Configuring DHCP Services for Accounting and Security

Last Updated: December 20, 2011

Cisco IOS software supports several capabilities that enhance DHCP security, reliability, and accounting in Public Wireless LANs (PWLANs). This functionality can also be used in other network implementations. This module describes the concepts and tasks needed to configure DHCP services for accounting and security.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring DHCP Services for Accounting and Security

Before you configure DHCP services for accounting and security, you should understand the concepts documented in the “DHCP Overview” module.

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

Information About DHCP Services for Accounting and Security

DHCP Operation in Public Wireless LANs

The configuration of DHCP in a 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

As more people start using PWLANs, security becomes an important concern. Most implementations of PWLANs rely on DHCP for users to obtain an IP address while in a hot spot (such as a coffee shop, airport terminal, hotel, and so on) and use this IP address provided by the DHCP server throughout their session.

IP spoofing is a common technique used by hackers to spoof IP addresses. For example, customer A obtains an IP address from DHCP and has already been authenticated to use the PWLAN, but a hacker spoofs the IP address of customer A and uses this IP address to send and receive traffic. Customer A will still be billed for the service even though he or she is not using the service.

Address Resolution Protocol (ARP) table entries are dynamic by design. Request and reply ARP packets are sent and received by all the networking devices in a network. In a DHCP network, the DHCP server stores the leased IP address to the MAC address or the client identifier of the client in the DHCP binding. But as ARP entries are learned dynamically, an unauthorized client can spoof the IP address given by the DHCP server and start using that IP address. The MAC address of this unauthorized client will replace the MAC address of the authorized client in the ARP table, allowing the unauthorized client to freely use the spoofed IP address.

DHCP Services for Security and Accounting Overview

DHCP security and accounting features have been designed and implemented to address the security concerns in PWLANs but also can be used in other network implementations.

DHCP accounting provides authentication, authorization, and accounting (AAA) and RADIUS support for DHCP. The AAA and RADIUS support improves security by sending secure START and STOP accounting messages. The configuration of DHCP accounting 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 an SSG.

This additional security can help to prevent hackers or unauthorized clients from gaining illegal entry to the network by spoofing authorized DHCP leases.

Three other features have been designed and implemented to address the security concerns in PWLANs. The first feature secures ARP table entries to DHCP leases in the DHCP database. The secure ARP functionality prevents IP spoofing by synchronizing the database of the DHCP server with the ARP table to avoid address hijacking. Secure ARP adds an entry to the ARP table for a client when an address is allocated that can be deleted by the DHCP server only when a binding expires.

The second feature is DHCP authorized ARP. This functionality provides a complete solution by addressing the need for DHCP to explicitly know when a user logs out. Before the introduction of DHCP authorized ARP, there was no mechanism to inform the DHCP server if a user had left the system ungracefully, which could result in excessive billing for a customer that had logged out but without the system detecting it. To prevent this problem, DHCP authorized ARP sends periodic ARP messages on a per-minute basis to determine if a user is still logged in. Only authorized users can respond to the ARP request. ARP responses from unauthorized users are blocked at the DHCP server, providing an extra level of security.

In addition, DHCP authorized ARP disables dynamic ARP learning on an interface. The address mapping can be installed only by the authorized component specified by the **arp authorized** interface configuration command. DHCP is the only authorized component allowed to install ARP entries.

The third feature is ARP Auto-logoff, which adds finer control for probing when authorized users log out. The **arp probe interval** command specifies when to start a probe (the timeout), how frequently a peer is probed (the interval), and the maximum number of retries (the count).

DHCP Lease Limits

You can control the number of subscribers globally or on a per-interface basis by configuring a DHCP lease limit. This functionality allows an ISP to limit the number of leases available to clients per household or connection.

How to Configure DHCP Services for Accounting and Security

Configuring 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 the table below. 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** *type number* [**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. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Router(config)# aaa new-model`	Enables the AAA access control model. • DHCP accounting functions only in the access control model. **Note** TACACS and extended TACACS commands are not available after this command is configured and are not supported by DHCP accounting.
Step 4	**aaa group server radius** *group-name* **Example:** `Router(config)# aaa group server radius RGROUP-1`	Creates a server group for AAA or TACACS+ services and enters server group RADIUS configuration mode. • The server group is created in this step so that accounting services can be applied.
Step 5	**server** *ip-address* **auth-port** *port-number* **acct-port** *port-number* **Example:** `Router(config-sg-radius)# server 10.0.0.1 auth-port 1645 acct-port 1646`	Specifies the servers that are members of the server group that was created in Step 4. • 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** *port-number*and **acct-port** *port-number* keywords and arguments must match the port numbers that will be configured in Step 10.
Step 6	**exit** **Example:** `Router(config-sg-radius)# exit`	Exits server group RADIUS configuration mode and enters global configuration mode.
Step 7	**aaa accounting** {**system** | **network** | **exec** | **connection** | **commands** *level*} {**default** | *list-name*} {**start-stop** | **stop-only** | **none**} [**broadcast**] **group** *group-name* **Example:** `Router(config)# aaa accounting network RADIUS-GROUP1 start-stop group RGROUP-1`	Configures RADIUS accounting for the specified server group. • The RADIUS accounting server is specified in the first *list-name* argument (RADIUS-GROUP1), and the target server group is specified in the second *group-name*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.

	Command or Action	Purpose
Step 8	**aaa session-id** {**common** | **unique**} **Example:** `Router(config)# aaa session-id common`	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.
Step 9	**ip radius source-interface** *type number* [**vrf** *vrf-name*] **Example:** `Router(config)# ip radius source-interface Ethernet 0`	Forces RADIUS to use the IP address of the specified interface for all outgoing RADIUS packets.
Step 10	**radius-server host** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] **Example:** `Router(config)# radius-server host 10.1.1.1 auth-port 1645 acct-port 1646`	Specifies the RADIUS server host. • The values entered for the **auth-port** *port-number*and **acct-port** *port-number* keywords and arguments must match the port numbers that were configured in Step 5.
Step 11	**radius-server retransmit** *number-of-retries* **Example:** `Router(config)# radius-server retransmit 3`	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:

debug radius accounting

Configuring DHCP Accounting

Perform this task to configure DHCP accounting.

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.

You must configure an SSG for client authentication. AAA and RADIUS must be enabled before DHCP accounting will operate.

Note The following restrictions apply to DHCP accounting:

- 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**command is entered, which also triggers an accounting STOP message. You should exercise caution when entering these commands if a pool is configured with DHCP accounting, because these commands will clear active leases.

>

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool-name* **Example:** `Router(config)# ip dhcp pool WIRELESS-POOL`	Configures a DHCP address pool and enters DHCP pool configuration mode.

	Command or Action	Purpose
Step 4	**accounting** *method-list-name* **Example:** `Router(config-dhcp)# accounting RADIUS-GROUP1`	Enables DHCP accounting if the specified server group is configured to run RADIUS accounting. • 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 be sent only if RADIUS-GROUP1 is configured as a stop-only group. See Step 7 in the Configuring AAA and RADIUS for DHCP Accounting, page 3 section for more details.

Verifying DHCP Accounting

Perform this task to verify the DHCP accounting configuration.

The **debug radius**, **debug radius accounting**, **debug ip dhcp server events**, **debug aaa accounting**, and **debug aaa id**commands need not be issued together or in the same session because 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 module 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	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug radius accounting** **Example:** `Router# debug radius accounting`	Displays 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 messages will be displayed in the output.

	Command or Action	Purpose
Step 3	**debug ip dhcp server events** **Example:** `Router# debug ip dhcp server events`	Displays DHCP IP address assignments, DHCP lease expirations, and DHCP database changes.
Step 4	**debug aaa accounting** **Example:** `Router# debug aaa accounting`	Displays AAA accounting events. • START and STOP accounting messages will be displayed in the output.
Step 5	**debug aaa id** **Example:** `Router# debug aaa id`	Displays AAA events as they relate to unique AAA session IDs.
Step 6	**show running-config | begin dhcp** **Example:** `Router# show running-config | begin dhcp`	Displays 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.

Securing ARP Table Entries to DHCP Leases

Perform this task to secure ARP table entries to DHCP leases in the DHCP database.

When the **update arp** command is used, ARP table entries and their corresponding DHCP leases are secured automatically for all 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. If this command is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool -name*
4. **update arp**
5. **renew deny unknown**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp pool** *pool -name* **Example:** `Router(config)# ip dhcp pool WIRELESS-POOL`	Configures a DHCP address pool and enters DHCP pool configuration mode.
Step 4	**update arp** **Example:** `Router(config-dhcp)# update arp`	Secures insecure ARP table entries to the corresponding DHCP leases. • Existing active DHCP leases will not be secured until they are renewed. Using the **no update arp** command will change secured ARP table entries back to dynamic ARP table entries.
Step 5	**renew deny unknown** **Example:** `Router(config-dhcp)# renew deny unknown`	(Optional) Configures the renewal policy for unknown clients. • See the "Troubleshooting Tips" section for information about when to use this command.

• Troubleshooting Tips, page 10

Troubleshooting Tips

In some usage scenarios, such as a wireless hot spot, where both DHCP and secure ARP are configured, a connected client device might go to sleep or suspend for a period of time. If the suspended time period is greater than the secure ARP timeout (default of 91 seconds), but less than the DHCP lease time, the client can awaken with a valid lease, but the secure ARP timeout has caused the lease binding to be removed because the client has been inactive. When the client awakens, the client still has a lease on the client side but is blocked from sending traffic. The client will try to renew its IP address but the DHCP server will ignore the request because the DHCP server has no lease for the client. The client must wait for the lease to expire before being able to recover and send traffic again.

To remedy this situation, use the **renew deny unknown** command in DHCP pool configuration mode. This command forces the DHCP server to reject renewal requests from clients if the requested address is present

at the server but is not leased. The DHCP server sends a DHCPNAK denial message to the client, which forces the client back to its initial state. The client can then negotiate for a new lease immediately, instead of waiting for its old lease to expire.

Configuring DHCP Authorized ARP

Perform this task to configure DHCP authorized ARP, which disables dynamic ARP learning on an interface.

DHCP authorized ARP has a limitation in supporting accurate one-minute billing. DHCP authorized ARP probes for authorized users once or twice, 30 seconds apart. In a busy network the possibility of missing reply packets increases, which can cause a premature logoff. If you need a more accurate and finer control for probing of the authorized user, configure the **arp probe interval** command. This command specifies when to start a probe, the interval between unsuccessful probes, and the maximum number of retries before triggering an automatic logoff.

Note If both static and authorized ARP are installing the same ARP entry, static configuration overrides authorized ARP. You can install a static ARP entry by using the **arp** global configuration command. You can only remove a nondynamic ARP entry by the same method in which it was installed.

The ARP timeout period should not be set to less than 30 seconds. The feature is designed to send out an ARP message every 30 seconds, beginning 90 seconds before the ARP timeout period specified by the **arp timeout**command. This behavior allows probing for the client at least three times before giving up on the client. If the ARP timeout is set to 60 seconds, an ARP message is sent twice, and if it is set to 30 seconds, an ARP message is sent once. An ARP timeout period set to less than 30 seconds can yield unpredictable results.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*
5. **arp authorized**
6. **arp timeout** *seconds*
7. **arp probe interval** *seconds* **count** *number*
8. **end**
9. **show arp**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 1`	Configures an interface type and enters interface configuration mode.
Step 4	**ip address** *ip-address mask* **Example:** `Router(config-if)# ip address 209.165.200.224 209.165.200.224`	Sets a primary IP address for an interface.
Step 5	**arp authorized** **Example:** `Router(config-if)# arp authorized`	Disables dynamic ARP learning on an interface. • The IP address to MAC address mapping can be installed only by the authorized subsystem.
Step 6	**arp timeout** *seconds* **Example:** `Router(config-if)# arp timeout 60`	Configures how long an entry remains in the ARP cache.

	Command or Action	Purpose
Step 7	**arp probe interval** *seconds* **count** *number* **Example:** `Router(config-if)# arp probe interval 5 count 30`	(Optional) Specifies an interval, in seconds, and number of probe retries. • *seconds* --Interval, in seconds, after which the next probe will be sent to see if a peer is present. The range is from 1 to 10. • *number* --Number of probe retries. If there is no reply after the count has been reached, the peer has logged off. The range is from 1 to 60. **Note** You must use the **no** form of the command to stop the probing process.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 9	**show arp** **Example:** `Router# show arp`	(Optional) Displays the entries in the ARP table.

Configuring a DHCP Lease Limit to Globally Control the Number of Subscribers

Perform this task to globally control the number of DHCP leases allowed for clients behind an ATM Routed Bridged Encapsulation (RBE) unnumbered interface or serial unnumbered interface.

This feature allows an ISP to globally limit the number of leases available to clients per household or connection.

If this feature is enabled on a Cisco IOS DHCP relay agent connected to clients through unnumbered interfaces, the relay agent keeps information about the DHCP leases offered to the clients per subinterface. When a DHCPACK message is forwarded to the client, the relay agent increments the number of leases offered to clients on that subinterface. If a new DHCP client tries to obtain an IP address and the number of leases has already reached the configured lease limit, DHCP messages from the client will be dropped and will not be forwarded to the DHCP server.

If this feature is enabled on the Cisco IOS DHCP server directly connected to clients through unnumbered interfaces, the server allocates addresses and increments the number of leases per subinterface. If a new client tries to obtain an IP address, the server will not offer an IP address if the number of leases on the subinterface has already reached the configured lease limit.

Note This feature is not supported on numbered interfaces. The lease limit can be applied only to ATM with RBE unnumbered interfaces or serial unnumbered interfaces.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease log**
4. **ip dhcp limit lease per interface** *lease-limit*
5. **end**
6. **show ip dhcp limit lease** [*type number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp limit lease log** **Example:** `Router(config)# ip dhcp limit lease log`	(Optional) Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded. • If this command is configured, any lease limit violations will display in the output of the **show ip dhcp limit lease** command.
Step 4	**ip dhcp limit lease per interface** *lease-limit* **Example:** `Router(config)# ip dhcp limit lease per interface 2`	Limits the number of leases offered to DHCP clients behind an ATM RBE unnumbered or serial unnumbered interface.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.
Step 6	**show ip dhcp limit lease** [*type number*] **Example:** `Router# show ip dhcp limit lease`	(Optional) Displays the number of times the lease limit threshold has been violated. • You can use the **clear ip dhcp limit lease** privileged EXEC command to manually clear the stored lease violation entries.

• Troubleshooting Tips, page 15

Troubleshooting Tips

You can use the **debug ip dhcp server packet** and **debug ip server events** commands to troubleshoot the DHCP lease limit.

Configuring a DHCP Lease Limit to Control the Number of Subscribers on an Interface

Perform this task to limit the number of DHCP leases allowed on an interface.

This feature allows an ISP to limit the number of leases available to clients per household or connection on an interface.

If this feature is enabled on the Cisco IOS DHCP server directly connected to clients through unnumbered interfaces, the server allocates addresses and increments the number of leases per subinterface. If a new client tries to obtain an IP address, the server will not offer an IP address if the number of leases on the subinterface has already reached the configured lease limit.

Note This feature is not supported on numbered interfaces. The lease limit can be applied only to ATM with RBE unnumbered interfaces or serial unnumbered interfaces.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip dhcp limit lease log**
4. **interface** *type number*
5. **ip dhcp limit lease** *lease-limit*
6. **end**
7. **show ip dhcp limit lease** [*type number*]
8. **show ip dhcp server statistics** [*type number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip dhcp limit lease log** **Example:** `Router(config)# ip dhcp limit lease log`	(Optional) Enables DHCP lease violation logging when a DHCP lease limit threshold is exceeded. • If this command is configured, any lease limit violations will display in the output of the **show ip dhcp limit lease** command.
Step 4	**interface** *type number* **Example:** `Router(config)# interface Seria l0/0`	Enters interface configuration mode.
Step 5	**ip dhcp limit lease** *lease-limit* **Example:** `Router(config-if)# ip dhcp limit lease 6`	Limits the number of leases offered to DHCP clients per interface. • The interface configuration will override any global setting specified by the **ip dhcp limit lease per interface** global configuration command.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**show ip dhcp limit lease** [*type number*] **Example:** `Router# show ip dhcp limit lease Serial 0/0`	(Optional) Displays the number of times the lease limit threshold has been violated. • You can use the **clear ip dhcp limit lease** privileged EXEC command to manually clear the stored lease violation entries.
Step 8	**show ip dhcp server statistics** [*type number*] **Example:** `Router# show ip dhcp server statistics Serial0/0`	(Optional) Displays DHCP server statistics. • This command was modified in Cisco IOS Release 12.2(33)SRC to display interface-level DHCP statistics.

- Troubleshooting Tips, page 17

Troubleshooting Tips

You can use the **debug ip dhcp server packet** and **debug ip server events** commands to troubleshoot the DHCP lease limit.

Configuration Examples for DHCP Services for Accounting and Security

Example Configuring AAA and RADIUS for DHCP Accounting

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 Ethernet 0
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
exit
```

Example Configuring 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. 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
```

Example Verifying DHCP Accounting

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 "RADIUS Accounting Attributes" task for a list of AAA attributes that have been introduced by 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 DHCPOFFER 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:DHCPREQUEST received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31.
00:45:52:DHCPD:Sending DHCPACK 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:

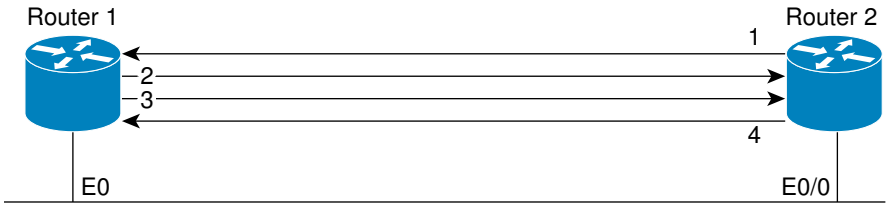
```
00:46:26:DHCPD:DHCPRELEASE message received from client
0063.6973.636f.2d30.3030.312e.3432.6339.2e65.6337.352d.4574.31 (10.10.10.16)
00:46:26:DHCPD:triggered Acct Stop for (10.10.10.16).
00:46:26:DHCPD:returned 10.10.10.16 to address pool WIRELESS-POOL.
```

Example Configuring DHCP Authorized ARP

Router 1 is the DHCP server that assigns IP addresses to the routers that are seeking IP addresses, and Router 2 is the DHCP client configured to obtain its IP address through the DHCP server. Because the **update arp** DHCP pool configuration command is configured on Router 1, the router will install a secure ARP entry in its ARP table. The **arp authorized** command stops any dynamic ARP on that interface. Router 1 sends periodic ARPs to Router 2 to make sure that the client is still active. Router 2 responds with an ARP reply. Unauthorized clients cannot respond to these periodic ARPs. The unauthorized ARP responses are blocked at the DHCP server. The timer for the entry is refreshed on Router 1 upon receiving the response from the authorized client.

See the figure below for a sample topology.

Figure 1 Sample Topology for DHCP Authorized ARP



1. Send request for IP address.
2. Assign IP address and install secure ARP entry for it in Router 1.
3. Send periodic ARPs to make sure Router 2 is still active.
4. Reply to periodic ARPs.

103063

Router 1 (DHCP Server)

```
ip dhcp pool name1
 network 10.0.0.0 255.255.255.0
 lease 0 0 20
 update arp
!
interface Ethernet 0
 ip address 10.0.0.1 255.255.255.0
 half-duplex
 arp authorized
 arp timeout 60
! optional command to adjust the periodic ARP probes sent to the peer
 arp probe interval 5 count 15
```

Router 2 (DHCP Client)

```
interface Ethernet 0/0
 ip address dhcp
 half-duplex
```

Example Verifying DHCP Authorized ARP

The following is sample output from the **show arp** command on Router 1 (see the figure above):

```
Router1# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.3               0   0004.dd0c.ffcb  ARPA   Ethernet01
Internet  10.0.0.1               -   0004.dd0c.ff86  ARPA   Ethernet0
```

The following is sample output from the **show arp** command on Router 2 (see the figure above):

```
Router2# show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.3               -   0004.dd0c.ffcb  ARPA   Ethernet0/02
Internet  10.0.0.1               0   0004.dd0c.ff86  ARPA   Ethernet0/0
```

Example Configuring a DHCP Lease Limit

In the following example, if more than three clients try to obtain an IP address from ATM interface 4/0.1, the DHCPDISCOVER packets will not be forwarded to the DHCP server. If the DHCP server resides on the same router, DHCP will not reply to more than three clients.

```
ip dhcp limit lease per interface 3
!
interface loopback 0
 ip address 10.1.1.129 255.255.255.192
!
interface ATM 4/0.1
 no ip address
!
interface ATM 4/0.1 point-to-point
 ip helper-address 172.16.1.2
 ip unnumbered loopback 0
 atm route-bridged ip
  pvc 88/800
  encapsulation aal5snap
```

In the following example, five DHCP clients are allowed to receive IP addresses. If a sixth client tries to obtain an IP address, the DHCPDISCOVER messages will not be forwarded to the DHCP server and a trap will be sent to the SNMP manager.

```
ip dhcp limit lease log
!
ip dhcp pool pool1
 network 10.1.1.0 255.255.255.0
!
interface loopback 0
 ip address 10.1.1.1 255.255.255.0
!
interface serial 0/0.2 point-to-point
 ip dhcp limit lease 5
 ip unnumbered loopback 0
 exit
snmp-server enable traps dhcp interface
```

Additional References

Related Documents

Related Topic	Document Title
ARP commands: complete command syntax, command modes, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP commands: complete command syntax, command modes, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
DHCP conceptual information	"DHCP Overview" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP server configuration	"Configuring the Cisco IOS DHCP Server" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP ODAP configuration	"Configuring the DHCP Server On-Demand Address Pool Manager" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP client configuration	"Configuring the Cisco IOS DHCP Client" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP relay agent configuration	"Configuring the Cisco IOS DHCP Relay Agent" module in the *Cisco IOS IP Addressing Configuration Guide*
DHCP enhancements for edge-session management	"Configuring DHCP Enhancements for Edge-Session Management" module in the *Cisco IOS IP Addressing Configuration Guide*
AAA and RADIUS configuration tasks	*Cisco IOS Security Configuration Guide*
AAA and RADIUS commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Security Command Reference*

Standards

Standards	Title
No new or modified standards are supported by this functionality.	--

MIBs

MIBs	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 locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for DHCP Services for Accounting and Security

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for DHCP Services for Accounting and Security

Feature Name	Releases	Feature Information
DHCP per Interface Lease Limit and Statistics	12.2(33)SRC	This feature limits the number of DHCP leases offered to DHCP clients on an interface. DHCP server statistics reporting was enhanced to display interface-level statistics. The following commands were introduced or modified by this feature: **clear ip dhcp limit lease**, **ip dhcp limit lease**, **ip dhcp limit lease log**, **show ip dhcp limit lease**, **show ip dhcp server statistics**.
DHCP Lease Limit per ATM RBE Unnumbered Interface	12.2(28)SB 12.3(2)T 15.1(1)S	This feature limits the number of DHCP leases per subinterface offered to DHCP clients connected from an ATM RBE unnumbered interface or serial unnumbered interface of the DHCP server or DHCP relay agent. The following command was introduced by this feature: **ip dhcp limit lease per interface**.
ARP Auto-logoff	12.3(14)T	The ARP Auto-logoff feature enhances DHCP authorized ARP by providing finer control and probing of authorized clients to detect a logoff. The following command was introduced by this feature: **arp probe interval**.

Feature Name	Releases	Feature Information
DHCP Authorized ARP	12.2(33)SRC 12.3(4)T	DHCP authorized ARP enhances the DHCP and ARP components of the Cisco IOS software to limit the leasing of IP addresses to mobile users to authorized users. This feature enhances security in PWLANs by blocking ARP responses from unauthorized users at the DHCP server. The following command was introduced by this feature: **arp authorized**.
DHCP Accounting	12.2(15)T 12.2(28)SB 12.2(33)SRB	DHCP accounting introduces AAA and RADIUS support for DHCP configuration. The following command was introduced by this feature: **accounting**.
DHCP Secured IP Address Assignment	12.2(15)T 12.2(28)SB 12.2(33)SRC	DHCP secure IP address assignment provides the capability to secure ARP table entries to DHCP leases in the DHCP database. This feature secures and synchronizes the MAC address of the client to the DHCP binding, preventing hackers or unauthorized clients from spoofing the DHCP server and taking over a DHCP lease of an authorized client. The following commands were introduced or modified by this feature: **show ip dhcp server statistics**, **update arp**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2011 Cisco Systems, Inc. All rights reserved.