



## DHCP Authorized ARP

---

The DHCP Authorized ARP feature enhances the Dynamic Host Configuration Protocol (DHCP) and Address Resolution Protocol (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 public wireless LANs (PWLANS) by blocking ARP responses from unauthorized users at the DHCP server.

### Feature History for the DHCP Authorized ARP Feature

Release	Modification
12.3(4)T	This feature was introduced.

### 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

- [Restrictions for DHCP Authorized ARP, page 1](#)
- [Information About DHCP Authorized ARP, page 2](#)
- [How to Configure DHCP Authorized ARP, page 3](#)
- [Configuration Examples for DHCP Authorized ARP, page 5](#)
- [Additional References, page 7](#)
- [Command Reference, page 8](#)
- [Glossary, page 10](#)

## Restrictions for DHCP Authorized ARP

When this feature is configured on an interface, dynamic learning of ARP for that interface is disabled.



---

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

This feature is supported only on Ethernet interfaces.

## Information About DHCP Authorized ARP

Before you configure this feature, you should understand the following concepts:

- [Security Vulnerabilities in Public Wireless LANs, page 2](#)
- [DHCP Authorized ARP Feature Design, page 2](#)
- [Benefits of DHCP Authorized ARP, page 2](#)

## Security Vulnerabilities in Public Wireless LANs

Wireless networking is gaining popularity. 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.

## DHCP Authorized ARP Feature Design

Two features have been designed and implemented to address the security concerns in PWLANs. The first is the DHCP Secured Address Assignment feature introduced in Cisco IOS Release 12.2(15)T. This feature secures ARP table entries to DHCP leases in the DHCP database. See [DHCP Secured IP Address Assignment](#) feature documentation for more information.

The second feature is DHCP Authorized ARP. This feature provides a complete solution by addressing the need for DHCP to explicitly know when a user logs out. Before the introduction of this feature, 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 the system had not detected the log out. To prevent this problem, the DHCP Authorized ARP feature 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. Unauthorized ARP responses 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 **authorized arp** interface configuration command. DHCP is the only authorized component currently allowed to install ARP entries.

## Benefits of DHCP Authorized ARP

This feature enhances security in PWLANs by blocking ARP responses from unauthorized users at the DHCP server.

# How to Configure DHCP Authorized ARP

This section contains the following procedures:

- [Securing ARP Table Entries to DHCP Leases, page 3](#) (required)
- [Configuring DHCP Authorized ARP, page 4](#) (required)

## Securing ARP Table Entries to DHCP Leases

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.

This task describes how to secure ARP table entries to DHCP leases:

### SUMMARY STEPS

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

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip dhcp pool</b> <i>pool-name</i>  <b>Example:</b> Router(config)# ip dhcp pool WIRELESS-POOL	Configures a DHCP address pool and enters DHCP pool configuration mode.
Step 4	<b>update arp</b>  <b>Example:</b> Router(dhcp-config)# update arp	Secures insecure ARP table entries to the corresponding DHCP leases. <ul style="list-style-type: none"><li>• Existing active DHCP leases will not be secured until they are renewed. Using the <b>no update arp</b> command will change secured ARP table entries back to dynamic ARP table entries.</li></ul>

## Configuring DHCP Authorized ARP

This task describes how to disable dynamic ARP learning on an interface.

### Restrictions

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 time out 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 time out 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 time out 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 time out 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. **end**
8. **show arp**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface ethernet 1	Configures an interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	<b>ip address</b> <i>ip-address mask</i>  <b>Example:</b> Router(config-if)# ip-address 168.71.6.23 255.255.255.0	Sets a primary IP address for an interface.
Step 5	<b>arp authorized</b>  <b>Example:</b> Router(config-if)# arp authorized	Disables dynamic ARP learning on an interface. <ul style="list-style-type: none"> <li>The IP address to MAC address mapping can only be installed by the authorized subsystem.</li> </ul>
Step 6	<b>arp timeout</b> <i>seconds</i>  <b>Example:</b> Router(config-if)# arp timeout 60	Configures how long an entry remains in the ARP cache. <ul style="list-style-type: none"> <li>Do not set the timeout period to less than 30 seconds as discussed in the “Restrictions” section.</li> </ul>
Step 7	<b>end</b>  <b>Example:</b> Router(config-if)# end	(Optional) Exits the configuration mode and returns to privileged EXEC mode.
Step 8	<b>show arp</b>  <b>Example:</b> Router# show arp	(Optional) Displays the entries in the ARP table.

## Configuration Examples for DHCP Authorized ARP

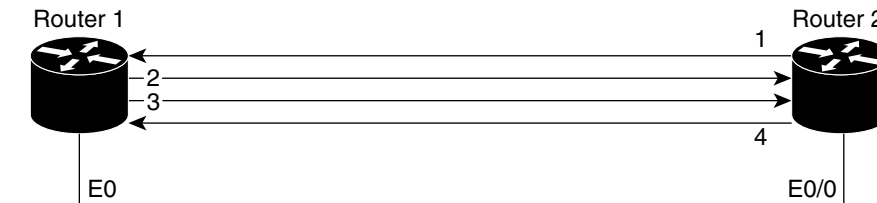
This section contains the following configuration examples:

- [DHCP Authorized ARP: Example, page 5](#)
- [Verifying DHCP Authorized ARP: Example, page 6](#)

### DHCP Authorized ARP: Example

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, it will install a secure ARP entry in its ARP table. The **arp authorized** command stops any dynamic ARP on that interface. Router 1 will send 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 [Figure 1](#) for an example topology.

**Figure 1 Example 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 Ethernet0
 ip address 10.0.0.1 255.255.255.0
 half-duplex
 arp authorized
 arp timeout 60
```

**Router 2 (DHCP Client)**

```
interface Ethernet0/0
 ip address dhcp
 half-duplex
```

## Verifying DHCP Authorized ARP: Example

The following is the output for the **show arp** command on Router 1:

```
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 the output for the **show arp** command on Router 2:

```
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
```

# Additional References

The following sections provide references related to the DHCP Authorized ARP feature.

## Related Documents

Related Topic	Document Title
ARP commands DHCP commands	<i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> , Release 12.3 T
ARP configuration tasks DHCP configuration tasks	<i>Cisco IOS IP Configuration Guide</i>
Secured IP Address Assignment feature documentation	<a href="#">DHCP Secured IP Address Assignment</a> feature module, Release 12.2(15)T

## Standards

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

## 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 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: <a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a>

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

## Command Reference

This section documents a new command. All other commands used with this feature are documented in the Cisco IOS Release 12.3 T command reference publications.

- [arp authorized](#)

# arp authorized

To disable dynamic ARP learning on an interface, use the **arp authorized** command in interface configuration mode. To reenable dynamic ARP learning, use the **no** form of this command.

**arp authorized**

**no arp authorized**

**Syntax Description** This command has no arguments or keywords.

**Defaults** No default behavior or values

**Command Modes** Interface configuration

Command History	Release	Modification
	12.3(4)T	This command was introduced.

**Usage Guidelines** The **arp authorized** command disables dynamic ARP learning on an interface. This command enhances security in public wireless LANs (PWLANS) by limiting the leasing of IP addresses to mobile users to authorized users. The IP address to MAC address mapping for that interface can only be installed by the authorized subsystem. Unauthorized clients can not respond to ARP requests.

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.

You can only use this command on Ethernet interfaces.

**Examples** The following example disables dynamic ARP learning on interface Ethernet 0:

```
interface Ethernet0
 ip address 10.0.0.1 255.255.255.0
 arp authorized
```

Related Commands	Command	Description
	<b>arp (global)</b>	Adds a permanent entry in the ARP cache.
	<b>update arp</b>	Secures dynamic ARP entries in the ARP table to their corresponding DHCP bindings.

# Glossary

**ARP**—Address Resolution Protocol. ARP is used to map a Layer 3 IP address to a Layer 2 MAC address. A Cisco router stores this mapped information in an ARP table. The ARP table provides MAC rewrite information when the router is forwarding a packet using Cisco Express Forwarding (CEF) or other IP switching technologies.

**DHCP**—Dynamic Host Configuration Protocol. DHCP provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.

**hot spot**—A specific geographic location in which an access point provides public wireless broadband network services to mobile visitors through a WLAN. Examples of hot spots include airports, coffee shops, hotels, and conference centers. Hot spots typically have a short range of access.

**Note**

---

Refer to [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

---

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

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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.