



DHCP Accounting

The DHCP Accounting feature introduces authentication, authorization, and accounting (AAA) and RADIUS support for Dynamic Host Configuration Protocol (DHCP) configuration. The introduction of AAA and RADIUS support improves public wireless LAN (PWLAN) security by sending secure START and STOP accounting messages. The configuration of this feature adds a layer of security that allows DHCP lease assignment and termination to be triggered for the appropriate RADIUS START and STOP accounting records so that the session state is properly maintained by upstream devices, such as a Service Selection Gateway (SSG). The additional security provided by this feature can help to prevent unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases.

Feature Specifications for the DHCP Accounting Feature

Release	Modification
12.2(15)T	This feature was introduced.
12.2(27)SBA	This feature was integrated into Cisco IOS Release 12.2(27)SBA.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for DHCP Accounting, page 2](#)
- [Restrictions for DHCP Accounting, page 2](#)
- [Information About DHCP Accounting, page 2](#)
- [How to Configure DHCP Accounting, page 4](#)
- [Configuration Examples for DHCP Accounting, page 9](#)
- [Additional References, page 11](#)
- [Command Reference, page 13](#)



Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2005 Cisco Systems, Inc. All rights reserved.

Prerequisites for DHCP Accounting

Your network should be configured to run DHCP. You will also need to complete the following tasks before you can configure this feature:

- Identify an external FTP, TFTP, or remote copy protocol (rcp) server that you will use to store the DHCP bindings database.
- Configure the pool of IP addresses that you will enable the DHCP server to assign and the IP addresses that you will exclude.
- Configure a SSG for client authentication.
- Configure AAA and RADIUS on a server within the PWLAN prior to the configuration of DHCP accounting START and STOP messages.

Restrictions for DHCP Accounting

The following restrictions apply to the DHCP Accounting feature:

- DHCP accounting can be configured only for DHCP network pools in which bindings are created automatically and destroyed upon lease termination or when the client sends a DHCPRELEASE message.
- DHCP bindings are destroyed when the **clear ip dhcp binding** or **no service dhcp** commands are entered, which also triggers an accounting STOP message. You should exercise caution when entering these commands if a pool is configured with DHCP accounting, as these commands will clear active leases.

Information About DHCP Accounting

To configure this feature, you must understand the following concepts:

- [DHCP Operation in Public Wireless LANs, page 2](#)
- [Security Vulnerabilities in Public Wireless LANs, page 3](#)
- [DHCP Accounting Operation, page 3](#)
- [DHCP Secured IP Address Assignment and DHCP Accounting, page 4](#)

DHCP Operation in Public Wireless LANs

The configuration of DHCP in a public wireless LAN (PWLAN) simplifies the configuration of wireless clients and reduces the overhead necessary to maintain the network. DHCP clients are leased IP addresses by the DHCP server and then authenticated by the Service Selection Gateway (SSG), which allows the clients to access network services. The DHCP server and client exchange DHCP messages for IP address assignments. When a DHCP server assigns an IP address to a client, a DHCP binding is created. The IP address is leased to the client until the client explicitly releases the IP address and disconnects from the network. If the client disconnects without releasing the address, the server terminates the lease after the lease time is over. In either case, the DHCP server removes the binding and the IP address is returned to the pool.

Security Vulnerabilities in Public Wireless LANs

If the DHCP lease is not explicitly terminated by the client, the SSG will terminate the lease only when the ping-idle timer expires. This type of termination typically occurs in a PWLAN when an authenticated client moves out of range of the access point. This type of disconnection can expose a security vulnerability during the period of time it takes for the ping-idle timer to expire. By design, DHCP will maintain this lease for the configured lease time. However, DHCP ARP table entries are dynamic and DHCP alone does not have the capability to secure the transmission and storage of the DHCP binding or verify the integrity of the information that is sent from the client, which exposes the PWLAN to the following security risks:

- An unauthorized client or hacker can gain unauthorized access to the network.
- The authorized client will be billed for cost-based services that the unauthorized client uses.

A hacker can exploit this vulnerability by snooping for leases that have been dropped by the client but have not expired in the DHCP database. Once the hacker detects the unexpired lease, he or she can quickly reconfigure a laptop to use the unexpired lease. Because DHCP ARP entries are dynamic, a hacker can take control of the unexpired lease and access the network, posing as the authenticated client.

DHCP Accounting Operation

The DHCP Accounting feature counteracts this security vulnerability by introducing AAA and RADIUS security features for DHCP support. RADIUS provides the accounting capability for the transmission of secure START and STOP accounting messages.

When the DHCP Accounting feature is configured, an accounting START message is generated and sent to the SSG when the authorized client is assigned an IP address by the DHCP server, and an accounting STOP message is generated and sent to the SSG when the client explicitly terminates the DHCP lease or when the DHCP server terminates the lease. The SSG authenticates the client and then uses the START and STOP accounting messages to control DHCP lease assignment and termination. The SSG will not maintain or terminate a DHCP lease unless a START or STOP accounting message is received.

The DHCP Accounting feature introduces the **accounting** DHCP pool configuration command. The **accounting** command is used to enable DHCP accounting. DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis. AAA and RADIUS are enabled prior to the configuration of the DHCP Accounting feature but can also be enabled in an existing DHCP network to upgrade the security of active preexisting leases.

When the **accounting** command is configured, RADIUS will automatically send a secure START accounting message to the SSG when the DHCP server responds to the client with the DHCPACK message that contains the committed IP address and network configuration options. The lease is maintained until a explicit STOP accounting message is received. A STOP accounting message is sent only when the client explicitly disconnects from the network by sending a DHCPRELEASE message or by the SSG if the DHCP lease times out. When a STOP message is received, the DHCP binding is destroyed and the IP address is returned to the DHCP pool. If the client moves out of range of the PWLAN or the DHCP lease otherwise times out, the lease can be maintained only by the authorized client because the SSG will not validate acknowledgements that are not authenticated through the SSG.

When the DHCP Accounting feature is enabled, RADIUS accounting is configured automatically for new leases and DHCP bindings. However, existing active leases are not secured. These leases are still insecure until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically.

**Note**

DHCP bindings are also destroyed when the commands **clear ip dhcp binding** or **no service dhcp** are entered, which also triggers an accounting STOP message. This secure lease will be renewed automatically when this feature is enabled. However, active sessions will be interrupted.

DHCP Secured IP Address Assignment and DHCP Accounting

For an additional layer of security, the DHCP Accounting feature can be configured with the DHCP Secured IP Address Assignment feature. The DHCP Secured IP Address Assignment feature provides an additional layer of security by binding the MAC address of the client interface to the DHCP binding with the configuration of the **update arp** DHCP pool configuration command. This command secures the DHCP lease to the MAC address of the client interface and secures the ARP table entry. The secured ARP table entry can be deleted only by an explicit termination message from the DHCP client or by the DHCP server if the binding expires. The configuration of the **update arp** command does not interrupt service and is not visible to the DHCP client. The configuration of these two features greatly improves the security of DHCP operation and can be used to protect PWLANs by preventing unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases. For more information about the DHCP Secured IP Address Assignment feature, refer to the following document:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122t/122t15/ftdsiaa.htm>

How to Configure DHCP Accounting

This section contains the following procedures for configuring DHCP Accounting:

- [Configuring AAA and RADIUS for DHCP Accounting, page 4](#) (required)
- [Configuring DHCP Accounting, page 7](#) (required)
- [Verifying DHCP Accounting, page 8](#) (optional)

Configuring AAA and RADIUS for DHCP Accounting

Perform this task to configure AAA and RADIUS for DHCP accounting.

RADIUS provides the accounting capability for the transmission of secure START and STOP messages. AAA and RADIUS are enabled prior to the configuration of DHCP accounting but can also be enabled to secure an insecure DHCP network. The configuration steps in this section are required for configuring DHCP accounting in a new or existing network.

RADIUS Accounting Attributes

DHCP accounting introduces the attributes shown in [Table 1](#). These attributes are processed directly by the RADIUS server when DHCP accounting is enabled. These attributes can be monitored in the output of the **debug radius** command. The output will show the status of the DHCP leases and specific configuration details about the client. The **accounting** keyword can be used with the **debug radius** command to filter the output and display only DHCP accounting messages.

Table 1 RADIUS Accounting Attributes

Attribute	Description
Calling-Station-ID	The output from this attribute displays the MAC address of the client.
Framed-IP-Address	The output from this attribute displays the IP address that is leased to the client.
Acct-Terminate-Cause	The output from this attribute displays the message “session-timeout” if a client does not explicitly disconnect.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name*
5. **server** *ip-address* **auth-port** *port-number* **acct-port** *port-number*
6. **exit**
7. **aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name*
8. **aaa session-id** {**common** | **unique**}
9. **ip radius source-interface** *interface-type* {**vrf** *vrf-name*}
10. **radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*]
11. **radius-server retransmit** *number-of-retries*

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>aaa new-model</pre> <p>Example: Router(config)# aaa new-model</p>	<p>Enables the AAA access control model.</p> <ul style="list-style-type: none"> DHCP accounting functions only in the access control model. <p>Note TACACS and extended TACACS commands are not available after this command is configured and are not supported by DHCP accounting.</p>
Step 4	<pre>aaa group server radius group-name</pre> <p>Example: Router(config)# aaa group server radius RGROUP-1</p>	<p>Creates a server group for AAA or TACACS+ services and enters server group configuration mode.</p> <ul style="list-style-type: none"> The server group is created in this step so that accounting services can be applied.
Step 5	<pre>server ip-address auth-port port-number acct-port port-number</pre> <p>Example: Router(config-sg-radius)# server 10.0.0.1 auth-port 1645 acct-port 1646</p>	<p>Specifies the servers that are members of the server group that was created in Step 4.</p> <ul style="list-style-type: none"> You must open port numbers for authorization and accounting. 1645 is the default port number for authorization, and 1646 is the default port number for accounting. The range of port numbers that can be specified is from 0 to 65535. The values entered for the auth-port <i>port-number</i> and acct-port <i>port-number</i> keywords and arguments must match the port numbers that will be configured in Step 10.
Step 6	<pre>exit</pre> <p>Example: Router(config-sg-radius)# exit</p>	<p>Exits server group configuration mode and enters global configuration mode.</p>
Step 7	<pre>aaa accounting {system network exec connection commands level} {default list-name} {start-stop stop-only none} [broadcast] group group-name</pre> <p>Example: Router(config)# aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1</p>	<p>Configures RADIUS accounting for the specified server group.</p> <ul style="list-style-type: none"> The RADIUS accounting server is specified in the first <i>list-name</i> argument (RADIUS-GROUP1), and the target server group is specified in the second <i>group-name</i> argument (RGROUP-1). This command enables start and stop accounting for DHCP accounting. The start-stop keyword enables the transmission of both START and STOP accounting messages. The stop-only keyword will enable the generation and verification of STOP accounting messages only.
Step 8	<pre>aaa session-id {common unique}</pre> <p>Example: Router(config)# aaa session-id common</p>	<p>Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.</p>

	Command or Action	Purpose
Step 9	<p>ip radius source-interface <i>interface-type</i> [vrf <i>vrf-name</i>]</p> <p>Example: Router(config)# ip radius source-interface Ethernet 0</p>	Forces RADIUS to use the IP address of the specified interface for all outgoing RADIUS packets.
Step 10	<p>radius-server host {<i>hostname</i> <i>ip-address</i>} [auth-port <i>port-number</i>] [acct-port <i>port-number</i>]</p> <p>Example: Router(config)# radius-server host 10.1.1.1 auth-port 1645 acct-port 1646</p>	<p>Specifies the radius server host.</p> <ul style="list-style-type: none"> The values entered for the auth-port <i>port-number</i> and acct-port <i>port-number</i> keywords and arguments must match the port numbers that were configured in Step 5.
Step 11	<p>radius-server retransmit <i>number-of-retries</i></p> <p>Example: Router(config)# radius-server retransmit 3</p>	Specifies the number of times that Cisco IOS software will look for RADIUS server hosts.

Troubleshooting Tips

To monitor and troubleshoot the configuration of RADIUS accounting, use the following command:

Command	Purpose
<p>debug radius accounting</p> <p>Example: Router# debug radius accounting</p>	The debug radius command is used to display RADIUS events on the console of the router. These events provide information about RADIUS processes. DHCP accounting information can be filtered with the accounting keyword. START and STOP accounting message information will also be displayed.

Configuring DHCP Accounting

Perform this task to configure DHCP accounting.

DHCP Accounting

AAA and RADIUS must be enabled before DHCP accounting will operate. DHCP accounting is enabled with the **accounting** DHCP pool configuration command. This command configures DHCP to operate with AAA and RADIUS to enable secure START and STOP accounting messages. This configuration adds a layer of security that allows DHCP lease assignment and termination to be triggered for the appropriate RADIUS START and STOP accounting records so that the session state is properly maintained by upstream devices, such as the SSG.

DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis.

Prerequisites

You must configure an SSG for client authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool *pool-name***
4. **accounting *method-list-name***

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	ip dhcp pool <i>pool-name</i> Example: Router(config)# ip dhcp pool WIRELESS-POOL	Configures a DHCP address pool and enters DHCP pool configuration mode.
Step 4	accounting <i>method-list-name</i> Example: Router(dhcp-config)# accounting RADIUS-GROUP1	Enables DHCP accounting if the specified server group is configured to run RADIUS accounting. <ul style="list-style-type: none"> • The example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group. See Step 7 in the Configuring AAA and RADIUS for DHCP Accounting configuration task table for more details.

Verifying DHCP Accounting

Perform this task to verify the DHCP accounting configuration.

The **debug radius**, **debug ip dhcp server events**, **debug aaa accounting**, **debug aaa id** commands do not need to be issued together or in the same session as there are differences in the information that is provided. These commands, however, can be used to display DHCP accounting start and stop events, AAA accounting messages, and information about AAA and DHCP hosts and clients. See the “[RADIUS Accounting Attributes](#)” section of this document for a list of AAA attributes that have been introduced by DHCP accounting. The **show running-config | begin dhcp** command can be used to display the local DHCP configuration including the configuration of DHCP accounting.

SUMMARY STEPS

1. `enable`
2. `debug radius accounting`
3. `debug ip dhcp server events`
4. `debug aaa accounting`
5. `debug aaa id`
6. `show running-config | begin dhcp`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p><code>debug radius accounting</code></p> <p>Example: Router# debug radius accounting</p>	<p>Displays RADIUS events on the console of the router.</p> <ul style="list-style-type: none"> • These events provide information about RADIUS processes. DHCP accounting information can be filtered with the accounting keyword. START and STOP accounting messages will be displayed in the output.
Step 3	<p><code>debug ip dhcp server events</code></p> <p>Example: Router# debug ip dhcp server events</p>	<p>Displays DHCP IP address assignments, DHCP lease expirations, and DHCP database changes.</p>
Step 4	<p><code>debug aaa accounting</code></p> <p>Example: Router# debug aaa accounting</p>	<p>Displays AAA accounting events.</p> <ul style="list-style-type: none"> • START and STOP accounting messages will be displayed in the output.
Step 5	<p><code>debug aaa id</code></p> <p>Example: Router# debug aaa id</p>	<p>Displays AAA events as they relate to unique AAA session IDs.</p>
Step 6	<p><code>show running-config</code></p> <p>Example: Router# show running-config begin dhcp</p>	<p>The show running-config command is used to display the local configuration of the router. The sample output is filtered with the begin keyword to start displaying output at the DHCP section of the running configuration.</p>

Configuration Examples for DHCP Accounting

- [AAA and RADIUS for DHCP Accounting: Example, page 10](#)
- [DHCP Accounting: Example, page 10](#)
- [Verifying DHCP Accounting: Example, page 10](#)

AAA and RADIUS for DHCP Accounting: Example

The following example shows how to configure AAA and RADIUS for DHCP accounting.

```
aaa new-model
aaa group server radius RGROUP-1
  server 10.1.1.1 auth-port 1645 acct-port 1646
  exit
aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1
aaa session-id common
ip radius source-interface Ethernet0
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
exit
```

DHCP Accounting: Example

DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis. The following example shows how to configure DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group.

```
ip dhcp pool WIRELESS-POOL
  accounting RADIUS-GROUP1
  exit
```

Verifying DHCP Accounting: Example

DHCP accounting is enabled after both RADIUS and AAA for DHCP are configured. DHCP START and STOP accounting generation information can be monitored with the **debug radius accounting** and **debug ip dhcp server events** commands. See the [How to Configure DHCP Accounting](#) section of this document for a list of AAA attributes that have been introduced by the DHCP accounting.

The following is sample output from the **debug radius accounting** command. The output shows the DHCP lease session ID, the MAC address, and the IP address of the client interface.

```
00:00:53: RADIUS: Pick NAS IP for uid=2 tableid=0 cfg_addr=10.0.18.3 best_addr=0.0.0.0
00:00:53: RADIUS(00000002): sending
00:00:53: RADIUS(00000002): Send to unknown id 21645/1 10.1.1.1 :1646, Accounting-Request,
len 76
00:00:53: RADIUS: authenticator C6 FE EA B2 1F 9A 85 A2 - 9A 5B 09 B5 36 B5 B9 27
00:00:53: RADIUS: Acct-Session-Id [44] 10 "00000002"
00:00:53: RADIUS: Framed-IP-Address [8] 6 10.0.0.10
00:00:53: RADIUS: Calling-Station-Id [31] 16 "00000c59df76"
00:00:53: RADIUS: Acct-Status-Type [40] 6 Start [1]
00:00:53: RADIUS: Service-Type [6] 6 Framed [2]
00:00:53: RADIUS: NAS-IP-Address [4] 6 10.0.18.3
00:00:53: RADIUS: Acct-Delay-Time [41] 6 0
```

The following is sample output from the **debug ip dhcp server events** command. The output was generated on a DHCP server and shows an exchange of DHCP messages between the client and server to negotiate a DHCP lease. The acknowledgment that confirms to the DHCP server that the client has accepted the assigned IP address triggers the accounting START message. It is shown in the last line of the following output:

```
00:45:50:DHCPD:DHCPDISCOVER received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 on
interface Ethernet0.
```

```
00:45:52:DHCPD:assigned IP address 10.10.10.16 to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.

00:45:52:DHCPD:Sending DHCP OFFER to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31(10.10.10.16)

00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.

00:45:52:DHCPD:DHC PREREQUEST received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.

00:45:52:DHCPD:Sending DHCP ACK to client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31
(10.10.10.16) .

00:45:52:DHCPD:broadcasting BOOTREPLY to client 0001.42c9.ec75.

00:45:52:DHCPD:triggered Acct Start for 0001.42c9.ec75 (10.10.10.16) .
```

The following is sample output from the **debug ip dhcp server events** command. The output was generated on a DHCP server and shows the receipt of an explicit release message from the DHCP client. The DHCP server triggers an accounting STOP message and then returns the IP address to the DHCP pool. Information about the accounting STOP message is shown in the third line of the following output:

```
00:46:26:DHCPD:DHC PRELEASE message received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 (10.10.10.16)

00:46:26:DHCPD:triggered Acct Stop for (10.10.10.16) .

00:46:26:DHCPD:returned 10.10.10.16 to address pool WIRELESS-POOL.
```

Additional References

For additional information related to DHCP Accounting, refer to the following references:

Related Documents

Related Topic	Document Title
DHCP commands	<i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> , Release 12.2
DHCP configuration tasks	<i>Cisco IOS IP Configuration Guide</i> , Release 12.2
Securing DHCP bindings	<i>DHCP Secured IP Address Assignment</i> : http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122t/122t15/ftdsiaa.htm
AAA configuration tasks	<i>Cisco IOS Security Configuration Guide</i> , Release 12.2
AAA commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.2T
RADIUS configuration tasks	<i>Cisco IOS Security Configuration Guide</i> , Release 12.2
RADIUS commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS Security Command Reference</i> , Release 12.2T
SSG configuration tasks and commands	“Service Selection Gateway” feature document, Release 12.2(8)T

Standards

Standards ¹	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

1. Not all supported standards are listed.

MIBs

MIBs ¹	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

1. Not all supported MIBs are listed.

RFCs

RFCs ¹	Title
RFC 2131	<i>Dynamic Host Configuration Protocol</i>

RFCs ¹	Title
RFC 2132	<i>DHCP Options and BOOTP Vendor Extensions</i>
RFC 2866	<i>RADIUS Accounting</i>

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and lots more. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents a new command. All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

- [accounting \(DHCP\)](#)

accounting (DHCP)

To enable DHCP accounting, use the **accounting** command in DHCP pool configuration mode. To disable DHCP accounting for the specified server group, use the **no** form of this command.

accounting *server-group-name*

no accounting *server-group-name*

Syntax Description

<i>server-group-name</i>	Name of a server group to apply DHCP accounting. The server group can have one or more members. The server group is defined in the configuration of the aaa group server and aaa accounting commands.
--------------------------	---

Defaults

No default behavior or values

Command Modes

DHCP pool configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(27)SBA	This command was integrated.

Usage Guidelines

The **accounting** DHCP pool configuration command is used to enable the DHCP accounting feature by sending secure DHCP START accounting messages when IP addresses are assigned to DHCP clients, and secure DHCP STOP accounting messages when DHCP leases are terminated. A DHCP lease is terminated when the client explicitly releases the lease, when the session times out, and when the DHCP bindings are cleared from the DHCP database. DHCP accounting is configured on a per-client or per-lease basis. Separate DHCP accounting processes can be configured on a per-pool basis.

The **accounting** command can be used only to network pools in which bindings are created automatically and destroyed upon lease termination (or when the client sends a DHCP RELEASE message). DHCP bindings are also destroyed when the **clear ip dhcp binding** or **no service dhcp** command is issued. These commands should be used with caution if an address pool is configured with DHCP accounting.

AAA and RADIUS must be configured before this command can be used to enable DHCP accounting. A server group must be defined with the **aaa group server** command. START and STOP message generation is configured with the **aaa accounting** command. The **aaa accounting** command can be configured to enable the DHCP accounting to send both START and STOP messages or STOP messages only.

Examples

The following example configures DHCP accounting START and STOP messages to be sent if RADIUS-GROUP1 is configured as a start-stop group. STOP messages will only be sent if RADIUS-GROUP1 is configured as a stop-only group.

```
Router(config)# ip dhcp pool WIRELESS-POOL
Router(dhcp-config)# accounting RADIUS-GROUP1
Router(dhcp-config)# exit
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
aaa session-id	Specifies whether the same session ID will be used for each AAA accounting service type within a call or whether a different session ID will be assigned to each accounting service type.
clear arp-cache	Deletes all dynamic entries from the ARP cache.
clear ip dhcp binding	Deletes an automatic address binding from the Cisco IOS DHCP server database.
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies the number of times that IOS will look for RADIUS server hosts.
service dhcp	Enables the Cisco IOS DHCP server and relay agent features.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.
update arp	Secures the MAC address of the authorized client interface to the DHCP binding.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

