Monitoring and Maintaining ARP Information

First Published: November 17, 2006
Last Updated: November 17, 2006

Address Resolution Protocol (ARP) is an Internet protocol used to map an IP address to a Media Access Control (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.

Development of additional ARP information monitoring and maintenance capabilities is an incremental step within an overall program to improve the management tools for ARP support in a Cisco IOS environment:

- To better support ARP analysis activities, the ARP administrative facilities have been enhanced to provide more detailed information about and more 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 (CEF) adjacency.
- The ARP debug trace facility has been enhanced to enable ARP packet debug trace for individual types of ARP events. The ARP debugging has also been enhanced to filter ARP entries for a specified interface, for hosts that match an access list, or 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.

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 in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for Monitoring and Maintaining ARP Information" section on page 23.

Cisco Systems

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

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

- Restrictions for Monitoring and Maintaining ARP Information, page 2
- Information About Monitoring and Maintaining ARP Information, page 3
- How to Monitor and Maintain ARP Information, page 10
- Additional References, page 20
- Feature Information for Monitoring and Maintaining ARP Information, page 23
- Glossary, page 25

Restrictions for Monitoring and Maintaining ARP Information

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

- ARP High Availability, page 2
- ARP Security Against ARP Attacks, page 2

ARP High Availability

The ARP subsystem supports ARP high availability (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

Before you begin monitoring and maintaining ARP information, you should understand the following concepts:

- Overview of Monitoring and Maintaining ARP Information, page 3
- Address Resolution Protocol, page 5
- ARP Table, page 6
- ARP Table Entry Modes, page 6
- ARP Table Entry Subblocks, page 7
- ARP Table Entry Synchronization with CEF Adjacency, page 8
- ARP Table Size Monitoring Per Interface, page 8
- ARP High Availability, page 9

Overview of Monitoring and Maintaining ARP Information

Development of additional ARP information monitoring and maintenance capabilities is an incremental step within an overall program to improve the management tools for ARP support in a Cisco IOS environment. For information about the entire ARP feature, see the "Additional References" section on page 20. The following sections summarize the ARP subsystem enhancements introduced in Cisco IOS Release 12.4(11)T:

- ARP Information Display Enhancements, page 3
- ARP Information Refresh Enhancements, page 4
- ARP Debug Trace Enhancements, page 4
- ARP Security Enhancement, page 5

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 high availability (HA), or ARP notification for Cisco Express Forwarding (CEF) adjacency. If the ARP subsystem needs to synchronize an ARP entry with CEF 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, CEF 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 non-static entries in the ARP table. The ARP information refresh facility enables you to manage selected ARP information:

- Refresh all non-static ARP table entries
- Refresh non-static ARP table entries associated with a particular interface
- Refresh non-static 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

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 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. This section provides background information about ARP:

- ARP Broadcast and Response Process, page 5
- ARP Caching, page 6

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 CEF, 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

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.
- Application Simple, Alias Application, and Timer Application 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 CEF Adjacency

If CEF 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). CEF 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 CEF 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 CEF 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 CEF 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:

- Co-Existence with Stateful Switchover, page 9
- Synchronization Queue, page 9
- Backup ARP Table, page 9
- ARP HA State Machine, page 10

Co-Existence with Stateful Switchover

In Cisco networking devices that support dual RPs, ARP uses the 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.

For more information about the SSO feature, see the "Additional References" section on page 20.

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 crashes, 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_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 standby RP comes up.
- 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_BULK—Transient state in which the active RP bulk-synchronizes the ENTIRE SET OF ARP entries to the standby RP and then waits for the standby RP to signal that it has finished processing 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.

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

This section contains the following procedures:

- Displaying ARP Table Entry Information, page 10
- Displaying ARP HA Status and Statistics, page 13
- Refreshing Dynamically Learned ARP Table Entries, page 15
- Resetting ARP HA Statistics, page 15
- Enabling Debug Trace for ARP Transactions, page 16
- Enabling ARP Trap on the Number of Learned Entries on an Interface, page 19

Displaying ARP Table Entry Information

To verify 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.

```
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.

```
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.

```
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.

```
Router# show arp vrf vrf1 dynamic 5.100.1.1 e3/1 detail

ARP entry for 5.100.1.1, 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 5.100.1.1 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.

```
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 70.1.1.1, link type IP.
  Static.
    Subblock data:
    Adjacency (for 70.1.1.1 on Ethernet3/1) was withdrawn.
    Connection ID: 0
ARP entry for 10.0.18.70, link type IP.
  Dynamic, via Ethernet3/0.
    Subblock data:
    Adjacency (for 10.0.18.70 on Ethernet3/0) was installed.
    Connection ID: 0
ARP entry for 10.0.18.78, link type IP.
  Dynamic, via Ethernet3/0.
    Subblock data:
    Adjacency (for 10.0.18.78 on Ethernet3/0) was installed.
    Connection ID: 0
ARP entry for 5.100.1.1, link type IP.
  Dynamic, via Ethernet3/1, in VRF vrf1.
    Subblock data:
    Adjacency (for 5.100.1.1 on Ethernet3/1) was installed.
    Connection ID: 0
ARP entry for 5.100.1.5, link type IP.
  Dynamic, via Ethernet3/1, in VRF vrf1.
    Subblock data:
    Adjacency (for 5.100.1.5 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.

```
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:

```
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:

```
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:

```
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.

Resetting ARP HA Statistics

Reset the ARP HA statistics 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 HA events
- ARP interface events
  - ARP/CEF 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 access control list (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.

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 ARP Trap on the Number of Learned Entries on an Interface

Enable interface-specific ARP syslog output if network administrators are to be alerted when the number of ARP entries for an interface reaches a configured threshold.

ARP Table Size as an Indicator of a Possible ARP Attack

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 the "ARP Table Size Monitoring Per Interface" section on page 8.

Prerequisites

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.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet0/0`	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 ethernet0/0`	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 threshold value.

Additional References

The following sections provide references related to monitoring and maintaining ARP information.

Related Documents

Related Topic	Document Title
IP addressing and services commands	"IP Addressing Commands" chapter in the *Cisco IOS IP Addressing Services Command Reference,* Release 12.4T
IP addressing and services tasks	"Configuring IP Addressing" chapter in the *Cisco IOS IP Addressing Services Configuration Guide,* Release 12.4
Address Resolution Protocol (ARP) commands	"ARP Commands" chapter in the *Cisco IOS IP Addressing Services Command Reference,* Release 12.4T

Related Topic	Document Title
Address Resolution Protocol (ARP) configuration tasks	"Configuring Address Resolution Protocol Options" chapter in the *Cisco IOS IP Addressing Services Configuration Guide,* Release 12.4
Cisco Express Forwarding (CEF) configuration tasks	"Configuring Cisco Express Forwarding" chapter in the *Cisco IOS IP Switching Configuration Guide,* Release 12.4T
Cisco Nonstop Forwarding (NSF)	*Cisco Nonstop Forwarding* feature module, Cisco IOS Release 12.0(25)S
Stateful switchover (SSO)	• *Stateful Switchover* feature module, Cisco IOS Release 12.0(23)S • "Stateful Switchover" section of the *Cisco Globally Resilient IP: Overview and Applications* technology white paper for IP routed protocols

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 Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Monitoring and Maintaining ARP Information

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 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	This functionality 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/CEF 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** This functionality was not marketed and does not appear in feature navigator.

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).

CEF—Cisco Express Forwarding. A Layer 3 switching technology. CEF can also refer to central CEF mode, one of two modes of CEF operation. CEF enables a Route Processor to perform express forwarding. Distributed CEF (dCEF) is the other mode of CEF 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. *See also* LLC.

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 impersonating 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 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. 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.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.