Contents

1 Configuring ARP....1
1.1 Introduction....1
1.1.1 Overview....1
1.1.2 Basic Concepts....1
1.1.3 Principles....2
1.1.4 Protocols and Standards....5
1.2 Configuration Task Summary....5
1.3 Configuring a Static ARP Entry....6
1.3.1 Overview....6
1.3.2 Restrictions and Guidelines....6
1.3.3 Procedure....6
1.4 Configuring Dynamic ARP Learning Attributes....7
1.4.1 Overview....7
1.4.2 Configuration Tasks....7
1.4.3 Configuring the ARP Timeout Time....7
1.4.4 Configuring ARP Request Retransmission....8
1.4.5 Disabling Dynamic ARP Learning....8
1.4.6 Configuring Strict Dynamic ARP Learning....9
1.4.7 Configuring ARP Scanning....9
1.4.8 Configuring Scheduled Automatic ARP Scanning....10
1.5 Configuring ARP Entry Management....10
1.5.1 Overview....10

1.5.2 Configuration Tasks....11
1.5.3 Configuring a Limit on the Number of Unresolved ARP Entries....11
1.5.4 Configuring an ARP Learning Limit for an Interface....11
1.5.5 Configuring Fast ARP Entry Aging for an Interface....12
1.5.6 Configuring ARP Packet Rate Statistics Collection....12
1.5.7 Configuring the ARP Alarm Rate Limit....13
1.6 Enabling Trusted ARP....13
1.6.1 Overview....13
1.6.2 Procedure....13
1.7 Enabling Gratuitous ARP....14
1.7.1 Overview....14
1.7.2 Restrictions and Guidelines....14
1.7.3 Procedure....14
1.8 Enabling Proxy ARP....15
1.8.1 Overview....15
1.8.2 Restrictions and Guidelines....15
1.8.3 Procedure....15
1.9 Configuring Local Proxy ARP....15
1.9.1 Overview....15
1.9.2 Restrictions and Guidelines....15
1.9.3 Procedure....15
1.10 Configuring Any IP ARP....16
1.10.1 Overview....16
1.10.2 Restrictions and Guidelines....16

1.10.3 Procedure....16
1.11 Enabling ARP Trust Detection....17
1.11.1 Overview....17
1.11.2 Restrictions and Guidelines....17
1.11.3 Procedure....17
1.12 Enabling ARP-based IP Guard....18
1.12.1 Overview....18
1.12.2 Procedure....18
1.13 Configuring ARP Packet Filtering....18
1.13.1 Overview....18
1.13.2 Procedure....18
1.14 Restraining the Device from Sending ARP Requests to Authenticated VLANs....19
1.14.1 Overview....19
1.14.2 Restrictions and Guidelines....19
1.14.3 Procedure....19
1.15 Configuring Host Existence Judgment Prior to Proxy ARP Service....20
1.15.1 Overview....20
1.15.2 Restrictions and Guidelines....20
1.15.3 Procedure....20
1.16 Configuring ARP Entry Update During Active/Standby Switchover....20
1.16.1 Overview....20
1.16.2 Procedure....21
1.17 Sending ARP Requests to a Specific Sub VLAN....21
1.17.1 Overview....21

1.17.2 Procedure.....21

1.18 Monitoring.....21

1.19 Configuration Examples.....23

1.19.1 Configuring Proxy ARP.....23

1 Configuring ARP

1.1 Introduction

1.1.1 Overview

If two IP-enabled hosts need to communicate, a sender must learn the IP address and media access control (MAC) address of the receiver. With the MAC address, the sending host encapsulates IP datagrams into the data link layer (DLL) frames and transmits them over the physical network. The process of converting an IP address to a MAC address is called address resolution. There are two types of address resolution: Address Resolution Protocol (ARP) and proxy ARP.

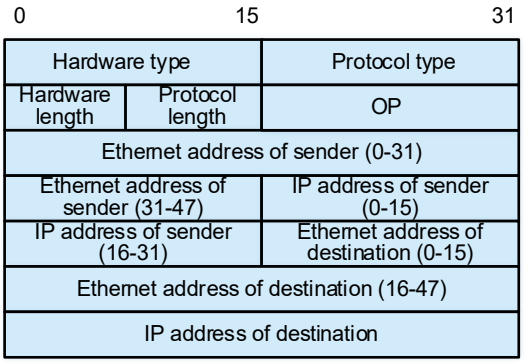
ARP maps an IP address into a MAC address. The mappings of IP and MAC addresses are stored in the ARP cache of the network device.

1.1.2 Basic Concepts

1. ARP Messages

An ARP message can be an ARP request or ARP reply. The format of an ARP message is as follows:

Figure 1-1ARP Message Format



The description of fields in the ARP message is as follows:

- Hardware type: Indicates the type of a hardware address. For an Ethernet network, this value is **1**.
- Protocol type: Indicates the type of the protocol address to be mapped. For the IP protocol, this value is **0x0800**.
- Hardware length: Indicates the length of a hardware address, in bytes. For an Ethernet network, this value is **6**.
- Protocol length: Indicates the length of a protocol address, in bytes. For ARP requests or replies, this value is **4**.
- OP: Indicates the operation type. **1** indicates ARP requests, and **2** indicates ARP replies.
- Ethernet address of sender: Indicates a source MAC address, that is, the hardware address of a sender

device.

- IP address of sender: Indicates a source IP address, that is, the IP address of a sender device.
- Ethernet address of destination: Indicates a destination MAC address, that is, the hardware address of a destination device. The value of this field is 0x00-00-00-00-00-00 for ARP requests.
- IP address of destination: Indicates a destination IP address, that is, the IP address of a destination device.

2. ARP Table

Each host maintains an ARP table that contains the mappings between IP addresses and MAC addresses. The mappings are called ARP entries.

Before sending an IP packet, a host first searches the ARP table for the MAC address corresponding to the destination IP address. If there is a corresponding MAC address in the ARP table, the host sends the IP packet directly to the MAC address instead of sending an ARP request message. If there is no corresponding MAC address in the ARP table, the host broadcasts an ARP request message to request the MAC address of the destination host. ARP entries can help greatly reduce the network traffic.

ARP entries can be classified as dynamic ARP entries or static ARP entries. The difference between them is as follows:

- Dynamic ARP entries are automatically generated and updated by the ARP protocol that exchanges ARP messages among devices, and will be aged and overwritten by new dynamic ARP entries.
- Static ARP entries are manually configured and maintained by the network administrator, and will not be aged or overwritten by dynamic ARP entries.

1.1.3 Principles

1. Static ARP Entries

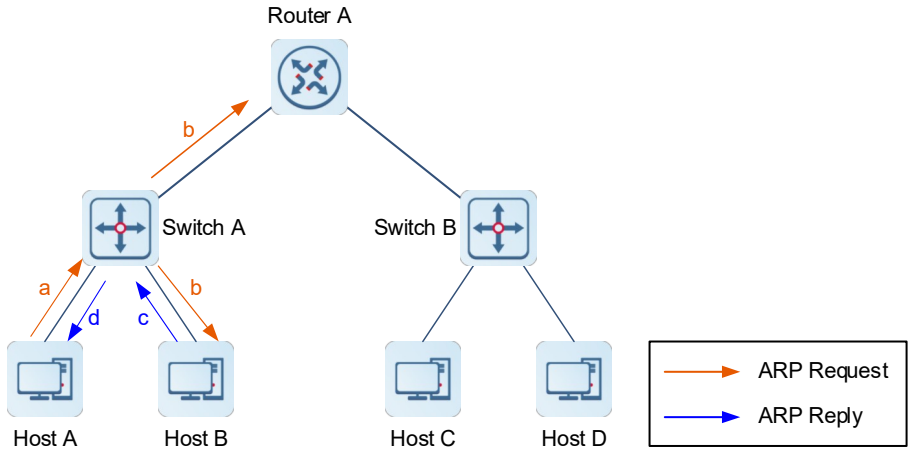
Static ARP entries are fixed mappings of IP and MAC addresses and they are created manually by the network administrator. The device cannot update the ARP entries. Static ARP entries can be deployed when communication security is a priority and network resources are sufficient.

2. Dynamic ARP Entries

Dynamic ARP allows devices to dynamically learn and update the mappings between IP and MAC addresses by exchanging ARP messages. Dynamic ARP entries can be deployed when real-time communication is priority or network resources are insufficient.

- **ARP implementation in the same network segment**

Figure 1-1ARP Implementation in the Same Network Segment



As illustrated in Figure 1-1, host A has learned the IP address of host B and wants to send IP packets to host B. The address resolution process is as follows:

a Host A looks up in its ARP table and does not find the mapping between the IP and MAC addresses of host B. Host A then broadcasts an ARP request to request the MAC address of host B.

b After switch A receives the ARP request, switch A broadcasts the ARP request on the local network segment.

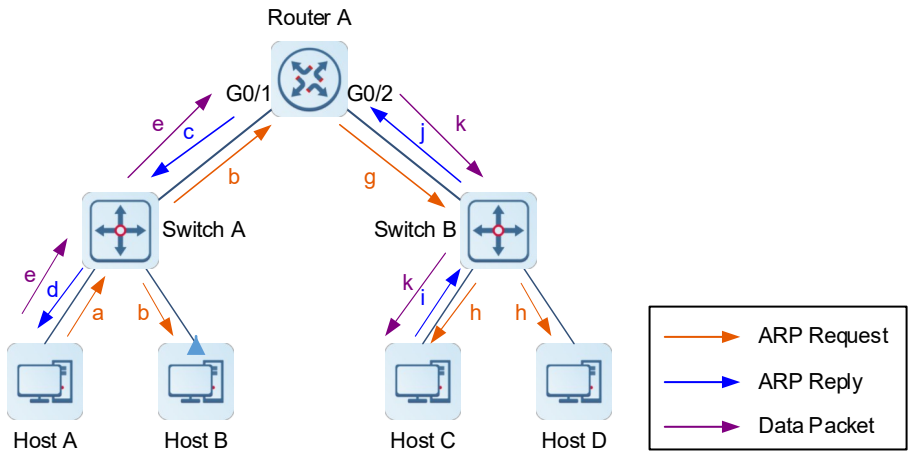
c After host B receives the ARP request, host B adds the MAC address of host A to its ARP table, and sends an ARP reply to host A. Since the destination IP address of the ARP request is not the IP address of router A, router A directly discards the ARP request after receiving it.

d Switch A forwards the ARP reply to the destination host A after receiving it.

e After host A receives the ARP reply, host A adds the MAC address of host B to its ARP table and sends the IP packets to host B.

- **ARP implementation in different network segments**

Figure 1-2ARP Implementation in Different Network Segments



As illustrated in Figure 1-2, host A has learned the IP address of host C. For example, when host A sends an IP packet to host C, the address resolution process is as follows:

a Host A looks up in its ARP table and does not find the mapping between IP and MAC addresses of port GigabitEthernet 0/1 on the default gateway router A that is reachable to host C. Host A then sends an ARP broadcast request to request the MAC address of port GigabitEthernet 0/1 of router A.

a After receiving the ARP request, switch A broadcasts the packet on the local network segment.

b After receiving the ARP request, router A adds the MAC address of host A into its ARP table, and sends an ARP reply to host A. Since the destination IP address of the ARP request is not the IP address of host B, host B directly discards the ARP request after receiving it.

c Switch A forwards the ARP reply to the destination host A after receiving it.

d After receiving the ARP reply, host A adds the MAC address of port GigabitEthernet 0/1 of router A into its ARP table and sends the IP packet to router A.

e Router A looks up in the routing table and sends the IP packet from port GigabitEthernet 0/1 to port GigabitEthernet 0/2.

f Router A looks up in its ARP table and finds that there is no MAC address of host C. Router A then sends an ARP broadcast request to request the MAC address of host C.

g After switch B receives the ARP request, switch B broadcasts the packet on the local network segment.

h After host C receives the ARP request, host C adds the MAC address of port GigabitEthernet 0/2 of router A into its ARP table, and sends an ARP reply to router A. Since the destination IP address of the ARP request is not the IP address of host D, host D directly discards the ARP request after receiving it.

i Switch B forwards the ARP reply to the destination router A after receiving it.

j After router A receives the ARP reply, router A adds the MAC address of host C into its ARP table and sends the IP packet to host C.

3. Trusted ARP

When a user goes online on a GPRS support node (GSN) client, the authentication server obtains the user's real the mapping between IP and MAC addresses through the access switch, and adds trusted ARP entries on the user's gateway switch. This process is transparent to network administrators and does not require their extra work.

Trusted ARP entries have characteristics of both static and dynamic ARP entries, with a priority higher than that of dynamic ARP entries and lower than that of static ARP entries. Trusted ARP entries have an aging mechanism similar to that of dynamic ARP entries. When an ARP entry ages, the device actively sends an ARP request to detect whether the peer host exists. If the host sends a reply, the device regards the host active and updates the aging time of the ARP entry. Otherwise, the device deletes the ARP entry. Trusted ARP entries have characteristics of static ARP entries. The device cannot dynamically update information about the MAC addresses and interfaces in the trusted ARP entries by learning ARP messages.

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeting the gateway.

4. Gratuitous ARP

A gratuitous ARP message is a special ARP message. In a gratuitous ARP message, both the source and the destination IP addresses carried are the IP address of the local device.

Gratuitous ARP packets have the following purposes:

- Detecting IP address conflict If the device receives a gratuitous ARP packet and finds that the IP address in

the packet is the same as its own IP address, it sends an ARP reply to notify the peer of the IP address conflict.

- Sending a gratuitous ARP packet to notify other devices to update ARP entries when the interface MAC address of a device changes. For example, in dual-node hot standby mode, when services are switched from the master device to the slave device, the MAC address of the previously slave device in the ARP entries on the connected device needs to be updated as that of the current master device. Generally, when services are switched from the master device to the slave device, the new master device after switchover sends a gratuitous ARP request to the network to notify other devices to update their ARP entries.
- Updating ARP entries based on gratuitous packets After receiving a gratuitous ARP message, the device checks whether a dynamic ARP entry corresponding to the source IP address in the gratuitous ARP packet exists. If yes, the device updates the ARP entry based on the information carried in the gratuitous ARP packet.

5. Proxy ARP

Proxy ARP allows devices on different subnets to resolve IP addresses into MAC addresses. If a device receives an ARP request whose source IP address is on a different network segment from the destination IP address and knows the route to the destination IP address, the device sends an ARP reply containing its own MAC address.

6. Local Proxy ARP

Local proxy ARP means that a device acts as a proxy ARP in the same virtual local area network (VLAN) that can be a common VLAN or sub VLAN.

After local proxy ARP is enabled on a device, the device can help hosts obtain the MAC addresses of other hosts in the VLAN. When port protection is enabled on the device, hosts connected to different ports are isolated at Layer 2. After receiving an ARP request, the device with local proxy ARP enabled serves as a proxy to send an ARP reply with its own Ethernet MAC address. In this case, hosts communicate with each other through Layer 3 routes.

7. Any IP ARP

Any IP ARP allows a device to access the network with any IP address. For example, a user is using a laptop in a hotel and wants to access the Internet without changing the configured IP address and gateway. After the gateway receives an ARP request and finds that the source IP address of the sender is in a different subnet and the destination address may not be its own address, the gateway still sends an ARP reply, with the MAC address of the gateway's Ethernet MAC address, and creates a direct route for the host.

1.1.4 Protocols and Standards

- RFC 826: An Ethernet Address Resolution Protocol
- RFC 1027: Using ARP to implement transparent subnet gateways

1.2 Configuration Task Summary

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring a Static ARP Entry
- Configuring Dynamic ARP Learning Attributes

- Configuring ARP Entry Management
- Enabling Trusted ARP
- Enabling Gratuitous ARP
- Enabling Proxy ARP
- Configuring Local Proxy ARP
- Configuring Any IP ARP
- Configuring other advanced ARP functions
  - Enabling ARP Trust Detection
  - Enabling ARP-based IP Guard
  - Configuring ARP Packet Filtering
  - Restraining the Device from Sending ARP Requests to Authenticated VLANs
  - Configuring Host Existence Judgment Prior to Proxy ARP Service
  - Configuring ARP Entry Update During Active/Standby Switchover
  - Sending ARP Requests to a Specific Sub VLAN

1.3 Configuring a Static ARP Entry

1.3.1 Overview

Users can manually configure static ARP entries to prevent the device from learning incorrect ARP entries, thus affecting the network connectivity.

1.3.2 Restrictions and Guidelines

After a static ARP entry is configured on an Layer 3 switch, the Layer 3 switch performs routing only after learning the physical port corresponding to MAC address carried in the static ARP entry.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a static ARP entry.

arp [**vrf** *vrf-name* | **oob** [*mgmt-name*]] *ip-address mac-address arp-type*

No static ARP entry is configured by default.

1.4 Configuring Dynamic ARP Learning Attributes

1.4.1 Overview

The dynamic ARP learning function is enabled by default. You can configure ARP learning attributes as needed, for example, specify ARP entry timeout time, the number of times and interval that an ARP request

can be transmitted consecutively, strict dynamic ARP learning function, ARP scanning, and scheduled automatic ARP scanning.

1.4.2 Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring the ARP Timeout Time
- Configuring ARP Request Retransmission
- Disabling Dynamic ARP Learning
- Configuring Strict Dynamic ARP Learning
- Configuring ARP Scanning
- Configuring Scheduled Automatic ARP Scanning

1.4.3 Configuring the ARP Timeout Time

1. Overview

Before an ARP entry times out, the device sends a unicast ARP request to detect whether the peer is online. If the device receives an ARP reply from the peer, it means that the peer is still online and the ARP entry is reserved. Otherwise, this ARP entry will be deleted. The ARP timeout time can be set as required.

2. Restrictions and Guidelines

The ARP timeout configuration only applies to dynamic mappings between IP and MAC addresses. When the ARP timeout time is set to a smaller value, the mapping table stored in the ARP cache is more accurate but ARP consumes more network bandwidth. In general, the ARP timeout time does not need to be set.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the ARP timeout time.

arp timeout *time*

The default timeout time of dynamic ARP entries in the ARP cache is **3600** seconds.

1.4.4 Configuring ARP Request Retransmission

1. Overview

The device sends a certain number of ARP requests at a certain time interval during address resolution until the device receives an ARP reply. This function is used to configure the interval and number of times that an ARP request can be transmitted consecutively.

2. Restrictions and Guidelines

The shorter the retransmission interval is, the faster the resolution is. The more times the ARP request can be transmitted consecutively, the more likely the resolution will succeed and the more bandwidth ARP will be consumed.

If the network resources are insufficient, you are advised to set the ARP request retransmission interval to a larger value and the number of retransmission times to a smaller value, to reduce bandwidth consumption.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the ARP request retransmission interval.

arp retry interval *interval*

The default ARP request retransmission interval is 1 second.

(5) Configure the number of times that an ARP request can be transmitted consecutively.

arp retry times *times*

The default number of times that an ARP request can be transmitted consecutively is 5. That is, if no ARP reply packet is received, the ARP request packet will be retransmitted for four consecutive times.

1.4.5 Disabling Dynamic ARP Learning

1. Overview

The dynamic ARP learning function can be disabled on an interface. Then, the interface will not perform dynamic ARP learning.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Disable dynamic ARP learning.

no arp-learning enable

The ARP learning function is enabled by default.

1.4.6 Configuring Strict Dynamic ARP Learning

1. Overview

After this function is enabled on a device, only the ARP replies in response to the ARP requests actively sent by the device can trigger the device to learn ARP entries.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) (Optional) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable strict dynamic ARP learning.

arp strict-learning enable

Strict dynamic ARP learning is disabled by default.

1.4.7 Configuring ARP Scanning

1. Overview

This function is usually used together with the Web-based dynamic-to-static ARP entry conversion function. After ARP scanning is enabled on an interface, the device scans neighbors in the specified range and learns the ARP entries of these neighbors.

2. Restrictions and Guidelines

The device can scan the neighbors in the network segments, to which the primary IP address and secondary IP addresses belong, on an interface or scans only the neighbors in the specified address range. ARP scanning takes effect once after it is configured, and can be executed when the Layer 3 interface is up (that is, the link is up and an IP address is configured for the interface). However, ARP scanning configuration cannot be saved and will lose effect the next time.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable ARP scanning.

arp scan [*start-ip-address end-ip-address*]

ARP scanning is disabled by default.

1.4.8 Configuring Scheduled Automatic ARP Scanning

1. Overview

After scheduled automatic ARP scanning is enabled on an interface, the device scans neighbors in the specified range and learns the ARP entries of these neighbors. If ARP entries are not learned from neighbors, after the current scanning ends, the device waits for the scanning interval (5 minutes by default) and then starts next scanning until the entries are learned.

2. Restrictions and Guidelines

- Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.
- The scanning interval ranges from 1 to 30, in minutes.
- The scanning rate ranges from 1 to 100, in IP addresses per second.
- Up to 30 instances can be configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable scheduled automatic ARP scanning.

arp scan auto [*start-ip-address end-ip-address*]

The scheduled automatic ARP scanning function is disabled by default.

(5) (Optional) Configure the scheduled automatic ARP scanning interval.

arp scan interval *time*

The default interval of scheduled automatic ARP scanning is 5 minutes.

(6) (Optional) Configure the scheduled automatic ARP scanning rate.

arp scan rate *rate-value*

The default scheduled automatic ARP scanning rate is **20** IP addresses per second.

1.5 Configuring ARP Entry Management

1.5.1 Overview

Entries in the ARP cache can be managed as required, such as limiting the capacity of ARP entries and configuring fast aging of ARP entries.

1.5.2 Configuration Tasks

All the configuration tasks below are optional. Perform the configuration tasks as required.

- Configuring a Limit on the Number of Unresolved ARP Entries
- Configuring an ARP Learning Limit for an Interface
- Configuring Fast ARP Entry Aging for an Interface
- Configuring ARP Packet Rate Statistics Collection
- Configuring the ARP Alarm Rate Limit

1.5.3 Configuring a Limit on the Number of Unresolved ARP Entries

1. Overview

In a local area network (LAN), ARP attacks and scanning may cause a large number of unresolved ARP entries generated on the gateway. As a result, the gateway fails to learn the MAC addresses of the hosts. To prevent this situation, if a large number of unresolved entries exist in the ARP cache and remain in the table after a while, you are advised to use this command to limit the number of unresolved ARP entries.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure a limit on the number of unresolved ARP entries.

arp unresolve *unresolved-number*

The maximum number of unresolved ARP entries that can be held in an ARP cache is the total capacity of ARP entries by default.

1.5.4 Configuring an ARP Learning Limit for an Interface

1. Overview

Limiting the number of ARP entries that can be learned by an interface can flexibly control the on-demand assignment of ARP entry resources, to prevent resource waste. In addition, this can prevent malicious ARP attacks. When the device is attacked maliciously and the ARP entry learning number is not limited, the device will generate a large number of ARP entries, which occupy excessive entry resources.

2. Restrictions and Guidelines

The configured value must be equal to or greater than the number of the ARP entries learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an ARP learning limit for the interface.

arp cache interface-limit *limit*

The number of ARP entries that can be learned by an interface is not limited by default.

1.5.5 Configuring Fast ARP Entry Aging for an Interface

1. Overview

If a host goes offline or encounters an abnormal condition, the device fails to learn the ARP entry. When the MAC address corresponding to the ARP entry ages, the dynamic ARP entry starts aging one hour after the aging time by default. If this feature is enabled on an interface, after the MAC address ages, the dynamic ARP entry ages rapidly to realize fast route convergence of the host.

2. Restrictions and Guidelines

- This function can be configured only on SVIs and OverlayRouter interfaces.
- When the conversion of ARP entries into host routes is enabled on the device, you are advised to also enable this function to help achieve fast route convergence.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable fast ARP entry aging.

arp fast-aging enable

The fast ARP entry aging function is disabled by default.

1.5.6 Configuring ARP Packet Rate Statistics Collection

1. Overview

After this function is enabled, the device collects statistics on ARP messages received by each interface in a fixed period of time by replies, requests, and unknown packets.

2. Restrictions and Guidelines

The default statistics collection interval is 5 seconds. If there are many interfaces and the rate is not as expected, appropriately adjust the statistics collection interval. The minimum statistics collection interval can be set to 1 second.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ARP packet rate statistics collection.

arp rate-statistic enable

The ARP packet rate statistics collection is disabled by default.

(4) (Optional) Configure the interval for ARP packet rate statistics collection.

arp rate-statistic compute interval *interval*

The default interval for collecting ARP packet rate statistics is 5 seconds.

1.5.7 Configuring the ARP Alarm Rate Limit

1. Overview

You can configure the ARP alarm rate limit to adjust the printing rate of ARP syslog alarms.

2. Restrictions and Guidelines

The actual ARP alarm rate may be lower than the configured rate, depending on system performance.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the ARP alarm rate limit.

arp warning-limit interval *interval* **times** *time*

The default ARP alarm rate limit interval is 50 seconds and the default upper limit of alarms allowed within this interval is 10.

1.6 Enabling Trusted ARP

1.6.1 Overview

Since trusted ARP entries come from authentic sources and will not be updated, they can efficiently prevent ARP spoofing targeting the gateway.

1.6.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable trusted ARP.

service trustedarp

Trusted ARP is disabled by default.

(4) (Optional) Enable VLAN translation when a trusted ARP entry is added.

arp trusted user-vlan *vlan-id* **translated-vlan** *vlan-id*

The VLAN translation is disabled when a trusted ARP entry is added by default.

Configure this command only when the VLAN delivered by the server differs from the valid VLAN in the trusted ARP entry.

(5) (Optional) Enable trusted ARP aging.

arp trusted aging

Trusted ARP entries are not aged by default.

After you configure this command, trusted ARP entries begin to age, and the aging time is the same as that of dynamic ARP entries. You can run the **arp timeout** command in interface configuration mode to set the aging time.

(6) (Optional) Adjust the capacity of trusted ARP entries.

arp trusted *number*

The maximum number of trusted ARP entries is half of the capacity of the ARP table by default.

Trusted ARP entries and other entries share the memory. If trusted ARP entries occupy much space, dynamic ARP entries may not have sufficient space. Set the capacity based on the actual requirement. Do not set it to an excessively large value.

1.7 Enabling Gratuitous ARP

1.7.1 Overview

Gratuitous ARP packets are special ARP messages. In a gratuitous ARP message, the source and destination IP addresses are the IP address of the local device. This function enables an interface to periodically send gratuitous ARP packets.

1.7.2 Restrictions and Guidelines

Generally, you need to enable this function on an interface that serves as the gateway of downlink devices so that the MAC address of the gateway of the downlink devices are updated periodically to prevent others from faking the gateway.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the function of sending gratuitous ARP requests.

arp gratuitous-send enable

The function of sending gratuitous ARP requests is enabled by default.

(5) Configure the interval for sending gratuitous ARP requests.

arp gratuitous-send interval *interval* [*number*]

The function of sending gratuitous ARP requests at intervals is disabled by default.

1.8 Enabling Proxy ARP

1.8.1 Overview

The device acts as a proxy to reply to ARP requests from other hosts. If a device receiving an ARP request finds the source IP address in a different network from the destination IP address and knows the route to the destination address, the device sends an ARP reply containing its own Ethernet MAC address.

1.8.2 Restrictions and Guidelines

By default, proxy ARP is disabled on Layer 3 switches.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enables proxy ARP.

ip proxy-arp

Proxy ARP is disabled by default.

1.9 Configuring Local Proxy ARP

1.9.1 Overview

After local proxy ARP is enabled, the device can help hosts obtain the MAC addresses of other hosts in the same subnet.

1.9.2 Restrictions and Guidelines

This function can be configured only on SVIs.

1.9.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enables local proxy ARP.

local-proxy-arp

Local proxy ARP is disabled by default.

1.10 Configuring Any IP ARP

1.10.1 Overview

Users can access the network with any IP address. This applies when a user uses a laptop in a hotel and wants to access the Internet without changing the configured IP address and gateway.

1.10.2 Restrictions and Guidelines

This function is not applicable in the following two scenarios, in which a user must modify the configuration before accessing the Internet.

- The user's IP address is in the same network segment as the interface directly connected to the device. However, the configured gateway IP address is not the IP address configured for the interface directly connected to the device.
- The user's IP address is not in the same network segment as the interface directly connected to the device, but in the network segment of another interface. That means an IP address conflict occurs.

  As the user's IP address is not in the same network segment as the interface directly connected to the device, the dynamic ARP entry and direct route are generated only when the user initiates an ARP request. Therefore, in some scenarios (including but not limited to the following ones), the user will not be able to access the Internet unless the ARP entry is cleared and the gateway address is relearned on the user host.

  - The device acts as a proxy to respond to ARP requests. After the user host learns the MAC address of the device, the administrator deletes the dynamic ARP entry on the device. As a result, the user's dynamic ARP entry and direct route are removed and the user cannot receive the reply.
    - The device acts as a proxy to respond to ARP requests. After the user host learns the MAC address of the device, if any IP ARP is disabled and then enabled again on the interface, the user cannot receive the reply The cause is that the user's dynamic ARP entry and direct route are immediately deleted when the any IP ARP function is disabled on the interface.

⚠ Caution

If static ARP entries or the ARP entries involving the Virtual Router Redundancy Protocol (VRRP) IP addresses exist, dynamic ARP entries generated by any IP ARP will be overwritten or fail to be added, and any IP ARP does not take effect.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable any IP ARP.

arp any-ip

The any IP ARP function is disabled by default.

1.11 Enabling ARP Trust Detection

1.11.1 Overview

ARP trust detection is used to prevent excessive useless ARP entries generated due to ARP spoofing from occupying device resources. After ARP trust detection is enabled on an Layer 3 interface and the device receives an ARP request from this interface:

(2) If the corresponding entry does not exist, the device creates a dynamic ARP entry and performs neighbor unreachability detection (NUD) after 1 to 5 seconds. That is, the device ages the newly learned ARP entry and sends a unicast ARP request. If the device receives an ARP update packet from the peer within the aging time, it stores the entry. Otherwise, it deletes the entry.

(3) If the corresponding ARP entry exists, the device does not perform NUD.

(4) If the MAC address in the existing dynamic ARP entry is updated, the device performs NUD.

1.11.2 Restrictions and Guidelines

- Since this function adds a strict confirmation procedure in the ARP learning process, it affects the efficiency of ARP learning.
- After this function is disabled, the device no longer performs NUD for learning or updating ARP entries.

1.11.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable ARP trust detection.

arp trust-monitor enable

ARP trust detection is disabled by default.

1.12 Enabling ARP-based IP Guard

1.12.1 Overview

When receiving unresolved IP packets, the device cannot forward them through the hardware but sends them to the CPU for address resolution, that is, ARP learning. If a large number of such packets are sent to the CPU, the CPU will be congested, affecting other services on the device.

After ARP-based IP guard is enabled, the device will count the number of received ARP packets based on the destination IP address. When the number of packets with the same destination IP address exceeds a certain threshold, the device deems it as a CPU attack and will send a drop entry to the hardware so that the hardware will not send subsequent ARP packets with this destination IP address to the CPU. After the address resolution is complete, the device updates the entry to the forwarding state and continues to forward the packets with this destination IP address.

1.12.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ARP-based IP guard.

arp anti-ip-attack *attack-num*

The default number of IP packets for triggering the discarding of ARP entries is 3.

1.13 Configuring ARP Packet Filtering

1.13.1 Overview

- ARP packet filtering supports the following functions:
  Filters out received gratuitous APR packets.
- Filters out ARP packets that hit ACL rules.
- Filters out ARP packets whose source MAC addresses is not consistent with the Ethernet source MAC address.
- Filters out ARP packets whose destination MAC addresses is not consistent with the Ethernet destination MAC address.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure ARP packet filtering. Perform at least one of the following configuration steps:

- Enable gratuitous ARP filtering.

  arp filter gratuitous

  Gratuitous ARP filtering is disabled by default.
- Enable ARP-based ACL filtering.

  arp filter acl *acl-number*

  ARP-based ACL filtering is disabled by default.
- Enables the function of checking the source MAC addresses of ARP packets.

arp filter smac-illegal

The function of checking the source MAC addresses of ARP packets is disabled by default.

- Enable the function of checking the destination MAC addresses of ARP packets.

  arp filter dmac-illegal

  The function of checking the destination MAC addresses of ARP packets is disabled by default.

1.14 Restraining the Device from Sending ARP Requests to Authenticated VLANs

1.14.1 Overview

In gateway authentication mode, all sub VLANs in a super VLAN are authenticated VLANs by default. Users in an authenticated VLAN have to pass authentication to access the network. After authentication, a static ARP entry is generated on the device. Therefore, when accessing an authenticated user, the device does not need to send ARP requests to the authenticated VLAN. If the device attempts to access users in an authentication-exempt VLAN, it only needs to send ARP requests to the authentication-exempt VLAN.

1.14.2 Restrictions and Guidelines

- This function can be configured only on SVIs.
- In gateway authentication mode, the device does not send ARP requests to the authenticated VLANs by default. If the device needs to access authentication-exempt users in an authenticated VLAN, disable this function.

1.14.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the device not to send ARP requests to authenticated VLANs.

arp suppress-auth-vlan-req

ARP requests are not sent to authenticated VLANs by default.

1.15 Configuring Host Existence Judgment Prior to Proxy ARP Service

1.15.1 Overview

When two devices form a VRRP network and local proxy ARP is enabled on them, if the slave VRRP device sends an ARP request to a terminal, the master VRRP device will act as a proxy of the terminal and send an ARP reply to the slave VRRP device regardless of whether the terminal exists. As a result, the slave VRRP device learns a large number of proxy ARP entries.

After the host existence judgment prior to proxy ARP service is enabled, the master VRRP device, upon receiving an ARP request, first judges whether the ARP entry corresponding to the destination IP address exists. If yes, the master VRRP device acts as a proxy ARP. If no, the master VRRP device does not act as a proxy ARP. In addition, the gateway automatically broadcasts an ARP request for the ARP entry corresponding to the destination IP address. This prevents the case that the gateway fails to act as a proxy to respond to an ARP request of the destination ARP address if it does not have an ARP entry corresponding to the destination IP address.

After the host existence judgment prior to proxy ARP service is disabled, if the proxy conditions are met, the master ARP device directly acts as a proxy upon receiving an ARP request, without judging whether the ARP entry corresponding to the destination IP address has been resolved.

1.15.2 Restrictions and Guidelines

The **arp proxy-resolved** command is enabled on devices by default. That is, the master VRRP device responds to an ARP request as a proxy only after the destination IP address has been resolved.

1.15.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the master VRRP device to forcibly respond to ARP requests as a proxy.

no arp proxy-resolved

By default, the master VRRP device judges the existence of the ARP entry corresponding to a destination IP address before the device responds to an ARP request as a proxy ARP.

1.16 Configuring ARP Entry Update During Active/Standby Switchover

1.16.1 Overview

This function can be enabled to quickly update ARP entries of a downlink device after VSU active/standby switchover, especially when the downlink device is similar to a server with dual network interface cards. When the slave device becomes the master, it will actively send ARP requests to SVIs (that are not in a super VLAN) of up to 1000 downlink terminals. After the terminals reply to these ARP requests, the device can update the ARP and MAC tables.

1.16.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the function of actively sending ARP requests to SVIs of downlink terminals during active/standby switchover.

arp switch-over resolve

ARP requests are not actively sent to downlink terminals during VSU active/standby switchover by default.

1.17 Sending ARP Requests to a Specific Sub VLAN

1.17.1 Overview

In a super VLAN scenario, the device actively broadcasts ARP resolution requests to the entire super VLAN by default. If there are many sub VLANs in the super VLAN, the ARP messages will be replicated in large quantities, which will affect device performance.

Most terminals (such as PCs and servers) request ARP information of the gateway before accessing the network. Therefore, there is no need to actively broadcast ARP resolution requests to the sub VLANs where these terminals reside. For dumb terminals (that do not actively send gratuitous ARP packets), this command can be deployed in a specified *vlan-list* to enable the device to actively send ARP resolution requests to these VLANs.

1.17.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable ARP to actively broadcast resolution requests to a specific sub VLAN in a super VLAN.

arp resolve vlan { *vlan-list* | **none** }

ARP does not actively broadcast resolution requests to a specific sub VLAN in a super VLAN by default.

1.18 Monitoring

Run the **show** command to check the configuration.

Run the **debug** command to output debugging information.

Caution

The output debugging information occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** command to clear information.

Caution

Inappropriate use of the **clear** command may lose vital information and thus interrupt services.

Table 1-1Monitoring

Command	Purpose
show arp trusted [*ip-address* [*mask*]]	Displays trusted ARP entries.
clear arp-cache trusted [*ip-address* [*mask*	Clears trusted ARP entries.

]]	
clear arp-cache [[**vrf** *vrf-name* | **oob**] [*ip-address* [*mask*]] | [**interface** *interface-type interface-number*]]	Clears dynamic ARP entries.
clear arp-cache packet statistics [*interface-type interface-number*]	Clears ARP packet statistics.
show arp [**detail**] [*interface-type interface-number* | [**vrf** *vrf-name*] [*ip-address* [*mask*] | *mac-address* | **static** | **complete** | **incomplete**] | **subvlan** { *subvlan-number* | **min-max** *min-value max-value* }]	Displays the ARP table.
show arp oob [*ip-address* [*mask*] | **static** | **complete** | **incomplete** | *mac-address*]	Displays the ARP table on the management interface.
show ip arp [**vrf** *vrf-name*]	Displays the ARP table.
show arp [**detail**] **trusted** [*ip-address* [mask]]	Displays the trusted ARP table.
show arp counter	Displays the count of ARP entries.
show arp timeout	Displays the aging time of dynamic ARP entries.
show arp packet statistics [*interface-type interface-number*]	Displays ARP packet statistics.
show arp rate-statistic [*interface-type interface-number*]	Displays ARP packet rate statistics.
show arp timeout	Displays the aging time of dynamic ARP entries.
show arp flapping record	Displays ARP flapping records.
show arp suppress table [**ip** *ip-address*]	Displays the ARP suppression table.
show arp anti-attack statistics	Displays the statistics on illegal ARP packets.
show arp dynamic-entry-limit	Displays the statistics on the ARP capacity limit of a line card.
debug arp	Displays the statistics on ARP packets sent and received.
debug arp event	Displays the creation and deletion status of ARP entries.

1.19 Configuration Examples

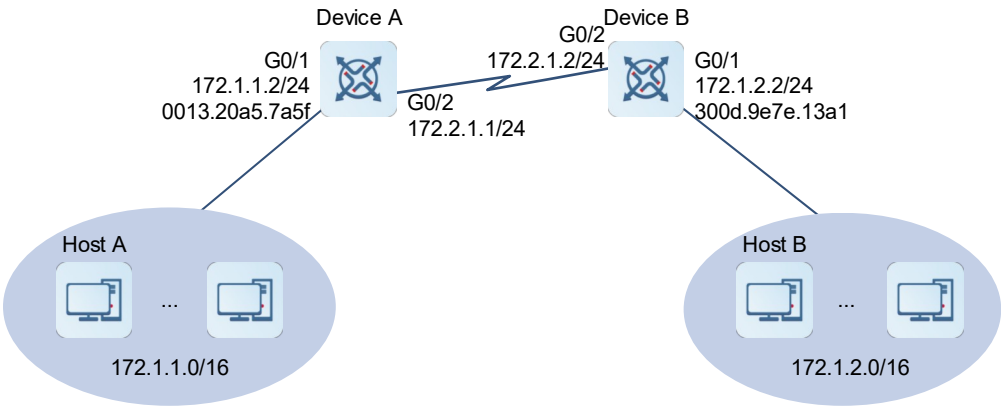
1.19.1 Configuring Proxy ARP

1. Requirements

As shown in Figure 1-1, the IP addresses of host A and host B are on the same network segment, but are isolated in two LANs by routers. Neither of the two hosts is configured with a default gateway, and the two routers are connected over a serial link. Enable proxy ARP on the routers to achieve direct communication between hosts in different LANs.

2. Topology

Figure 1-1Topology of Proxy ARP



3. Notes

- Enable proxy ARP on interfaces of device A and device B that are connected to hosts.
- Configure default routes on device A and device B.

4. Procedure

(1) Configure device A.

Configure an IP address for port GigabitEthernet 0/1.

```
DeviceA> enable
DeviceA# configure terminal
DeviceA(config)# interface gigabitethernet 0/1
DeviceA(config-if-GigabitEthernet 0/1)# ip address 172.1.1.2 24
```

Enable proxy ARP on port GigabitEthernet 0/1.

```
DeviceA(config-if-GigabitEthernet 0/1)# ip proxy-arp
DeviceA(config-if-GigabitEthernet 0/1)# exit
```

Configure an IP address for port GigabitEthernet 0/2.

```
DeviceA(config)# interface gigabitethernet 0/2
DeviceA(config-if-GigabitEthernet 0/2)# ip address 172.2.1.1 24
DeviceA(config-if-GigabitEthernet 0/2)# exit
```

Configure the static route to 172.1.2.0/16.

```
DeviceA(config)# ip route 172.1.2.0 255.255.0.0 gigabitethernet 0/2
```

(2) Configure device B.

Configure an IP address for port GigabitEthernet 0/1.

```
DeviceB> enable
DeviceB# configure terminal
DeviceB(config)# interface gigabitethernet 0/1
DeviceB(config-if-GigabitEthernet 0/1)# ip address 172.1.2.2 24
```

Enable proxy ARP on port GigabitEthernet 0/1.

```
DeviceB(config-if-GigabitEthernet 0/1)# ip proxy-arp
DeviceB(config-if-GigabitEthernet 0/1)# exit
```

Configure an IP address for port GigabitEthernet 0/2.

```
DeviceB(config)# interface gigabitethernet 0/2
DeviceB(config-if-GigabitEthernet 0/2)# ip address 172.2.1.2 24
DeviceB(config-if-GigabitEthernet 0/2)# exit
```

Configure the static route to 172.1.1.0/16.

```
DeviceB(config)# ip route 172.1.1.0 255.255.0.0 gigabitethernet 0/2
```

(3) Configure hosts.

Set the IP address of host A to 10.0.1.1/24.

Set the IP address of host B to 10.0.2.1/24.

5. Verification

Host A can ping host B successfully.

You can check the ARP table of host A and find that the MAC address corresponding to host B is the MAC address of port GigabitEthernet 0/1 on device A.

6. Configuration Files

- Device A configuration file

```
!
hostname DeviceA
ip route 172.1.2.0 255.255.0.0 gigabitethernet 0/2
!
 interface gigabitethernet 0/1
 ip address 172.1.1.2 24
 ip proxy-arp
!
 interface gigabitethernet 0/2
 ip address 172.2.1.1 24
!
```

- Device B configuration file

```
!
hostname DeviceB
ip route 172.1.1.0 255.255.0.0 gigabitethernet 0/2
```

```
!
 interface gigabitethernet 0/1
 ip address 172.1.2.2 24
 ip proxy-arp
!
 interface gigabitethernet 0/2
 ip address 172.2.1.2 24
!
```