



IP Addressing: ARP Configuration Guide, Cisco IOS Release 12.4

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.



CONTENTS

Configuring Address Resolution Protocol Options	1
Finding Feature Information	1
Information About Address Resolution Protocol Options	1
Layer 2 and Layer 3 Addressing	2
Address Resolution Protocol	3
ARP Caching	4
Static and Dynamic Entries in the ARP Cache	4
Devices That Do Not Use ARP	4
Inverse ARP	5
Reverse ARP	5
Proxy ARP	6
Serial Line Address Resolution Protocol	6
Authorized ARP	6
How to Configure Address Resolution Protocol Options	7
Enabling the Interface Encapsulation	7
Defining Static ARP Entries	8
Setting an Expiration Time for Dynamic Entries in the ARP Cache	10
Globally Disabling Proxy ARP	11
Disabling Proxy ARP on an Interface	11
Clearing the ARP Cache	12
Verifying the ARP Configuration	13
Configuration Examples for Address Resolution Protocol Options	15
Static ARP Entry Configuration Example	15
Encapsulation Type Configuration Example	15
Proxy ARP Configuration Example	16
Clearing the ARP Cache Example	16
Additional References	16
Feature Information for Configuring Address Resolution Protocol Options	17



Configuring Address Resolution Protocol Options

Address Resolution Protocol (ARP) performs a required function in IP routing. ARP finds the hardware address, also known as Media Access Control (MAC) address, of a host from its known IP address. ARP maintains a cache (table) in which MAC addresses are mapped to IP addresses. ARP is part of all Cisco IOS systems running IP.

This document explains ARP for IP routing and the optional ARP features you can configure, such as static ARP entries, time out for dynamic ARP entries, clearing the cache, and Proxy ARP.

- [Finding Feature Information, page 1](#)
- [Information About Address Resolution Protocol Options, page 1](#)
- [How to Configure Address Resolution Protocol Options, page 7](#)
- [Configuration Examples for Address Resolution Protocol Options, page 15](#)
- [Additional References, page 16](#)
- [Feature Information for Configuring Address Resolution Protocol Options, page 17](#)

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.

Information About Address Resolution Protocol Options

- [Layer 2 and Layer 3 Addressing, page 2](#)
- [Address Resolution Protocol, page 3](#)
- [ARP Caching, page 4](#)
- [Static and Dynamic Entries in the ARP Cache, page 4](#)
- [Devices That Do Not Use ARP, page 4](#)
- [Inverse ARP, page 5](#)
- [Reverse ARP, page 5](#)
- [Proxy ARP, page 6](#)

- [Serial Line Address Resolution Protocol, page 6](#)
- [Authorized ARP, page 6](#)

Layer 2 and Layer 3 Addressing

IP addressing occurs at Layer 2 (data link) and Layer 3 (network) of the Open System Interconnection (OSI) reference model. OSI is an architectural network model developed by ISO and ITU-T that consists of seven layers, each of which specifies particular network functions such as addressing, flow control, error control, encapsulation, and reliable message transfer.

Layer 2 addresses are used for local transmissions between devices that are directly connected. Layer 3 addresses are used for indirectly connected devices in an internetwork environment. Each network uses addressing to identify and group devices so that transmissions can be sent and received. Ethernet (802.2, 802.3, Ethernet II, and Subnetwork Access Protocol [SNAP]), Token Ring, and Fiber Distributed Data Interface (FDDI) use Media Access Control (MAC) addresses that are “burned in” to the Network Interface Card (NIC). The most commonly used network types are Ethernet II and SNAP.

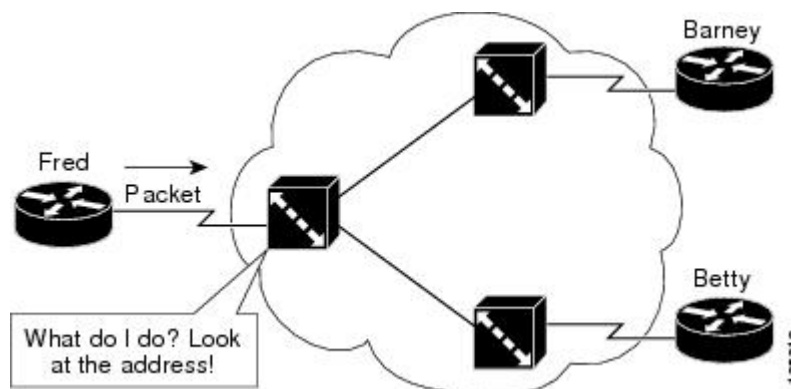
In order for devices to be able to communicate with each when they are not part of the same network, the 48-bit MAC address must be mapped to an IP address. Some of the Layer 3 protocols used to perform the mapping are:

- Address Resolution Protocol (ARP)
- Reverse ARP (RARP)
- Serial Line ARP (SLARP)
- Inverse ARP

For the purposes of IP mapping, Ethernet, Token Ring, and FDDI frames contain the destination and source addresses. Frame Relay and Asynchronous Transfer Mode (ATM) networks, which are packet switched, data packets take different routes to reach the same destination. At the receiving end, the packet is reassembled in the correct order.

In a Frame Relay network, there is one physical link that has many logical circuits called virtual circuits (VCs). The address field in the frame contains a data-link connection identifier (DLCI) which identifies each VC. For example, in the figure below, the Frame Relay switch to which router Fred is connected receives frames; the switch forwards the frames to either Barney or Betty based on the DLCI which identifies each VC. So Fred has one physical connection but multiple logical connections.

Figure 1 Frame Relay Network



ATM networks use point-to-point serial links with the High-Level Data Link Control (HDLC) protocol. HDLC includes a meaningless address field included in five bytes of the frame header frame with the recipient implied since there can only be one.

AppleTalk is designed for Apple computers and has a special addressing scheme that uses 24-bit addresses and its own method for resolving addresses. Once the data reaches the internetwork, address resolution beyond the device connecting it to the internetwork operates the same as IP address resolution. For more information about AppleTalk networks, refer to Core Competence AppleTalk (white paper) at www.corecom.com/html/appletalk.html.

Address Resolution Protocol

Address Resolution Protocol (ARP) was developed to enable communications on an internetwork and is defined by RFC 826. Routers and Layer 3 switches need ARP to map IP addresses to MAC hardware addresses so that IP packets can be sent across networks. Before a device sends a datagram to another device, it looks in its own ARP cache to see if there is a MAC address and corresponding IP address for the destination device. If there is no entry, the source device sends a broadcast message to every device on the network. Each device compares the IP address to its own. Only the device with the matching IP address replies to the sending device with a packet containing the MAC address for the device (except in the case of "Proxy ARP"). The source device adds the destination device MAC address to its ARP table for future reference, creates a data-link header and trailer that encapsulates the packet, and proceeds to transfer the data. The figure below illustrates the ARP broadcast and response process.

Figure 2 **ARP Process**



When the destination device lies on a remote network, one beyond another router, the process is the same except that the sending device sends an ARP request for the MAC address of the default gateway. After the address is resolved and the default gateway receives the packet, the default gateway broadcasts the destination IP address over the networks connected to it. The router on the destination device network uses ARP to obtain the MAC address of the destination device and delivers the packet.

Encapsulation of IP datagrams and ARP requests and replies on IEEE 802 networks other than Ethernet use Subnetwork Access Protocol (SNAP).

The ARP request message has the following fields:

- HLN--Hardware address length. Specifies how long the hardware addresses are in the message. For IEEE 802 MAC addresses (Ethernet) the value is 6.
- PLN--Protocol address length. Specifies how long the protocol (Layer 3) addresses are in the message. For IPv4, the value is 4.
- OP--Opcode. Specifies the nature of the message by code:
 - 1--ARP request.
 - 2--ARP reply.
 - 3 through 9--RARP and Inverse ARP requests and replies.
- SHA--Sender hardware address. Specifies the Layer 2 hardware address of the device sending the message.

- SPA--Sender protocol address. Specifies the IP address of the sending device.
- THA--Target hardware address. Specifies the Layer 2 hardware address of the receiving device.
- TPA--Target protocol address. Specifies the IP address of the receiving device.

ARP Caching

Because the mapping of IP addresses to MAC addresses occurs at each hop (router) on the network for every datagram sent over an internetwork, performance of the network could be compromised. To minimize broadcasts and limit wasteful use of network resources, ARP caching was implemented.

ARP caching is the method of storing network addresses and the associated data-link addresses in memory for a period of time as the addresses are learned. This minimizes the use of valuable network resources to broadcast for the same address each time a datagram is sent. The cache entries must be maintained because the information could become outdated, so it is critical that the cache entries are set to expire periodically. Every device on a network updates its tables as addresses are broadcast.

There are static ARP cache entries and dynamic ARP cache entries. Static entries are manually configured and kept in the cache table on a permanent basis. They are best for devices that have to communicate with other devices usually in the same network on a regular basis. Dynamic entries are added by the Cisco IOS software and kept for a period of time, then removed.

Static and Dynamic Entries in the ARP Cache

Static routing requires an administrator to manually enter IP addresses, subnet masks, gateways, and corresponding MAC addresses for each interface of each router into a table. Static routing enables more control but requires more work to maintain the table. The table must be updated each time routes are added or changed.

Dynamic routing uses protocols that enable the routers in a network to exchange routing table information with each other. The table is built and changed automatically. No administrative tasks are needed unless a time limit is added, so dynamic routing is more efficient than static routing. The default time limit is 4 hours. If the network has a great many routes that are added and deleted from the cache, the time limit should be adjusted.

The routing protocols that dynamic routing uses to learn routes, such as distance-vector and link-state, is beyond the scope of this document. For more information, refer to *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4.

Devices That Do Not Use ARP

When a network is divided into two segments, a bridge joins the segments and filters traffic to each segment based on MAC addresses. The bridge builds its own address table, which uses MAC addresses only, as opposed to a router, which has an ARP cache that contains both IP addresses and the corresponding MAC addresses.

Passive hubs are central-connection devices that physically connect other devices in a network. They send messages out all of their ports to the devices and operate at Layer 1, but do not maintain an address table.

Layer 2 switches determine which port is connected to a device to which the message is addressed and send only to that port, unlike a hub, which sends the message out all its ports. However, Layer 3 switches are routers that build an ARP cache (table).

For more information about bridges, refer to the *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.4. For more information about switches, refer to *Cisco IOS Switching Services Configuration Guide*, Release 12.4.

Inverse ARP

Inverse ARP, which is enabled by default in ATM networks, builds an ATM map entry and is necessary to send unicast packets to a server (or relay agent) on the other end of a connection. Inverse ARP is only supported for the **aal5snap** encapsulation type.

For multipoint interfaces, an IP address can be acquired using other encapsulation types because broadcast packets are used. However, unicast packets to the other end will fail because there is no ATM map entry and thus DHCP renewals and releases also fail.

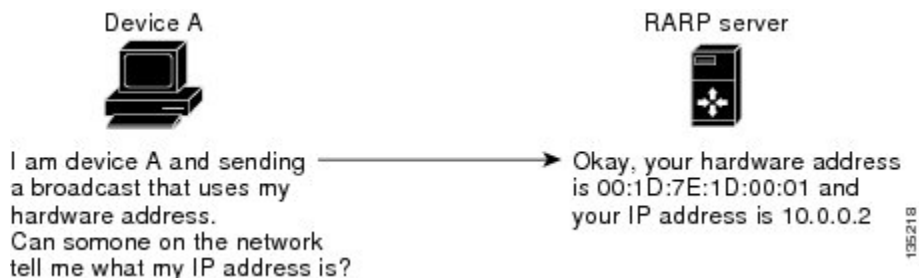
For more information about Inverse ARP and ATM networks, refer to the “Configuring ATM” chapter of the *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.4.

Reverse ARP

Reverse ARP (RARP) as defined by RFC 903 works the same way as ARP, except that the RARP request packet requests an IP address instead of a MAC address. RARP often is used by diskless workstations because this type of device has no way to store IP addresses to use when they boot. The only address that is known is the MAC address because it is burned into the hardware.

Use of RARP requires an RARP server on the same network segment as the router interface. The figure below illustrates how RARP works.

Figure 3 RARP Process



There are several limitations of RARP. Because of these limitations, most businesses use DHCP to assign IP addresses dynamically. DHCP is cost effective and requires less maintenance than RARP. The most important limitations are as follows:

- Since RARP uses hardware addresses, if the internetwork is large with many physical networks, a RARP server must be on every segment with an additional server for redundancy. Maintaining two servers for every segment is costly.
- Each server must be configured with a table of static mappings between the hardware addresses and IP addresses. Maintenance of the IP addresses is difficult.
- RARP only provides IP addresses of the hosts and not subnet masks or default gateways.

The Cisco IOS software attempts to use RARP if it does not know the IP address of an interface at startup to respond to RARP requests that they are able to answer. A feature of Cisco IOS software automates the configuration of Cisco devices and is called AutoInstall.

AutoInstall supports RARP and enables a network manager to connect a new router to a network, turn it on, and load a pre-existing configuration file automatically. The process begins when no valid configuration file is found in NVRAM. For more information about AutoInstall, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4.

Proxy ARP

Proxy ARP, as defined in RFC 1027, was implemented to enable devices that are separated into physical network segments connected by a router in the same IP network or subnetwork to resolve the IP-to-MAC addresses. When devices are not in the same data link layer network but in the same IP network, they try to transmit data to each other as if they are on the local network. However, the router that separates the devices will not send a broadcast message because routers do not pass hardware-layer broadcasts. The addresses cannot be resolved.

Proxy ARP is enabled by default so the “proxy router” that resides between the local networks will respond with its MAC address as if it is the router to which the broadcast is addressed. When the sending device receives the MAC address of the proxy router, it sends the datagram to the proxy router that in turns sends the datagram to the designated device.

Proxy ARP is invoked by the following conditions:

- The target IP address is not on the same physical network (LAN) on which the request is received.
- The networking device has one or more routes to the target IP address.
- All of the routes to the target IP address go through interfaces other than the one on which the request is received.

When proxy ARP is disabled, a device will respond to ARP requests received on its interface only if the target IP address is the same as its IP address, or the target IP address in the ARP request has a statically configured ARP alias.

Serial Line Address Resolution Protocol

Serial Line ARP (SLARP) is used for serial interfaces that use High-Level Data Link Control (HDLC) encapsulation. A SLARP server, intermediate (staging) router, and another router providing a SLARP service may be required in addition to a TFTP server. If an interface is not directly connected to a server, the staging router is required to forward the address resolution requests to the server, otherwise a directly connected router with SLARP service is required. The Cisco IOS software attempts to use SLARP if it does not know the IP address of an interface at startup to respond to SLARP requests that software is able to answer.

A feature of Cisco IOS software automates the configuration of Cisco devices and is called AutoInstall. AutoInstall supports SLARP and enables a network manager to connect a new router to a network, turn it on, and load a pre-existing configuration file automatically. The process begins when no valid configuration file is found in NVRAM. For more information about AutoInstall, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4.

**Note**

Serial interfaces that use Frame Relay encapsulation are supported by AutoInstall.

Authorized ARP

Authorized ARP addresses a requirement of explicitly knowing when a user has logged off, either voluntarily or due to a failure of a network device. It is implemented for Public wireless LANs (WLANs) and DHCP. For more information about authorized ARP, refer to the “Configuring DHCP Services for Accounting and Security” chapter of the *DHCP Configuration Guide*, Cisco IOS Release 12.4.

How to Configure Address Resolution Protocol Options

ARP is enabled by default and is set to use Ethernet encapsulation by default. Perform the following tasks to change or verify ARP functionality:

- [Enabling the Interface Encapsulation, page 7](#)
- [Defining Static ARP Entries, page 8](#)
- [Setting an Expiration Time for Dynamic Entries in the ARP Cache, page 10](#)
- [Globally Disabling Proxy ARP, page 11](#)
- [Disabling Proxy ARP on an Interface, page 11](#)
- [Clearing the ARP Cache, page 12](#)
- [Verifying the ARP Configuration, page 13](#)

Enabling the Interface Encapsulation

Perform this task to support a type of encapsulation for a specific network, such as Ethernet, Frame Relay, FDDI, or Token Ring. When Frame Relay encapsulation is specified, the interface is configured for a Frame Relay subnetwork in which there is one physical link that has many logical circuits called virtual circuits (VCs). The address field in the frame contains a data-link connection identifier (DLCI) which identifies each VC. When SNAP encapsulation is specified, the interface is configured for FDDI or Token Ring networks.



Note

The encapsulation type specified in this task should match the encapsulation type specified in the "Defining Static ARP Entries" task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **arp** {arpa | frame-relay | snap}
5. **exit**

DETAILED STEPS

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

Command or Action	Purpose
Step 2 <code>configure terminal</code> Example: <pre>Router# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>interface type number</code> Example: <pre>Router(config)# interface ethernet0/0</pre>	Enters interface configuration mode.
Step 4 <code>arp {arpa frame-relay snap}</code> Example: <pre>Router(config-if)# arp arpa</pre>	Specifies the encapsulation type for an interface by type of network, such as Ethernet, FDDI, Frame Relay, and Token Ring. The keywords are as follows: <ul style="list-style-type: none"> • arpa --Enables encapsulation for an Ethernet 802.3 network. • frame-relay --Enables encapsulation for a Frame Relay network. • snap --Enables encapsulation for FDDI and Token Ring networks.
Step 5 <code>exit</code> Example: <pre>Router(config-if)# exit</pre>	Exits interface configuration mode.

Defining Static ARP Entries

Perform this task to define static mapping between IP addresses (32-bit address) and a MAC address (48-bit address) for hosts that do not support dynamic ARP. Because most hosts support dynamic address resolution, defining static ARP cache entries is usually not required. Performing this task installs a permanent entry in the ARP cache that never times out. The entries remain in the ARP table until they are removed using the **no arp** command or the **clear arp interface** command for each interface.



Note

The encapsulation type specified in this task should match the encapsulation type specified in the "Enabling the Interface Encapsulation" task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **arp** { *ip-address* | **vrf** *vrf-name* } *hardware-address* *encap-type* [*interface-type*]
4. **exit**

DETAILED STEPS

Command or Action	Purpose
<p>Step 1 enable</p> <p>Example:</p> <pre>Router> enable</pre>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
<p>Step 2 configure terminal</p> <p>Example:</p> <pre>Router# configure terminal</pre>	<p>Enters global configuration mode.</p>
<p>Step 3 arp { <i>ip-address</i> vrf <i>vrf-name</i> } <i>hardware-address</i> <i>encap-type</i> [<i>interface-type</i>]</p> <p>Example:</p> <pre>Router(config)# arp 10.0.0.0 aabb.cc03.8200 arpa</pre>	<p>Globally associates an IP address with a MAC address in the ARP cache. The arguments and keyword are as follows:</p> <ul style="list-style-type: none"> <i>ip-address</i> --IP address in four-part dotted decimal format corresponding to the local data-link address. vrf <i>vrf-name</i> --Virtual routing and forwarding instance for a Virtual Private Network (VPN). The <i>vrf-name</i> argument can be any name. <i>hardware-address</i> --Local data-link address (a 48-bit address). <i>encap-type</i> --Encapsulation type for the static entry. The keywords are as follows: <ul style="list-style-type: none"> arpa--For Ethernet interfaces. sap--For Hewlett Packard interfaces. smds--For Switched Multimegabit Data Service (SMDS) interfaces. snap--For FDDI and Token Ring interfaces. srp-a--Switch route processor-side A (SRP-A) interfaces. srp-b--Switch route processor-side B (SRP-B) interfaces. <i>interface-type</i> --(Optional) Interface type. The keywords are as follows: <ul style="list-style-type: none"> ethernet--IEEE 802.3 interface. loopback--Loopback interface. null--No interface. serial--Serial interface alias--Device responds to ARP requests as if it were the interface of the specified address.
<p>Step 4 exit</p> <p>Example:</p> <pre>Router(config)# exit</pre>	<p>Exits to privileged EXEC mode.</p>

Setting an Expiration Time for Dynamic Entries in the ARP Cache

Perform this task to set a time limit for dynamic entries in the ARP cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **arp timeout** *seconds*
5. **exit**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 interface <i>type number</i> Example: Router(config)# interface ethernet0/0	Enters interface configuration mode.
Step 4 arp timeout <i>seconds</i> Example: Router(config-if)# arp timeout 30	Sets the length of time, in seconds, an ARP cache entry will stay in the cache. A value of zero means that entries are never cleared from the cache. The default is 14400 seconds (4 hours). Note If the network has frequent changes to cache entries, the default should be changed to a shorter time period.
Step 5 exit Example: Router(config-if)# exit	Exits interface configuration mode.

Globally Disabling Proxy ARP

Proxy ARP is enabled by default; perform this task to globally disable proxy ARP on all interfaces.

The Cisco IOS software uses proxy ARP (as defined in RFC 1027) to help hosts with no knowledge of routing determine the MAC addresses of hosts on other networks or subnets. For example, if hosts A and B are on different physical networks, host B will not receive the ARP broadcast request from host A and cannot respond to it. However, if the physical network of host A is connected by a gateway to the physical network of host B, the gateway will see the ARP request from host A.

Assuming that subnet numbers were assigned to correspond to physical networks, the gateway can also tell that the request is for a host that is on a different physical network. The gateway can then respond for host B, saying that the network address for host B is that of the gateway itself. Host A will see this reply, cache it, and send future IP packets for host B to the gateway.

The gateway will forward such packets to host B by using the configured IP routing protocols. The gateway is also referred to as a transparent subnet gateway or ARP subnet gateway.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip arp proxy disable**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 ip arp proxy disable Example: Router(config)# ip arp proxy disable	Disables proxy ARP on all interfaces. <ul style="list-style-type: none"> • The ip arp proxy disable command overrides any proxy ARP interface configuration. • To reenable proxy ARP, use the no ip arp proxy disable command. • You can also use the default ip proxy arp command to return to the default proxy ARP behavior, which is enabled.

Disabling Proxy ARP on an Interface

Proxy ARP is enabled by default; perform this task to disable proxy ARP on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip proxy-arp**
5. **exit**

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3 interface <i>type number</i> Example: Router(config)# interface ethernet0/0	Enters interface configuration mode.
Step 4 no ip proxy-arp Example: Router(config-if)# ip proxy-arp	Disables proxy ARP on the interface. <ul style="list-style-type: none"> • To reenable proxy ARP, use the ip proxy-arp command. • You can also use the default ip proxy-arp command to return to the default proxy ARP behavior on the interface, which is enabled.
Step 5 exit Example: Router(config-if)# exit	Exits to global configuration mode.

Clearing the ARP Cache

Perform the following tasks to clear the ARP cache of entries associated with an interface and to clear all dynamic entries from the ARP cache, the fast-switching cache, and the IP route cache.

SUMMARY STEPS

1. enable
2. clear arp interface *type number*
3. clear arp-cache
4. exit

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2 clear arp interface <i>type number</i> Example: Router# clear arp interface ethernet0/0	Clears the entire ARP cache on the interface. The <i>type</i> and <i>number</i> arguments are the type of interface and the assigned number for the interface.
Step 3 clear arp-cache Example: Router# clear arp-cache	Clears all dynamic entries from the ARP cache, the fast-switching cache, and the IP route cache.
Step 4 exit Example: Router# exit	Exits to EXEC mode.

Verifying the ARP Configuration

To verify the ARP configuration, perform the following steps.

SUMMARY STEPS

1. show interfaces
2. show arp
3. show ip arp
4. show processes cpu | include (ARP|PID)

DETAILED STEPS

Step 1 show interfaces

To display the type of ARP being used on a particular interface and also display the ARP timeout value, use the **show interfaces EXEC** command.

Example:

```
Router# show interfaces
Ethernet 0 is up, line protocol is up
Hardware is MCI Ethernet, address is 0000.0c00.750c (bia 0000.0c00.750c)
Internet address is 10.108.28.8, subnet mask is 255.255.255.0
MTU 1500 bytes, BW 10000 Kbit, DLY 100000 usec, rely 255/255, load 1/255
Encapsulation ARPA, loopback not set, keepalive set (10 sec)
ARP type: ARPA, ARP Timeout 4:00:00
Last input 0:00:00, output 0:00:00, output hang never
Last clearing of "show interface" counters 0:00:00
Output queue 0/40, 0 drops; input queue 0/75, 0 drops
Five minute input rate 0 bits/sec, 0 packets/sec
Five minute output rate 2000 bits/sec, 4 packets/sec
1127576 packets input, 447251251 bytes, 0 no buffer
Received 354125 broadcasts, 0 runts, 0 giants, 57186* throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
5332142 packets output, 496316039 bytes, 0 underruns
0 output errors, 432 collisions, 0 interface resets, 0 restarts
```

Step 2 show arp

Use the **show arp EXEC** command to examine the contents of the ARP cache.

Example:

```
Router# show arp
Protocol    Address          Age (min)    Hardware Addr    Type    Interface
Internet   10.108.42.112    120         0000.a710.4baf   ARPA    Ethernet3
AppleTalk   4028.5           29          0000.0c01.0e56   SNAP    Ethernet2
Internet   110.108.42.114   105         0000.a710.859b   ARPA    Ethernet3
AppleTalk   4028.9           -           0000.0c02.a03c   SNAP    Ethernet2
Internet   10.108.42.121    42          0000.a710.68cd   ARPA    Ethernet3
Internet   10.108.36.9      -           0000.3080.6fd4   SNAP    TokenRing0
AppleTalk   4036.9           -           0000.3080.6fd4   SNAP    TokenRing0
Internet   10.108.33.9      -           0000.0c01.7bbd   SNAP    Fddi0
```

Step 3 show ip arp

Use the **show ip arp EXEC** command to show IP entries. To remove all nonstatic entries from the ARP cache, use the **clear arp-cacheprivileged EXEC** command.

Example:

```
Router# show ip arp
Protocol    Address          Age(min)     Hardware Addr    Type    Interface
Internet   171.69.233.22    9           0000.0c59.f892   ARPA    Ethernet0/0
Internet   171.69.233.21    8           0000.0c07.ac00   ARPA    Ethernet0/0
Internet   171.69.233.19    -           0000.0c63.1300   ARPA    Ethernet0/0
Internet   171.69.233.30    9           0000.0c36.6965   ARPA    Ethernet0/0
Internet   172.19.168.11    -           0000.0c63.1300   ARPA    Ethernet0/0
Internet   172.19.168.254  9           0000.0c36.6965   ARPA    Ethernet0/0
```

Step 4 show processes cpu | include (ARP|PID)

Use the **show processes cpu | include (ARP|PID)** command to display ARP and RARP processes.

Example:

```

Router# show processes cpu | include (ARP|PID)
PID      Runtime(ms)  Invoked  uSecs   5Sec   1Min   5Min   TTY Process
1         1736         58      29931   0%     0%     0%     Check heaps
2          68         585      116    1.00%  1.00%  0%     IP Input
3          0           744       0      0%     0%     0%     TCP Timer
4          0            2         0      0%     0%     0%     TCP Protocols
5          0            1         0      0%     0%     0%     BOOTP Server
6         16          130      123    0%     0%     0%     ARP Input
7          0            1         0      0%     0%     0%     Probe Input
8          0            7         0      0%     0%     0%     MOP Protocols
9          0            2         0      0%     0%     0%     Timers
10        692          64     10812   0%     0%     0%     Net Background
11         0            5         0      0%     0%     0%     Logger
12         0           38         0      0%     0%     0%     BGP Open
13         0            1         0      0%     0%     0%     Net Input
14        540        3466     155    0%     0%     0%     TTY Background
15         0            1         0      0%     0%     0%     BGP I/O
16       5100        1367    3730   0%     0%     0%     IGRP Router
17         88          4232     20    0.20%  1.00%  0%     BGP Router
18        152        14650     10    0%     0%     0%     BGP Scanner
19        224         99      2262   0%     0%    1.00%  Exec

```

Configuration Examples for Address Resolution Protocol Options

- [Static ARP Entry Configuration Example, page 15](#)
- [Encapsulation Type Configuration Example, page 15](#)
- [Proxy ARP Configuration Example, page 16](#)
- [Clearing the ARP Cache Example, page 16](#)

Static ARP Entry Configuration Example

The following example shows how to configure a static ARP entry in the cache and by using the **alias** keyword, Cisco IOS software can respond to ARP requests as if it were the interface of the specified address:

```

arp 10.0.0.0 aabb.cc03.8200 alias
interface ethernet0/0

```

Encapsulation Type Configuration Example

The following example shows how to configure the encapsulation on the interface. The **snap** keyword indicates that interface Ethernet0/0 is connected to an FDDI or Token Ring network:

```

interface ethernet0/0
ip address 10.108.10.1 255.255.255.0
arp snap

```

Proxy ARP Configuration Example

The following example shows how to configure proxy ARP because it was disabled for interface Ethernet0/0:

```
interface ethernet0/0
 ip proxy-arp
```

Clearing the ARP Cache Example

The following example shows how to clear all of the entries in the ARP cache associated with an interface:

```
Router# clear arp interface ethernet0/0
```

The following example shows how to clear all of the dynamic entries in the ARP cache:

```
Router# clear arp-cache
```

Additional References

Related Documents

Related Topic	Document Title
ARP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	<i>Cisco IOS IP Addressing Services Command Reference</i>
Monitoring and maintaining ARP tasks	“Monitoring and Maintaining ARP Information” module

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

RFCs

RFCs	Title
RFC 826	<i>Address Resolution Protocol</i>
RFC 903	<i>Reverse Address Resolution Protocol</i>
RFC 1027	<i>Proxy Address Resolution Protocol</i>
RFC 1042	<i>Standard for the Transmission of IP Datagrams over IEEE 802 Networks</i>

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of 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.	http://www.cisco.com/techsupport

Feature Information for Configuring Address Resolution Protocol Options

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 1 **Feature Information for Configuring Address Resolution Protocol Options**

Feature Name	Software Releases	Feature Information
ARP Optimization	12.2(15)T 15.0(1)S	<p>In previous versions of Cisco IOS software, the ARP table was organized for easy searching on an entry based on the IP address. However, there are cases such as interface flapping on the router and a topology change in the network where all related ARP entries need to be refreshed for correct forwarding. This situation could consume a substantial amount of CPU time in the ARP process to search and clean up all the entries. The ARP Optimization feature improves ARP performance by reducing the ARP searching time by using an improved data structure.</p> <p>The following command was introduced by this feature:clear arp interface.</p>

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.