ARP Rewrite

First Published: August 24, 2006
Last Updated: August 24, 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 the ARP Rewrite feature 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 the ARP Rewrite feature. The ARP-related enhancements introduced by this feature 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 ARP Rewrite" section on page 44.

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.

CISCO SYSTEMS

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

Contents

Restrictions for ARP Rewrite

For Cisco IOS Release 12.2(33)ZW, the following restrictions apply to the ARP Rewrite feature:

Application-specific ARP Table Entries

The ARP Rewrite feature introduces new ARP table entry modes to support application-specific ARP table entries. Applications that use these new mode types (Application Simple, Application Alias, and Application Timer) receive enhanced support in terms of software architecture and debugging tools. However, Cisco IOS Release 12.2(33)ZW does not support the Application Timer mode.

ARP High Availability

The ARP Rewrite feature 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 Route Processor (RP) to the standby RP. Statically configured ARP entries are not synchronized to the standby RP.

ARP Security Against ARP Attacks

The ARP Rewrite feature introduces 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. 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 ARP Rewrite

To use the ARP Rewrite feature, you should understand the following concepts:

ARP Rewrite Feature Overview

Development of the ARP Rewrite feature 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 enhancements introduced in the ARP Rewrite feature:

ARP Information Display Enhancements

The ARP information display capabilities have been expanded to support display of selected ARP entries, display of ARP entry details, and display of 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 12.2(33)ZW, 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 12.2(33)ZW, the **clear arp** command refreshes all non-static entries in the ARP table. The ARP Rewrite feature introduces enhancements to the ARP information refresh facility that enable 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 12.2(33)ZW, the **debug arp** command supports debugging information for ARP packet traffic only. The ARP Rewrite feature introduces enhancements to the ARP debug trace facility that provide more detailed selection and filter options for ARP debug trace.

Debug Trace for Selected ARP Events

The ARP Rewrite feature includes enhancements that allow ARP debugging information to 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 ARP Rewrite feature also includes enhancements to ARP debugging so that 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

The ARP Rewrite feature introduces trap-based enabling of ARP system message logging (syslog) output. When this feature 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 exceed 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 Rewrite feature 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 Rewrite feature introduces the ARP entry subblock structure as a 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 Rewrite feature 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 feature 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 Rewrite feature uses to implement ARP HA:

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 a Summary of All ARP Table Entries, page 11 (Optional)
- Displaying All ARP Table Entries, page 11 (Optional)
- Displaying Only the ARP Table Entries for a Specific Type of ARP Application, page 12 (Optional)
- Displaying ARP HA Status and Statistics, page 13 (Optional)
- Refreshing Dynamically Learned ARP Table Entries, page 14 (Optional)

- Resetting ARP HA Statistics, page 15 (Optional)
- Enabling Debug Trace for ARP Transactions, page 15 (Optional)
- Enabling ARP Trap on the Number of Learned Entries on an Interface, page 18 (Optional)

Displaying a Summary of All ARP Table Entries

The summary of all ARP table entries provides a high-level view of the contents of the ARP table.

SUMMARY STEPS

1. **enable**
2. **show arp summary**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show arp summary** **Example:** `Router# show arp summary`	Displays the total number of ARP table entries, the number of ARP table entries for each ARP mode, and the number of ARP table entries for each router interface.

Displaying All ARP Table Entries

The following information can be displayed for any entry in the ARP table:

- Entry age in minutes
- IP host or network information:
  - Protocol and network address
  - LAN hardware address of a MAC address that corresponds to the network address
  - Encapsulation type the Cisco IOS software is using for the network address
  - Interface associated with the network address
- Associated router interface—for floating static ARP entries only
- ARP adjacency notification status—for entries of certain ARP mode types (Dynamic, Static, or Alias) and entries for certain ARP application types (Application Simple or Application Timer)
- Entry details about the following information:
  - Protocol used to create the entry
  - ARP mode type
  - Subblocks (if any)

SUMMARY STEPS

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

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. **Note** This information is useful if you will be displaying the ARP table entries for a particular router interface.
Step 3	**show arp** [[**vrf** *vrf-name*] [[*arp-mode*] [[*ip-address* [*mask*]] [*interface-type interface-number*]]]] [**detail**]] **Example:** `Router# show arp vrf vpn1 dynamic 192.0.2.212 Ethernet2/1 detail`	Displays all ARP table entries or only the ARP table entries that meet the selection criteria.

Displaying Only the ARP Table Entries for a Specific Type of ARP Application

The following information can be displayed for any ARP table entry for an application supported by ARP and running on a registered client:

- ARP application name
- ARP application ID number
- Number of subblocks attached
- ARP application details:
  - IP address or network
  - ARP table entry type (dynamic, interface, static, or alias) or ARP application mode (Simple Application or Application Alias)
  - Associated interface
  - Brief description of subblocks (if any)

SUMMARY STEPS

1. **enable**
2. **show arp application** [*application-id*] [**detail**]

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`show arp application` [*application-id*] [`detail`] **Example:** `Router# show arp application 200 detail`	Displays ARP table entries for ARP applications running on registered clients. **Note** To display the ID of each ARP application, use this command without the *application-id* argument.

Displaying ARP HA Status and Statistics

ARP HA status and statistics provide a detailed view of ARP HA processing. 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

Restrictions

The ARP HA status and statistics are collected only on HA-capable platforms (that is, Cisco networking devices that support dual RPs).

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show arp ha** **Example:** `Router# show arp ha`	Displays ARP HA status and statistics for the current RP state.

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.

	Command or Action	Purpose
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 the ARP Rewrite feature.

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
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 12.4
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 • The "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

Command Reference

This section documents new and modified commands only.

New Commands

- **arp log threshold entries**
- **clear arp-cache counters ha**
- **show arp application**
- **show arp ha**
- **show arp summary**

Modified Commands

- **clear arp-cache**
- **debug arp**
- **show arp**

arp log threshold entries

To enable an Address Resolution Protocol (ARP) trap so that the ARP log is triggered when a specific number of dynamically learned entries is reached on the router interface, use the **arp log threshold entries** command in interface configuration mode. To disable the ARP trap for the interface, use the **no** form of this command.

arp log threshold entries *entry-count*

no arp log threshold entries

Syntax Description

entry-count	Triggers the ARP log service when the number of dynamically learned entries on the interface reaches this threshold. The range is from 1 to 2147483647.

Command Default

ARP trap is disabled for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(33)ZW	This command was introduced.

Usage Guidelines

This command enables an ARP trap for the router interface. When the number of dynamically learned entries on the interface exceeds the preconfigured amount, an ARP event message is written to system message logging (syslog) output.

A high number of learned entries on the interface might indicate anomalies such as an attempt to breach security through an ARP attack on the router. The threshold at which to configure the ARP log service trigger should be determined heuristically, based on the expected number of nodes the router will serve and the number of hosts on the interface.

To display information about the setting configured by the **arp log threshold entries** command, use the **show running-config** command. If an ARP trap is enabled for a given interface, the information for that **interface** command includes the **arp log threshold entries** command, followed by the threshold value.

To display the syslog history statistics and buffer contents, use the **show logging** command.

Examples

The following example shows how to enable an ARP trap so that the ARP log is triggered when 50 dynamically learned entries is reached on the Ethernet interface at slot 2, port 1:

```
Router(config)# interface ethernet2/1
Router(config-if)# arp log threshold entries 50
```

The following sample output from the **show logging** command shows that the ARP trap entry was triggered when 50 dynamic ARP entries was reached on the Ethernet interface at slot 2, port 1:

```
Router# show logging
```

```
Syslog logging: enabled (0 messages dropped, 39 messages rate-limited, 0 flushes, 0
overruns, xml disabled, filtering disabled)
    Console logging: disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level debugging, 309 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (8192 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 312 message lines logged

Log Buffer (65536 bytes):

Jan 27 18:27:32.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:27:31 PST
Fri Jan 27 2006 to 10:27:32 PST Fri Jan 27 2006, configured from console by console.
Jan 27 18:27:32.431: %SYS-5-CONFIG_I: Configured from console by console
Jan 27 18:27:34.051: %ARP-4-TRAPENTRY: 50 dynamic ARP entries on Ethernet2/1 installed in
the ARP table
```

Related Commands

Command	Description
interface	Selects an interface to configure and enters interface configuration mode.
show logging	Displays the contents of logging buffers.
show running-config	Displays the contents of the currently running configuration file of your routing device.

clear arp-cache

To refresh dynamically created entries from the Address Resolution Protocol (ARP) cache, use the **clear arp-cache** command in privileged EXEC mode.

clear arp-cache [**interface** *type number* | [**vrf** *vrf-name*] *ip-address*]

Syntax Description

interface *type number*	(Optional) Refreshes only the ARP table entries associated with this interface.
vrf *vrf-name*	(Optional) Refreshes only the ARP table entries for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance and the IP address specified by the *ip-address* argument.
ip-address	(Optional) Refreshes only the ARP table entries for the specified IP address.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)ZW	The **interface** keyword and the *type* and *number* arguments were made optional to support refreshing of entries for a single router interface. The **vrf** keyword, the *vrf-name* argument, and the *ip-address* argument were added to support refreshing of entries of a specified address and an optionally specified VRF.

Usage Guidelines

This command updates the dynamically learned IP address and MAC address mapping information in the ARP table to ensure the validity of those entries. If the refresh operation encounters any stale entries (dynamic ARP entries that have expired but have not yet been aged out by an internal, timer-driven process), those entries are aged out of the ARP table immediately as opposed to at the next refresh interval.

Note By default, dynamically learned ARP entries remain in the ARP table for four minutes.

The **clear arp-cache** command can be entered multiple times to refresh dynamically created entries from the ARP cache using different selection criteria.

- Use this command without any arguments or keywords to refresh all ARP cache entries for all enabled interfaces.

- To refresh ARP cache entries for a specific interface, use this command with the **interface** keyword and *type* and *number* arguments.

Tip 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. Use the appropriate interface specification, typed exactly as it is displayed under the Interface column of the **show interfaces** command output, to replace the *type* and *number* arguments in the **clear arp-cache interface** command.

- To refresh ARP cache entries from the global VRF and for a specific host, use this command with the *ip-address* argument.
- To refresh ARP cache entries from a named VRF and for a specific host, use this command with the **vrf** keyword and the *vrf-name* and *ip-address* arguments.

To display ARP table entries, use the **show arp** command.

This command does not affect permanent entries in the ARP cache, and it does not affect the ARP HA statistics.

- To remove static ARP entries from the ARP cache, use the **no** form of the **arp** command.
- To remove alias ARP entries from the ARP cache use the **no** form of the **arp** command with the **alias** keyword.
- To reset the ARP HA status and statistics, use the clear arp-cache counters ha command.

Examples

The following example shows how to refresh all dynamically learned ARP cache entries for all enabled interfaces:

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

The following example shows how to refresh dynamically learned ARP cache entries for the Ethernet interface at slot 1, port 2:

```
Router# clear arp-cache interface ethernet1/2
```

The following example shows how to refresh dynamically learned ARP cache entries for the host at 192.0.2.140:

```
Router# clear arp-cache 192.0.2.140
```

The following example shows how to refresh dynamically learned ARP cache entries from the VRF named vpn3 and for the host at 192.0.2.151:

```
Router# clear arp-cache vrf vpn3 192.0.2.151
```

Related Commands

Command	Description
arp (global)	Configures a permanent entry in the ARP cache.
arp timeout	Configures how long a dynamically learned IP address and its corresponding MAC address remain in the ARP cache.
clear arp-cache counters ha	Resets the ARP HA statistics.

Command	Description
show arp	Displays ARP table entries.
show interfaces	Displays statistics for all interfaces configured on the router or access server.

clear arp-cache counters ha

To reset the Address Resolution Protocol (ARP) high availability (HA) statistics, use the **clear arp-cache counters ha** command in privileged EXEC mode.

clear arp-cache counters ha

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)ZW	This command was introduced.

Usage Guidelines

Use the **clear arp-cache counters ha** command to reset all ARP high availability statistics for all enabled interfaces.

To display the ARP HA status and statistics, use the **show arp ha** command.

Note The **clear arp-cache counters ha** command and the **show arp ha** command are available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

Examples

The following example shows how to reset the ARP HA statistics:

```
Router# clear arp-cache counters ha
```

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
show arp ha	Displays the ARP HA status and statistics.

debug arp

To enable debugging output for Address Resolution Protocol (ARP) transactions, use the **debug arp** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug arp [*arp-entry-event* | *arp-table-event* | **ha** | *interface-interaction*]

no debug arp [*arp-entry-event* | *arp-table-event* | **ha** | *interface-interaction*]

Syntax Description

arp-entry-event	(Optional) Enables debug trace for ARP entry events by specifying one of the following keywords: • **dynamic**—Enables debugging output for dynamic ARP entry events. • **interface**—Enables debugging output for interface ARP entry events. • **static**—Enables debugging output for static ARP entry events. • **subblocking**—Enables debugging output for ARP subblocking events.
arp-table-event	(Optional) Enables debug trace for ARP table events by specifying one of the following keywords: • **table**—Enables debugging output for ARP table operations. • **timer**—Enables debugging output for ARP timer operations.
ha	(Optional) Enables debug trace for ARP high availability (HA) events. **Note** This keyword is available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).
interface-interaction	(Optional) Enables debug trace for ARP interface interaction by specifying one of the following keywords: • **adjacency**—Enables debugging output for ARP interface events and Cisco Express Forwarding (CEF) adjacency interface events. • **application**—Enables debugging output for ARP application interface events.

Command Default

Debugging output is disabled for ARP transactions.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)ZW	The following keywords were added: **adjacency**, **application**, **dynamic**, **ha**, **interface**, **static**, **subblocking**, **table**, and **timer**.

Usage Guidelines

To enable ARP packet debugging, use this command without a keyword. The debugging information shows whether the router is sending ARP packets and whether it is receiving ARP packets. Use this command when some nodes on a TCP/IP network are responding, but others are not.

The amount of debug information displayed is filtered based on an interface, an access list, or both, as specified by the **debug list** command.

To list the debugging options enabled on this router, use the **show debugging** command.

Examples

The following example shows how to enable ARP packet debugging filtered on ARP table entries for the host at 192.0.2.10:

```
Router(config)# access-list 10 permit host 192.0.2.10
Router(config)# exit
Router# debug list 10
Router# debug arp

ARP packet debugging is on
        for access list: 10
```

The following is sample output from the **debug arp** command:

```
IP ARP: sent req src 192.0.2.7 0000.0c01.e117, dst 192.0.2.96 0000.0000.0000
IP ARP: rcvd rep src 192.0.2.96 0800.2010.b908, dst 192.0.2.7
IP ARP: rcvd req src 172.16.6.10 0000.0c00.6fa2, dst 192.0.2.62
IP ARP: rep filtered src 192.0.2.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff
IP ARP: rep filtered src 192.0.2.240 0000.0c00.6b31, dst 192.0.2.7 0800.2010.b908
```

In the output, each line of output represents an ARP packet that the router sent or received. Explanations for the individual lines of output follow.

The first line indicates that the router at IP address 192.0.2.7 and MAC address 0000.0c01.e117 sent an ARP request for the MAC address of the host at 192.0.2.96. The series of zeros (0000.0000.0000) following this address indicate that the router is currently unaware of the MAC address.

```
IP ARP: sent req src 192.0.2.7 0000.0c01.e117, dst 192.0.2.96 0000.0000.0000
```

The second line indicates that the router at IP address 192.0.2.7 receives a reply from the host at 192.0.2.96 indicating that its MAC address is 0800.2010.b908:

```
IP ARP: rcvd rep src 192.0.2.96 0800.2010.b908, dst 192.0.2.7
```

The third line indicates that the router receives an ARP request from the host at 172.16.6.10 requesting the MAC address for the host at 192.0.2.62:

```
IP ARP: rcvd req src 172.16.6.10 0000.0c00.6fa2, dst 192.0.2.62
```

The fourth line indicates that another host on the network attempted to send the router an ARP reply for its own address. The router ignores meaningless replies. Usually, meaningless replies happen if a bridge is being run in parallel with the router and is allowing ARP to be bridged. This condition indicates a network misconfiguration.

```
IP ARP: rep filtered src 192.0.2.7 aa92.1b36.a456, dst 255.255.255.255 ffff.ffff.ffff
```

The fifth line indicates that another host on the network attempted to inform the router that it is on network 192.0.2.240, but the router does not know that the network is attached to a different router interface. The remote host (probably a PC or an X terminal) is misconfigured. If the router were to install this entry, it would deny service to the real machine on the proper cable.

```
IP ARP: rep filtered src 192.0.2.240 0000.0c00.6b31, dst 192.0.2.7 0800.2010.b908
```

Related Commands

Command	Description
access-list (extended-ibm)	Configures the extended access list mechanism for filtering frames by both source and destination addresses and arbitrary bytes in the packet.
debug list	Enables filtering of debug trace on a per-interface or per-access list basis.
show debugging	Lists the debugging options enabled on this router.

show arp

To display the entries in the Address Resolution Protocol (ARP) table, use the **show arp** command in user EXEC or privileged EXEC mode.

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

Syntax Description

vrf *vrf-name*	(Optional) Displays the entries under the Virtual Private Network (VPN) routing and forwarding (VRF) instance specified by the *vrf-name* argument. If this option is specified, it can be followed by any valid combination of the *arp-mode*, *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
arp-mode	(Optional) Displays the entries that are in a specific ARP mode. This argument can be replaced by one of the following keywords: • **alias**—Displays only alias ARP entries. An alias ARP entry is a statically configured (permanent) ARP table entry that is associated with a local IP address. This type of entry can be configured or removed using the **arp** (global) command with the **alias** keyword. • **dynamic**—Displays only dynamic ARP entries. A dynamic ARP entry is learned through an ARP request and completed with the MAC address of the external host. • **incomplete**—Displays only incomplete ARP entries. An incomplete ARP entry is learned through an ARP request but has not yet been completed with the MAC address of the external host. • **interface**—Displaysonly interface ARP entries. An interface ARP entry contains a local IP address and is derived from an interface. • **static**—Displays only static ARP entries. A static ARP entry is a statically configured (permanent) ARP entry that is associated with an external host. This type of entry can be configured or removed using the **arp** (global) command. **Note** If this option is specified, it can be followed by any valid combination of the *ip-address*, *mask*, *interface-type*, and *interface-number* arguments and the **detail** keyword.
ip-address [*mask*]	(Optional) Displays the entries associated with a specific host or network. **Note** If this option is specified, it can be followed by any valid combination of the *interface-type* and *interface-number* arguments and the **detail** keyword.
interface-type interface-number	(Optional) Displays the specified entries that are also associated with this router interface. **Note** If this option is specified, it can be followed by the **detail** keyword.
detail	(Optional) Displays the specified entries with mode-specific details and information about subblocks (if any).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)ZW	The **vrf** keyword and *vrf-name* argument were added to limit the display to entries under a specific VRF. The **alias**, **dynamic**, **incomplete**, **interface**, and **static** keywords were added to limit the display to entries in a specific ARP mode. The *ip-address* and *mask* arguments were added to limit the display to entries for a specific host or network. The *interface-type* and *interface-number* arguments were added to limit the display to entries for a specific interface. The **detail** keyword was added to display additional details about the entries.

Usage Guidelines

To display all entries in the ARP cache, use this command without any arguments or keywords.

Tip 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. 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.

ARP Adjacency Notification

If Cisco Express Forwarding (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.

- To verify that IPv4 CEF is running, use the **show ip cef** command.
- To verify that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct, use the **show adjacency** command.

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. If the synchronization succeeds, IP ARP adjacency is said to be “installed”; if the synchronization fails, IP ARP adjacency is said to have been “withdrawn.”

Note Attachment to an outbound interface occurs only for ARP entries in the following modes: alias, dynamic, static, Application Simple, and Application Timer.

To display detailed information about any ARP adjacency notification that may have occurred, use the **show arp** command with the **detail** keyword. You can use this information to supplement the information available through ARP/CEF adjacency debug trace. To enable debug trace for ARP/CEF adjacency interactions, use the **debug arp** command with the **adjacency** keyword.

ARP Cache Administration

To refresh all entries for the specified interface (or all interfaces) or to refresh all entries of the specified address (or all addresses) in the specified VRF table (or in the global VRF table), use the **clear arp-cache** command.

To enable debugging output for ARP transactions, use the **debug arp** command.

Examples

The following is sample output from the **show arp** command with no optional keywords or arguments specified:

```
Router# show arp

Protocol   Address          Age (min)   Hardware Addr    Type    Interface

Internet   192.0.2.112      120         0000.a710.4baf   ARPA    Ethernet3
AppleTalk  4028.5           29          0000.0c01.0e56   SNAP    Ethernet2
Internet   192.0.2.114      105         0000.a710.859b   ARPA    Ethernet3
AppleTalk  4028.9           -           0000.0c02.a03c   SNAP    Ethernet2
Internet   192.0.2.121      42          0000.a710.68cd   ARPA    Ethernet3
Internet   192.0.2.9        -           0000.3080.6fd4   SNAP    TokenRing0
AppleTalk  4036.9           -           0000.3080.6fd4   SNAP    TokenRing0
Internet   192.0.2.9        -           0000.0c01.7bbd   SNAP    Fddi0
```

Table 1 describes the fields shown in the display.

Table 1 show arp Field Descriptions

Field	Description
Protocol	Protocol for network address in the Address field.
Address	The network address that corresponds to the Hardware Address.
Age (min)	Age in minutes of the cache entry. A hyphen (-) means the address is local.
Hardware Addr	LAN hardware address of a MAC address that corresponds to the network address.

Table 1 show arp Field Descriptions (continued)

Field	Description
Type	Indicates the encapsulation type the Cisco IOS software is using for the network address in this entry. Possible values include: • 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—For Switch Route Processor, side A (SRP-A) interfaces. • SRP-B—For Switch Route Processor, side B (SRP-B) interfaces.
Interface	Indicates the interface associated with this network address.

When this command is used to display dynamic ARP entries, the display information includes the time of the last update and the amount of time before the next scheduled refresh is to occur. The following is sample output from the **show arp** command for the dynamic ARP entry at network address 192.0.2.1:

```
Router# show arp 192.0.2.1 detail

ARP entry for 192.0.2.1, link type IP.
  Alias, last updated 13323 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
    Entry is complete, attached to GigabitEthernet1/1.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.1 on GigabitEthernet1/1) was installed.
```

When this command is used to display floating static ARP entries, the display information includes the associated interface, if any.The following is sample output from the **show arp** command for the floating static ARP entry at network address 192.0.2.2 whose intended interface is down:

```
Router# show arp 192.0.2.2 detail

ARP entry for 192.0.2.2, link type IP.
  Alias, last updated 13327 minutes ago.
  Encap type is ARPA, hardware address is 1234.1234.1234, 6 bytes long.
  ARP subblocks:
  * Static ARP Subblock
    Floating entry.
    Entry is incomplete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.2 on GigabitEthernet1/1) was withdrawn.
```

The following is sample detailed output from the **show arp** command for the Application Alias ARP entry at network address 192.0.2.3:

```
Router# show arp 192.0.2.3 detail

ARP entry for 192.0.2.3, link type IP.
  Application Alias, via Ethernet2/2, last updated 0 minute ago.
```

```
  Created by "HSRP".
  Encap type is ARPA, hardware address is 0000.0c07.ac02, 6 bytes long.
  ARP subblocks:
  * Application Alias ARP Subblock
  * HSRP
    ARP Application entry for application HSRP.
```

The following is sample detailed output from the **show arp** command for all dynamic ARP entries:

```
Router# show arp dynamic detail

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1, last updated 0 minute ago.
  Encap type is ARPA, hardware address is 0000.0000.0014, 6 bytes long.
  ARP subblocks:
  * Dynamic ARP Subblock
    Entry will be refreshed in 0 minute and 1 second.
    It has 1 chance to be refreshed before it is purged.
    Entry is complete.
  * IP ARP Adjacency
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
```

Related Commands

Command	Description
arp (global)	Configures a permanent entry in the ARP cache.
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
debug arp	Enables debugging output for ARP packet transactions.
show adjacency	Verifies that an adjacency exists for a connected device, that the adjacency is valid, and that the MAC header rewrite string is correct.
show arp application	Displays only the ARP table entries for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.
show interfaces	Displays statistics for all interfaces configured on the router or access server.
show ip cef	Display entries in the FIB or to display a summary of the FIB.

show arp application

To display Address Resolution Protocol (ARP) table entries for a specific ARP application or for all applications supported by ARP and running on registered clients, use the **show arp application** command in user EXEC or privileged EXEC mode.

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

Syntax Description

application-id	(Optional) Displays ARP table information for a specific ARP application. The range is from 200 to 4294967295. If no ID is specified, ARP table information is displayed for all supported ARP applications running on registered clients.
detail	(Optional) Includes detailed information about subblocks for ARP table information displayed (for the specified application or for all applications supported by ARP and running on registered clients).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)ZW	This command was introduced.

Usage Guidelines

To display ARP table information about all supported ARP applications running on registered clients, use this command without any arguments or keywords.

Examples

The following is sample output from the **show arp application** command:

```
Router# show arp application

Number of clients registered: 7

Application         ID        Num of Subblocks
ARP Backup          200       1
IP SIP              201       0
LEC                 202       0
DHCPD               203       0
IP Mobility         204       0
HSRP                209       1
IP ARP Adjacency    212       2
```

The following is sample detailed output from the **show arp application detail** command:

```
Router# show arp application detail

Number of clients registered: 7

Application         ID        Num of Subblocks
ARP Backup          200       1
```

```
ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    Backup for Interface on Ethernet2/2

Application         ID        Num of Subblocks
IP SIP              201       0

Application         ID        Num of Subblocks
LEC                 202       0

Application         ID        Num of Subblocks
DHCPD               203       0

Application         ID        Num of Subblocks
IP Mobility         204       0

Application         ID        Num of Subblocks
HSRP                209       1

ARP entry for 192.0.2.10, link type IP.
  Application Alias, via Ethernet2/2.
    Subblock data:
    ARP Application entry for application HSRP.

Application         ID        Num of Subblocks
IP ARP Adjacency    212       2

ARP entry for 192.0.2.4, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.4 on Ethernet2/1) was installed.
ARP entry for 192.0.2.2, link type IP.
  Dynamic, via Ethernet2/1.
    Subblock data:
    Adjacency (for 192.0.2.2 on Ethernet2/1) was installed.
```

Table 2 describes the significant fields shown in the display.

Table 2 show arp application Field Descriptions

Field	Description
Application	ARP application name
ID	ARP application ID number
Num of Subblocks	Number of subblocks attached

Related Commands

Command	Description
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp ha	Displays the ARP HA status and statistics.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp ha

To display the status and statistics of Address Resolution Protocol (ARP) high availability (HA), use the **show arp ha** command in user EXEC or privileged EXEC mode.

show arp ha

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)ZW	This command was introduced.

Usage Guidelines

Use this command to display the ARP HA status and statistics.

HA-Capable Platforms

This command is available only on HA-capable platforms (that is, Cisco networking devices that support dual Route Processors [RPs]).

ARP HA Statistics

The ARP HA process collects one set of statistics for the active RP (described in Table 3 on page 40) and a different set of statistics for the standby RP (described in Table 4 on page 41). These statistics can be used to track the RP state transitions when debugging ARP HA issues.

The output from this command depends on the current and most recent states of the RP:

- For the active RP that has been the active RP since the last time the router was rebooted, this command displays the HA statistics for the active RP.
- For the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (SSO) occurred, this command displays the HA statistics for the active RP plus the HA statistics collected when the RP was a standby RP.
- For a standby RP, this command displays the HA statistics for a standby RP.

Examples

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).
  2 ARP entries in the synchronization queue.
  No ARP entry waiting to be synchronized.
  806 synchronization packets sent.
  No error in allocating synchronization packets.
  No error in sending synchronization packets.
```

```
  No error in encoding interface names.
```

The following is sample output from the **show arp ha** command on the active RP that had been a standby RP and became the active RP after the most recent stateful switchover (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).
  1 ARP entry in the synchronization queue.
  1 ARP entry waiting to be synchronized.
  No synchronization packet 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.
  808 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
  2 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.
```

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).
  2 ARP entries in the backup table.
  806 synchronization packets processed.
  No synchronization packet dropped in invalid state.
  No error in decoding interface names.
```

Table 3 describes the significant fields shown in the display collected for an active RP.

Table 3 show arp ha Field Descriptions for Statistics Collected for an Active RP

Field	Description
ARP HA in active state	The current state that the event-driven state machine contains for the active RP: • 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. • 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 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 entries in the synchronization queue	Number of ARP entries that are queued to be synchronized or have already been synchronized to the standby RP. **Note** Entries that have already been synchronized are kept in the synchronization queue in case the standby RP crashes. After the standby RP reboots, the entire queue (including entries that were already synchronized to the standby RP before the crash) must be bulk-synchronized to the standby RP.
ARP entries waiting to be synchronized	Number of ARP entries that are queued to be synchronized to the standby RP.
synchronization packets sent	Number of synchronization packets that have been sent to the standby RP.
error in allocating synchronization packets	Number of errors that occurred while synchronization packets were being allocated.
error in sending synchronization packets.	Number of errors that occurred while synchronization packets were being sent to the standby RP.
error in encoding interface names	Number of errors that occurred while interface names were being encoded.

Table 4 describes the significant fields shown in the display collected for a standby RP or for an active RP that was previously in the active state.

Table 4 show arp ha Field Descriptions for Statistics Collected for a Standby RP

Field	Description
ARP HA in standby state	The current state that the event-driven state machine contains for the standby RP: • 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.
ARP entries in the backup table	Number of ARP entries contained in the backup ARP table.
synchronization packets processed	Number of synchronization packets that were processed.
synchronization packet dropped in invalid state	Number of synchronization packets that were dropped due to an invalid state.
error in decoding interface names	Number of errors that occurred in decoding interface names.
ARP entries restored before timer	Number of ARP entries that the new active RP restored prior to expiration of the “flush” timer.
ARP entry restored on timer	Number of ARP entries that the new active RP restored upon expiration of the “flush” timer.
ARP entry purged since interface is down	Number of ARP entries that the new active RP purged because the interface went down.
ARP entry purged on timer	Number of ARP entries that the new active RP purged upon expiration of the “flush” timer.

Related Commands

Command	Description
clear arp-cache counters ha	Resets the ARP HA statistics.
debug arp	Enables debugging output for ARP packet transactions.
show arp	Displays ARP table entries.
show arp application	Displays only the ARP table entries for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp summary	Displays the number of the ARP table entries of each mode.

show arp summary

To display the total number of Address Resolution Protocol (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, use the **show arp summary** command in user EXEC or privileged EXEC mode.

show arp summary

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)ZW	This command was introduced.

Usage Guidelines

Use this command to display high-level statistics about the ARP table entries:

- Total number of ARP table entries
- Number of ARP table entries for each ARP mode
- Number of ARP table entries for each router interface

Examples

The following is sample output from the **show arp summary** command:

```
Router# show arp summary

Total number of entries in the ARP table: 63928.
Total number of Dynamic ARP entries: 63925.
Total number of Incomplete ARP entries: 0.
Total number of Interface ARP entries: 2.
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.

Interface               Entry Count
GigabitEthernet5/2                1
GigabitEthernet5/1            63926
EOBC0/0                           1
```

Related Commands

Command	Description
clear arp-cache	Refreshes dynamically learned entries in the ARP cache.
show arp	Displays ARP table entries.

Command	Description
show arp application	Displays only the ARP table entries for a specific ARP application or for all applications supported by ARP and running on registered clients.
show arp ha	Displays the ARP HA status and statistics.

Feature Information for ARP Rewrite

Table 5 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 5 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 5 Feature Information for ARP Rewrite

Feature Name	Releases	Feature Information
ARP Rewrite	12.2(33)ZW	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/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**

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).

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.

dCEF—distributed Cisco Express Forwarding. A mode of CEF switching in which line cards (such as Versatile Interface Processor [VIP] line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching 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.

EtherTalk—Apple Computer's data-link product that allows an AppleTalk network to be connected by Ethernet cable.

FIB—Forwarding Information Base. Next-hop address information that is based on the information in the IP routing table and is used by CEF to make IP destination prefix-based switching decisions.

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

HSRP—Hot Standby Routing Protocol. Provides high network availability and transparent network topology changes. HSRP creates a Hot Standby router group with a lead router that services all packets sent to the Hot Standby address. The lead router is monitored by other routers in the group, and if it fails, one of these standby routers inherits the lead position and the Hot Standby group address.

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.

LLC—Logical Link Control. The higher of the two data link layer sublayers defined by the IEEE. The LLC sublayer handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants. *See also* MAC.

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.

QoS—quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

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.*

SMDS—Switched Multimegabit Data Service. High-speed, packet-switched, datagram-based WAN networking technology offered by the telephone companies.

SNAP—Subnetwork Access Protocol. Internet protocol that operates between a network entity in the subnetwork and a network entity in the end system. SNAP specifies a standard method of encapsulating IP datagrams and ARP messages on IEEE networks. The SNAP entity in the end system makes use of the services of the subnetwork and performs three key functions: data transfer, connection management, and QoS selection.

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.

Stateful failover—Stateful failover for the Cisco IOS firewall enables a router to continue processing and forwarding firewall session packets after a planned or unplanned outage occurs. You employ a backup (secondary) router that automatically takes over the tasks of the active (primary) router if the active router loses connectivity for any reason. This process is transparent and does not require adjustment or reconfiguration of any remote peer.

Stateful failover for the Cisco IOS firewall is designed to work in conjunction with stateful switchover (SSO) and Hot Standby Routing Protocol (HSRP). To configure stateful failover for the Cisco IOS firewall, a network administrator should enable HSRP, assign a virtual IP address, and enable the SSO protocol.

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.