DHCP Secured IP Address Assignment

The DHCP Secure IP Address Assignment feature introduces the capability to secure ARP table entries to Dynamic Host Configuration Protocol (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. When this feature is enabled and the DHCP server assigns an IP address to the DHCP client, the DHCP server adds a secure ARP entry to the ARP table with the assigned IP address and the MAC address of the client. This ARP entry cannot be updated by any other dynamic ARP packets, and this ARP entry will exist in the ARP table for the configured lease time or as long as the lease is active. The secured ARP entry can be deleted only by an explicit termination message from the DHCP client or by the DHCP server when the DHCP binding expires. This feature can be configured for a new DHCP network or used to upgrade the security of an existing network. The configuration of this feature does not interrupt service and is not visible to the DHCP client.

Feature Specifications for the DHCP Secured IP Address Assignment feature

Feature History	
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

CISCO SYSTEMS

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

Prerequisites for DHCP Secured IP Address Assignment

This document assumes that your network is configured to run DHCP. You will also need to complete the following tasks before you can configure this feature:

- Identify an external File Transport Protocol (FTP), Trivial File Transfer Protocol (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.

Restrictions for DHCP Secured IP Address Assignment

The following restrictions apply to the DHCP Secured IP Address Assignment feature:

- This feature can only be configured for directly connected clients on LAN interfaces and wireless LAN interfaces.
- When this feature is configured, client ARP entries that are created by a DHCP server cannot be removed from the ARP table by the **clear arp-cache** command. This is designed behavior.

Information About DHCP Secured IP Address Assignment

To configure this feature, you must understand the following concepts

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. When the client explicitly disconnects from the network, the DHCP lease is terminated by the DHCP server, and the IP address is returned to the DHCP 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 if it receives an acknowledgement from the client. 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. This 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.

ARP Entries and DHCP Bindings

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 and this will allow the unauthorized client to freely use the spoofed IP address.

DHCP Secure IP Address Assignment

The DHCP Secure IP Address Assignment feature introduces the capability to add an ARP entry binding the MAC address of the client to the DHCP offered IP address. The ARP table entry and DHCP binding can only be deleted by the DHCP server when a DHCP lease expires or is terminated by the client. The ARP table entry will not be overwritten if the DHCP server receives any unsolicited ARP request messages. When the DHCP lease expires or the client terminates the lease, the DHCP server will destroy the DHCP binding and the leased IP address is returned to the DHCP address pool. The secure ARP entry will be removed from the ARP table.

Note This feature does not secure ARP table entries for BOOTP clients.

When the DHCP Secured IP Address feature is enabled, the ARP table entries and 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 feature is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

Configuring Database Agents to Store DHCP Secured IP Addresses

The DHCP Secured IP Address feature also supports the configuration of DHCP database agents. Database agents are used to configure an IOS DHCP server to store DHCP binding information for recovery after a router is reloaded. When this feature is enabled, secure ARP table entries can also be saved to a file, like DHCP bindings, by a DHCP database agent for recovery. These files are transferred using the File Transfer Protocol (FTP), Trivial File Transport Protocol (TFTP), or remote copy protocol (rcp). If a DHCP database agent is configured, the secured lease information is saved in a remote file system. See the following sample output:

```
!IP address     Type  Hardware address  Interface-index
arp 10.0.0.1     1    0060.837b.964c     0 0
```

The “arp” keyword that precedes the IP address indicates that the secure ARP entry will be saved before the router reloads. When a router is reloaded, the DHCP bindings are added to the DHCP database and secured ARP entries are added to the ARP table.

The **ip dhcp database** command is used to configure a database agent on an IOS DHCP server. The database agent will automatically store secure ARP table entries when this feature is configured. No new task are introduced by this feature. For more information about configuring database agents, refer to the “Configuring DHCP” chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

Configuring DHCP Accounting and DHCP Secured IP Address Assignment

For an additional layer of security, the DHCP Accounting feature can be configured with the DHCP Secured IP Address Assignment feature. The DHCP Accounting feature introduces authentication, authorization, and accounting (AAA) and Remote Authentication Dial-In User Service (RADIUS) support for DHCP configuration. The introduction of AAA and RADIUS support improves PWLAN security by sending secure START and STOP accounting messages. The configuration of this feature adds a layer of security to prevent unauthorized clients or hackers from gaining illegal entry to the network by spoofing authorized DHCP leases. 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 Accounting feature, see the following document:

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

How to Configure DHCP Secured IP Address Assignment

This section contains the following procedures for configuring the DHCP Secured IP Address Assignment feature:

- Securing ARP Table Entries to DHCP Leases, page 5
- Verifying that ARP Table Entries Have Been Secured, page 6

Securing ARP Table Entries to DHCP Leases

Use the following steps to enable the DHCP Secured IP Address Assignment feature:

Securing Insecure ARP Table Entries

When the DHCP Secured IP Address feature is enabled, 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 feature 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** | **memory** | **network**}
3. **ip dhcp pool** *pool-name*
4. **update arp**
5. **exit**

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	**`configure`** {**`terminal`** | **`memory`** | **`network`**}
	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. Issuing the **no update arp** command will change secured ARP table entries back to dynamic ARP table entries.

Step 5	**`Exit`**
	Example:
	`Router(dhcp-config)# exit`
		Exits DHCP pool configuration mode and enters global configuration mode.

Troubleshooting Tips

The **clear ip dhcp binding** command can be used to clear DHCP bindings and secured ARP table entries.

What to Do Next

The DHCP Accounting feature can be configured to provide an additional layer of security. When this feature is configured, the SSG will use secure START and STOP accounting messages to control DHCP lease assignment and termination. For more information about the DHCP Accounting feature, refer to the following document:

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

The **ip dhcp database** command can be used to configure a database agent on an IOS DHCP server. The database agent will automatically store secure ARP table entries when this feature is configured. No new task are introduced by this feature. For more information about configuring database agents, refer to the "Configuring DHCP" chapter of the *Cisco IOS IP Configuration Guide*, Release 12.2:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm

Verifying that ARP Table Entries Have Been Secured

Use the following steps to verify that ARP table entries have been secured to their corresponding DHCP leases:

Securing Insecure ARP Table Entries

The **show ip dhcp server statistics** command has been enhanced for this feature to show how many secure ARP entries have been added by the DHCP server.

SUMMARY STEPS

1. **enable**
2. **show ip dhcp server statistics**

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	`show ip dhcp server statistics`
	Example:
	`Router# show ip server statistics`
		Displays Cisco IOS Dynamic Host Configuration Protocol (DHCP) Server statistics, including secured ARP table entries.

Configuration Examples for DHCP Secured IP Address Assignment

Securing an ARP Table Entry to an DHCP Lease Example

The following example configures the Cisco IOS DHCP server to secure ARP table entries to their corresponding DHCP leases within the DHCP pool named WIRELESS-POOL:

```
Router(config)# ip dhcp pool WIRELESS-POOL
Router(dhcp-config)# update arp
Router(dhcp-config)# exit
```

Note Existing active leases are not secured until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically. If the **no update arp** command is issued, all existing secured ARP table entries will automatically be changed to dynamic ARP entries.

Verifying Secured ARP Table Entries Example

To verify that the ARP table entries have been secured to their corresponding DHCP leases, use the **show ip dhcp server statistics** command. The output from this command displays the number of secure ARP table entries on the last line in the first section of the output. The following output shows that 1 secured ARP table entry exists:

```
Router# show ip dhcp server statistics

Memory usage         13745
Address pools        1
Database agents      0
Automatic bindings   1
Manual bindings      0
Expired bindings     0
Malformed messages   0
Secure arp entries   1

Message              Received
BOOTREQUEST          2
DHCPDISCOVER         2
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          1
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              2
DHCPNAK              0
```

Where to Go Next

For information about configuring the DHCP Accounting feature, refer to the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdhcpac.htm

Additional References

For additional information related to DHCP Secured IP Address Assignment, refer to the following references:

Related Documents

Related Topic	Document Title
DHCP commands	*Cisco IOS IP Command Reference, Volume1 of 3: Addressing and Services*, Release 12.2
DHCP configuration tasks, including the configuration of DHCP database agents	*Cisco IOS IP Configuration Guide*, Release 12.2
DHCP accounting for the transmission of secure START and STOP messages.	*DHCP Accounting*, Release 12.2(15)T http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftdhcpac.htm

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.

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

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

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs[1]	Title
RFC 2131	*Dynamic Host Configuration Protocol*
RFC 2132	*DHCP Options and BOOTP Vendor Extensions*

[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 new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command reference publications.

New Commands

- **update arp**

Modified Commands

- **show ip dhcp server statistics**

update arp

To secure dynamic Address Resolution Protocol (ARP) entries in the ARP table to their corresponding DHCP bindings, use the **update arp** command in DHCP pool configuration mode. To disable this command and change secure ARP entries to dynamic ARP entries, use the **no** form of this command.

update arp

no update arp

Syntax Description

This command has no keywords or arguments.

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 into Cisco IOS Release 12.2(27)SBA.

Usage Guidelines

The **update arp** DHCP pool configuration command is used to secure ARP table entries and their corresponding DHCP leases. However, existing active leases are not secured. These leases will remain insecure until they are renewed. When the lease is renewed, it is treated as a new lease and will be secured automatically. If this feature is disabled on the DHCP server, all existing secured ARP table entries will automatically change to dynamic ARP entries.

This command can be configured only under the following conditions:

- DHCP network pools in which bindings are created automatically and destroyed upon lease termination or when the client sends a DHCPRELEASE message.
- Directly connected clients on LAN interfaces and wireless LAN interfaces.

The configuration of this command is not visible to the client. When this command is configured, secured ARP table entries that are created by a DHCP server cannot be removed from the ARP table by the **clear arp-cache** command. This is designed behavior. If a secure ARP entry created by the DHCP server must be removed, the **clear ip dhcp binding** command can be used. This command will clear the DHCP binding and secured ARP table entry.

Note This command does not secure ARP table entries for BOOTP clients.

Examples

The following example configures the Cisco IOS DHCP server to secure ARP table entries to their corresponding DHCP leases within the DHCP pool named WIRELESS-POOL:

```
Router(config)# ip dhcp pool WIRELESS-POOL
Router(dhcp-config)# update arp
Router(dhcp-config)# exit
```

Related Commands

Command	Description
accounting (DHCP)	Enables DHCP accounting for the specified server group.
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 database	Configures a Cisco IOS DHCP Server to save automatic bindings on a remote host called a database agent.
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 Cisco IOS will look for RADIUS server hosts.
show ip dhcp binding	Displays address bindings on the Cisco IOS DHCP server.
show ip dhcp server statistics	Displays Cisco IOS DHCP server statistics.

show ip dhcp server statistics

To display Cisco IOS Dynamic Host Configuration Protocol (DHCP) server statistics, use the **show ip dhcp server statistics** command in privileged EXEC mode.

show ip dhcp server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(1)T	This command was introduced.
12.2(27)SBA	This command was integrated into Cisco IOS Release 12.2(27)SBA.

Examples

The following example displays DHCP server statistics. Table 1 lists descriptions for each field in the example.

```
Router> show ip dhcp server statistics

Memory usage           40392
Address pools          3
Database agents        1
Automatic bindings     190
Manual bindings        1
Expired bindings       3
Malformed messages     0
Secure arp entries     1

Message                Received
BOOTREQUEST            12
DHCPDISCOVER           200
DHCPREQUEST            178
DHCPDECLINE            0
DHCPRELEASE            0
DHCPINFORM             0

Message                Sent
BOOTREPLY              12
DHCPOFFER              190
DHCPACK                172
DHCPNAK                6
```

Table 1 show ip dhcp server statistics Field Descriptions

Field	Description
Memory usage	The number of bytes of RAM allocated by the DHCP server.
Address pools	The number of configured address pools in the DHCP database.
Database agents	The number of database agents configured in the DHCP database.

Table 1 show ip dhcp server statistics Field Descriptions (continued)

Field	Description
Automatic bindings	The number of IP addresses that have been automatically mapped to the MAC addresses of hosts that are found in the DHCP database.
Manual bindings	The number of IP addresses that have been manually mapped to the MAC addresses of hosts that are found in the DHCP database.
Expired bindings	The number of expired leases.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.
Secure arp entries	The number of ARP entries that heve been secured to the MAC address of the client interface.
Message	The DHCP message type that was received by the DHCP server.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

Related Commands

Command	Description
clear ip dhcp server statistics	Resets all Cisco IOS DHCP server counters.