1 ARP Commands

Command	Function
arp	Configure static Address Resolution Protocol (ARP) mapping entries.
arp-learning enable	Enable the ARP learning function.
arp anti-ip-attack	Configure the number of IP packets for triggering the discarding of ARP entries.
arp any-ip	Enable the any IP ARP function.
arp cache interface-limit	Set a limit on the number of ARP entries that can be learned by an interface.
arp fast-aging enable	Enable the fast ARP entry aging on an interface.
arp gratuitous-arp-learning enable	Enable the function of learning gratuitous ARP requests.
arp gratuitous-send interval	Enable the function of sending gratuitous ARP requests at intervals.
arp oob	Configure a static ARP entry for a management interface.
arp proxy-resolved	Configure the master VRRP device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as a proxy ARP.
arp rate-statistic enable	Enable the ARP packet rate statistics collection.
arp rate-statistic compute interval	Configure the interval for collecting ARP packet rate statistics.
arp resolve vlan	Configure ARP to actively send broadcast resolution requests to a specified sub VLAN in a super VLAN.
arp retry interval	Specify the ARP request retransmission interval.
arp retry times	Configure the number of times that an ARP request can be transmitted consecutively.
arp scan	Enable ARP scanning.
arp scan auto	Enable scheduled automatic ARP scanning.

arp scan interval	Configure the interval for scheduled automatic ARP scanning.
arp scan rate	Configure the rate of scheduled automatic ARP scanning.
arp suppress-auth-vlan-req	Restrain the device from sending ARP requests to authenticated VLANs.
arp switch-over resolve	Actively send ARP requests to terminals after active and standby VSU switchover.
arp timeout	Configure the timeout time for dynamic ARP entries in the ARP cache.
arp trusted	Configure the maximum number of trusted ARP entries.
arp trust-monitor enable	Enable ARP trust monitoring.
arp trusted aging	Enable trusted ARP aging.
arp trust user-vlan	Enable VLAN translation when a trusted ARP entry is added.
arp unresolve	Configure the maximum number of unresolved ARP entries.
arp strict-learning enable	Enable strict dynamic ARP learning.
arp filter gratuitous	Enable gratuitous ARP filtering.
arp filter acl	Enable ARP-based access control list (ACL) filtering.
arp filter smac-illegal	Enable the function of checking the source MAC addresses of ARP packets.
arp filter dmac-illegal	Enable the function of checking the destination MAC addresses of ARP packets.
arp warning-limit	Configure the ARP alarm rate limit.
clear arp-cache	Clear dynamic ARP mapping records in the ARP cache.
clear arp-cache trusted	Clear trusted ARP entries in the ARP cache.
clear arp-cache packet statistics	Clear ARP packet statistics.
ip proxy-arp	Enable proxy ARP on an interface.
local-proxy-arp	Enable local proxy ARP.
service trustedarp	Enable trusted ARP.

show arp	Display the ARP cache.
show arp oob	Display the ARP cache on a management interface.
show arp counter	Display the number of ARP entries in the ARP cache.
show arp detail	Display the details about the ARP cache.
show arp packet statistics	Display ARP packet statistics.
show arp rate-statistic	Display the ARP packet rate statistics.
show arp timeout	Display the aging time of dynamic ARP entries.
show arp flapping record	Display ARP flapping records.
show arp suppress table	Display the details about the ARP suppression table.
show ip arp	Display the ARP cache.
show arp anti-attack statistics	Display the statistics on illegal ARP packets.

1.1 arp

Function

Run the **arp** command to configure static Address Resolution Protocol (ARP) mapping entries.

Run the **no** form of this command to remove this configuration.

No ARP static entry is configured by default.

Syntax

arp [**vrf** *vrf-name*] *ip-address mac-address arp-type*

no arp [**vrf** *vrf-name*] *ip-address*

Parameter Description

vrf *vrf-name*: Specifies a virtual routing and forwarding (VRF) instance. No VRF instance is specified by default. Static ARP entries are applied globally.

ip-address: IP address corresponding to a MAC address. The IP address is expressed in dotted decimal notation.

mac-address: Data link layer (DLL) address, consisting of 48 bits.

arp-type: ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Users can manually specify mappings between IP and MAC addresses to prevent the device from learning incorrect ARP entries.

After a static ARP entry is configured on a Layer 3 device, the device must learn the physical port corresponding to the MAC address in the entry before it performs Layer 3 routing.

Examples

The following example configures a static ARP entry for a host on the Ethernet by setting the IP address to 1.1.1.1 and the MAC address to 4e54.3800.0002.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp 1.1.1.1 4e54.3800.0002 arpa
```

The following example configures a static ARP entry for a host on the Ethernet by setting the IP address to 1.1.1.1 and the MAC address to 4e54.3800.0002, and specifying a description of ABC.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp 1.1.1.1 4e54.3800.0002 arpa description ABC
```

Notifications

A VRF instance named xyz does not exist or the **address-family ipv4** command is not configured. When a static ARP entry is added to or deleted from the VRF instance, the following notification will be displayed:

```
% ARP:vrf xyz does not exist. Create first.
% ARP:vrf xyz ipv4 address-family is not enable. Enable first.
```

When a nonexistent static ARP entry or a reserved entry is deleted, the following notification will be displayed:

```
Cannot remove ARP. ARP entry does not exist or reserved.
```

When the ARP cache is fully occupied or the corresponding IP address is the local IP address, a static ARP entry fails to be added and the following notification will be displayed:

```
Cannot add static ARP.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- arp oob
- show arp
- show arp oob
- show arp counter
- show arp detail

1.2 arp-learning enable

Function

Run the **arp-learning enable** command to enable the ARP learning function.

Run the **no** form of this command to disable this feature.

The ARP learning function is enabled by default.

Syntax

arp-learning enable

no arp-learning enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

If this function is disabled on an interface, the interface does not learn dynamic ARP entries. Functions such as any IP ARP and authorized ARP detection will not take effect, either.

Examples

The following example disables the dynamic ARP learning function on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no arp-learning enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp**
- **show arp counter**
- **show arp detail**

1.3 arp anti-ip-attack

Function

Run the **arp anti-ip-attack** command to configure the number of IP packets for triggering the discarding of ARP entries.

Run the **no** form of this command to restore the default configuration.

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

Syntax

arp anti-ip-attack *attack-num*

no arp anti-ip-attack

Parameter Description

attack-num: Number of IP packets for triggering the discarding of ARP entries. The value range is from 0 to 100, and the default value is **3**. The value **0** indicates that ARP-based IP guard is disabled.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When receiving unresolved IP packets, the device sends them to the CPU for address resolution, that is, ARP learning, instead of forwarding them through the hardware. If a large number of such packets are sent to the CPU, the CPU will be congested, affecting 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. Then 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.

This function requires routing resources on the device hardware. Therefore, if hardware resources are sufficient, set *attack-num* to a smaller value. If hardware resources are insufficient, set *attack-num* to a larger value or disable this function.

Examples

The following example sets the number of IP packets for triggering the discarding of ARP entries to 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp anti-ip-attack 5
```

The following example disables ARP-based IP guard.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp anti-ip-attack 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.4 arp any-ip

Function

Run the **arp any-ip** command to enable the any IP ARP function.

Run the **no** form of this command to disable this feature.

The any IP ARP function is disabled by default.

Syntax

arp any-ip

no arp any-ip

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The any IP ARP function allows users to access the Internet 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.

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

- The user's IP address is on 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 on the same network segment as the interface directly connected to the device, but on the network segment of another interface. That means an IP address conflict occurs.

  As the user's IP address is not on 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 from the device. As a result, the user's dynamic ARP entry and direct route are removed and the user cannot receive the reply packet.
  - The device acts as a proxy to respond to ARP requests. After the user host learns the MAC address of the device, any IP ARP is disabled and then enabled again on the interface. When the any IP ARP function is disabled on the interface, the user's dynamic ARP entries and direct routes are immediately deleted. As a result, the user cannot receive the reply.

⚠ 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.

Examples

The following example enables any IP ARP on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp any-ip
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp**
- **show arp counter**
- **show arp detail**

1.5 arp cache interface-limit

Function

Run the **arp cache interface-limit** command to set a limit on the number of ARP entries that can be learned by an interface.

Run the **no** form of this command to restore the default configuration.

No limit is set for the number of ARP entries that can be learned by an interface by default.

Syntax

arp cache interface-limit *limit*

no arp cache interface-limit

Parameter Description

limit: Maximum number of ARP entries that can be learned by an interface, including static ARP entries and dynamic ARP entries. The value range is from 0 to 16000. The default value is **0**, indicating no limit on the number of ARP entries that can be learned by an interface.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

Limiting the number of ARP entries that can be learned by an interface can protect the device against malicious ARP attacks that can result in excessive ARP entries and CPU resource consumption. The configured *limit* value must be equal to or greater than the number of the ARP entries that have been learned by the interface. Otherwise, the configuration does not take effect. The configuration is subject to the ARP entry capacity supported by the device.

Examples

The following example sets the limit on the number of ARP entries that can be learned by port GigabitEthernet 0/1 to 300.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp cache interface-limit 300
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp**

1.6 arp fast-aging enable

Function

Run the **arp fast-aging enable** command to enable the fast ARP entry aging on an interface.

Run the **no** form of this command to restore the default configuration.

The fast ARP entry aging function is disabled by default.

Syntax

arp fast-aging enable

no arp fast-aging enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

Dynamic ARP entries start aging one hour after the aging of their corresponding MAC addresses. If this feature is configured, after their corresponding MAC address age, the dynamic ARP entries age immediately. Pay attention to the following points:

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

Examples

The following example enables fast ARP entry aging on interface VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp fast-aging enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp timeout**

1.7 arp gratuitous-arp-learning enable

Function

Run the **arp gratuitous-arp-learning enable** command to enable the function of learning gratuitous ARP requests.

Run the **no** form of this command to disable this feature.

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

Syntax

arp gratuitous-arp-learning enable

no arp gratuitous-arp-learning enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example disables the function of learning gratuitous ARP requests.

```
Hostname> enable
Hostname# configure terminalHostname(config-if-VLAN 1)# no arp gratuitous-arp-learning enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp gratuitous-send interval**

1.8 arp gratuitous-send interval

Function

Run the **arp gratuitous-send interval** command to enable the function of sending gratuitous ARP requests at intervals.

Run the **no** form of this command to disable this feature.

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

Syntax

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

no arp gratuitous-send

Parameter Description

interval: Interval for sending gratuitous ARP requests, in seconds. The value range is from 1 to 3600.

number: Number of gratuitous ARP requests to be sent. The value range is from 1 to 100, and the default value is **1**.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

When a network interface of a device acts as the gateway of downlink devices, if a downlink device pretends to be the gateway, you can enable the function of sending gratuitous ARP requests at intervals on the interface to advertise the MAC address of the real gateway.

Examples

The following example sends a gratuitous ARP request to interface VLAN 1 every second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp gratuitous-send interval 1 1
```

The following example disables the function of sending gratuitous ARP requests to interface VLAN 1 at intervals.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# no arp gratuitous-send
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- arp gratuitous-arp-learning enable

1.9 arp oob

Function

Run the **arp oob** command to configure a static ARP entry for a management interface.

Run the **no** form of this command to remove this configuration.

No static ARP entry of any management interface is configured in the ARP cache by default.

Syntax

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

no arp oob [*mgmt-name*] *ip-address*

Parameter Description

mgmt-name: Management interface bound to a static ARP entry when multiple management interfaces are supported. The first management interface of a device is bound when *mgmt-name* is not specified.

ip-address: IP address corresponding to a MAC address. The IP address is expressed in dotted decimal notation.

mac-address: DLL address, consisting of 48 bits.

arp-type: ARP encapsulation type. For an Ethernet interface, the keyword is **arpa**.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example configures a static ARP entry for the host management interface on the Ethernet. The IP address is set to 1.1.1.1 and the MAC address is set to 4e54.3800.0002.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp oob 1.1.1.1 4e54.3800.0002 arpa
```

Notifications

When the ARP cache is fully occupied or the corresponding IP address is the local IP address, a static ARP entry fails to be added and the following notification will be displayed:

```
Cannot add static ARP.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp oob**

1.10 arp proxy-resolved

Function

Run the **arp proxy-resolved** command to configure the master VRRP device to judge the existence of the ARP entry corresponding to a destination IP address when the device responds to an ARP request as a proxy ARP.

Run the **no** form of this command to remove this configuration.

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

Syntax

arp proxy-resolved

no arp proxy-resolved

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After the **arp proxy-resolved** command is configured, 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 to give a reply. If no, the master VRRP device does not act as a proxy ARP. In addition, the gateway automatically broadcasts the ARP request for 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 IP address due to absence of the ARP entry corresponding to the destination IP address.

After the **no arp proxy-resolved** command is configured, if the proxy conditions are met, the master VRRP 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.

Examples

The following example configures the master VRRP device not to judge the existence of the ARP entry corresponding to a destination IP address when the device acts as a proxy ARP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no arp proxy-resolved
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.11 arp rate-statistic enable

Function

Run the **arp rate-statistic enable** command to enable the ARP packet rate statistics collection.

Run the **no** form of this command to disable this feature.

The ARP packet rate statistics collection is disabled by default.

Syntax

arp rate-statistic enable

no arp rate-statistic enable

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example enables the ARP packet rate statistics collection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp rate-statistic enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show arp rate-statistic

1.12 arp rate-statistic compute interval

Function

Run the **arp rate-statistic compute interval** command to configure the interval for collecting ARP packet rate statistics.

Run the **no** form of this command to remove this configuration.

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

Syntax

arp rate-statistic compute interval *interval*

no arp rate-statistic compute interval

Parameter Description

interval: Sampling interval, in seconds. The value range is from 1 to 2147483647.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example sets the interval for collecting ARP packet rate statistics to 10 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp rate-statistic compute interval 10
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show arp rate-statistic
- arp rate-statistic enable

1.13 arp resolve vlan

Function

Run the **arp resolve vlan** command to configure ARP to actively send broadcast resolution requests to a specified sub VLAN in a super VLAN.

Run the **no** form of this command to remove this configuration.

Run the **default** form of this command to restore the default configuration.

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

Syntax

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

no arp resolve vlan { *vlan-list* | **none** }

default arp resolve vlan

Parameter Description

vlan-list: Sub VLAN segment. When ARP is configured to actively send broadcast resolution requests to VLANs in the sub VLAN segments in a super VLAN, ARP will only send ARP broadcast packets to these VLANs. The start and end VLANs in a sub VLAN segment are connected by a hyphen (-), and multiple sub VLAN segments are separated by commas (,), for example, 1, 3-5.

none: Indicates that no ARP broadcast requests will be sent to any sub VLAN in a super VLAN.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

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

Most terminals (such as PCs or servers) request ARP information of the gateway before accessing the network. Therefore, there is no need to actively broadcast the 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.

Caution

After the **arp resolve vlan** *vlan-list* command is run, the device will only send ARP broadcast requests to the VLANs specified in *vlan-list* in the super VLAN, and other sub VLANs not in *vlan-list* will not receive ARP broadcast requests. In particular, if an authentication-exempt VLAN is configured and the authentication-exempt VLAN is not in *vlan-list* of **arp resolve vlan**, ARP requests will not be broadcast to the authentication-exempt VLAN.

Examples

The following example configures ARP to actively send broadcast resolution requests to sub VLANs 0-20 and 25-30 in the super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp resolve vlan 10-20,25-30
```

The following example cancels sending resolution requests to VLANs 10-20.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no arp resolve vlan 10-20
```

The following example configures the device not to actively send ARP resolution requests to any sub VLAN in the super VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp resolve vlan none
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 arp retry interval

Function

Run the **arp retry interval** command to specify the ARP request retransmission interval.

Run the **no** form of this command to restore the default configuration.

The default ARP request retransmission interval is 1 second.

Syntax

arp retry interval *interval*

no arp retry interval

Parameter Description

interval: ARP request retransmission interval, in seconds. The value range is from 1 to 3600.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

2

Usage Guidelines

The ARP request retransmission interval can be configured globally and on a Layer 3 interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the ARP request retransmission interval is set to 5 seconds in global configuration mode and set to 2 seconds on SVI 1, the ARP request retransmission interval of SVI 1 is 2 seconds. The ARP request retransmission interval of other interfaces (including new interfaces) is subject to global configuration, that is, 5 seconds.

The shorter the retransmission interval is, the faster the resolution is, and the more bandwidth will be consumed. If the network resources are insufficient, you are advised to set the ARP request retransmission interval to a larger value to reduce the consumption of network bandwidths. Generally, the interval should not be greater than the aging time of dynamic ARP entries.

Examples

The following example sets the ARP request retransmission interval to 30 seconds in global configuration mode.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp retry interval 30
```

The following example sets the ARP request retransmission interval of SVI 1 to 18 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp retry interval 18
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp retry times**

1.15 arp retry times

Function

Run the **arp retry times** command to configure the number of times that an ARP request can be transmitted consecutively.

Run the **no** form of this command to restore the default configuration.

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 device sends the ARP request packets for another four times.

Syntax

arp retry times *times*

no arp retry times

Parameter Description

times: Number of times that the same ARP request can be transmitted. The value range is from 1 to 100, and the default value is **5**. When the value is set to **1**, an ARP request is sent once, and will not be retransmitted.

Command Modes

Global configuration mode

Interface configuration mode

Default Level

2

Usage Guidelines

The number of times that an ARP request can be transmitted consecutively can be configured globally and on a Layer 3 interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the number of times that an ARP request can be transmitted consecutively is set to 1 in global configuration mode and set to 3 on SVI 1, the number of times that an ARP request can be transmitted is 3 for SVI 1. The number of times that an ARP request can be transmitted on other interfaces (including new interfaces) is subject to global configuration, that is, 1.

The more times an ARP packet can be transmitted consecutively, the more likely the resolution will succeed, and the more bandwidth will be consumed. If the network resources are insufficient, you are advised to set the number of times to a smaller value to reduce the consumption of network bandwidths.

Examples

The following example sets the number of times that an ARP request packet can be transmitted consecutively to 1 in global configuration mode, that is, ARP request packets will not be retransmitted.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp retry times 1
```

The following example sets the number of times that an ARP request packet can be transmitted consecutively to 2 in global configuration mode, that is, an ARP request packet will be retransmitted once.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp retry times 2
```

The following example sets the number of times that an ARP request packet can be transmitted consecutively to 5 for SVI 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp retry times 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp retry interval**

1.16 arp scan

Function

Run the **arp scan** command to enable ARP scanning.

Run the **no** form of this command to disable this feature.

ARP scanning is disabled by default.

Syntax

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

no arp scan [*start-ip-address end-ip-address*]

Parameter Description

start-ip-address: Start IP address of the ARP scanning range. The start IP address must be smaller than or equal to the end IP address.

end-ip-address: End IP address of the ARP scanning range. The end IP address must be greater than or equal to the start IP address.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

This function is usually used together with the Web-based dynamic-to-static ARP entry conversion function.

By configuring the IP address range for ARP scanning, users can scan neighbors in this range, thereby reducing the waiting time. The number of hosts in the ARP scanning range must not exceed 1,024.

The start and end IP addresses of the ARP scanning range must be on the same network segment as the interface IP address that may serve as the master or slave IP address.

If the start and end IP addresses are not specified, only the neighbors on the same network segment as the master IP address of the interface are scanned. The subnet mask of the master IP address must consist of at least 22 bits.

ARP scanning configuration takes effect only once. It cannot be saved and will lose effect the next time. ARP scanning takes effect when the Layer 3 interface is up (that is, the link is up and an IP address is configured).

Examples

The following example enables ARP scanning on port GigabitEthernet 0/1 without specifying the IP address range.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp scan
```

The following example enables ARP scanning on port GigabitEthernet 0/0 with the IP address range specified.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/0
Hostname(config-if-GigabitEthernet 0/0)# arp scan 1.1.1.1 1.1.1.10
```

Notifications

When a start IP address or end IP address is not a valid host address, or the start IP address is greater than the end IP address, or the start IP address and end IP address are not on the same network segment as the interface IP address, the following notification will be displayed:

```
%notice: Invalid ip address range.
```

When the number of hosts in a specified range is greater than 1,024, the following notification will be displayed:

```
%notice: Failed to scan because ip address range is larger than 1024.
```

When no Layer 3 interface is up, the following notification will be displayed:

```
%notice: Failed to scan because this interface is not up.
```

Common Errors

- The start IP address is greater than the end IP address.
- The start IP address and the end IP address are not on the same network segment as the IP interface address.

Platform Description

This command is supported only on egress gateways (EGs), network provider edges (NPEs), and network border routers (NBRs).

Related Commands

- **arp scan auto**

1.17 arp scan auto

Function

Run the **arp scan auto** command to enable scheduled automatic ARP scanning.

Run the **no** form of this command to disable this feature.

The scheduled automatic ARP scanning function is disabled by default.

Syntax

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

no arp scan auto [*start-ip-address end-ip-address*]

Parameter Description

start-ip-address: Start IP address of the ARP scanning range. The start IP address must be smaller than or equal to the end IP address.

end-ip-address: End IP address of the ARP scanning range. The end IP address must be greater than or equal to the start IP address.

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The scheduled automatic ARP scanning function is enabled by default, and scheduled automatic ARP scanning is performed once every 5 minutes. It takes effect only on interfaces in the up state.

By configuring the IP address range for ARP scanning, users can scan neighbors in this range, thereby reducing the waiting time. The number of hosts in the ARP scanning range must not exceed 1,024.

The IP addresses of neighbors with ARP entries available will not be scanned.

Up to 30 instances can be configured.

Examples

The following example enables scheduled automatic ARP scanning on VLAN 1, with the IP address range from 1.1.1.1 to 1.1.1.10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# arp scan auto 1.1.1.1 1.1.1.10
```

Notifications

When a start IP address or end IP address is not a valid host address, or the start IP address is greater than the end IP address, the following notification will be displayed:

```
 Invalid ip address range.
```

When the number of hosts in a specified range is greater than 1,024, the following notification will be displayed:

```
Failed to scan because ip address range is larger than 1024.
```

When more than 30 instances are configured, the following notification will be displayed:

```
The number of arp auto-scan ip exceed 30.
```

Common Errors

- The start IP address is greater than the end IP address.
- The number of hosts in a specified range is greater than 1,024.

Platform Description

N/A

Related Commands

- **arp scan**
- **arp scan interval**
- **arp scan rate**

1.18 arp scan interval

Function

Run the **arp scan interval** command to configure the interval for scheduled automatic ARP scanning.

Run the **no** form of this command to restore the default configuration.

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

Syntax

arp scan interval *time*

no arp scan interval

Parameter Description

time: Interval of scheduled ARP scanning, in minutes. The range is from 1 to 30.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

The interval is the duration between the end of scanning on all interfaces and the start of the next scanning.

Examples

The following example sets the interval of scheduled ARP scanning to 1 minute.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp scan interval 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp scan auto**
- **arp scan rate**

1.19 arp scan rate

Function

Run the **arp scan rate** command to configure the rate of scheduled automatic ARP scanning.

Run the **no** form of this command to remove this configuration.

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

Syntax

arp scan rate *rate-value*

no arp scan rate

Parameter Description

rate-value: Rate of scheduled automatic ARP scanning, in IP addresses per second. The value range is from 1 to 100.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

The scanning rate is the number of IP addresses that the device scans and successfully learns the ARP packets from per second. For example, when the rate is set to 100, the device scans a maximum of 100 IP addresses per second.

If scanning has be done on all the required network segments and ARP packets have been successfully learned, the next scanning rate is 0.

Examples

The following example sets the rate of scheduled automatic ARP scanning to 8 0 IP addresses per second.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp scan rate 80
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp scan auto**
- **arp scan interval**

1.20 arp suppress-auth-vlan-req

Function

Run the **arp suppress-auth-vlan-req** command to restrain the device from sending ARP requests to authenticated VLANs.

Run the **no** form of this command to remove this configuration.

ARP requests are not sent to authenticated VLANs by default.

Syntax

arp suppress-auth-vlan-req

no arp suppress-auth-vlan-req

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

This configuration is supported only on SVIs.

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 before accessing 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.

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

Examples

The following example enables the function of sending ARP requests to authenticated VLANs on VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# no arp suppress-auth-vlan-req
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 arp switch-over resolve

Function

Run the **arp switch-over resolve** command to actively send ARP requests to terminals after active and standby VSU switchover.

Run the **no** form of this command to remove this configuration.

ARP requests are not actively sent to terminals after active and standby VSU switchover by default.

Syntax

arp switch-over resolve

no arp switch-over resolve

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

This function can be enabled to quickly update ARP entries of a downlink device after active and standby VSU 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 (instead of interfaces not in a super VLAN) of up to 1000 downlink terminals to trigger the terminals to reply to these ARP requests. Then, the device can update the ARP and MAC tables.

Examples

The following example actively sends ARP requests to terminals after active and standby VSU switchover.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp switch-over resolve
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.22 arp timeout

Function

Run the **arp timeout** command to configure the timeout time for dynamic ARP entries in the ARP cache.

Run the **no** form of this command to restore the default configuration.

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

Syntax

arp timeout *time*

no arp timeout

Parameter Description

time: Timeout time, in seconds. The value range is from 0 to 2147483.

Command Modes

Interface configuration mode

Global configuration mode

Default Level

2

Usage Guidelines

The ARP timeout configuration only applies to the 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. Unless otherwise specified, the ARP timeout time does not need to be configured.

The ARP aging time can be configured globally and on a specified interface. The configuration in interface configuration mode takes priority over that in global configuration mode. For example, when the ARP aging time is set to 3,000 seconds in global configuration mode and to 1,800 seconds on interface 1, the ARP aging time of interface 1 is 1800s. The ARP aging time of other interfaces (including new interfaces) is subject to the global ARP aging time, that is, 3,000s.

Examples

The following example sets the timeout time of dynamic ARP entries learned by port GigabitEthernet 0/1 to 120s.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp timeout 120
```

The following example sets the ARP aging time to 3,000 seconds globally. If no aging time is configured for an interface, the ARP aging time is 3000 seconds for all Layer 3 interfaces.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp timeout 3000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp timeout**

1.23 arp trusted

Function

Run the **arp trusted** command to configure the maximum number of trusted ARP entries.

Run the **no** form of this command to restore the default configuration.

The maximum number of trusted ARP entries is **8000** by default.

Syntax

arp trusted *number*

no arp trusted

Parameter Description

number: Maximum number of trusted ARP entries. The value range is from 10 to 14976.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Enable trusted ARP before configuring this function. 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 number based on the actual requirement. Do not set it to an excessively large value.

The maximum value of the *number* parameter can be the capacity of the ARP table minus 1,024.

Examples

The following example sets the maximum number of trusted ARP entries to 1,000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp trusted 1000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **service trustedarp**

1.24 arp trust-monitor enable

Function

Run the **arp trust-monitor enable** command to enable ARP trust monitoring.

Run the **no** form of this command to disable this feature.

ARP trust monitoring is disabled by default.

Syntax

arp trust-monitor enable

no arp trust-monitor enable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

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

(1) 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 unicasts an 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.

(2) If the corresponding ARP entry exists and the MAC address is not updated, the device does not perform NUD.

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

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 does not perform NUD for learning or updating ARP entries.

Examples

The following example enables ARP trust detection on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# arp trust-monitor enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.25 arp trusted aging

Function

Run the **arp trusted aging** command to enable trusted ARP aging.

Run the **no** form of this command to restore the default configuration.

Trusted ARP entries are not aged by default.

Syntax

arp trusted aging

no arp trusted aging

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Trusted ARP aging can be configured, with the aging time same as the dynamic ARP aging time. You can run the **arp timeout** command in interface configuration mode to configure the aging time.

Examples

The following example enables trusted ARP aging.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp trusted aging
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp timeout**

1.26 arp trust user-vlan

Function

Run the **arp trust user-vlan** command to enable VLAN translation when a trusted ARP entry is added.

Run the **no** form of this command to remove this configuration.

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

Syntax

arp trust user-vlan *vlan-id* **translated-vlan** *vlan-id*

no arp trust user-vlan *vlan-id* **translated-vlan** *vlan-id*

Parameter Description

user-vlan *vlan-id*: Indicates the VLAN ID set for a server.

translated-vlan *vlan-id*: Indicated the VLAN ID after translation.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

Enable trusted APR before configuring this function.

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

Examples

The following example enables VLAN translation when a trusted ARP entry is added. A server delivers VLAN 3 but actually, trusted ARP takes effect on VLAN 5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp trust user-vlan 3 translated-vlan 5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.27 arp unresolve

Function

Run the **arp unresolve** command to configure the maximum number of unresolved ARP entries.

Run the **no** form of this command to restore the default configuration.

The maximum number of unresolved ARP entries that can be held in an ARP cache is **16000** by default.

Syntax

arp unresolve *unresolved-number*

no arp unresolve

Parameter Description

unresolved-number: Maximum number of unresolved ARP entries. The value range is from 1 to 16000.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

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 cache after a while, you are advised to use this command to limit the number of unresolved ARP entries.

Examples

The following example sets the maximum number of unresolved ARP entries on the device to 500.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp unresolve 500
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

-
-
-

1.28 arp strict-learning enable

Function

Run the **arp strict-learning enable** command to enable strict dynamic ARP learning.

Run the **no** form of this command to disable this feature.

Strict dynamic ARP learning is disabled by default.

Syntax

arp strict-learning enable

no arp strict-learning enable

Parameter Description

N/A

Command Modes

Global configuration mode

Interface configuration mode

Default Level

2

Usage Guidelines

After strict dynamic ARP learning is enabled, only the reply packets in response to the ARP request packets actively sent by the device can trigger the device to learn ARP entries.

The strict dynamic ARP learning can be configured globally and on an interface. The configuration in interface configuration mode takes priority over that in global configuration mode.

Examples

The following example enables strict dynamic ARP learning globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp strict-learning enable
```

The following example disables strict dynamic ARP learning globally.

```
Hostname> enable
```

```
Hostname# configure terminal
Hostname(config)# no arp strict-learning enable
```

The following example enables strict dynamic ARP learning on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/10)# arp strict-learning enable
```

The following example disables strict dynamic ARP learning on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# no arp strict-learning enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show arp anti-attack statistics

1.29 arp filter gratuitous

Function

Run the **arp filter gratuitous** command to enable gratuitous ARP filtering.

Run the **no** form of this command to disable this feature.

Gratuitous ARP filtering is disabled by default.

Syntax

arp filter gratuitous

no arp filter gratuitous

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example enables gratuitous ARP filtering.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp filter gratuitous
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.30 arp filter acl

Function

Run the **arp filter acl** command to enable ARP-based access control list (ACL) filtering.

Run the **no** form of this command to disable this feature.

ARP-based ACL filtering is disabled by default.

Syntax

arp filter acl *acl-number*

no arp filter acl

Parameter Description

acl-number: Associated ACL. The value range is from 1 to 199 and 1300 to 2899.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After this function is enabled, a device will filter out ARP packets that hit ACL rules.

Examples

The following example enables ARP-based ACL filtering.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp filter acl 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**

1.31 arp filter smac-illegal

Function

Run the **arp filter smac-illegal** command to enable the function of checking the source MAC addresses of ARP packets.

Run the **no** form of this command to disable this feature.

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

Syntax

arp filter smac-illegal

no arp filter smac-illegal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After this function is enabled, a device will filter out ARP packets whose source MAC addresses is not consistent with the Ethernet source MAC address.

Examples

The following example enables the function of checking the source MAC addresses of ARP packets.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp filter smac-illegal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show arp anti-attack statistics

1.32 arp filter dmac-illegal

Function

Run the **arp filter dmac-illegal** command to enable the function of checking the destination MAC addresses of ARP packets.

Run the **no** form of this command to disable this feature.

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

Syntax

arp filter dmac-illegal

no arp filter dmac-illegal

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

After this function is enabled, a device will filter out ARP packets whose destination MAC addresses is not consistent with the Ethernet destination MAC address.

Examples

The following example enables the function of checking the destination MAC addresses of ARP packets.

```
Hostname> enable
Hostname# configure terminal
```

```
Hostname(config)# arp filter dmac-illegal
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp anti-attack statistics**
-

1.33 arp warning-limit

Function

Run the **arp warning-limit** command to configure the ARP alarm rate limit.

Run the **no** form of this command to restore the default configuration.

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

Syntax

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

no arp warning-limit

Parameter Description

interval *interval*: Specifies the ARP alarm rate limit interval, in seconds. The value range is 1 to 180. The default value is **50**.

times *time*: Specifies the upper limit of alarms allowed within the ARP alarm rate limit interval. The value range is from 1 to 1,024, and the default value is **10**.

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

This command can be used to adjust the printing rate of ARP syslog alarms. The actual ARP alarm rate may be lower than the configured rate, depending on system performance.

Examples

The following example sets the ARP alarm rate limit interval to 60 seconds and the upper limit of alarms allowed within this interval to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# arp warning-limit interval 60 times 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

This is applicable to devices with multiple line cards.

Related Commands

N/A

1.34 clear arp-cache

Function

Run the **clear arp-cache** command to clear dynamic ARP mapping records in the ARP cache.

Syntax

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

Parameter Description

vrf *vrf-name*: Deletes dynamic ARP entries of a specified VRF instance. If this parameter is not specified, it indicates the public network instance.

oob: Configures out-of-band management.

ip-address: IP address whose dynamic ARP entries are to be deleted. All dynamic ARP entries are deleted by default.

mask: Subnet mask. After this parameter is specified, dynamic ARP entries in the subnet will be deleted and the preceding IP address must be set to a subnet ID. Dynamic ARP entries specified in the *ip-address* parameter are deleted by default.

interface *interface-type interface-number*: Clears the dynamic ARP entries of a specified interface. Dynamic ARP entries of all interfaces are deleted by default.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

In gateway authentication mode, dynamic ARP entries in authenticated VLANs will not be cleared.

On devices enabled with the Network Foundation Protection Policy (NFPP), only one ARP packet is received for each MAC address (or IP address) per second by default. If the **clear arp-cache** command is run twice within 1 second, the second reply may be filtered out and the ARP resolution may fail.

Examples

The following example clears all dynamic ARP entries in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache
```

The following example clears dynamic entry 1.1.1.1 in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache 1.1.1.1
```

The following example deletes dynamic ARP entries of SVI 1.

```
Hostname> enable
Hostname# clear arp-cache interface Vlan 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.35 clear arp-cache trusted

Function

Run the **clear arp-cache trusted** command to clear trusted ARP entries in the ARP cache.

Syntax

clear arp-cache [**vrf** *vrf-name* | **oob**] **trusted** [*ip-address* [*mask*]]

Parameter Description

vrf *vrf-name*: Deletes dynamic ARP entries of a specified VRF instance. If this parameter is not specified, it indicates the public network instance.

oob: Configures out-of-band management.

ip-address: IP address whose trusted ARP entries are to be deleted. All trusted ARP entries are deleted by default.

mask: Subnet mask. After this parameter is specified, trusted ARP entries in the subnet will be deleted and the preceding IP address must be set to a subnet ID. Trusted ARP entries specified in the *ip-address* parameter are deleted by default.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

N/A

Examples

The following example clears all trusted ARP entries in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache trusted
```

The following example clears trusted ARP entries with the IP address of 1.1.1.1 in the ARP cache.

```
Hostname> enable
Hostname# clear arp-cache trusted 1.1.1.1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 clear arp-cache packet statistics

Function

Run the **clear arp-cache packet statistics** command to clear ARP packet statistics.

Syntax

clear arp-cache packet statistics [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface number.

Command Modes

Privileged EXEC mode

Default Level

2

Usage Guidelines

After ARP packet statistics are cleared, packet statistic starts from 0 again.

Examples

The following example clears ARP packet statistics.

```
Hostname> enable
Hostname# clear arp-cache packet statistics
```

The following example clears ARP packet statistics on VLAN 1.

```
Hostname> enable
Hostname# clear arp-cache packet statistics vlan 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show arp packet statistics**

1.37 ip proxy-arp

Function

Run the **ip proxy-arp** command to enable proxy ARP on an interface.

Run the **no** form of this command to disable this feature.

Proxy ARP is disabled by default.

Syntax

ip proxy-arp

no ip proxy-arp

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

The device enabled with proxy ARP can help a host obtain MAC addresses of IP hosts in other networks or subnets. When a proxy device receives an ARP request whose sender's source IP address is in a different network from the destination IP address, if the device knows the route to the destination IP address, it sends an ARP reply containing its own Ethernet MAC address.

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

Examples

The following example enables proxy ARP on port GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface gigabitethernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# ip proxy-arp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface** (IP service information/IPv4 basic information)

1.38 local-proxy-arp

Function

Run the **local-proxy-arp** command to enable local proxy ARP.

Run the **no** form of this command to disable this feature.

Local proxy ARP is disabled by default.

Syntax

local-proxy-arp

no local-proxy-arp

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

2

Usage Guidelines

After local proxy ARP is enabled, the device can help hosts obtain the MAC addresses of other hosts in the same subnet. For example, when port protection is enabled on the device, users connected to different ports of the device are isolated at Layer 2. After local proxy ARP is enabled and the device receives an ARP request, the device acts as a proxy and sends an ARP reply containing its own Ethernet MAC address. In this case, different users communicate with each other through Layer 3 routes.

Examples

The following example enables local proxy ARP in VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface vlan 1
Hostname(config-if-VLAN 1)# local-proxy-arp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **show ip interface** (IP service information/IPv4 basic information)

1.39 service trustedarp

Function

Run the **service trustedarp** command to enable trusted ARP.

Run the **no** form of this command to disable this feature.

Trusted ARP is disabled by default.

Syntax

service trustedarp

no service trustedarp

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

2

Usage Guidelines

When a user goes online on a GPRS support node (GSN) client, the authentication server obtains the user's real 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 the network administrator and does not require extra work from them.

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. Before an ARP entry ages, the device actively sends an ARP request to detect whether the corresponding 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 will not dynamically update the MAC addresses and interfaces in the trusted ARP entries by learning ARP packets.

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

Examples

The following example enables trusted ARP.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# service trustedarp
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **arp trusted**
- **arp trusted aging**
- **arp trust user-vlan**

1.40 show arp

Function

Run the **show arp** command to display the ARP cache.

Syntax

show arp [*interface-type interface-number* | **trusted** [*ip-address* [*mask*]] | [**vrf** *vrf-name*] [*ip-address* [*mask*] | *mac-address* | **complete** | **incomplete** | **static**]

Parameter Description

interface-type interface-number: *interface-type* indicates the interface type and *interface-number* indicates the interface number. After the parameter is specified, the ARP entries of a specified Layer 3 interface or Layer 2 interface are displayed.

vrf *vrf-name*: Displays the ARP entries of a specified VRF instance.

trusted: Displays trusted ARP entries. Currently, only the global VRF instance supports trusted ARP entries.

ip-address: IP address whose ARP entries need to be displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.

mask: Subnet mask. After this parameter is specified, ARP entries within the IP subnet will be displayed. If keyword **trusted** is specified, only the trusted ARP entries are displayed. Otherwise, the non-trusted ARP entries are displayed.

mac-address: MAC address whose ARP entries need to be displayed.

complete: Displays all resolved dynamic ARP entries.

incomplete: Displays all unresolved dynamic ARP entries.

static: Displays all static ARP entries and their sources.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP cache.

```
Hostname> enable
Hostname# show arp
Total Numbers of Arp: 7
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   0         0013.20a5.7a5f  arpa   VLAN 1
Internet  192.168.195.67   0         001a.a0b5.378d  arpa   VLAN 1
Internet  192.168.195.65   0         0018.8b7b.713e  arpa   VLAN 1
Internet  192.168.195.64   0         0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.63   0         001a.a0b5.3990  arpa   VLAN 1
Internet  192.168.195.62   0         001a.a0b5.0b25  arpa   VLAN 1
Internet  192.168.195.5    --        00d0.f822.33b1  arpa   VLAN 1
```

The following example displays the ARP entry of IP address 192.168.195.68.

```
Hostname> enable
Hostname# show arp 192.168.195.68
Protocol  Address    Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   1   0013.20a5.7a5f  arpa   VLAN 1
```

The following example displays ARP entries of IP subnet 92.168.195.0/24.

```
Hostname> enable
Hostname# show arp 192.168.195.0 255.255.255.0
Protocol  Address    Age(min)  Hardware   Type   Interface
Internet  192.168.195.64   0   0018.8b7b.9106  arpa   VLAN 1
Internet  192.168.195.2    1   00d0.f8ff.f00e  arpa   VLAN 1
Internet  192.168.195.5    --   00d0.f822.33b1  arpa   VLAN 1
Internet  192.168.195.1    0   00d0.f8a6.5af7  arpa   VLAN 1
Internet  192.168.195.51   1   0018.8b82.8691  arpa   VLAN 1
```

The following example displays the ARP entry of MAC address 001a.a0b5.378d.

```
Hostname> enable
Hostname# show arp 001a.a0b5.378d
Protocol  Address  Age(min)  Hardware  Type   Interface
Internet  192.168.195.67   4   001a.a0b5.378d  arpa   VLAN 1
```

The following example displays all static ARP entries and their sources.

```
Hostname> enable
Hostname# show arp static
Protocol  Address  Age(min)  Hardware  Type   Interface         Origin
Internet  192.168.23.55    <static>  0000.0000.0010  arpa   VLAN 100   Configure
Internet  192.168.23.56    <static>  0000.0000.0020  arpa   VLAN 100
Authentication
Internet  192.168.23.57    <static>  0000.0000.0020  arpa   VLAN 100   DHCP-
Snooping
2  static arp entries exist.
```

Table 1-1Output Fields of the show arp Command

Field	Description
Protocol	Protocol. **Internet** indicates the Internet protocol.
Address	IPv4 address.
Age(min)	Duration of an entry. ● For a local IP address, "--" is displayed. ● For a static entry, "static" is displayed. ● For a dynamic entry, the duration of the entry is displayed in minutes.
Hardware	Hardware address, that is, a 48-bit MAC address consisting of three parts separated by dots (.), with each part containing 16 bits. The address is expressed in hexadecimal notation.
Type	Type of a hardware address. It is ARPA for all Ethernet addresses.
Interface	Layer 3 interface corresponding to an ARP entry. Nothing is displayed if the IP address of a static ARP is not in any directly connected network segment of the device.

Field	Description
Origin	Source of a static ARP entry. ● **Configure** indicates that the entry is manually configured. ● **Authentication** indicates that the entry is generated via authentication.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.41 show arp oob

Function

Run the **show arp oob** command to display the ARP cache on a management interface.

Syntax

show arp oob [*ip-address* [*mask*] | *mac-address* | **complete | incomplete | static**]

Parameter Description

ip-address: IP address whose ARP entries need to be displayed.

mask: Subnet mask. After this parameter is specified, ARP entries within the IP subnet will be displayed.

mac-address: MAC address whose ARP entries need to be displayed.

static: Displays all static ARP entries.

complete: Displays all resolved dynamic ARP entries.

incomplete: Displays all unresolved dynamic ARP entries.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP cache on the management interface.

```
Hostname> enable
```

```
Hostname# show arp oob
Total Numbers of Arp: 7
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   0         0013.20a5.7a5f  arpa   mgmt 0
Internet  192.168.195.67   0         001a.a0b5.378d  arpa   mgmt 0
Internet  192.168.195.65   0         0018.8b7b.713e  arpa   mgmt 0
Internet  192.168.195.64   0         0018.8b7b.9106  arpa   mgmt 0
Internet  192.168.195.63   0         001a.a0b5.3990  arpa   mgmt 0
Internet  192.168.195.62   0         001a.a0b5.0b25  arpa   mgmt 0
Internet  192.168.195.5    --        00d0.f822.33b1  arpa   mgmt 0
```

The following example displays the ARP entry of IP address 192.168.195.68 on the management interface.

```
Hostname> enable
Hostname# show arp oob 192.168.195.68
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.68   1         0013.20a5.7a5f  arpa   mgmt 0
```

The following example displays ARP entries of IP subnet 92.168.195.0/24 on the management interface.

```
Hostname> enable
Hostname# show arp 192.168.195.0 255.255.255.0
Protocol  Address         Age(min)  Hardware        Type   Interface
Internet  192.168.195.64   0        0018.8b7b.9106  arpa   mgmt 0
Internet  192.168.195.2    1        00d0.f8ff.f00e  arpa   mgmt 0
Internet  192.168.195.5    --       00d0.f822.33b1  arpa   mgmt 0
Internet  192.168.195.1    0        00d0.f8a6.5af7  arpa   mgmt 0
Internet  192.168.195.51   1        0018.8b82.8691  arpa   mgmt 0
```

The following example displays the ARP entry of MAC address 001a.a0b5.378d on the management interface.

```
Hostname> enable
Hostname# show arp 001a.a0b5.378d
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  192.168.195.67   4         001a.a0b5.378d  arpa   mgmt 0
```

Table 1-1Output Fields of the show arp oob Command

Field	Description
Protocol	Protocol. **Internet** indicates the Internet protocol.
Address	IPv4 address.
Age(min)	Duration of an entry. ● For a local IP address, "--" is displayed. ● For a static entry, "static" is displayed. For a dynamic entry, the duration of the entry is displayed in minutes.
Hardware	Hardware address, that is, a 48-bit MAC address consisting of three parts separated by dots (.), with each part containing 16 bits. The address is expressed in hexadecimal notation.
Type	Type of a hardware address. It is ARPA for all Ethernet addresses.

Field	Description
Interface	Layer 3 interface corresponding to an ARP entry. Nothing is displayed if the IP address of a static ARP is not in any directly connected network segment of the device.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.42 show arp counter

Function

Run the **show arp counter** command to display the number of ARP entries in the ARP cache.

Syntax

show arp counter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

This command is used to display the number of ARP entries in the ARP cache, including static ARP entries and dynamic ARP entries.

Examples

The following example displays the number of ARP entries in the ARP cache.

```
Hostname> enable
Hostname# show arp counter
ARP Limit:                75000
Count of static entries:  0
Count of dynamic entries: 1 (complete: 1  incomplete: 0)
Total:                    1
```

Table 1-1Output Fields of the show arp counter Command

Field	Description
ARP Limit	ARP capacity limit.
Count of static entries	Number of static entries.
Count of dynamic entries	Number of dynamic entries.
complete	Number of resolved ARP entries.
incomplete	Number of unresolved ARP entries.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.43 show arp detail

Function

Run the **show arp detail** command to display the details about the ARP cache.

Syntax

show arp detail [*interface-type interface-number* | **trusted** [*ip-address* [*mask*]] | [**vrf** *vrf-name*] [*ip-address* [*mask*] | *mac-address* | **complete** | **incomplete | static**] | **subvlan** { **min-max** *min-value max-value* | *subvlan-number* }]

Parameter Description

interface-type interface-number: *interface-type* indicates the interface type and *interface-number* indicates the interface number. After the parameter is specified, the ARP entries of a specified Layer 3 interface or Layer 2 interface are displayed.

vrf *vrf-name*: Displays ARP entries of a specified VRF instance.

trusted: Displays trusted ARP entries. Currently, only the global VRF instance supports trusted ARP entries.

ip-address: IP address whose ARP entries need to be displayed.

mask: Subnet mask. After this parameter is specified, ARP entries of a specified network segment will be displayed.

mac-address: MAC address whose ARP entries need to be displayed.

complete: Displays all resolved dynamic ARP entries.

incomplete: Displays all unresolved dynamic ARP entries.

static: Displays all static ARP entries.

subvlan: Displays ARP entries of a specified sub VLAN.

min-max: Displays the maximum and minimum values of sub VLAN IDs corresponding to ARP entries in a specified sub VLAN range.

min-value: Minimum value of sub VLAN IDs corresponding to ARP entries in a specified sub VLAN range.

max-value: Maximum value of sub VLAN IDs corresponding to ARP entries in a specified sub VLAN range.

subvlan-number: Sub VLAN ID. After this parameter is specified, ARP entries of a specified single sub VLAN will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

This command is used to display the details about the ARP cache, including the type of ARP entries (dynamic, static, local, or trusted entries) and the Layer 2 ports.

Note

If the entered *min-value* is greater than *max-value*, no error is displayed, and ARP entries in the specified sub VLAN range are displayed.

Examples

The following example displays the details about the ARP cache.

```
Hostname> enable
Hostname# show arp detail
IP Address     MAC Address      Type      Age(min)   Interface  Port     SubVlan
Gid
20.1.1.2       0020.0101.0002   Static     --         Te2/5      --       --
0
20.1.1.1       00d0.f822.33bb   Local      --         Te2/5      --       --
0
1.1.1.2        00d0.1111.1112   Dynamic    1          Vl2        Te2/1    4
0
1.1.1.1        00d0.f822.33bb   Local      --         Vl2        --       --
0
```

Table 1-1 Output Fields of the show arp detail Command

Field	Description
IP Address	IP address corresponding to a hardware address.
MAC Address	Hardware address corresponding to the IP address.

Field	Description
Type	ARP entry types, including static, dynamic, trusted, and local.
Age	ARP aging time, in minutes.
Interface	Layer 3 interface associated with an IP address.
Port	Layer 2 port associated with an ARP entry.
SubVlan	Sub VLAN associated with an ARP entry.
Gid	IMLAG group ID.

Notifications

N/A

Platform Description

N/A

Related Commands

- show arp

1.44 show arp packet statistics

Function

Run the **show arp packet statistics** command to display ARP packet statistics.

Syntax

show arp packet statistics [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface name. After this parameter is specified, the ARP packet statistics of a specified interface will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP packet statistics of all interfaces.

```
Hostname> enable
Hostname# show arp packet statistics
Interface              Received  Received Received  Sent      Sent
Name                   Requests  Replies  Others    Requests  Replies
--------   ----  -------  ----  ---
GigabitEthernet 0/0    0         0        0         0         0
GigabitEthernet 0/1    143649    232      0         2         0
GigabitEthernet 0/2    0         0        0         0         0
GigabitEthernet 0/3    0         0        0         0         0
GigabitEthernet 0/4    0         0        0         0         0
GigabitEthernet 0/5    0         0        0         0         0
GigabitEthernet 0/6    0         0        0         0         0
Loopback 1             0         0        0         0         0
```

Table 1-1Output Field of the show arp packet statistics Command

Field	Description
Interface Name	Interface name.
Received Requests	Number of received ARP requests.
Received Replies	Number of received ARP replies.
Received Others	Number of received other ARP packets.
Sent Requests	Number of sent ARP requests.
Sent Replies	Number of sent ARP replies.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.45 show arp rate-statistic

Function

Run the **show arp rate-statistic** command to display the ARP packet rate statistics.

Syntax

show arp rate-statistic [*interface-type interface-number*]

Parameter Description

interface-type interface-number: Interface type and interface ID. After this parameter is specified, the statistics on ARP packets of a specified interface will be displayed.

Command Modes

All modes except the user EXEC mode

Default Level

2

Usage Guidelines

This command is used to display the ARP packet rate statistics (including received ARP requests, received ARP replies, received other ARP packets, sent ARP requests, and sent ARP replies).

Examples

The following example displays the ARP packet rate statistics of all interfaces.

```
Hostname> enable
Hostname(config)# show arp rate-statistic
Interface Sampling Received     Received     Received    Sent           Sent
Name      time    Requests(pps) Replies(pps) Others(pps) Requests(pps)
Replies(pps)
--------      ----      ----      ----      ----      ---
TenGigabitEthernet 0/15     1     0      0          0         1       0
Mgmt 0                      1     7      0          0         0       0
```

The following example displays the ARP packet rate statistics of SVI 1.

```
Hostname> enable
Hostname(config)# show arp rate-statistic interface vlan 1
Interface Sampling Received     Received     Received    Sent           Sent
Name      time    Requests(pps) Replies(pps) Others(pps) Requests(pps)
Replies(pps)
--------       ----      ----      ----      ----      ----      ---
VLAN 1      1          0                0             0               0
0
```

Table 1-1Output Field of the show arp rate-statistic Command

Field	Description
Interface Name	Interface name.
Sampling time	Sampling time.
Received Requests(pps)	Rate of received ARP requests.
Received Replies(pps)	Rate of received ARP replies.
Received Others(pps)	Rate of received other ARP packets.

Field	Description
Sent Requests(pps)	Rate of sent ARP requests.
Sent Replies(pps)	Rate of sent ARP replies.

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

Related Commands

N/A

1.46 show arp timeout

Function

Run the **show arp timeout** command to display the aging time of dynamic ARP entries.

Syntax

show arp timeout

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the aging time of dynamic ARP entries.

```
Hostname> enable
Hostname# show arp timeout
```

```
Interface               arp timeout(sec)
--------  ------
VLAN 1                  3600
```

Table 1-1Output Fields of the show arp timeout Command

Field	Description
Interface	Interface name.
arp timeout(sec)	Aging time of ARP entries, in seconds.

Notifications

N/A

Platform Description

N/A

Related Commands

- **arp timeout**

1.47 show arp flapping record

Function

Run the **show arp flapping record** command to display ARP flapping records.

Syntax

show arp flapping record [*ipv4-address*]

Parameter Description

***ipv4-address*: ARP records of the specified IPv4 address. Command Modes**

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

ARP flapping occurs when a device learns an entry with the same IP address twice but the MAC addresses are different.

Examples

The following example displays ARP flapping records.

```
Hostname> enable
Hostname# show arp flapping record
Hostname> enable
```

```
Hostname# show arp flapping record
Arp flapping recorded:
  Arp flapping record max count: 10240
  Arp flapping record current count: 2
  Arp flapping record history count: 2
  Move-Time                  ip-address         Original-Mac         Move-Mac
Port               Vid
  1970/01/02 02:54:20         192.168.193.52     300d.9e15.bda1
00d0.f822.358b     --                 0
  1970/01/02 03:39:20         192.168.193.59     300d.9e15.bda1
00d0.f822.33f8     --                 0
Total flapping record: 2
```

Table 1-1Output Field of the show arp flapping record Command

Field	Description
Arp flapping recorded	ARP flapping records.
Arp flapping record max count	Maximum count of ARP flapping records.
Arp flapping record history count	Historical count of ARP flapping records.
Move-Time	Flapping occurrence time.
Ip-address	ARP IP address where flapping occurs.
Original-Mac	ARP MAC address before flapping.
Move-Mac	ARP MAC address after flapping.
Port	ARP outbound interface where flapping occurs.
Vid	ARP VLAN ID where flapping occurs.
Total flapping record	Total number of ARP flapping records.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.48 show arp suppress table

Function

Run the **show arp suppress table** command to display the details about the ARP suppression table.

Syntax

show arp suppress table [**ip** *ip-address*]

Parameter Description

ip *ip-address*: Indicates an IP address.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays all ARP suppression entries.

```
Hostname> enable
Hostname# show arp suppress table
ip address     vrf    vni   vid   port   interface  hardware addr   host mac
location
192.30.30.2     1     0      30   0t6166  Or30      0001.0001.0001
0000.0000.0000  remote
192.30.30.3     1     0      30   ag1     Or30      0001.0001.0002
0000.0000.0000  local
```

The following example displays ARP suppression entries of IP address 192.30.30.2.

```
Hostname> enable
Hostname# show arp suppress table ip 192.30.30.2
ip address     vrf    vni   vid   port   interface  hardware addr   host mac
location
192.30.30.2     1     0      30   0t6166  Or30      0001.0001.0001
0000.0000.0000  remote
```

Table 1-1Output Field of the show arp suppress table Command

Field	Description
ip address	IP address corresponding to an ARP entry.
vrf	Index of a VRF instance where an ARP entry resides.
vni	ID of a VXLAN where an ARP entry resides.
vid	ID of a VLAN where an ARP entry resides.
port	Layer 2 outbound interface corresponding to an ARP entry.
interface	Interface corresponding to an ARP entry.

Field	Description
hardware addr	Actual MAC address of the remote host.
host mac	Virtual MAC address of the remote host in a VXLAN network.
location	Local or remote attribute of an ARP entry. ● **Remote** indicates that the entry is synchronized by an EVPN. ● **Local** indicates that the entry is locally learned.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A

1.49 show ip arp

Function

Run the **show ip arp** command to display the ARP cache.

Syntax

show ip arp [**vrf** *vrf-name*]

Parameter Description

vrf *vrf-name*: Displays the ARP entries of a specified VRF instance.

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the ARP cache.

```
Hostname> enable
Hostname# show ip arp
Protocol Address       Age(min)Hardware        Type
Interface
Internet 192.168.7.233  23   0007.e9d9.0488  ARPA GigabitEthernet 0/0
```

```
Internet 192.168.7.112  10   0050.eb08.6617  ARPA GigabitEthernet 0/0
Internet 192.168.7.79   12   00d0.f808.3d5c  ARPA GigabitEthernet 0/0
Internet 192.168.7.1    50   00d0.f84e.1c7f  ARPA GigabitEthernet 0/0
Internet 192.168.7.215  36   00d0.f80d.1090  ARPA GigabitEthernet 0/0
Internet 192.168.7.127  0    0060.97bd.ebee  ARPA GigabitEthernet 0/0
Internet 192.168.7.195  57   0060.97bd.ef2d  ARPA GigabitEthernet 0/0
Internet 192.168.7.183  --   00d0.f8fb.108b  ARPA GigabitEthernet 0/0
```

The following example displays the ARP entries of a VRF instance named vpnv4.

```
Hostname> enable
Hostname# show ip arp vrf vpnv4
Protocol  Address          Age(min)  Hardware        Type   Interface
Internet  11.1.1.1         0         78e3.b5b6.f4dc  arpa   GigabitEthernet 0/0
Internet  11.1.1.2         --        1111.2222.1111  arpa   GigabitEthernet 0/0
Total number of ARP entries: 2
```

Table 1-1Output Fields of the show ip arp Command

Field	Description
Protocol	Network address protocol. This field is always **Internet**.
Address	IP address corresponding to a hardware address.
Age(min)	Aging time of ARP cache records, in minutes. For local or static entries, this field is filled with a hyphen (-).
Hardware	Hardware address corresponding to the IP address.
Type	Type of a hardware address. It is ARPA for all Ethernet addresses.
Interface	Interface associated with an IP address.
Total number of ARP entries	Total number of ARP entries.

Notifications

N/A

Platform Description

N/A

Related Commands

- **show arp**

1.50 show arp anti-attack statistics

Function

Run the **show arp anti-attack statistics** command to display the statistics on illegal ARP packets.

Syntax

show arp anti-attack statistics

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

1

Usage Guidelines

N/A

Examples

The following example displays the statistics on illegal ARP packets.

```
Hostname> enable
Hostname# show arp anti-attack statistics
Number of ARP packet(s) dropped by strict learning:         55
Number of ARP packet(s) dropped by sender-mac checking:     5
Number of ARP packet(s) dropped by target-mac checking:     66
Number of ARP packet(s) dropped by gratuitous checking:     101
Number of ARP packet(s) dropped by acl checking:            7
Number of ARP packet(s) dropped by hardware-type checking:  2
Number of ARP packet(s) dropped by hardware-size checking:  9
Number of ARP packet(s) dropped by protocol-type checking:  78
Number of ARP packet(s) dropped by protocol-size checking:  11
Number of ARP packet(s) dropped by opcode checking:         35
Number of ARP packet(s) dropped by ip checking:             0
```

Table 1-1Output Field of the show arp anti-attack statistics Command

Field	Description
Number of ARP packet(s) dropped by strict learning	Number of illegal ARP packets that are dropped due to strict learning.
Number of ARP packet(s) dropped by sender-mac checking	Number of illegal ARP packets that are dropped due to source MAC address check carried by the sender.
Age (Number of ARP packet(s) dropped by target-mac checking)	Number of illegal ARP packets that are dropped due to destination MAC address check.
Number of ARP packet(s) dropped by gratuitous checking	Number of illegal ARP packets that are dropped due to gratuitous ARP check.

Field	Description
Number of ARP packet(s) dropped by acl checking	Number of illegal ARP packets that are dropped due to ACL check.
Number of ARP packet(s) dropped by hardware-type checking	Number of illegal ARP packets that are dropped due to hardware type check.
Number of ARP packet(s) dropped by hardware-size checking	Number of illegal ARP packets that are dropped due to hardware size check.
Number of ARP packet(s) dropped by protocol-type checking	Number of illegal ARP packets that are dropped due to protocol type check.
Number of ARP packet(s) dropped by protocol-size checking	Number of illegal ARP packets that are dropped due to protocol size check.
Number of ARP packet(s) dropped by opcode checking	Number of illegal ARP packets that are dropped due to operation code check.
Number of ARP packet(s) dropped by ip checking	Number of illegal ARP packets that are dropped due to IP address check.

Notifications

N/A

Platform Description

N/A

Related Commands

N/A