Contents

Configuring ARP

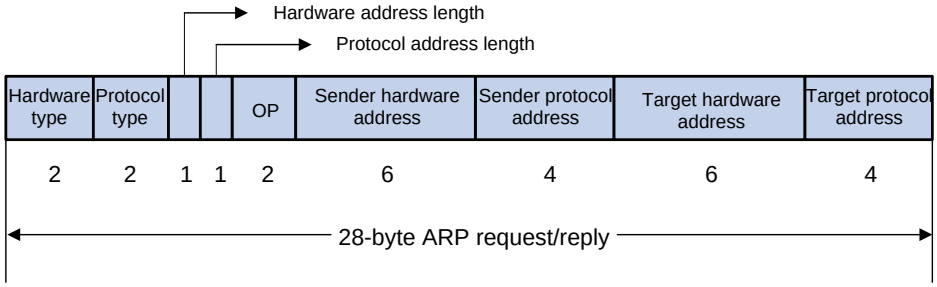
About ARP

ARP resolves IP addresses into MAC addresses on Ethernet networks.

ARP message format

ARP uses two types of messages: ARP request and ARP reply. Figure 1 shows the format of ARP request/reply messages. Numbers in the figure refer to field lengths.

Figure 1 ARP message format



- **Hardware type**—Hardware address type. The value 1 represents Ethernet.
- **Protocol type**—Type of the protocol address to be mapped. The hexadecimal value 0x0800 represents IP.
- **Hardware address length and protocol address length**—Length, in bytes, of a hardware address and a protocol address. For an Ethernet address, the value of the hardware address length field is 6. For an IPv4 address, the value of the protocol address length field is 4.
- **OP**—Operation code, which describes the type of ARP message. The value 1 represents an ARP request, and the value 2 represents an ARP reply.
- **Sender hardware address**—Hardware address of the device sending the message.
- **Sender protocol address**—Protocol address of the device sending the message.
- **Target hardware address**—Hardware address of the device to which the message is being sent.
- **Target protocol address**—Protocol address of the device to which the message is being sent.

ARP operating mechanism

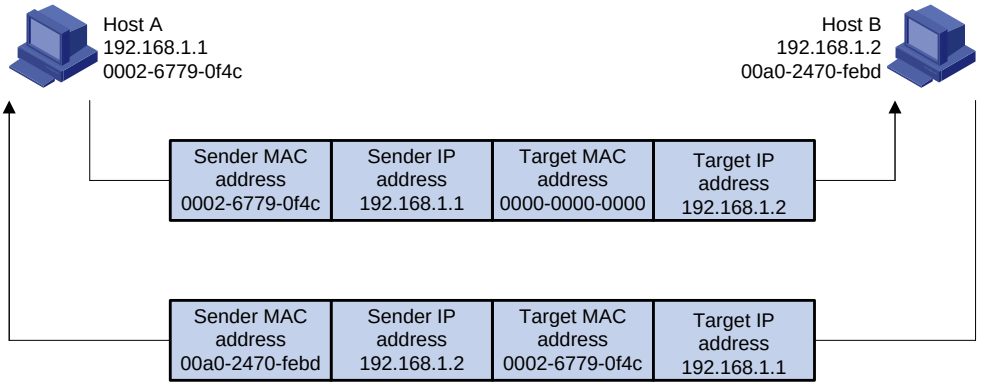
As shown in Figure 2, Host A and Host B are on the same subnet. Host A sends a packet to Host B as follows:

1. Host A looks through the ARP table for an ARP entry for Host B. If one entry is found, Host A uses the MAC address in the entry to encapsulate the IP packet into a data link layer frame. Then Host A sends the frame to Host B.
2. If Host A finds no entry for Host B, Host A buffers the packet and broadcasts an ARP request. The payload of the ARP request contains the following information:
   - **Sender IP address and sender MAC address**—Host A's IP address and MAC address.
   - **Target IP address**—Host B's IP address.
   - **Target MAC address**—An all-zero MAC address.

All hosts on this subnet can receive the broadcast request, but only the requested host (Host B) processes the request.

3. Host B compares its own IP address with the target IP address in the ARP request. If they are the same, Host B operates as follows:
   a. Adds the sender IP address and sender MAC address into its ARP table.
   b. Encapsulates its MAC address into an ARP reply.
   c. Unicasts the ARP reply to Host A.
4. After receiving the ARP reply, Host A operates as follows:
   a. Adds the MAC address of Host B into its ARP table.
   b. Encapsulates the MAC address into the packet and sends the packet to Host B.

Figure 2 ARP address resolution process



If Host A and Host B are on different subnets, Host A sends a packet to Host B as follows:

5. Host A broadcasts an ARP request where the target IP address is the IP address of the gateway.
6. The gateway responds with its MAC address in an ARP reply to Host A.
7. Host A uses the gateway's MAC address to encapsulate the packet, and then sends the packet to the gateway.
8. If the gateway has an ARP entry for Host B, it forwards the packet to Host B directly. If not, the gateway broadcasts an ARP request, in which the target IP address is the IP address of Host B.
9. After the gateway gets the MAC address of Host B, it sends the packet to Host B.

ARP entry types

An ARP table stores dynamic ARP entries, OpenFlow ARP entries, Rule ARP entries, and static ARP entries.

Dynamic ARP entry

ARP automatically creates and updates dynamic entries. A dynamic ARP entry is removed when its aging timer expires or the output interface goes down. In addition, a dynamic ARP entry can be overwritten by a static ARP entry.

Static ARP entry

A static ARP entry is manually configured and maintained. It does not age out and cannot be overwritten by any dynamic ARP entry.

Static ARP entries protect communication between devices because attack packets cannot modify the IP-to-MAC mapping in a static ARP entry.

The device supports the following types of static ARP entries:

- **Long static ARP entry**—It is directly used for forwarding packets. A long static ARP entry contains the IP address, MAC address, and one of the following combinations:
  - VLAN and output interface.
  - Input and output interfaces.
- **Short static ARP entry**—It contains only the IP address and MAC address.

  If the output interface is a Layer 3 Ethernet interface, the short ARP entry can be directly used to forward packets.

  If the output interface is a VLAN interface, the device sends an ARP request whose target IP address is the IP address in the short entry. If the sender IP and MAC addresses in the received ARP reply match the short static ARP entry, the device performs the following operations:
  - Adds the interface that received the ARP reply to the short static ARP entry.
  - Uses the resolved short static ARP entry to forward IP packets.
- **Multiport ARP entry**—It contains the IP address, MAC address, VLAN information.

  The device can use a multiport ARP entry that has the same MAC address, VLAN as a multicast or multiport unicast MAC address entry for packet forwarding. A multiport ARP entry is manually configured. It does not age out and cannot be overwritten by any dynamic ARP entry.

To communicate with a host by using a fixed IP-to-MAC mapping, configure a short static ARP entry on the device. To communicate with a host by using a fixed IP-to-MAC mapping through an interface in a VLAN, configure a long static ARP entry on the device.

OpenFlow ARP entry

ARP creates OpenFlow ARP entries by learning from the OpenFlow module. An OpenFlow ARP entry does not age out, and it cannot be updated. An OpenFlow ARP entry can be used directly to forward packets. For more information about OpenFlow, see *OpenFlow Configuration Guide*.

Rule ARP entry

Rule ARP entries can be directly used for packet forwarding. A Rule ARP entry does not age out, and it cannot be updated. It can be overwritten by a static ARP entry.

ARP creates Rule ARP entries by learning from the following modules:

- Portal. For more information about portal, see *Security Configuration Guide*.
- VXLAN. For more information about VXLAN, see *VXLAN Configuration Guide*.
- OVSDB. For more information about OVSDB, see VXLAN configuration in *VXLAN Configuration Guide.*

ARP tasks at a glance

All ARP tasks are optional.

- Configuring a static ARP entry
  - Configuring a short static ARP entry
  - Configuring a long static ARP entry
  - Configuring a multiport ARP entry
- Configuring features for dynamic ARP entries
  - Setting the dynamic ARP learning limit for a device
  - Setting the dynamic ARP learning limit for an interface
  - Setting the aging timer for dynamic ARP entries
  - Setting the maximum number of probes for dynamic ARP entries
  - Setting the interval for probing dynamic ARP entries
  - Enabling dynamic ARP entry check

- Synchronizing ARP entries across all member devices
- Configuring a customer-side or network-side port
- Enabling user information checking for ARP entries:
  - Enabling recording user IP address conflicts
  - Enabling interface consistency check between ARP and MAC address entries
  - Enabling recording user port migrations
- Enabling ARP logging

Configuring a static ARP entry

Static ARP entries are effective when the device functions correctly.

Configuring a short static ARP entry

Restrictions and guidelines

A resolved short static ARP entry becomes unresolved upon certain events, for example, when the resolved output interface goes down, or the corresponding VLAN or VLAN interface is deleted.

Procedure

1. Enter system view.
   system-view
2. Configure a short static ARP entry.
   arp static *ip-address mac-address* [**vpn-instance** *vpn-instance-name*]

Configuring a long static ARP entry

About long static ARP entries

Long static ARP entries can be effective or ineffective. Ineffective long static ARP entries cannot be used for packet forwarding. A long static ARP entry is ineffective when any of the following conditions exists:

- The IP address in the entry conflicts with a local IP address.
- No local interface has an IP address in the same subnet as the IP address in the ARP entry.

A long static ARP entry for a VLAN is deleted if the VLAN or VLAN interface is deleted.

Procedure

1. Enter system view.
   system-view
2. Configure a long static ARP entry.
   arp static *ip-address mac-address* [*vlan-id interface-type interface-number* | **vsi-interface** *vsi-interface-id* **tunnel** *number* **vsi** *vsi-name* | **vsi-interface** *vsi-interface-id interface-type interface-number* **service-instance** *instance-id* **vsi** *vsi-name*] [**vpn-instance** *vpn-instance-name*]

Configuring a multiport ARP entry

About multiport ARP entries

A multiport ARP entry contains an IP address, MAC address, output interface, and VLAN ID information. The VLAN and output interfaces are specified by a multiport unicast MAC address entry or a multicast MAC address entry. For more information about multiport unicast MAC address entries, see *Layer—2 LAN Switching Configuration Guide*. For more information about multicast MAC address entries, see *IP Multicast Configuration Guide*.

A multiport ARP entry can overwrite a dynamic, short static or long static ARP entry. Conversely, a short static or long static ARP entry can overwrite a multiport ARP entry.

Restrictions and guidelines

For a multiport ARP entry to be effective for packet forwarding, make sure the following conditions are met:

- A multiport unicast MAC address entry or a multicast MAC address entry exists.
- The multiport ARP entry must have the same MAC address and VLAN ID as the multiport unicast MAC address entry or the multicast MAC address entry.
- The IP address in the multiport ARP entry must reside on the same subnet as the VLAN interface of the specified VLAN.

Prerequisites

A service loopback group that supports the multiport ARP service must be created. The service loopback group has a minimum of one member port that is not used for any other purposes and does not have any configuration. For information about creating and configuring a service loopback group, see *Layer 2—LAN Switching Configuration Guide*.

Procedure

1. Enter system view.

   system-view

2. Configure a multiport unicast MAC address entry or a multicast MAC address entry.
   - In a common network, configure a multiport unicast MAC address entry.

     mac-address multiport *mac-address* **interface** *interface-list* **vlan** *vlan-id*
   - In a common network, configure a multicast MAC address entry.

     mac-address multicast *mac-address* **interface** *interface-list* **vlan** *vlan-id*

3. Configure a multiport ARP entry.

   arp multiport *ip-address mac-address vlan-id* [**vpn-instance** *vpn-instance-name*]

Configuring features for dynamic ARP entries

Setting the dynamic ARP learning limit for a device

About the dynamic ARP learning limit for a device

A device can dynamically learn ARP entries. To prevent a device from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the device can learn. When the limit is reached, the device stops ARP learning.

If you set a value lower than the number of existing dynamic ARP entries, the device does not delete the existing entries unless they age out. You can use the **reset arp dynamic** command to clear dynamic ARP entries.

Procedure

1. Enter system view.

   system-view

2. Set the dynamic ARP learning limit for the device.

   arp max-learning-number *max-number* **slot** *slot-number*

   By default, the dynamic ARP learning limit for a device depends on the ARP table capacity set by using the **hardware-resource switch-mode** command. For information about the **hardware-resource switch-mode** command, see the device management in *Fundamentals Command Reference*.

   To disable the device from dynamic ARP learning, set the value to 0.

Setting the dynamic ARP learning limit for an interface

About setting the dynamic ARP learning limit for an interface

An interface can dynamically learn ARP entries. To prevent an interface from holding too many ARP entries, you can set the maximum number of dynamic ARP entries that the interface can learn. When the limit is reached, the interface stops ARP learning.

You can set limits for both a Layer 2 interface and the VLAN interface for a permitted VLAN on the Layer 2 interface. The Layer 2 interface learns an ARP entry only when neither limit is reached.

The total dynamic ARP learning limit for all interfaces will not be higher than the dynamic ARP learning limit for the device.

Procedure

1. Enter system view.

   system-view

2. Enter interface view.

   interface *interface-type interface-number*

3. Set the dynamic ARP learning limit for the interface.

   arp max-learning-num *max-number* [**alarm** *alarm-threshold*]

   By default, the maximum number of dynamic ARP entries that an interface can learn depends on the ARP table capacity set by using the **hardware-resource switch-mode** command. For information about the **hardware-resource switch-mode** command, see the device management in *Fundamentals Command Reference*.

   To disable the interface from dynamic ARP learning, set the value to 0.

Setting the aging timer for dynamic ARP entries

About the aging timer for dynamic ARP entries

Each dynamic ARP entry in the ARP table has a limited lifetime, called an aging timer. The aging timer of a dynamic ARP entry is reset each time the dynamic ARP entry is updated. A dynamic ARP entry that is not updated before its aging timer expires is deleted from the ARP table.

You can set the aging timer for dynamic ARP entries in system view or in interface view. The aging timer set in interface view takes precedence over the aging timer set in system view.

Procedure

1. Enter system view.

   system-view

2. Set the aging timer for dynamic ARP entries.
   - Set the aging timer for dynamic ARP entries in system view.

     arp timer aging { *aging-minutes* | **second** *aging-seconds* }

     By default, the aging timer for dynamic ARP entries in system view is 20 minutes.
   - Execute the following commands in sequence to set the aging timer for dynamic ARP entries in interface view:

     interface *interface-type interface-number*

     arp timer aging { *aging-minutes* | **second** *aging-seconds* }

     By default, the aging timer for dynamic ARP entries in interface view is the aging timer set in system view.

Setting the maximum number of probes for dynamic ARP entries

About the maximum number of probes for dynamic ARP entries

This probe mechanism keeps legal dynamic ARP entries valid and avoids unnecessary ARP resolution during later traffic forwarding. It sends ARP requests for the IP address in a dynamic ARP entry.

- If the device receives an ARP reply before the entry aging timer expires, the device resets the aging timer.
- If the device does not receive any ARP reply after the maximum number of probes is made, the device deletes the entry when the entry aging timer expires.

You can set the maximum number of probes in system view or in interface view. The probe count set in interface view takes precedence over the probe count set in system view.

Procedure

1. Enter system view.

   system-view

2. Set the maximum number of probes for dynamic ARP entries.
   - Set the maximum number of probes for dynamic ARP entries in system view.

     arp timer aging probe-count *count*

     By default, the maximum number of probes in system view for dynamic ARP entries is 3.
   - Execute the following commands in sequence to set the maximum number of probes for dynamic ARP entries:

     interface *interface-type interface-number*

     arp timer aging probe-count *count*

     By default, the maximum number of probes in interface view for dynamic ARP entries is the maximum number of probes set in system view.

Setting the interval for probing dynamic ARP entries

About the interval for probing dynamic ARP entries

The probing feature keeps legal dynamic ARP entries valid and avoids unnecessary ARP resolution during later traffic forwarding.

Before a dynamic ARP entry is aged out, the device sends ARP requests for the IP address in the ARP entry.

- If the device receives an ARP reply during the probe interval, the device resets the aging timer.
- If the device does not receive any ARP reply during the probe interval, the device starts a new probe.
- If the maximum number probes are made, and still no ARP reply is received, the device deletes the entry.

You can set the probe interval in system view and in interface view. The probe interval in interface view takes precedence over the probe interval in system view.

Restrictions and guidelines

- If massive traffic exists in the network, set a long interval.
- During the dynamic ARP entry probing process, a dynamic ARP entry will not be deleted if its aging time expires. If a reply is received during the probe, the aging timer of the ARP entry is reset.
- For the device to perform the specified number of probes, make sure the following requirement is met:

  Aging time of the dynamic ARP entries > the maximum number of probes × probe interval

Procedure

1. Enter system view.

   system-view
2. Set the interval for probing dynamic ARP entries.
   - Set the interval for probing dynamic ARP entries in system view.

     arp timer aging probe-interval *interval*

     By default, the probe interval is 5 seconds.
   - Execute the following commands in sequence to set the interval for probing dynamic ARP entries:

     interface *interface-type interface-number*

     arp timer aging probe-interval *interval*

     By default, the probe interval depends on the setting in system view.

Enabling dynamic ARP entry check

About dynamic ARP entry check

The dynamic ARP entry check feature disables the device from supporting dynamic ARP entries that contain multicast MAC addresses. The device cannot learn dynamic ARP entries containing multicast MAC addresses. You cannot manually add static ARP entries containing multicast MAC addresses.

When dynamic ARP entry check is disabled, ARP entries containing multicast MAC addresses are supported. The device can learn dynamic ARP entries containing multicast MAC addresses obtained from the ARP packets sourced from a unicast MAC address. You can also manually add static ARP entries containing multicast MAC addresses.

Procedure

1. Enter system view.
   system-view
2. Enable dynamic ARP entry check.
   arp check enable
   By default, dynamic ARP entry check is enabled.

Synchronizing ARP entries across all member devices

About ARP entry synchronization

This task ensures that all IRF member devices in an IRF fabric have the same ARP entries.

Restrictions and guidelines

To synchronize ARP entries across all member devices in a timely manner, you can schedule the device to automatically execute the **arp smooth** command. For information about scheduling a task, see the device management configuration in *Fundamentals Configuration Guide*.

Procedure

To synchronize ARP entries from the master device to all subordinate devices, execute the following command in user view:

arp smooth

Configuring a customer-side or network-side port

About the customer-side and network-side port

The device generates a host route when it learns an ARP entry from a network-side port. To save hardware resources, you can specify a port that connects to a user terminal as a customer-side port. The device will not generate a host route for the learned ARP entry of the user terminal.

Restrictions and guidelines

Select a proper operating mode (customer-side port or network-side port) for an interface according to your actual network requirements. For a VLAN interface configured as a customer-side port, issuing ARP entries to the driver will occupy double entry resources. In this case, the actual ARP table size will be much smaller than the specification.

Procedure

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Configure the interface as a customer-side port or a network-side port.
   - Configure the interface as a customer-side port.
     arp mode uni
   - Configure the interface as a network-side port.
     undo arp mode uni

   By default, a port operates as a network-side port.

Enabling recording user IP address conflicts

About recording user IP address conflicts

This feature enables the device to detect and record user IP address conflicts. The device determines that a conflict occurs if an incoming non-gratuitous ARP packet has the same sender IP address as an existing ARP entry but a different sender MAC address. The device generates a user IP address conflict record, logs the conflict, and sends the log to the information center. For information about the log destination and output rule configuration in the information center, see the information center in *Network Management and Monitoring Configuration Guide*.

Procedure

1. Enter system view.

   `system-view`

2. Enable recording user IP address conflicts.

   `arp user-ip-conflict record enable`

   By default, recording user IP address conflicts is disabled.

Enabling interface consistency check between ARP and MAC address entries

About interface consistency check between ARP and MAC address entries

In an unstable network, the receiving interface for packets from a user might change. The interface in the MAC address entry can be updated immediately while the interface in the ARP entry cannot. In this case, the packets matching the ARP entry will be sent out of an incorrect interface. To solve this problem, you can use this feature to periodically check the interface consistency between the ARP and MAC address entry for a user. If the interfaces are not the same, ARP sends ARP requests in the VLAN of the ARP entry and updates the entry with the ARP reply receiving interface.

Use **`display mac-address`** to display MAC address entries. For more information about this command, see MAC address table in *Layer 2—LAN Switching Command Reference.*

Procedure

1. Enter system view.

   `system-view`

2. Enable interface consistency check between ARP and MAC address entries.

   `arp mac-interface-consistency check enable`

   By default, interface consistency check between ARP and MAC address entries is disabled.

Enabling recording user port migrations

About recording user port migrations

This feature enables the device to detect and record user port migration events. A user port migrates if an incoming ARP packet has the same sender IP address and sender MAC address as an existing ARP entry but a different ingress port. The device generates a user port migration record, logs the migration event, sends the log to the information center, and updates the interface for the ARP entry. For information about the log destination and output rule configuration in the information center, see the information center in *Network Management and Monitoring Configuration Guide*.

Restrictions and guidelines

To avoid device performance degradation, disable recording user port migrations if too many user port migration logs are generated.

Procedure

1. Enter system view.
   system-view
2. Enable recording user port migrations.
   arp user-move record enable
   By default, recording user port migrations is disabled.

Enabling ARP logging

About ARP logging

This feature enables a device to log ARP events when ARP cannot resolve IP addresses correctly. The log information helps administrators locate and solve problems. The device can log the following ARP events:

- On a proxy ARP-disabled interface, the target IP address of a received ARP packet is not one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.
- The sender IP address of a received ARP reply conflicts with one of the following IP addresses:
  - The IP address of the receiving interface.
  - The virtual IP address of the VRRP group.

The device sends ARP log messages to the information center. You can use the **info-center source** command to specify the log output rules for the information center. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

Procedure

1. Enter system view.
   system-view
2. Enable ARP logging.
   arp check log enable
   By default, ARP logging is disabled.

Display and maintenance commands for ARP

IMPORTANT:

Clearing ARP entries from the ARP table might cause communication failures. Make sure the entries to be cleared do not affect current communications.

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display ARP entries.	**display arp** [[**all** | **dynamic** | **multiport** | **static**] [**slot** *slot-number*] | **vlan** *vlan-id* | **interface** *interface-type*

Task	Command
	interface-number] [**count** | **verbose**]
Display the maximum number of ARP entries that a device supports.	**display arp entry-limit**
Display the ARP entry for an IP address.	**display arp** *ip-address* [**slot** *slot-number*] [**verbose**]
Display the number of OpenFlow ARP entries.	**display arp openflow count** [**slot** *slot-number*]
Display the aging timer of dynamic ARP entries.	**display arp timer aging**
Display user IP address conflicts.	**display arp user-ip-conflict record** [**slot** *slot-number*]
Display user port migrations.	**display arp user-move record** [**slot** *slot-number*]
Display the ARP entries for a VPN instance.	**display arp vpn-instance** *vpn-instance-name* [**count**]
Clear ARP entries from the ARP table.	**reset arp** { **all** | **dynamic** | **interface** *interface-type interface-number* | **multiport** | **slot** *slot-number* | **static** }

ARP configuration examples

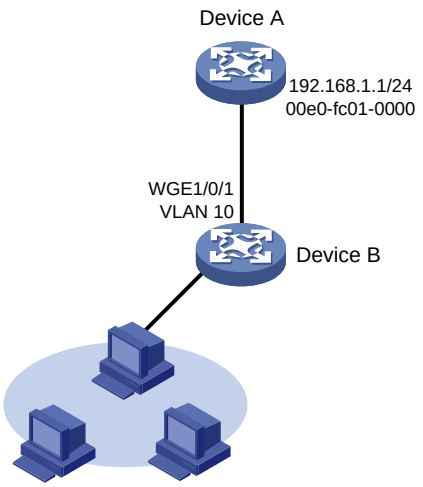
Example: Configuring a long static ARP entry

Network configuration

As shown in Figure 3, hosts are connected to Device B. Device B is connected to Device A through interface Twenty-FiveGigE 1/0/1 in VLAN 10.

To ensure secure communications between Device A and Device B, configure a long static ARP entry for Device A on Device B.

Figure 3 Network diagram



Procedure

Create VLAN 10.

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

Add interface Twenty-FiveGigE 1/0/1 to VLAN 10.

```
[DeviceB] interface twenty-fivegige 1/0/1
[DeviceB-Twenty-FiveGigE1/0/1] port access vlan 10
[DeviceB-Twenty-FiveGigE1/0/1] quit
```

Create VLAN-interface 10 and configure its IP address.

```
[DeviceB] interface vlan-interface 10
[DeviceB-vlan-interface10] ip address 192.168.1.2 8
[DeviceB-vlan-interface10] quit
```

Configure a long static ARP entry that has IP address 192.168.1.1, MAC address 00e0-fc01-0000, and output interface Twenty-FiveGigE 1/0/1 in VLAN 10.

```
[DeviceB] arp static 192.168.1.1 00e0-fc01-0000 10 twenty-fivegige 1/0/1
```

Verifying the configuration

Verify that Device B has a long static ARP entry for Device A.

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI   Interface               Aging Type
192.168.1.1     00e0-fc01-0000 10         WGE1/0/1                --    S
```

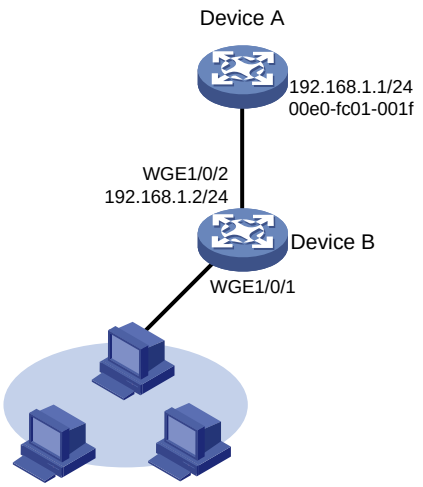
Example: Configuring a short static ARP entry

Network configuration

As shown in Figure 4, hosts are connected to Device B. Device B is connected to Device A through interface Twenty-FiveGigE 1/0/2.

To ensure secure communications between Device A and Device B, configure a short static ARP entry for Device A on Device B.

Figure 4 Network diagram



Procedure

Configure an IP address for Twenty-FiveGigE 1/0/2.

```
<DeviceB> system-view
[DeviceB] interface twenty-fivegige 1/0/2
[DeviceB-Twenty-FiveGigE1/0/2] ip address 192.168.1.2 24
[DeviceB-Twenty-FiveGigE1/0/2] quit
```

Configure a short static ARP entry that has IP address 192.168.1.1 and MAC address 00e0-fc01-001f.

```
[DeviceB] arp static 192.168.1.1 00e0-fc01-001f
```

Verifying the configuration

Verify that Device B has a short static ARP entry for Device A

```
[DeviceB] display arp static
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI   Interface                Aging Type
192.168.1.1     00e0-fc01-001f --         --                       --    S
```

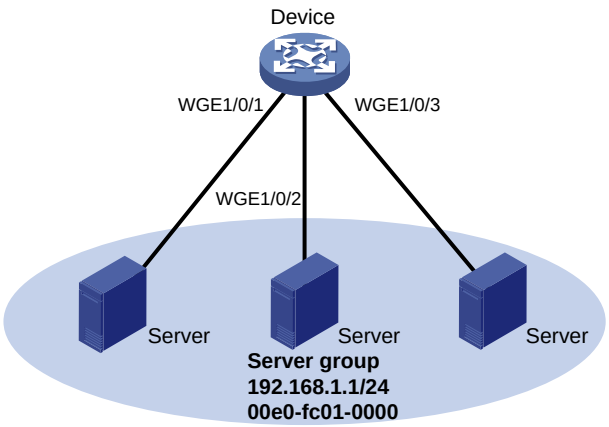
Example: Configuring a multiport ARP entry

Network configuration

As shown in Figure 5, a device connects to three servers through interfaces Twenty-FiveGigE 1/0/1, Twenty-FiveGigE 1/0/2, and Twenty-FiveGigE 1/0/3 in VLAN 10. The servers share the IP address 192.168.1.1/24 and MAC address 00e0-fc01-0000.

Configure a multiport ARP entry so that the device sends IP packets with the destination IP address 192.168.1.1 to the three servers.

Figure 5 Network diagram



Procedure

Create VLAN 10.

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] quit
```

Add Twenty-FiveGigE 1/0/1, Twenty-FiveGigE 1/0/2, and Twenty-FiveGigE 1/0/3 to VLAN 10.

```
[Device] interface twenty-fivegige 1/0/1
[Device-Twenty-FiveGigE1/0/1] port access vlan 10
[Device-Twenty-FiveGigE1/0/1] quit
```

```
[Device] interface twenty-fivegige 1/0/2
[Device-Twenty-FiveGigE1/0/2] port access vlan 10
[Device-Twenty-FiveGigE1/0/2] quit
[Device] interface twenty-fivegige 1/0/3
[Device-Twenty-FiveGigE1/0/3] port access vlan 10
[Device-Twenty-FiveGigE1/0/3] quit
```

Create VLAN-interface 10 and specify its IP address.

```
[Device] interface vlan-interface 10
[Device-vlan-interface10] ip address 192.168.1.2 24
[Device-vlan-interface10] quit
```

Configure a multiport unicast MAC address entry that has MAC address 00e0-fc01-0000, and output interfaces Twenty-FiveGigE 1/0/1, Twenty-FiveGigE 1/0/2, and Twenty-FiveGigE 1/0/3 in VLAN 10.

```
[Device] mac-address multiport 00e0-fc01-0000 interface twenty-fivegige 1/0/1 to
twenty-fivegige 1/0/3 vlan 10
```

Configure a multiport ARP entry with IP address 192.168.1.1 and MAC address 00e0-fc01-0000.

```
[Device] arp multiport 192.168.1.1 00e0-fc01-0000 10
```

Verifying the configuration

Verify that the device has a multiport ARP entry with IP address 192.168.1.1 and MAC address 00e0-fc01-0000.

```
[Device] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport  I-Invalid
IP address      MAC address    VLAN/VSI   Interface                Aging Type
192.168.1.1     00e0-fc01-0000 10         --                       --    M
```

Configuring gratuitous ARP

About gratuitous ARP

In a gratuitous ARP packet, the sender IP address and the target IP address are the IP address of the sending device.

A device sends a gratuitous ARP packet for either of the following purposes:

- Determine whether its IP address is already used by another device. If the IP address is already used, the device is informed of the conflict by an ARP reply.
- Inform other devices of a MAC address change.

IP conflict detection

When an interface obtains an IP address, the device broadcasts gratuitous ARP packets in the LAN where the interface resides. If the device receives an ARP reply, its IP address conflicts with the IP address of another device in the LAN. The device displays a log message about the conflict and informs the administrator to change the IP address. The device will not use the conflicting IP address. If no ARP reply is received, the device uses the IP address.

Gratuitous ARP packet learning

This feature enables a device to create or update ARP entries by using the sender IP and MAC addresses in received gratuitous ARP packets.

When this feature is disabled, the device uses received gratuitous ARP packets to update existing ARP entries only. ARP entries are not created based on the received gratuitous ARP packets, which saves ARP table space.

Periodic sending of gratuitous ARP packets

Periodic sending of gratuitous ARP packets helps downstream devices update ARP entries or MAC entries in a timely manner.

This feature can implement the following functions:

- Prevent gateway spoofing.

  Gateway spoofing occurs when an attacker uses the gateway address to send gratuitous ARP packets to the hosts on a network. The traffic destined for the gateway from the hosts is sent to the attacker instead. As a result, the hosts cannot access the external network.

  To prevent such gateway spoofing attacks, you can enable the gateway to send gratuitous ARP packets at intervals. Gratuitous ARP packets contain the primary IP address and manually configured secondary IP addresses of the gateway, so hosts can learn correct gateway information.
- Prevent ARP entries from aging out.

  If network traffic is heavy or if the host CPU usage is high, received ARP packets can be discarded or are not promptly processed. Eventually, the dynamic ARP entries on the receiving host age out. The traffic between the host and the corresponding devices is interrupted until the host re-creates the ARP entries.

  To prevent this problem, you can enable the gateway to send gratuitous ARP packets periodically. Gratuitous ARP packets contain the primary IP address and manually configured

secondary IP addresses of the gateway, so the receiving hosts can update ARP entries in a timely manner.

- Prevent the virtual IP address of a VRRP group from being used by a host.

  The master router of a VRRP group can periodically send gratuitous ARP packets to the hosts on the local network. The hosts can then update local ARP entries and avoid using the virtual IP address of the VRRP group. The sender MAC address in the gratuitous ARP packet is the virtual MAC address of the virtual router. For more information about VRRP, see *High Availability Configuration Guide*.

Gratuitous ARP tasks at a glance

All gratuitous ARP tasks are optional. If all of the following features are disabled, gratuitous ARP still provides the IP conflict detection function.

- Enabling IP conflict notification
- Enabling gratuitous ARP packet learning
- Enabling periodic sending of gratuitous ARP packets
- Enabling sending gratuitous ARP packets for ARP requests with sender IP address on a different subnet
- Configuring gratuitous ARP packet retransmission for the device MAC address change

Enabling IP conflict notification

About IP conflict notification

Upon detecting an IP conflict, the device will sends a gratuitous ARP request. By default, the device displays an error message only after it receives an ARP reply. You can enable this feature to allow the device to display an error message immediately upon detecting an IP conflict.

Procedure

1. Enter system view.

   `system-view`
2. Enable IP conflict notification.

   `arp ip-conflict log prompt`

   By default, IP conflict notification is disabled.

Enabling gratuitous ARP packet learning

1. Enter system view.

   `system-view`
2. Enable gratuitous ARP packet learning.

   `gratuitous-arp-learning enable`

   By default, gratuitous ARP packet learning is enabled.

Enabling periodic sending of gratuitous ARP packets

Restrictions and guidelines

- You can enable periodic sending of gratuitous ARP packets on a maximum of 1024 interfaces.
- Periodic sending of gratuitous ARP packets takes effect on an interface only when the following conditions are met:
  - The data link layer state of the interface is up.
  - The interface has an IP address.
- If you change the sending interval for gratuitous ARP packets, the configuration takes effect at the next sending interval.
- The sending interval for gratuitous ARP packets might be much longer than the specified sending interval in any of the following circumstances:
  - This feature is enabled on multiple interfaces.
  - Each interface is configured with multiple secondary IP addresses.
  - A small sending interval is configured when the previous two conditions exist.

Procedure

1. Enter system view.

   system-view
2. Enter interface view.

   interface *interface-type interface-number*
3. Enable periodic sending of gratuitous ARP packets.

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

   By default, periodic sending of gratuitous ARP packets is disabled.

Enabling sending gratuitous ARP packets for ARP requests with sender IP address on a different subnet

1. Enter system view.

   system-view
2. Enable the device to send gratuitous ARP packets upon receiving ARP requests whose sender IP address belongs to a different subnet.

   gratuitous-arp-sending enable

   By default, a device does not send gratuitous ARP packets upon receiving ARP requests whose sender IP address belongs to a different subnet.

Configuring gratuitous ARP packet retransmission for the device MAC address change

About gratuitous ARP packet retransmission for the device MAC address change

The device sends a gratuitous ARP packet to inform other devices of its MAC address change. However, the other devices might fail to receive the packet because the device sends the gratuitous ARP packet once only by default. Configure the gratuitous ARP packet retransmission feature to ensure that the other devices can receive the packet.

Procedure

1. Enter system view.

   system-view

2. Set the times and the interval for retransmitting a gratuitous ARP packet for the device MAC address change.

   gratuitous-arp mac-change retransmit *times* **interval** *seconds*

   By default, the device sends a gratuitous packet to inform its MAC address change once only

   .

Configuring proxy ARP

About proxy ARP

Proxy ARP enables a device on one network to answer ARP requests for an IP address on another network. With proxy ARP, hosts on different broadcast domains can communicate with each other as they would on the same broadcast domain.

Proxy ARP includes common proxy ARP and local proxy ARP.

- **Common proxy ARP**—Allows communication between hosts that connect to different Layer 3 interfaces and reside in different broadcast domains.
- **Local proxy ARP**—Allows communication between hosts that connect to the same Layer 3 interface and reside in different broadcast domains.

Enabling common proxy ARP

1. Enter system view.
   `system-view`
2. Enter interface view.
   `interface` *`interface-type interface-number`*
   The following interface types are supported:
   - VLAN interface.
   - Layer 3 Ethernet interface.
   - Layer 3 Ethernet subinterface.
   - Layer 3 aggregate interface.
   - Layer 3 aggregate subinterface.
3. Enable common proxy ARP.
   `proxy-arp enable`
   By default, common proxy ARP is disabled.

Enabling local proxy ARP

1. Enter system view.
   `system-view`
2. Enter interface view.
   `interface` *`interface-type interface-number`*
   The following interface types are supported:
   - VLAN interface.
   - Layer 3 Ethernet interface.
   - Layer 3 Ethernet subinterface.
   - Layer 3 aggregate interface.
   - Layer 3 aggregate subinterface.
3. Enable local proxy ARP.

local-proxy-arp enable [**ip-range** *start-ip-address* **to** *end-ip-address*]

By default, local proxy ARP is disabled.

Display and maintenance commands for proxy ARP

Execute **display** commands in any view.

Task	Command
Display common proxy ARP status.	**display proxy-arp** [**interface** *interface-type interface-number*]
Display local proxy ARP status.	**display local-proxy-arp** [**interface** *interface-type interface-number*]

Common proxy ARP configuration example

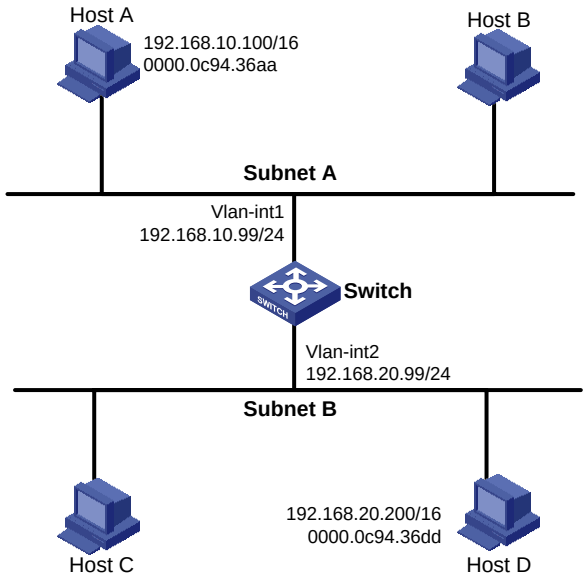
Example: Configuring common proxy ARP

Network configuration

As shown in Figure 6, Host A and Host D have the same IP prefix and mask, but they are located on different subnets separated by the switch. Host A belongs to VLAN 1, and Host D belongs to VLAN 2. No default gateway is configured on Host A and Host D.

Configure common proxy ARP on the switch to enable communication between the two hosts.

Figure 6 Network diagram



Procedure

Create VLAN 2.

```
<Switch> system-view
```

```
[Switch] vlan 2
[Switch-vlan2] quit
```

Configure the IP address of VLAN-interface 1.

```
[Switch] interface vlan-interface 1
[Switch-Vlan-interface1] ip address 192.168.10.99 255.255.255.0
```

Enable common proxy ARP on VLAN-interface 1.

```
[Switch-Vlan-interface1] proxy-arp enable
[Switch-Vlan-interface1] quit
```

Configure the IP address of VLAN-interface 2.

```
[Switch] interface vlan-interface 2
[Switch-Vlan-interface2] ip address 192.168.20.99 255.255.255.0
```

Enable common proxy ARP on VLAN-interface 2.

```
[Switch-Vlan-interface2] proxy-arp enable.
```

Verifying the configuration

Verify that Host A and Host D can ping each other.

Configuring ARP snooping

About ARP snooping

ARP snooping is used in Layer 2 switching networks. It creates ARP snooping entries by using information in ARP packets. ARP fast-reply and MFF can use the ARP snooping entries. For more information about MFF, see *Security Configuration Guide*.

Creation of ARP snooping entries

If you enable ARP snooping for a VLAN or VXLAN, ARP packets received in the VLAN or VXLAN are redirected to the CPU. For the VLAN, the CPU uses the sender IP and MAC addresses of the ARP packets, and the receiving VLAN and port to create ARP snooping entries. For the VXLAN, the CPU uses the sender IP and MAC addresses of the ARP packets, VSI name, and link ID to create ARP snooping entries. For more information about VXLAN, see *VXLAN Configuration Guide*.

Aging of ARP snooping entries

The aging timer and valid period of an ARP snooping entry are 25 minutes and 15 minutes. If an ARP snooping entry is not updated in 12 minutes, the device sends an ARP request. The ARP request uses the IP address of the entry as the target IP address. If an ARP snooping entry is not updated in 15 minutes, it becomes invalid and cannot be used. After that, if an ARP packet matching the entry is received, the entry becomes valid, and its aging timer restarts.

If the aging timer of an ARP snooping entry expires, the entry is removed.

Protection for ARP snooping

An attack occurs if an ARP packet has the same sender IP address as a valid ARP snooping entry but a different sender MAC address. The ARP snooping entry becomes invalid, and it is removed in 1 minute.

Enabling ARP snooping for a VLAN

1. Enter system view.
   system-view
2. Enter VLAN view.
   vlan *vlan-id*
3. Enable ARP snooping for the VLAN.
   arp snooping enable
   By default, ARP snooping is disabled for a VLAN.

Enabling ARP snooping for a VSI

1. Enter system view.
   system-view
2. Enter VSI view.

vsi *vsi-name*

3. Enable ARP snooping for the VSI.

   arp snooping enable

   By default, ARP snooping is disabled for a VSI.

Display and maintenance commands for ARP snooping

Execute **display** commands in any view and **reset** commands in user view.

Task	Command
Display ARP snooping entries.	**display arp snooping** { **vlan** [*vlan-id*]| **vsi** [*vsi-name*] } [**slot** *slot-number*] [**count**] **display arp snooping vlan ip** *ip-address* [**slot** *slot-number*]
Delete ARP snooping entries.	**reset arp snooping** { **vlan** [*vlan-id*] | **vsi** [*vsi-name*] } **reset arp snooping vlan ip** *ip-address*

Configuring ARP fast-reply

About ARP fast-reply

ARP fast-reply enables a device to directly answer ARP requests according to IP source guard entries or ARP snooping entries. ARP fast-reply functions in a VLAN. For information about IP source guard, see IP source guard configuration in *Security Configuration Guide*.

If the target IP address of a received ARP request is the IP address of the VLAN interface, the device delivers the request to the ARP module. If not, the device takes the following steps to process the packet:

1. Search the IP source guard binding table for a match by using the target IP address.
2. If a match is found, whether the device returns a reply depends on the type of interface in the matching entry.
   - If the interface is the Ethernet interface that received the ARP request, the device does not return any reply.
   - If the interface is an Ethernet interface other than the receiving interface, the device returns a reply according to the matching entry.
3. If no matching IP source guard entry is found and ARP snooping is enabled, the device searches the ARP snooping table.
   - If the interface in the matching entry is the Ethernet interface that received the ARP request, the device does not return any reply.
   - If the interface is an Ethernet interface other than the receiving interface, the device returns a reply according to the ARP snooping entry.
4. If no match is found in both tables, the ARP request is forwarded to other interfaces except the receiving interface in the VLAN, or delivered to other modules.

Enabling ARP fast-reply

Restrictions and guidelines

To improve the availability of ARP fast-reply, enable ARP snooping at the same time.

Procedure

1. Enter system view.

   system-view
2. Enter VLAN view.

   vlan *vlan-id*
3. Enable ARP fast-reply.

   arp fast-reply enable

   By default, ARP fast-reply is disabled.

ARP fast-reply configuration example

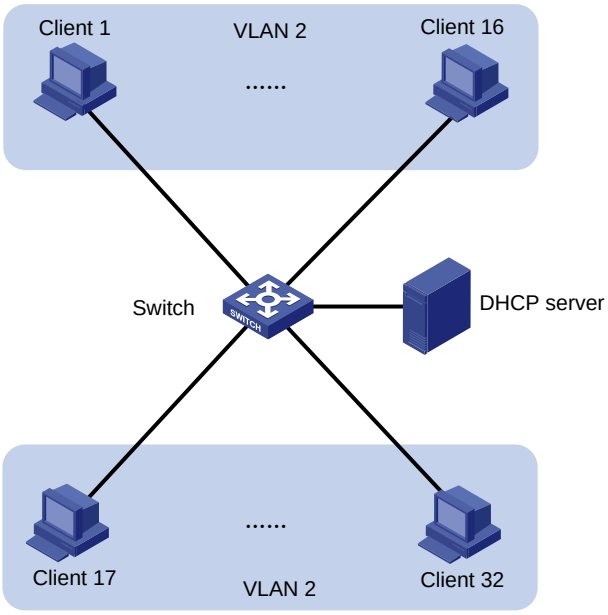
Example: Configuring ARP fast-reply

Network configuration

As shown in Figure 7, all clients are in VLAN 2, and access the network through the switch. They have obtained IP addresses through DHCP.

Enable ARP snooping and ARP fast-reply for VLAN 2. The switch directly returns an ARP reply without broadcasting received ARP requests in the VLAN.

Figure 7 Network diagram



Procedure

Enable ARP snooping for VLAN 2 on the switch.

```
<Switch> system-view
[Switch] vlan 2
[Switch-vlan2] arp snooping enable
```

Enable ARP fast-reply for VLAN 2 on the switch.

```
[Switch-vlan2] arp fast-reply enable
[Switch-vlan2] quit
```

Configuring ARP direct route advertisement

About ARP direct route advertisement

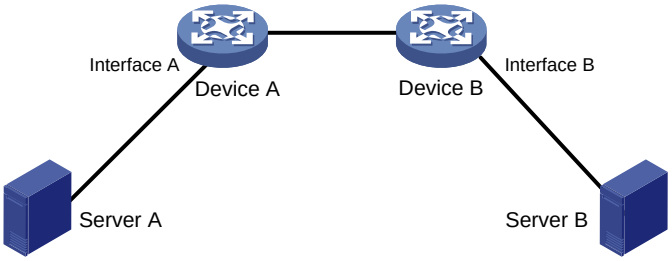
Mechanism of ARP direct route advertisement

This feature generates host routes based on ARP entries for packet forwarding and route advertisement.

Application in Layer 3 access networks

As shown in Figure 8, ARP direct route advertisement is enabled on Interface A and Interface B. This feature generates a host route to Server A and a host route to Server B for the routing protocols to advertise. So each device forwards only the traffic destined to the server within the network, which saves bandwidth.

Figure 8 Application in a Layer 3 access network



Enabling ARP direct route advertisement

1. Enter system view.
   system-view
2. Enter interface view.
   interface *interface-type interface-number*
3. Enable the ARP direct route advertisement feature.
   arp route-direct advertise
   By default, the ARP direct route advertisement feature is disabled.