

Address Resolution Protocol

The Address Resolution Protocol (ARP) feature 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 systems that run IP.

This feature module explains ARP for IP routing and the optional ARP features you can configure, such as static ARP entries, timeout for dynamic ARP entries, clearing the cache, and proxy ARP.

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

- Information About the Address Resolution Protocol, on page 1
- How to Configure the Address Resolution Protocol, on page 7
- Configuration Examples for the Address Resolution Protocol, on page 16
- Additional References, on page 17
- Feature Information for the Address Resolution Protocol, on page 18

Information About the Address Resolution Protocol

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.

Note For the supported interface types, see the data sheet for your hardware platform.

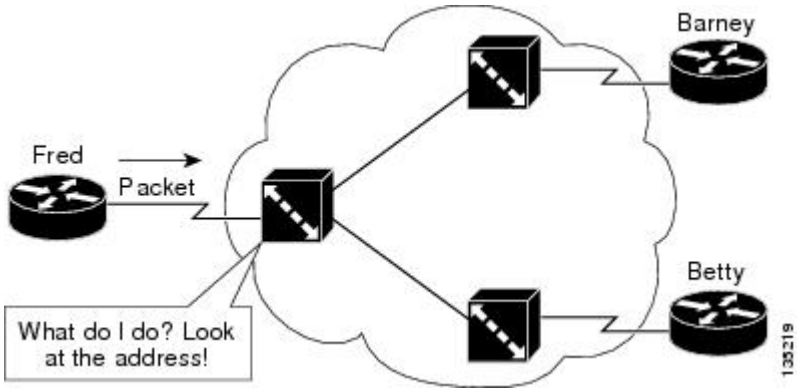
In order for devices to be able to communicate with each when they are not part of the same network, the 48-bit MAC address must be mapped to an IP address. Some of the Layer 3 protocols used to perform the mapping are:

- 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 device Fred is connected receives frames; the switch forwards the frames to either Barney or Betty based on the DLCI that 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 be only one.

Overview of the Address Resolution Protocol

The Address Resolution Protocol (ARP) was developed to enable communications on an internetwork and is defined by RFC 826. Layer 3 devices need ARP to map IP network 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 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 Layer 3 device, 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 Layer 3 device 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 media access control (MAC) addresses occurs at each hop (Layer 3 device) 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, Address Resolution Protocol (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. Static entries 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 Cisco software, kept for a period of time, and 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 media access control (MAC) addresses for each interface of each device 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 devices 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.



Note The Cisco IOS XE does not install the ARPs and forward entries instantaneously. So, there will be some delay in the installation process based on the system performance.



Note In IOS XE 17.4.x and later, to protect control-plane memory from excessive ARP traffic, the maximum number of ARP entries is limited according to the router's DRAM capacity:

- Devices with ≤ 8 GB DRAM: maximum of 15000 ARP entries
- Devices with > 8 GB DRAM: maximum of 25000 ARP entries

This protection mechanism applies across all affected platforms, including Cisco 1000 Series Integrated Services Routers,Cisco 4000 Series Integrated Services Routers and Cisco Catalyst 8000 Edge Platforms.

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 Media Access Control (MAC) addresses. The bridge builds its own address table, which uses MAC addresses only, as opposed to a router, which has an Address Resolution Protocol (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 ports to the devices and operate at Layer 1, but they 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 the message 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).

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 supported only 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.

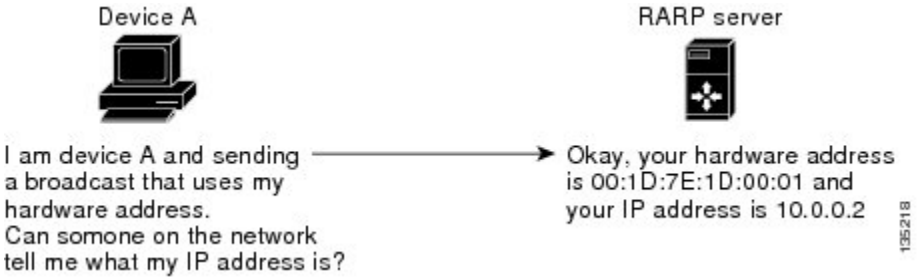
For more information about Inverse ARP and ATM networks, see the "Configuring ATM" feature module in the *Asynchronous Transfer Mode Configuration Guide*.

Reverse ARP

Reverse ARP (RARP) as defined by RFC 903 works the same way as the Address Resolution Protocol (ARP), except that the RARP request packet requests an IP address instead of a media access control (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 in to the hardware.

RARP requires a RARP server on the same network segment as the device interface. The figure below illustrates how RARP works.

Figure 3: RARP Process



Because of the limitations with RARP, most businesses use Dynamic Host Configuration Protocol (DHCP) to assign IP addresses dynamically. DHCP is cost-effective and requires less maintenance than RARP. The most important limitations with RARP are as follows:

- Because 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 the IP addresses. Maintenance of the IP addresses is difficult.
- RARP only provides IP addresses of the hosts but not subnet masks or default gateways.

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

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

Proxy ARP

Proxy Address Resolution Protocol, 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 IP-to-MAC addresses. When devices are not in the same data link layer network but are in the same IP network, they try to transmit data to each other as if they were 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. Therefore, the addresses cannot be resolved.

Proxy ARP is enabled by default so the “proxy router” that resides between the local networks responds with its MAC address as if it were 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, which 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 responds to ARP requests received on its interface only if the target IP address is the same as its IP address or if the target IP address in the ARP request has a statically configured ARP alias.



Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

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) device, and another device providing a SLARP service might be required in addition to a TFTP server. If an interface is not directly connected to a server, the staging device is required to forward the address-resolution requests to the server. Otherwise, a directly connected device with SLARP service is required. Cisco 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.

Cisco software automates the configuration of Cisco devices with the AutoInstall feature. AutoInstall supports SLARP and enables a network manager to connect a new device to a network, turn it on, and automatically

load a pre-existing configuration file. The process begins when no valid configuration file is found in NVRAM. For more information about AutoInstall, see the *Configuration Fundamentals Configuration Guide*.



Note AutoInstall supports serial interfaces that use Frame Relay encapsulation.

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.

Security (ARP/NDP cache entries) Enhancements

The Security (ARP/NDP cache entries) Enhancements feature implements ARP global limit and ARP interface limit. You can set a limit on the dynamic ARP entries per interface. Using the Security (ARP/NDP cache entries) Enhancements feature you can set a limit at either global level or interface level. Interface level configuration overrides the value of global limit when set. When the interface limit is not set, the global limit value is applied if the global limit is configured. When you disable interface-limit on an interface, you must execute the **no arp entries interface-limit** command to enable the interface-limit.

How to Configure the Address Resolution Protocol

By default, the Address Resolution Protocol (ARP) feature is enabled and is set to use Ethernet encapsulation. Perform the following tasks to change or verify ARP functionality:

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 with 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) that 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. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet0/0/0`	Enters interface configuration mode.
Step 4	**arp** {**arpa** | **frame-relay** | **snap**} **Example:** `Device(config-if)# arp arpa`	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: • **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	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Defining Static ARP Entries

Perform this task to define static mapping between an IP address (32-bit address) and a Media Access Control (MAC) address (48-bit address) for hosts that do not support dynamic Address Resolution Protocol (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. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**arp** {*ip-address* | **vrf** *vrf-name*} *hardware-address encap-type* [*interface-type*]
	Example:
	`Device(config)# arp 10.0.0.0 aabb.cc03.8200 arpa`
		Globally associates an IP address with a MAC address in the ARP cache.
		• *ip-address*—IP address in four-part dotted decimal format corresponding to the local data-link address.
		• **vrf** *vrf-name*—Virtual routing and forwarding instance for a Virtual Private Network (VPN). The *vrf-name* argument is the name of the VRF table.
		• *hardware-address*—Local data-link address (a 48-bit address).
		• *encap-type*—Encapsulation type for the static entry. The keywords are as follows:
		  • **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.

	Command or Action	Purpose
		• **srp-b**—Switch route processor side B (SRP-B) interfaces.  **Note** Some keywords might not apply to your ha • *interface-type*—(Optional) Interface type (for more information, use the question mark (?) online help).
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Setting an Expiration Time for Dynamic Entries in the ARP Cache

SUMMARY STEPS

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

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet0/0/0`	Enters interface configuration mode.

	Command or Action	Purpose
Step 4	**arp timeout** *seconds* **Example:** `Device(config-if)# arp timeout 30`	Sets the duration of time, in seconds, an Address Resolution Protocol (ARP) cache entry stays in the cache. The default is 14400 seconds (4 hours). The general recommended value for ARP timeout is the configured default value, which is 4 hours. If the network has frequent changes to cache entries, change the default to a shorter time period. As you reduce the ARP timeout, your network traffic increases. A low ARP timeout value might lead to network outage, and a value less than an hour (or 3600 seconds) will generate significantly increased traffic across the network. **Caution** We recommend that you set an ARP tim
Step 5	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Globally Disabling Proxy ARP

Proxy Address Resolution Protocol (ARP) is enabled by default; perform this task to globally disable proxy ARP on all interfaces.

The Cisco software uses proxy ARP (as defined in RFC 1027) to help hosts with no knowledge of routing determine the media access control (MAC) addresses of hosts on other networks or subnets. For example, if hosts A and B are on different physical networks, host B does 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 sees 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 sees this reply, caches it, and sends future IP packets for host B to the gateway.

The gateway forwards 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**
4. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**ip arp proxy disable** **Example:** `Device(config)# ip arp proxy disable`	Disables proxy ARP on all interfaces. • 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.
Step 4	**end** **Example:** `Device(config)# end`	Returns to privileged EXEC mode.

Disabling Proxy ARP on an Interface

Proxy Address Resolution Protocol (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. **end**

DETAILED STEPS

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet0/0/0`	Enters interface configuration mode.
Step 4	**no ip proxy-arp** **Example:** `Device(config-if)# no ip proxy-arp`	Disables proxy ARP on the interface. • 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	**end** **Example:** `Device(config-if)# end`	Returns to privileged EXEC mode.

Clearing the ARP Cache

Perform the following tasks to clear the Address Resolution Protocol (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

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear arp interface** *type number* **Example:** `Device# clear arp interface Gigabitethernet0/0/0`	Clears the entire ARP cache on the interface.
Step 3	**clear arp-cache** **Example:** `Device# clear arp-cache`	Clears all dynamic entries from the ARP cache, the fast-switching cache, and the IP route cache.
Step 4	**exit** **Example:** `Device# exit`	Returns to user EXEC mode.

Configuring Security (ARP/NDP cache entries) Enhancements

To configure ARP entry limit globally:

```
enable
configure terminal
 arp entries interface-limit 1 log 1
 end
```

To configure ARP entry limit on an interface:

```
enable
configure terminal
 interface Ethernet 0/0
    ip address 1.1.1.40 255.255.255.0
    arp entries interface-limit 1 log 1
    end
```

To disable ARP entry limit:

```
enable
configure terminal
 interface Ethernet 0/1
    ip address 2.1.1.1 255.255.255.0
    arp entries interface-limit disable
    end
```

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

Procedure

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-cache**privileged 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 the Address Resolution Protocol

Example: Static ARP Entry Configuration

The following example shows how to configure a static Address Resolution Protocol (ARP) entry in the cache by using the **alias** keyword, allowing the software to respond to ARP requests as if it were the interface of the specified address:

```
arp 10.0.0.0 aabb.cc03.8200 alias
interface gigabitethernet0/0/0
```

Example: Encapsulation Type Configuration

The following example shows how to configure the encapsulation on the interface. The **arpa** keyword indicates that interface is connected to an Ethernet 802.3 network:

```
interface gigabitethernet0/0/0
 ip address 10.108.10.1 255.255.255.0
 arp arpa
```

Example: Proxy ARP Configuration

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

```
interface gigabitethernet0/0/0
 ip proxy-arp
```

Examples: Clearing the ARP Cache

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

```
Device# clear arp interface gigabitethernet0/0/0
```

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

```
Device# clear arp-cache
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
ARP commands	Cisco IOS IP Addressing Services Command Reference
AppleTalk addressing scheme	Core Competence AppleTalk (white paper) at www.corecom.com/html/appletalk.html
Authorized ARP	"Configuring DHCP Services for Accounting and Security" feature module in the *IP Addressing: DHCP Configuration Guide* (part of the *IP Addressing Configuration Guide Library*)
Inverse ARP and ATM networks	"Configuring ATM" feature module in the *Asynchronous Transfer Mode Configuration Guide*
AutoInstall	*Configuration Fundamentals Configuration Guide*

RFCs

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

Technical Assistance

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

Feature Information for the Address Resolution Protocol

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 the Address Resolution Protocol

Feature Name	Software Releases	Feature Information
Address Resolution Protocol		The Address Resolution Protocol (ARP) feature 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 systems that run IP.
Security (ARP/NDP cache entries) Enhancements	Cisco IOS XE Everest 16.4.1	The Security (ARP/NDP cache entries) Enhancements feature implements ARP global limit and ARP interface limit. You can set a limit on the dynamic ARP entries per interface. The following command was introduced: **arp entries interface-limit**