK, Cancel, Restore Defaults

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 access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.
- **Minimum delay time to report stop (sec.)**—Enter the number of seconds the access point waits before sending a stop report to the server when a client device disassociates from the access point. The delay reduces accounting activity for client devices that disassociate from the access point and then quickly reassociate.
- **Server Name/IP**—Enter the name or IP address of the server to which the access point 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 access point and the server. The default setting, 1813, is the correct setting for Cisco Aironet access points and 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 access point should wait before giving up contacting the server. If the server does not respond within this time, the access point tries to contact the next accounting server in the list if one is specified. The access point uses backup servers in list order when the previous server times out.
- **Max Retran**—Enter the number of times the access point should attempt to contact the server before giving up. If the server does not respond after these retries, the access point tries to contact the next accounting server in the list if one is specified. The access point 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 access point sends an accounting start message when a wireless client associates to the access point, sends updates at regular intervals while the wireless client is associated to the access point, and sends an accounting stop message when the client disassociates from the access point. With updates disabled, the access point 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 access point 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 access point 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 access point sends data to the server for client devices using authentication types other than EAP, such as open, shared key, or MAC-based authentication.

Accounting Attributes

Table 9-1 lists the accounting attributes the access point sends to the accounting server.

Table 9-1 Accounting Attributes the Access Point Sends to the Accounting Server

Attribute	Definition
Acct-Status-Type	The client device's current accounting status; possible statuses include ACCT_START, ACCT_STOP, and ACCT_UPDATE. The access point sends an ACCT_START frame to the accounting server when a client device successfully authenticates on a RADIUS server through the access point; the access point sends an ACCT_STOP frame to the server when a client device disassociates from the access point; and the access point sends an ACCT_UPDATE frame to the server periodically while the authenticated client device is associated to the access point.
Acct-Session-ID	A unique accounting identifier for each connection activity that is bounded by ACCT_START and ACCT_STOP. The access point 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 access point sends this attribute to the server with all three status types.
NAS-Port	The port number used for the client device's connection. The access point 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 access point 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 access point sending the accounting information. The access point 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 access point. The access point 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 access point since the client device associated to the access point. The access point sends this attribute only with the ACCT_STOP and ACCT_UPDATE status types.

Table 9-1 Accounting Attributes the Access Point Sends to the Accounting Server (continued)

Attribute	Definition
Acct-Output-Octets	The number of octets sent on the wireless network through the access point since the client device associated to the access point. The access point 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 access point since the client device associated to the access point. The access point 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 access point since the client device associated to the access point. The access point 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 access point 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 access point sends this attribute to the server with all three status types.
RADIUS_IPADR	The IP address of the access point sending the accounting information. The access point sends this attribute to the server with all three status types.