Configuring DHCP Services for Accounting and Security

Last Updated: December 20, 2011

Cisco IOS XE 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 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

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 Remote Authentication Dial-In User Service (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 unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases.

The DHCP Secured IP Address Assignment feature prevents IP spoofing by synchronizing the database of the DHCP server with the ARP table to avoid address hijacking. This secure ARP functionality 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.

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 Internet service provider (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

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.

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.
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 configuration mode. • The server group is created in this step so that accounting services can be applied.

	Command or Action	Purpose
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 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.

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 GigabitEthernet 0/0/0`	Forces RADIUS to use the IP address of the specified interface for all outgoing RADIUS packets.

	Command or Action	Purpose
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 XE software will look for RADIUS server hosts.

- Troubleshooting Tips, page 6

Troubleshooting Tips

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

Command	Purpose
debug radius accounting `Router# debug radius accounting`	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 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 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.

>

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(dhcp-config)# 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 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 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 higher privilege levels, such as 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`	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.

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(dhcp-config)# 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(dhcp-config)# renew deny unknown`	(Optional) Configures the renewal policy for unknown clients. • See the Troubleshooting Tips, page 6 section for information about when to use this command.

- Troubleshooting Tips, page 10

Troubleshooting Tips

In some usage scenarios, such as a wireless hotspot, 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 awake 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 awakes, 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 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 XE 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.

	Command or Action	Purpose
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 Serial0/0/0`	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.

Step 6	**end**
	Example:
	`Router(config-if)# end`
		Exits the configuration mode and returns to privileged EXEC mode.

Step 7	**show ip dhcp limit lease** [*type number*] **Example:** `Router# show ip dhcp limit lease Serial0/0/0`	(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 Serial0/0/0`	(Optional) Displays DHCP server statistics.

- Troubleshooting Tips, page 12

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

Configuring 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 GigabitEthernet0/0/0
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server retransmit 3
exit
```

Configuring 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 "RADIUS Accounting Attributes" section of this module 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 GigabitEthernet0/0/0.
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.
```

Configuring a DHCP Lease Limit Examples

In the following example, 5 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 loopback0
 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 loopback0
 exit
snmp-server enable traps dhcp interface
```

Additional References

The following sections provide references related to configuring DHCP services for accounting and security.

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
DHCP server configuration	“Configuring the Cisco IOS XE DHCP Server” module
DHCP ODAP configuration	“Configuring the DHCP Server On-Demand Address Pool Manager” module
DHCP client configuration	“Configuring the Cisco IOS XE DHCP Client” module
DHCP relay agent configuration	“Configuring the Cisco IOS XE DHCP Relay Agent” module
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 IOS XE 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 website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

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 Configuration Information
DHCP Per Interface Lease Limit and Statistics	Cisco IOS XE Release 2.1	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: **ip dhcp limit lease**, **ip dhcp limit lease log**, **clear ip dhcp limit lease**, **show ip dhcp limit lease**, and **show ip dhcp server statistics**.
DHCP Accounting	Cisco IOS XE Release 2.1	DHCP accounting introduces AAA and RADIUS support for DHCP configuration. The following command was introduced by this feature: **accounting**.
DHCP Secured IP Address Assignment	Cisco IOS XE Release 2.3	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 unauthorized clients or hackers from spoofing the DHCP server and taking over a DHCP lease of an authorized client. The following command was introduced by this feature: **update arp**. The following command was modified by this feature: **show ip dhcp server statistics**.

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.