IP Addressing: ARP Configuration Guide, Cisco IOS Release 12.2SR

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

CONTENTS

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

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

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.

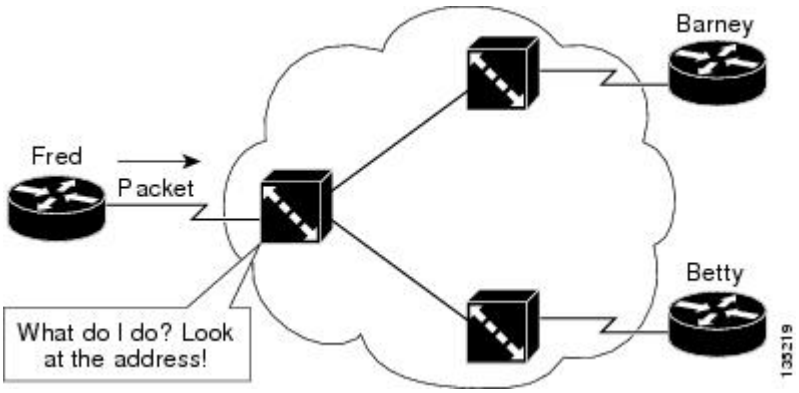
In order for devices to be able to communicate with each when they are not part of the same network, the 48-bit MAC address must be mapped to an IP address. Some of the Layer 3 protocols used to perform the mapping are:

- 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 a 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.

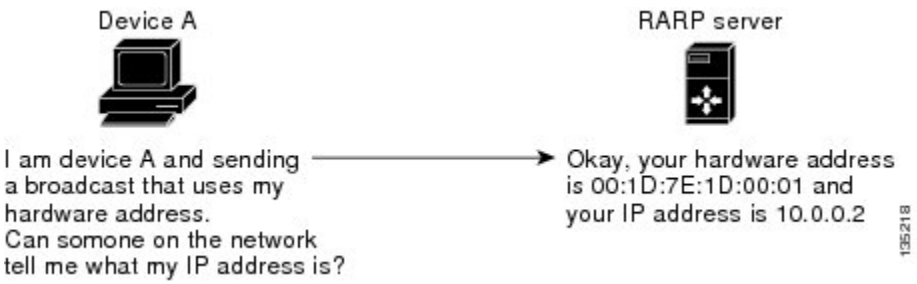
For more information about Inverse ARP and ATM networks, refer to the "Configuring ATM" chapter of the *Cisco IOS Wide-Area Networking Configuration Guide* , Release 12.4.

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

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. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet0/0`	Enters interface configuration mode.
Step 4	**arp** {**arpa** | **frame-relay** | **snap**} **Example:** `Router(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	**exit** **Example:** `Router(config-if)# exit`	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
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**arp** {*ip-address*| **vrf** *vrf-name*} *hardware-address encap-type* [*interface-type*] **Example:** `Router(config)# arp 10.0.0.0 aabb.cc03.8200 arpa`	Globally associates an IP address with a MAC address in the ARP cache. The arguments and keyword are as follows: • *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 can be any name. • *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. ◦ **srp-b**--Switch route processor-side B (SRP-B) interfaces. • *interface-type* --(Optional) Interface type. The keywords are as follows: ◦ **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.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits to privileged EXEC mode.

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet0/0`	Enters interface configuration mode.
Step 4	**arp timeout** *seconds* **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. • 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. • 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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **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. • 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. • Enter your password if prompted.
Step 2	**clear arp interface** *type number* **Example:** `Router# clear arp interface ethernet0/0`	Clears the entire ARP cache on the interface. The *type* and *number* 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-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 Address Resolution Protocol Options

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	*Cisco IOS IP Addressing Services Command Reference*
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	*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 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	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. The following command was introduced by this feature:**clear arp interface**.

Monitoring and Maintaining ARP Information

The Monitoring and Maintaining ARP Information feature document describes the practices involved in monitoring and maintaining arp information.

Address Resolution Protocol (ARP) is an Internet protocol used to map an IP address to a MAC address. ARP finds the MAC address, also known as the hardware address, of an IP-routed host from its known IP address and maintains this mapping information in a table. The router uses this IP address and MAC address mapping information to send IP packets to the next-hop router in the network.

ARP information monitoring and maintenance capabilities improves the management tools for ARP support in a Cisco IOS environment:

- To better support ARP analysis activities, the ARP administrative facilities provide detailed information about and granular control over ARP information. This information can be used to investigate issues with ARP packet traffic, ARP high availability (HA), or ARP synchronization with Cisco Express Forwarding adjacency.
- The ARP debug trace facility enables ARP packet debug trace for individual types of ARP events. The ARP debugging provides filtering of ARP entries for a specified interface, for hosts that match an access list, or for both.
- For increased security against ARP attacks, trap-based enabling of ARP system message logging can be configured per interface to alert network administrators of possible anomalies.
- To prevent the possibility of system instability due to memory exhaustion, the number of ARP entries that can be learned by the system can be limited. This feature is supported only on the Cisco 7600 platform, starting from Cisco IOS Release 12.2(33)SRD3.

No configuration tasks are associated with these additional ARP information monitoring and maintenance capabilities. The ARP-related enhancements introduced by this functionality are expanded forms of existing ARP management tasks.

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.

Restrictions for Monitoring and Maintaining ARP Information

For Cisco IOS Release 12.4(11)T, the restrictions described in the following sections apply to the ARP information monitoring and maintenance capabilities:

- ARP High Availability, page 20
- ARP Security Against ARP Attacks, page 20

ARP High Availability

The ARP subsystem supports ARP HA on Cisco networking devices that support dual Route Processors (RPs) for redundant processing capability. However, ARP HA is limited to the synchronization of dynamically learned ARP entries from the active RP to the standby RP. Statically configured ARP entries are not synchronized to the standby RP.

ARP Security Against ARP Attacks

The ARP subsystem supports a method for detecting a possible ARP attack by monitoring the number of ARP table entries for specific interfaces. However, no router-level security feature can prevent Man-in-the-Middle (MiM) types of ARP-spoofing attacks, which are a form of wiretapping attack where the attacker intercepts and selectively modifies communicated data to masquerade as one or more of the entities involved in a communication association. There are no ARP features to be implemented to resolve this security issue. Protecting the router from ARP attacks is best handled in switches through the ARP Access Control List (ACL) filters rather than at the router level.

Information About Monitoring and Maintaining ARP Information

- Overview of Monitoring and Maintaining ARP Information, page 20
- Address Resolution Protocol, page 23
- ARP Table, page 23
- ARP Table Entry Modes, page 24
- ARP Table Entry Subblocks, page 25
- ARP Table Entry Synchronization with Cisco Express Forwarding Adjacency, page 25
- ARP Table Size Monitoring per Interface, page 26
- ARP High Availability, page 26

Overview of Monitoring and Maintaining ARP Information

ARP information monitoring and maintenance capabilities improves the management tools for ARP support in a Cisco IOS environment. For information about the entire ARP feature, see the Additional

References, page 39. The following sections summarize the ARP subsystem enhancements introduced in Cisco IOS Release 12.4(11)T:

ARP Information Display Enhancements

The ARP information display capabilities have been expanded to support display of selected ARP entries, ARP entry details, and other ARP information.

Display of Selected ARP Entries

ARP table entries can be selected for display based on the following criteria:

- Virtual Private Network (VPN) routing and forwarding (VRF) instance
- ARP mode type
- Host or network
- Router interface

In Cisco IOS software versions prior to Release 12.4(11)T, the **show arp** command displays the entire ARP table.

Display of ARP Entry Details

The following detailed ARP information can be displayed:

- Adjacency notification--This information can be used to investigate issues with ARP packet traffic, ARP HA, or ARP notification for Cisco Express Forwarding adjacency. If the ARP subsystem needs to synchronize an ARP entry with Cisco Express Forwarding adjacency, that information is included when the affected entry is displayed.
- Associated interface for floating static ARP entries--If the ARP subsystem succeeds in finding the associated interface for a floating static ARP entry, that information can be included when the affected entry is displayed.
- Application subblocks--If an application-specific ARP entry is displayed, information about the subblock data can be included in the display.

The **show ip arp** command, introduced in Cisco IOS Release 9.0, allows you to display only certain ARP table entries based on specified criteria (IP address, interface, or hardware address). However, that command does not display the ARP entry modes, Cisco Express Forwarding adjacency notification information, or the associated interface for floating static ARP entries.

Display of Other ARP Information

The following ARP information--other than the contents of the ARP table entries--can be displayed:

- ARP table summary statistics--The numbers of entries in the table of each mode type and per interface.

- ARP HA status and statistics--Different types of switchover statistics are displayed based on the current state and recent activities of the RP.

ARP Information Refresh Enhancements

In Cisco IOS software versions prior to Release 12.4(11)T, the **clear arp** command refreshes all nonstatic entries in the ARP table. The ARP information refresh facility enables you to manage selected ARP information:

- Refresh all nonstatic ARP table entries
- Refresh nonstatic ARP table entries associated with a particular interface
- Refresh nonstatic ARP table entries for a particular IP address in a particular VRF
- Reset ARP HA statistics

ARP Debug Trace Enhancements

In Cisco IOS software versions prior to Release 12.4(11)T, the **debug arp** command supports debugging information for ARP packet traffic only. The ARP debug trace facility now provides more detailed selection and filter options for ARP debug trace.

- Debug Trace for Selected ARP Events, page 22
- Support for Filtering Debug Trace by Interface or Access List, page 22

Debug Trace for Selected ARP Events

The ARP debugging information can be enabled for the following types of ARP events:

- ARP table entry events
- ARP table events
- ARP interface interactions
- ARP HA events

Support for Filtering Debug Trace by Interface or Access List

The **debug arp** command supports debug trace filtering as defined by the **debug list** command. This enhancement enables ARP debugging information to be focused on desired debugging information based on a specific router interface, an access list of IP addresses, or both.

ARP Security Enhancement

When trap-based enabling of ARP system message logging (syslog) output is configured, the router monitors the number of dynamically learned ARP table entries for each interface and triggers ARP logging whenever the number of learned ARP entries for a particular interface exceeds the preconfigured value.

Such syslog traps can in turn alert network administrators (via protocols such as Simple Network Management Protocol (SNMP)) with the identity of the affected interface and the number of learned ARP entries over that interface. The administrator can then investigate why the ARP table has grown to the configured thresholds, and take the necessary action to resolve possible security breaching. Alternatively, the router can take self-defense actions automatically, with the action depending on the severity, from more frequent refreshing to shutting down the interface port.

Note This router-level security feature can help detect a MiM ARP-spoofing attack, but it cannot prevent such an attack. There are no ARP features to be implemented to resolve this security issue. Protecting the router from ARP attacks is best handled in switches through the ARP-ACL filters rather than at the router level.

Address Resolution Protocol

ARP was developed to enable communications on an internetwork, as 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. The following sections provide background information about ARP:

- ARP Broadcast and Response Process, page 23
- ARP Caching, page 23

ARP Broadcast and Response Process

Before a device sends a datagram to another device, it looks in its own ARP information 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. 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.

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.

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.

ARP Table

The ARP table provides a database in which a Cisco router caches learned and configured route-mapping information. Each entry in the ARP table is associated with either a local IP address (which represents a device owned by the router) or a remote host IP address (which represents an external device). The contents of the entry define the following ARP-intrinsic information:

- The association of the 32-bit IP address and 48-bit MAC address of that port

- Other information needed to support ARP in a Cisco IOS environment (such as link type, VRF table ID, and encapsulation type)

When the router forwards a packet using an IP switching technology such as Cisco Express Forwarding, the ARP table entries supply MAC rewrite information.

ARP Table Entry Modes

Each entry in the ARP table is designated with a mode type. The ARP subsystem supports the basic ARP table entry modes and also introduces new, application-specific modes.

- Basic ARP Table Entry Modes, page 24
- Application-Specific ARP Table Entry Modes, page 24

Basic ARP Table Entry Modes

The ARP subsystem uses the following basic ARP table entry modes to organize the ARP entries for ARP-internal processing:

- Alias--This mode is assigned to an entry that has been explicitly configured by an administrator with a local IP address, subnet mask, gateway, and corresponding MAC address. Static ARP entries are kept in the cache table on a permanent basis. They are best for local addresses that need to communicate with other devices in the same network on a regular basis.
- Dynamic--This mode is assigned to a dynamically learned entry that was initiated by an ARP request and is associated with an external host. Dynamic ARP entries are automatically added by the Cisco IOS software and maintained for a period of time, then removed. No administrative tasks are needed unless a time limit is added. The default time limit is four hours. If the network has a large number routes that are added and deleted from the cache, the time limit should be adjusted. A dynamic ARP entry is considered “complete” in that the entry contains the MAC address of the external host, as supplied by an ARP reply.
- Incomplete--This mode is a transient mode for a dynamic ARP entry. This mode indicates an entry that was initiated by an ARP request and is associated with an external host but does not contain a MAC address.
- Interface--This mode is assigned to an entry for a local IP address that has been derived from an interface.
- Static--This mode is assigned to an entry that has been explicitly configured by an administrator with an external IP address, subnet mask, gateway, and corresponding MAC address. Static ARP entries are kept in the cache table on a permanent basis. They are best for external devices that need to communicate with other devices in the same network on a regular basis. A static ARP entry is said to be “floating” if it is not associated with any interface when it is configured.

To maintain the validity of dynamically learned routes, the ARP subsystem refreshes dynamic ARP entries periodically (as configured or every four hours by default) so that the ARP table reflects any changed, aged-out, or removed dynamic routes.

To maintain the validity of statically configured routes, the ARP subsystem updates static ARP entries and alias ARP entries once per minute so that the ARP table reflects any changed or removed statically configured routes.

Application-Specific ARP Table Entry Modes

The ARP subsystem uses the application-specific ARP table entry modes to support applications that need to add ARP table entries for their solutions. ARP applications can register with the ARP subsystem to

obtain an application type handle. With this handle, the applications can insert ARP entries with the appropriate application-specific entry mode:

- Simple Application--This mode is assigned to an application-created entry that represents an external device.
- Application Alias--This mode is assigned to an application-created entry that is associated with a local address.
- Application Timer--This mode is assigned to an application-created entry that is associated with an external device. The ARP subsystem provides timer-based services to applications that create entries of this mode.

Application-specific entries do not expire, but instead are maintained by the application.

ARP Table Entry Subblocks

The ARP entry subblock structure provides the means to attach non-ARP intrinsic data to selected ARP entries. When an ARP entry inserted into the ARP table requires special, ARP-internal handling, the information needed by the process that performs the special handling is defined in a subblock that is attached to the ARP entry.

The ARP subsystem attaches subblocks to the following types of ARP entries, as needed:

- Alias, dynamic, and static ARP entries--A subblock is attached to all entries of these types in order to specify information needed by the ARP timer process that coordinates the periodic refresh operation that ensures the validity of the associations between IP addresses and MAC address defined by these entries.
- Interface ARP entries--A subblock is attached to all interface ARP entries in order to store information about the interface.
- Simple Application, Application Alias, and Application Timer entries--An application that creates an ARP entry can include any application-specific data necessary for its work, such as timer structures for timer services or data structure pointers for grouping related subblocks.

ARP Table Entry Synchronization with Cisco Express Forwarding Adjacency

If Cisco Express Forwarding is enabled on the router, the router maintains forwarding information (outbound interface and MAC header rewrite) for adjacent nodes. A node is said to be adjacent to another node if the node can be reached with a single hop across a link layer (Layer 2). Cisco Express Forwarding stores the forwarding information in an adjacency database so that Layer 2 addressing information can be inserted into link-layer headers attached to the ARP packets.

The ARP table information is one of the sources for Cisco Express Forwarding adjacency. Whenever the ARP subsystem attaches an ARP table entry to an outbound interface with a valid hardware address, the subsystem issues an internal “ARP adjacency” notification. The notification causes an ARP background process to synchronize that ARP entry with Cisco Express Forwarding adjacency via the adjacency database.

Attachment to an outbound interface occurs only for entries in the following modes:

- Alias
- Dynamic
- Floating Static
- Application Simple
- Application Timer

The ARP subsystem processes each floating static ARP entry to find the attached interface by using the IP address in the entry to locate the connected or proxy-ARP interface. The addition of this interface information completes the ARP entry so that it can be synchronized with Cisco Express Forwarding adjacency.

ARP Table Size Monitoring per Interface

The ARP protocol can be used as a vehicle to attack router systems. One ARP attack method, spoofing, is applied on the medium to forge the identity of the host. The Cisco IOS routers have implemented a self-defense scheme to protect the router's own interface address. Other features, such as secure ARP and authorized ARP learning, are implemented in some Cisco IOS releases to limit the scope of ARP learning.

Another ARP attack method, denial-of-service (DoS), includes sending ARP packets to the router in an attempt to overwhelm the CPU processing the ARP packets and to deplete system memory by the ARP table entries created as a result of the ARP packets, resulting in a service outage on the network. A high rate of incoming ARP packets can also cause the ARP input queue to fill up quickly and exceed the maximum default or router-configured capacity, causing an out-of-service condition.

One way to detect a possible attempt to breach security through an ARP attack on the router is to monitor the size of the ARP table and trigger an alert when the number of entries reaches a configured threshold. With a simple limit on the overall ARP table size, though, it is difficult to distinguish between a valid ARP packet and a rogue packet. For a more accurate view of the incoming packets, the ARP subsystem monitors the ARP table size at the interface level. Based on the number of nodes the router serves and the number of hosts on an interface, the expected maximum number of interface-specific entries can be determined. If the number of ARP table entries for an interface exceeds the predetermined threshold, that condition might indicate an attempt to breach security through an ARP attack on the router.

ARP High Availability

ARP HA is a function of the Cisco nonstop forwarding (NSF) feature in the Cisco IOS software. On a Cisco networking device that contains dual RPs and has been configured for stateful switchover (SSO), ARP HA provides a method for increasing network availability for processing ARP entries.

This section summarizes the internal processes and data structures that the ARP subsystem uses to implement ARP HA:

- Coexistence with Stateful Switchover, page 26
- Synchronization Queue, page 27
- Backup ARP Table, page 27
- ARP HA State Machine, page 27

Coexistence with Stateful Switchover

In Cisco networking devices that support dual RPs, ARP uses the stateful switchover (SSO) feature in the Cisco IOS software. SSO provides redundancy and synchronization for many Cisco IOS applications and features. SSO takes advantage of RP redundancy by establishing one of the RPs as the active processor while the other RP is designated as the standby processor, and then synchronizing critical state information between them.

Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between the processors. A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

Synchronization Queue

The active RP maintains a synchronization queue, which contains two lists of ARP table entries:

- ARP entries from the main ARP table that are to be synchronized to the standby RP
- ARP entries from the main ARP table that have already been synchronized to the standby RP

Note The synchronization queue consists of two lists of links to entries in the main ARP table.

When switchover occurs, the ARP HA process uses the list of not-yet-synchronized entries to determine which of the entries in the redundant ARP table in the new standby RP (originally the active RP) to synchronize with the main ARP table.

If the standby RP reloads, the ARP HA process bulk synchronizes the entire synchronization queue (entries from both of the lists) to the standby RP when the standby RP reboots.

Backup ARP Table

The standby RP maintains a backup ARP table, which stores backup ARP entries that the standby RP receives from the active RP. During a switchover, the ARP HA process monitors the interface up events. For interfaces that come up, the process searches the backup table on the new active RP (originally the standby RP) for the related ARP entries. The process then adds any related backup ARP entries to the main ARP table.

ARP HA State Machine

The ARP HA process is controlled by an event-driven state machine that consists of two halves: one half for the active RP and the other half for the standby RP. When a switchover occurs, the standby RP transitions to the active half of the state machine. The state machine tracks the status of active/standby synchronization and switchover.

The active half of the state machine can be in any one of the following states:

- ARP_HA_ST_A_BULK--Transient state in which the active RP waits for the standby RP to signal that it has finished processing of the entries sent by the bulk-synchronization operation.
- ARP_HA_ST_A_SSO--Transient state in which the new active RP waits for the signal to be fully operational.
- ARP_HA_ST_A_UP--Active state in which the active RP does not send entries to the standby RP. The active RP transitions into this state either because the standby RP has not come up yet or because a previous synchronization has failed.
- ARP_HA_ST_A_UP_SYNC--Active state in which the active RP sends entries from the synchronization queue to the standby RP. The active RP transitions into this state when the number of entries to be synchronized reaches a threshold or when the synchronization timer expires, whichever occurs first.

The standby half of the state machine contains the following states:

- ARP_HA_ST_S_BULK--Transient state in which the standby RP processes the entries sent by the bulk-synchronization operation. After the active RP signals that it has finished sending entries, the standby RP transitions into the ARP_HA_ST_S_UP state and then signals back to the active RP that it has finished processing the entries sent by the bulk-synchronization operation.

- ARP_HA_ST_S_UP--Active state in which the standby RP processes the incremental ARP synchronization entries from the active RP. When the switchover occurs, the standby RP transitions to the ARP_HA_ST_A_SSO state.

These states and recent activities of the RP can be displayed for monitoring the ARP HA activities.

How to Monitor and Maintain ARP Information

Displaying ARP Table Entry Information

To display ARP table entry information, use the **show arp summary**, **show arp**, and **show arp application** commands:

- Step 2 is useful for obtaining a high-level view of the contents of the ARP table.
- Step 3 and Step 4 are useful for displaying the contents of all ARP table entries and any entry subblocks.
- Step 5 is useful for displaying ARP table information about external applications that are supported by ARP and are running on registered clients.

SUMMARY STEPS

1. **enable**
2. **show arp summary**
3. **show interfaces** [**summary**]
4. **show arp** [[**vrf** *vrf-name*] [[*arp-mode*] [[*ip-address* [*mask*]] [*interface-type interface-number*]]]] [**detail**]
5. **show arp application** [*application-id*] [**detail**]

DETAILED STEPS

Step 1 **enable**

This command enables privileged EXEC mode:

Example:

```
Router> enable
```

Step 2 **show arp summary**

This command displays the total number of ARP table entries, the number of ARP table entries for each ARP entry mode, and the number of ARP table entries for each interface on the router:

Example:

```
Router# show arp summary

Total number of entries in the ARP table: 10.
Total number of Dynamic ARP entries: 4.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 4.
Total number of Static ARP entries: 2.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
Interface              Entry Count
Ethernet3/2                      1
Ethernet3/1                      4
Ethernet3/0                      3
```

Step 3 **show interfaces** [**summary**]

This command lists all the interfaces configured on the router or access server. The valid interface types and numbers can vary according to the router and the interfaces on the router. To list all the interfaces configured on a particular router, use the **show interfaces** command with the **summary** keyword. This information is useful if you will be displaying the ARP table entries for a particular router interface.

Example:

```
Router# show interfaces summary

*: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count
  Interface               IHQ   IQD  OHQ   OQD  RXBS RXPS  TXBS TXPS TRTL
------------------------------------------------------------------------
  FastEthernet1/0          0     0    0     0     0    0     0    0    0
  ATM2/0                   0     0    0     0     0    0     0    0    0
* Ethernet3/0              0     0    0     0     0    0     0    0    0
* Ethernet3/1              0     0    0     0     0    0     0    0    0
* Ethernet3/2              0     0    0     0     0    0     0    0    0
  Ethernet3/3              0     0    0     0     0    0     0    0    0
  Serial4/0                0     0    0     0     0    0     0    0    0
  Serial4/1                0     0    0     0     0    0     0    0    0
  Serial4/2                0     0    0     0     0    0     0    0    0
  Serial4/3                0     0    0     0     0    0     0    0    0
  Fddi5/0                  0     0    0     0     0    0     0    0    0
* Loopback0                0     0    0     0     0    0     0    0    0
```

Step 4 **show arp** [[**vrf** *vrf-name*] [[*arp-mode*] [[*ip-address* [*mask*]] [*interface-type interface-number*]]]] [**detail**]

This command displays all ARP table entries or only the ARP table entries that meet the optional selection criteria.

Tip The valid interface types and numbers can vary according to the router and the interfaces on the router. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *interface-type* and *interface-number* arguments in the **show arp** command.

Example:

```
Router# show arp vrf vrf1 dynamic 209.165.200.225 e3/1 detail

ARP entry for 209.165.200.225, link type IP.
  Dynamic, via Ethernet3/1, last updated 147 minutes ago.
```

```
  Encap type is ARPA, hardware address is 0050.d173.e881, 6 bytes long.
  ARP subblocks:
  * Dynamic ARP Subblock
    Entry will be refreshed in 109 minutes and 52 seconds.
    It has 2 chances to be refreshed before it is purged.
    Entry is complete.
  * IP ARP Adjacency
    Adjacency (for 209.165.200.225 on Ethernet3/1) was installed.
    Connection ID: 0
```

Step 5 **show arp application** [*application-id*] [**detail**]

This command displays ARP table information for a specific ARP application or for all applications supported by ARP and running on registered clients:

Example:

```
Router# show arp application detail

Number of clients registered: 8
Application         ID        Num of Subblocks
ARP Backup          200       0
Application         ID        Num of Subblocks
IP ARP Adj Conn ID  201       0
Application         ID        Num of Subblocks
IP Subscriber       202       0
Application         ID        Num of Subblocks
LEC                 203       0
Application         ID        Num of Subblocks
DHCPD               204       0
Application         ID        Num of Subblocks
DSS                 205       0
Application         ID        Num of Subblocks
IP Mobility         206       0
Application         ID        Num of Subblocks
IP ARP Adjacency    207       5

ARP entry for 209.165.200.226, link type IP.
  Static.
    Subblock data:
    Adjacency (for 209.165.200.226 on Ethernet3/1) was withdrawn.
    Connection ID: 0
ARP entry for 209.165.200.227, link type IP.
  Dynamic, via Ethernet3/0.
    Subblock data:
    Adjacency (for 209.165.200.227 on Ethernet3/0) was installed.
    Connection ID: 0
ARP entry for 209.165.200.228, link type IP.
  Dynamic, via Ethernet3/0.
    Subblock data:
    Adjacency (for 209.165.200.228 on Ethernet3/0) was installed.
    Connection ID: 0
ARP entry for 209.165.200.225, link type IP.
  Dynamic, via Ethernet3/1, in VRF vrf1.
    Subblock data:
    Adjacency (for 209.165.200.225 on Ethernet3/1) was installed.
    Connection ID: 0
ARP entry for 209.165.200.229, link type IP.
  Dynamic, via Ethernet3/1, in VRF vrf1.
    Subblock data:
    Adjacency (for 209.165.200.229 on Ethernet3/1) was installed.
    Connection ID: 0
```

Displaying ARP HA Status and Statistics

To display the ARP HA status and statistics for a Cisco networking device that contains dual RPs and has been configured for SSO, use the **show arp ha** command. Different HA details are displayed, depending on the current RP state:

- The active RP that was the active RP from last time the router was rebooted
- The active RP that was a standby RP and became the active RP after an SSO occurred
- The standby RP

SUMMARY STEPS

1. **enable**
2. **show arp ha**

DETAILED STEPS

Step 1 **enable**

This command enables privileged EXEC mode:

Example:

```
Router> enable
```

Step 2 **show arp ha**

This command displays the ARP HA status and statistics collected for an HA-capable platform, such as a Cisco 7600 series router, that has been configured for SSO. The output from this command depends on the current and most recent states of the RP.

Active RP

The following is sample output from the **show arp ha** command on the active RP that has been the active RP since the last time the router was rebooted. ARP HA statistics are displayed for the active state only.

Example:

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP_SYNC).
  4 ARP entries in the synchronization queue.
  No ARP entry waiting to be synchronized.
  4022 synchronization packets sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.
```

Active RP That Was Previously a Standby RP

The following is sample output from the **show arp ha** command on the active RP that had been the standby RP and became the active RP after the most recent SSO occurred. ARP HA statistics are displayed for the active state and also for the previous standby state.

Example:

```
Router# show arp ha

ARP HA in active state (ARP_HA_ST_A_UP_SYNC).
  4 ARP entries in the synchronization queue.
  No ARP entry waiting to be synchronized.
  4022 synchronization packets sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
  No error in encoding interface names.
Statistics collected when ARP HA in standby state:
  No ARP entry in the backup table.
  5 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
  4 ARP entries restored before timer.
  No ARP entry restored on timer.
  No ARP entry purged since interface is down.
  No ARP entry purged on timer.
```

Standby RP

The following is sample output from the **show arp ha** command on the standby RP. ARP HA statistics are displayed for the standby state only.

Example:

```
Router# show arp ha

ARP HA in standby state (ARP_HA_ST_S_UP).
  4 ARP entries in the backup table.
  4005 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
```

Refreshing Dynamically Learned ARP Table Entries

Refresh dynamically learned ARP table entries to ensure the validity of the IP address and MAC address mapping information and to immediately age out any stale entries (dynamic ARP entries that have expired but have not yet been aged out by the default, timer-based process).

The scope of the refresh operation can be limited to the entries that match any one of the following selection criteria:

- ARP cache entries for a specific interface
- ARP cache entries for the global VRF and for a specific host
- ARP cache entries for a named VRF and for a specific host

SUMMARY STEPS

1. **enable**
2. **show interfaces** [**summary**]
3. **clear arp-cache** [**interface** *type number* | [**vrf** *vrf-name*] *ip-address*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show interfaces** [**summary**] **Example:** `Router# show interfaces summary`	(Optional) Lists all the interfaces configured on the router or access server. • To list the interfaces in a summary table, use the **summary** keyword. This form of the command output is useful if you will be refreshing the ARP table entries for a particular router interface.
Step 3	**clear arp-cache** [**interface** *type number* | [**vrf** *vrf-name*] *ip-address*] **Example:** `Router# clear arp-cache 192.0.2.240`	Refreshes all dynamically created ARP table entries or only the dynamically created ARP table entries that meet the selection criteria.

Setting the Maximum Limit for Learned ARP Table Entries

Limiting the number of ARP entries that can be learned by the system helps to prevent the possibility of system instability due to memory exhaustion.

The default behavior of the system is not to enforce any such maximum limit on the number of learned ARP entries in the system. Under these normal circumstances, the number of ARP entries learned from each interface is related to the number of directly connected hosts on the LAN. Scaling ARP entries to a very large number can have the following major impacts on the device:

- Increase in CPU time to process the ARP packets and to age ARP entries
- Significantly increased memory consumption in system memory and hardware table memories (for hardware forwarding platforms), which could lead to memory fragmentation and exhaustion

When the number of ARP entries that can be created by the system is not limited, memory exhaustion can cause system instability. Setting a maximum limit for the number of learned ARP table entries can help prevent this scenario from arising.

Once the limit is set, upon reaching the learn ARP entry threshold limit or 80 percent of the configured maximum limit, the system will generate a syslog message with a priority set to Level 3 (LOG_NOTICE). Upon reaching the configured maximum limit, the system will:

- Start discarding newly learned ARP entries
- Generate a syslog message with a priority set to Level 3 (LOG_NOTICE). The administrator will have to take appropriate action.

When learned ARP entries in the ARP table drop down from the maximum limit to the permit threshold limit or 95 percent of the maximum, a syslog message is generated to notify the system administrator that the ARP table is back in the normal operational state.

- Consult the support documentation for the router to determine the maximum number of ARP entries that can be learned and entered in the ARP table before setting it at the command-line interface (CLI).

Note

- The maximum limit for the number of learned ARP entries is platform dependent.

Note The setting of a maximum limit for learned ARP table entries limit functionality is supported on Cisco 7600 platform. This support started in Cisco IOS Release 12.2(33)SRD3.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip arp entry learn max-limit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip arp entry learn max-limit** **Example:** `Router#` **ip arp entry learn 256**	Setting the maximum number of learned ARP entries for the platform.

Resetting ARP HA Statistics

This task allows the user to reset the ARP HA statistics. It may be useful when debugging the ARP HA subsystem.

SUMMARY STEPS

1. **enable**
2. **clear arp-cache counters ha**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**clear arp-cache counters ha** **Example:** `Router# clear arp-cache counters ha`	Resets the ARP HA statistics.

Enabling Debug Trace for ARP Transactions

Enable debug trace for ARP transactions to monitor the ARP subsystem.

Debug trace can be enabled for all IP ARP packet traffic, or it can be enabled for an individual type of ARP event, such as:

- ARP entry events
  - Any dynamic ARP entry event
  - Any interface ARP entry event
  - Any static ARP entry event
  - Any ARP entry subblock event
- ARP table events
  - ARP table operations (entry insertion, modification, or deletion)
  - ARP table timer events
  - ARP table database events (database read/write events)
- ARP HA events
- ARP interface events
  - ARP/Cisco Express Forwarding Adjacency interface transactions
  - ARP Application interface transactions

Debug Filtering Support

The amount of ARP debug information displayed is filtered according to the interface and access list specified by the **debug list** command.

SUMMARY STEPS

1. **enable**
2. **debug list** [*list*] [*interface*]
3. **debug arp** [*arp-entry-event* | *arp-table-event* | **ha** | *interface-interaction*]
4. **show debugging**
5. **no debug arp** [*arp-entry-event* | *arp-table-event* | **ha** | *interface-interaction*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**debug list** [*list*] [*interface*] **Example:** `Router# debug list 1102 serial`	(Optional) Enables the filtering of ARP debugging information (or debugging information for any of the other protocols supported by this command) by using either or both of the following criteria: • To display debugging information for a specific interface rather than for all interfaces on a router, identify the interface by using the *interface* argument. If the interface needs to be configured, use the **interface**command. • To display information for a specific type of packet rather than for all packets, identify the packet details by using the *list* argument to identify an extended ACL. The ACL specifies a source MAC Ethernet address, the destination MAC Ethernet address, and arbitrary bytes in the packet. If the extended access list needs to be configured, use the **access-list** (extended-ibm) command.
Step 3	**debug arp** [*arp-entry-event*	*arp-table-event*	**ha**	*interface-interaction*] **Example:** `Router# debug arp static`	Enables debug trace for ARP packets. • When used with a keyword, this command enables debug trace for one of the following specific types of ARP events: ◦ ARP entry events ◦ ARP table events ◦ ARP HA events (on HA-capable platforms) ◦ Interactions on an ARP interface
Step 4	**show debugging** **Example:** `Router# show debugging`	Lists the debugging options enabled on this router.

	Command or Action	Purpose
Step 5	**no debug arp** [*arp-entry-event* | *arp-table-event* | **ha** | *interface-interaction*] **Example:** `Router# no debug arp static`	(Optional) Disables debug trace for ARP packets. • When used with a keyword, this command disables debug trace for one of the following specific types of ARP events: ◦ ARP entry events ◦ ARP table events ◦ ARP HA events (on HA-capable platforms) ◦ Interactions on an ARP interface

Enabling an ARP Trap on the Number of Learned Entries on an Interface

Enable an ARP trap or threshold for the number of dynamically learned arp entries if network administrators are to be alerted when the number of ARP entries for an interface reaches a configured threshold. The alert will be in the form of interface-specific ARP syslog output.

If the number of ARP table entries for an interface reaches a high level (based on the number of nodes the router serves and the number of hosts on that interface), the cause might be an ARP DoS attack on the router through that interface. This condition is described in "ARP Table Size Monitoring per Interface".

Determine the expected maximum number of entries for an interface. Such an estimate is typically based on the following information:

- The number of nodes the router serves
- The number of hosts on the interface

Depending on your network configuration, other factors such as whether proxy ARP is enabled can affect the number of ARP table entries for a given interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **arp log threshold entries** *entry-count*
5. **end**
6. **show running-config interface** *type number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Configures an interface type and enters interface configuration mode so that the specific interface can be configured.
Step 4	**arp log threshold entries** *entry-count* **Example:** `Router(config-if)# arp log threshold entries 1000`	Enables an ARP trap so that the ARP log is triggered when a specific number of dynamically learned entries is reached on the router interface.
Step 5	**end** **Example:** `Router(config-if) end`	Returns to privileged EXEC mode.
Step 6	**show running-config interface** *type number* **Example:** `Router# show running-config interface ethernet 0/0`	Displays information about the current operating configuration for the specified interface. • If an ARP trap is enabled for a given interface, the information for the **interface** command includes the **arp log threshold entries** command, followed by the threshold value.

Configuration Examples for Monitoring and Maintaining ARP Information

Setting the Maximum Limit for Learned ARP Table Entries Example

The following example displays how to set the maximum limit for the number of learned ARP table entries. A maximum limit of 512,000 learned ARP entries is set.

```
Router> enable
```

```
Router# configure terminal
Router(config)# ip arp entry learn 512000
```

Displaying the Maximum Limit for Learned ARP Table Entries Example

The following example displays the maximum limit for the number of learned ARP table entries after it has been set at the CLI:

```
Router# show arp summary
Total number of entries in the ARP table: 4.
Total number of Dynamic ARP entries: 0.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 3.
Total number of Static ARP entries: 1.
Total number of Alias ARP entries: 0.
Total number of Simple Application ARP entries: 0.
Total number of Application Alias ARP entries: 0.
Total number of Application Timer ARP entries: 0.
Maximum limit of Learn ARP entry : 512000.
Maximum configured Learn ARP entry limit : 512000.
Learn ARP Entry Threshold is 409600 and Permit Threshold is 486400.
Total number of Learn ARP entries: 0.
Interface              Entry Count
GigabitEthernet4/7               1
GigabitEthernet4/1.1             1
GigabitEthernet4/1               1
EOBC0/0
```

The maximum limit is shown as being set to 512,000 (Maximum configured Learn ARP entry limit: 512000.). The allowed maximum limit for learned ARP table entries is 512,000 (Maximum limit of Learn ARP entry: 512000). A maximum limit greater than this figure cannot be set.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
ARP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Addressing Services Command Reference*
IP addressing tasks	"Configuring IPv4 Addresses" module
ARP configuration tasks	"Configuring Address Resolution Protocol Options" module

Standards

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

MIBs

MIB	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

RFC	Title
RFC 1812	*Requirements for IP Version 4 Routers*

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 Monitoring and Maintaining ARP Information

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 2 Feature Information for Monitoring and Maintaining ARP Information

Feature Name	Releases	Feature Information
Monitoring and Maintaining ARP Information	12.4(11)T 12.2(31)SB2 12.2(33)SRB 12.2(33)SRD3 12.2(33)SRE	This feature introduces enhancements to ARP support in a Cisco IOS environment: • New ARP table entry types to support the attachment of application-specific data within individual entries • Enabling of ARP debug trace for specific ARP events • Filtering of ARP debug trace on a per-interface or per-access list basis • Displaying or refreshing of dynamically learned ARP table entries based on various selection criteria • Displaying or resetting of ARP HA status and statistics for HA-capable platforms • Displaying of ARP/Cisco Express Forwarding adjacency notification status • Enabling the ARP log if a specific number of dynamically learned entries is reached on a particular router interface The following commands were added: • **arp log threshold entries** • **clear arp-cache counters ha** • **show arp application** • **show arp ha** • **show arp summary** The following commands were modified: • **clear arp-cache** • **debug arp** • **show arp**

Feature Name	Releases	Feature Information
		This feature was not marketed and does not appear in Feature Navigator. In 12.2(33)SRD3, support for setting the maximum limit for learned ARP table entries on the Cisco 7600 platform was added. The following commands were introduced or modified: **ip arp entry learn**, **show arp summary**. This feature was integrated into Cisco IOS Release 12.2(33)SRE. The following command was introduced or modified: **debug arp**.

Glossary

ACL --access control list. A list kept by routers to control access to or from the router for a number of services (for example, to prevent packets with a certain IP address from leaving a particular interface on the router).

active RP --The RP that controls the system, runs the routing protocols, and presents the system management interface.

adjacency --A relationship formed between selected neighboring routers and end nodes for the purpose of exchanging routing information. Adjacency is based upon the use of a common media segment by the routers and nodes involved.

ARP --Address Resolution Protocol. Internet protocol used to map an IP address to a MAC address. Used to obtain the physical address when only the logical address is known. Defined in RFC 826.

ARPA --Advanced Research Projects Agency. Research and development organization that is part of the Department of Defense (DoD). ARPA is responsible for numerous technological advances in communications and networking. ARPA evolved into DARPA, and then back into ARPA again (in 1994).

Cisco Express Forwarding --A Layer 3 switching technology. Cisco Express Forwarding can also refer to central Cisco Express Forwarding mode, one of two modes of Cisco Express Forwarding operation. Cisco Express Forwarding enables a Route Processor to perform express forwarding. Distributed Cisco Express Forwarding is the other mode of Cisco Express Forwarding operation.

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

hop --Passage of a data packet between two network nodes (for example, between two routers).

IP --Internet Protocol. Network layer for the TCP/IP protocol suite. Internet Protocol version 4 is a connectionless, best-effort packet switching protocol. Defined in RFC 791.

IP datagram --Fundamental unit of information passed across the Internet. An IP datagram contains source and destination addresses along with data and a number of fields that define such things as the length of the datagram, the header checksum, and flags to indicate whether the datagram can be (or was) fragmented.

MAC --Media Access Control. Lower of the two sublayers of the data link layer defined by the IEEE. The MAC sublayer handles access to shared media, such as whether token passing or contention will be used.

MAC address --Media Access Control address. Standardized data link layer address that is required for every port or device that connects to a LAN. Also known as a hardware address, MAC-layer address, and physical address.

MiM --Man-in-the-Middle. A type of ARP attack performed by mimicking another device (for example, the default gateway) in the ARP packets sent to the attacked device so that the end station or router learns counterfeited device identities. This deception allows a malicious user to pose as an intermediary who can launch an ARP-spoofing attack.

proxy ARP --proxy Address Resolution Protocol. Variation of the ARP protocol in which an intermediate device (for example, a router) sends an ARP response on behalf of an end node to the requesting host. Proxy ARP can lessen bandwidth use on slow-speed WAN links. *See also* ARP.

RP --Route Processor. Processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a supervisory processor.

SSO --stateful switchover. A method of providing redundancy and synchronization for many Cisco IOS applications and features. SSO is necessary for the Cisco IOS firewall to learn about the redundancy state of the network and to synchronize their internal application state with their redundant peers. SSO allows the active and standby routers to share firewall session state information so that each router has enough information to become the active router at any time.

standby RP --The RP that waits in case the active RP fails.

VPN --Virtual Private Network. Framework that consists of multiple peers transmitting private data securely to one another over an otherwise public infrastructure. A VPN protects inbound and outbound network traffic by using protocols that tunnel and encrypt all data at the IP level. This framework permits networks to extend beyond their local topology, while remote users are provided with the appearance and functionality of a direct network connection. A VPN enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses “tunneling” to encrypt all information at the IP level.

VRF --VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router. Each VPN instantiated on the PE router has its own VRF.