Contents

ARP attack protection commands

Unresolvable IP attack protection commands

arp resolving-route enable

Use **arp resolving-route enable** to enable ARP blackhole routing.

Use **undo arp resolving-route enable** to disable ARP blackhole routing.

Syntax

arp resolving-route enable

undo arp resolving-route enable

Default

ARP blackhole routing is enabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this command on the gateways.

Examples

Enable ARP blackhole routing.

```
<Sysname> system-view
[Sysname] arp resolving-route enable
```

Related commands

arp resolving-route probe-count

arp resolving-route probe-interval

arp resolving-route probe-count

Use **arp resolving-route probe-count** to set the number of ARP blackhole route probes for each unresolved IP address.

Use **undo arp resolving-route probe-count** to restore the default.

Syntax

arp resolving-route probe-count *count*

undo arp resolving-route probe-count

Default

The device performs three ARP blackhole route probes for each unresolved IP address.

Views

System view

Predefined user roles

network-admin

Parameters

count: Sets the number of probes, in the range of 1 to 25.

Examples

Configure the device to perform five ARP blackhole route probes for each unresolved IP address.

```
<Sysname> system-view
[Sysname] arp resolving-route probe-count 5
```

Related commands

arp resolving-route enable

arp resolving-route probe-interval

arp resolving-route probe-interval

Use **arp resolving-route probe-interval** to set the interval at which the device probes ARP blackhole routes.

Use **undo arp resolving-route probe-interval** to restore the default.

Syntax

arp resolving-route probe-interval *interval*

undo arp resolving-route probe-interval

Default

The device probes ARP blackhole routes every 1 second.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the probe interval in the range of 1 to 5 seconds.

Examples

Configure the device to probe ARP blackhole routes every 3 seconds.

```
<Sysname> system-view
[Sysname] arp resolving-route probe-interval 3
```

Related commands

arp resolving-route enable

arp resolving-route probe-count

arp source-suppression enable

Use **arp source-suppression enable** to enable the ARP source suppression feature.

Use **undo arp source-suppression enable** to disable the ARP source suppression feature.

Syntax

arp source-suppression enable

undo arp source-suppression enable

Default

The ARP source suppression feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this feature on the gateways.

Examples

Enable the ARP source suppression feature.

```
<Sysname> system-view
[Sysname] arp source-suppression enable
```

Related commands

display arp source-suppression

arp source-suppression limit

Use **arp source-suppression limit** to set the maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

Use **undo arp source-suppression limit** to restore the default.

Syntax

arp source-suppression limit *limit-value*

undo arp source-suppression limit

Default

The device can process a maximum of 10 unresolvable packets per source IP address within 5 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

limit-value: Specifies the limit in the range of 2 to 1024.

Usage guidelines

If unresolvable packets received from an IP address within 5 seconds exceed the limit, the device stops processing the packets from that IP address until the 5 seconds elapse.

Examples

Configure the device to process a maximum of 100 unresolvable packets per source IP address within 5 seconds.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

Related commands

display arp source-suppression

display arp source-suppression

Use **display arp source-suppression** to display information about the current ARP source suppression configuration.

Syntax

display arp source-suppression

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
```

Table 1 Command output

Field	Description
Current suppression limit	Maximum number of unresolvable packets that can be processed per source IP address within 5 seconds.

ARP packet rate limit commands

arp rate-limit

Use **arp rate-limit** to enable the ARP packet rate limit feature on an interface.

Use **undo arp rate-limit** to disable the ARP packet rate limit feature on an interface.

Syntax

arp rate-limit [*pps*]

undo arp rate-limit

Default

The ARP packet rate limit feature is enabled on an interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

pps: Specifies the upper limit for ARP packet rate in pps. The value range for this argument is 5 to 200.

Usage guidelines

If you do not specify a value for the *pps* argument in the **arp rate-limit** command, the default rate limit value applies. Packets that exceed the rate limit are discarded.

Examples

Enable the ARP packet rate limit feature on GigabitEthernet 1/0/1, and set the maximum ARP packet rate to 50 pps.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp rate-limit 50
```

arp rate-limit log enable

Use **arp rate-limit log enable** to enable logging for ARP packet rate limit.

Use **undo arp rate-limit log enable** to disable logging for ARP packet rate limit.

Syntax

arp rate-limit log enable

undo arp rate-limit log enable

Default

Logging for ARP packet rate limit is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

When logging for ARP packet rate limit is enabled, the device sends the highest threshold-crossed ARP packet rate within the sending interval in a log message to the information center. You can configure the information center module to set the log output rules. For more information about information center, see *Network Management and Monitoring Configuration Guide*.

Examples

Enable logging for ARP packet rate limit.

```
<Sysname> system-view
[Sysname] arp rate-limit log enable
```

arp rate-limit log interval

Use **arp rate-limit log interval** to set the notification and log message sending interval for ARP packet rate limit.

Use **undo arp rate-limit log interval** to restore the default.

Syntax

arp rate-limit log interval *interval*

undo arp rate-limit log interval

Default

The device sends notifications or log messages every 60 seconds when the rate of ARP packets received on an interface exceeds the limit.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies an interval in the range of 1 to 86400 seconds.

Usage guidelines

To change the default interval and activate it, you must enable ARP packet rate limit and enable sending notifications or log messages for ARP packet rate limit.

Examples

Set the device to send notifications and log messages every 120 seconds when the rate of ARP packets received on an interface exceeds the limit.

```
<Sysname> system-view
[Sysname] arp rate-limit log interval 120
```

Related commands

arp rate-limit

arp rate-limit log enable

snmp-agent trap enable arp

snmp-agent trap enable arp

Use **snmp-agent trap enable arp** to enable SNMP notifications for ARP.

Use **undo snmp-agent trap enable arp** to disable SNMP notifications for ARP.

Syntax

snmp-agent trap enable arp [**rate-limit**]

undo snmp-agent trap enable arp [**rate-limit**]

Default

SNMP notifications for ARP is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

rate-limit: Specifies the ARP packet rate limit feature.

Usage guidelines

After you enable SNMP notifications for ARP, the device generates a notification that includes the highest threshold-crossed ARP packet rate within the sending interval.

For ARP event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see the network management and monitoring configuration guide for the device.

Examples

Enable SNMP notifications for ARP packet rate limit.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable arp rate-limit
```

Source MAC-based ARP attack detection commands

arp source-mac

Use **arp source-mac** to enable the source MAC-based ARP attack detection feature and specify a handling method.

Use **undo arp source-mac** to disable the source MAC-based ARP attack detection feature.

Syntax

arp source-mac { **filter** | **monitor** }

undo arp source-mac [**filter** | **monitor**]

Default

The source MAC-based ARP attack detection feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

filter: Specifies the filter handling method.

monitor: Specifies the monitor handling method.

Usage guidelines

Configure this feature on the gateways.

This feature checks the number of ARP packets delivered to the CPU. If the number of packets from the same MAC address within 5 seconds exceeds a threshold, the device generates an ARP attack entry for the MAC address. Before the entry ages out, the device handles the attack by using either of the following methods:

- **Monitor**—Only generates log messages.
- **Filter**—Generates log messages and filters out subsequent ARP packets from the MAC address.

Make sure you have enabled the ARP logging feature before enabling the source MAC-based ARP attack detection feature. For information about the ARP logging feature, see *Layer 3—IP Services Configuration Guide*.

If you do not specify any handling method in the **undo arp source-mac** command, the command disables this feature.

Examples

Enable the source MAC-based ARP attack detection feature and specify the filter handling method.

```
<Sysname> system-view
[Sysname] arp source-mac filter
```

arp source-mac aging-time

Use **arp source-mac aging-time** to set the aging time for ARP attack entries.

Use **undo arp source-mac aging-time** to restore the default.

Syntax

arp source-mac aging-time *time*

undo arp source-mac aging-time

Default

The aging time for ARP attack entries is 300 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time: Sets the aging time for ARP attack entries, in the range of 60 to 6000 seconds.

Examples

Set the aging time for ARP attack entries to 60 seconds.

```
<Sysname> system-view
[Sysname] arp source-mac aging-time 60
```

arp source-mac exclude-mac

Use **arp source-mac exclude-mac** to exclude specific MAC addresses from source MAC-based ARP attack detection.

Use **undo arp source-mac exclude-mac** to remove the excluded MAC addresses from source MAC-based ARP attack detection.

Syntax

arp source-mac exclude-mac *mac-address*&<1-10>

undo arp source-mac exclude-mac [*mac-address*&<1-10>]

Default

No MAC addresses are excluded from source MAC-based ARP attack detection.

Views

System view

Predefined user roles

network-admin

Parameters

mac-address&<1-10>: Specifies a MAC address list. The *mac-address* argument indicates an excluded MAC address in the format of H-H-H. &<1-10> indicates that you can configure a maximum of 10 excluded MAC addresses.

Usage guidelines

If you do not specify a MAC address, the **undo arp source-mac exclude-mac** command removes all excluded MAC addresses.

Examples

Exclude a MAC address from source MAC-based ARP attack detection.

```
<Sysname> system-view
[Sysname] arp source-mac exclude-mac 001e-1200-0213
```

arp source-mac threshold

Use **arp source-mac threshold** to set the threshold for source MAC-based ARP attack detection. If the number of ARP packets sent from a MAC address within 5 seconds exceeds this threshold, the device recognizes this as an attack.

Use **undo arp source-mac threshold** to restore the default.

Syntax

arp source-mac threshold *threshold-value*

undo arp source-mac threshold

Default

The threshold for source MAC-based ARP attack detection is 30.

Views

System view

Predefined user roles

network-admin

Parameters

threshold-value: Specifies the threshold for source MAC-based ARP attack detection. The value range for this argument is 1 to 5000.

Examples

Set the threshold for source MAC-based ARP attack detection to 30.

```
<Sysname> system-view
[Sysname] arp source-mac threshold 30
```

display arp source-mac

Use **display arp source-mac** to display ARP attack entries detected by source MAC-based ARP attack detection.

Syntax

display arp source-mac { **interface** *interface-type interface-number* | **slot** *slot-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack entries for the master device.

Examples

Display the ARP attack entries detected by source MAC-based ARP attack detection on GigabitEthernet 1/0/1.

```
<Sysname> display arp source-mac interface gigabitethernet 1/0/1
Source-MAC          VLAN ID  Interface               Aging-time
23f3-1122-3344      4094     GE1/0/1                 10
```

Table 2 Command output

Field	Description
Source-MAC	Source MAC address of the attack.
VLAN ID	ID of the VLAN in which the attack was detected.
Interface	Interface on which the attack was detected.
Aging-time	Aging time for the ARP attack entry, in seconds.

ARP packet source MAC consistency check commands

arp valid-check enable

Use **arp valid-check enable** to enable ARP packet source MAC address consistency check.

Use **undo arp valid-check enable** to disable ARP packet source MAC address consistency check.

Syntax

arp valid-check enable

undo arp valid-check enable

Default

ARP packet source MAC address consistency check is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Configure this feature on gateways. The gateways can filter out ARP packets whose source MAC address in the Ethernet header is different from the sender MAC address in the message body.

Examples

Enable ARP packet source MAC address consistency check.

```
<Sysname> system-view
[Sysname] arp valid-check enable
```

ARP active acknowledgement commands

arp active-ack enable

Use **arp active-ack enable** to enable the ARP active acknowledgement feature.

Use **undo arp active-ack enable** to disable the ARP active acknowledgement feature.

Syntax

arp active-ack [**strict**] **enable**

undo arp active-ack [**strict**] **enable**

Default

The ARP active acknowledgement feature is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

strict: Enables strict mode for ARP active acknowledgement.

Usage guidelines

Configure this feature on gateways to prevent user spoofing.

In strict mode, a gateway learns an entry only when ARP active acknowledgement is successful based on the correct ARP resolution.

Examples

Enable the ARP active acknowledgement feature.

```
<Sysname> system-view
[Sysname] arp active-ack enable
```

Authorized ARP commands

arp authorized enable

Use **arp authorized enable** to enable authorized ARP on an interface.

Use **undo arp authorized enable** to disable authorized ARP on an interface.

Syntax

arp authorized enable

undo arp authorized enable

Default

Authorized ARP is disabled on the interface.

Views

VLAN interface view

Predefined user roles

network-admin

Examples

Enable authorized ARP on VLAN-interface 200.

```
<Sysname> system-view
[Sysname] interface vlan-interface 200
[Sysname-Vlan-interface200] arp authorized enable
```

ARP attack detection commands

arp detection enable

Use **arp detection enable** to enable ARP attack detection.

Use **undo arp detection enable** to disable ARP attack detection.

Syntax

arp detection enable

undo arp detection enable

Default

ARP attack detection is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP attack detection for VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

Related commands

arp detection rule

display arp detection

display arp detection statistics attack-source

reset arp detection statistics attack-source

arp detection log enable

Use **arp detection log enable** to enable ARP attack detection logging.

Use **undo arp detection log enable** to disable ARP attack detection logging.

Syntax

arp detection log enable [**interval** *interval*]

undo arp detection log enable

Default

ARP attack detection logging is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies the interval for sending ARP detection logs to the information center, in seconds. The value for this argument can be 0 or a value in the range of 10 to 3600. The default value is 60. If you set the interval to 0 seconds, the device sends ARP detection logs to the information center immediately.

Usage guidelines

This feature enables the device to generate ARP detection logs and send them to the information center. For information about the log destination and output rule configuration in the information center, see *Network Management and Monitoring Configuration Guide*.

As a best practice, disable this feature if the log generation affects the device performance.

An IRF member device can send a maximum of 128 ARP detection logs each time.

Examples

Enable ARP attack detection logging.

```
<Sysname> system-view
[Sysname] arp detection log enable
```

arp detection port-match-ignore

Use **arp detection port-match-ignore** to ignore ingress ports of ARP packets during user validity check.

Use **undo arp detection port-match-ignore** to remove the configuration.

Syntax

arp detection port-match-ignore

undo arp detection port-match-ignore

Default

Ingress ports of ARP packets are checked for user invalidity.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command configures ARP attack detection to ignore the ingress port information of ARP packets when the packets are compared with the entries used for user validity check.

Examples

Ignore ingress ports of ARP packets during user validity check.

```
<Sysname> system-view
[Sysname] arp detection port-match-ignore
```

Related commands

arp detection enable

arp detection rule

Use **arp detection rule** to configure a user validity check rule.

Use **undo arp detection rule** to delete a user validity check rule.

Syntax

arp detection rule *rule-id* { **deny** | **permit** } **ip** { *ip-address* [*mask*] | **any** } **mac** { *mac-address* [*mask*] | **any** } [**vlan** *vlan-id*]

undo arp detection rule [*rule-id*]

Default

No user validity check rule is configured.

Views

System view

Predefined user roles

network-admin

Parameters

rule-id: Assigns an ID to the user validity check rule. The ID value range is 0 to 511. A smaller value represents a higher priority.

deny: Denies matching ARP packets.

permit: Permits matching ARP packets.

ip { *ip-address* [*mask*] | **any** }: Specifies the sender IP address as the match criterion.

- *ip-address*: Specifies an IP address in dotted decimal notation.
- *mask*: Specifies the address mask in dotted decimal notation. If you do not specify the mask, the *ip-address* argument specifies a host IP address.
- **any**: Matches any IP address.

mac { *mac-address* [*mask*] | **any** }: Specifies the sender MAC address as the match criterion.

- *mac-address*: Specifies a MAC address in the H-H-H format.
- *mask*: Specifies the MAC address mask in the H-H-H format. If you do not specify the mask, the argument specifies the host MAC address.

- **any**: Matches any MAC address.

vlan *vlan-id*: Specifies the ID of a VLAN in the specified rule. The value range for the *vlan-id* argument is 1 to 4094. If you do not specify a VLAN, the packets' VLAN information is not checked.

Usage guidelines

A user validity check rule takes effect only when ARP attack detection is enabled.

If you do not specify a rule ID, the **undo arp detection rule** command deletes all user validity check rules.

Examples

Configure a user validity check rule and enable ARP detection for VLAN 2.

```
<Sysname> system-view
[Sysname] arp detection rule 0 permit ip 10.1.1.1 255.255.0.0 mac 0001-0203-0405
ffff-ffff-0000
[Sysname] vlan 2
[Sysname-vlan2] arp detection enable
```

Related commands

arp detection enable

arp detection trust

Use **arp detection trust** to configure an interface as an ARP trusted interface.

Use **undo arp detection trust** to restore the default.

Syntax

arp detection trust

undo arp detection trust

Default

An interface is an ARP untrusted interface.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Examples

Configure GigabitEthernet 1/0/1 as an ARP trusted interface.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp detection trust
```

arp detection validate

Use **arp detection validate** to enable ARP packet validity check.

Use **undo arp detection validate** to disable ARP packet validity check.

Syntax

arp detection validate { **dst-mac** | **ip** | **src-mac** } *

undo arp detection validate [**dst-mac** | **ip** | **src-mac**] *

Default

ARP packet validity check is disabled.

Views

System view

Predefined user roles

network-admin

Parameters

dst-mac: Checks the target MAC address of ARP responses. If the target MAC address is all-zero, all-one, or inconsistent with the destination MAC address in the Ethernet header, the packet is considered invalid and discarded.

ip: Checks the sender and target IP addresses of ARP replies, and the sender IP address of ARP requests. All-one or multicast IP addresses are considered invalid and the corresponding packets are discarded.

src-mac: Checks whether the sender MAC address in the message body is identical to the source MAC address in the Ethernet header. If they are identical, the packet is forwarded. Otherwise, the packet is discarded.

Usage guidelines

You can specify more than one object to be checked in one command line.

If no keyword is specified, the **undo arp detection validate** command disables ARP packet validity check for all objects.

Examples

Enable ARP packet validity check by checking the MAC addresses and IP addresses of ARP packets.

```
<Sysname> system-view
[Sysname] arp detection validate dst-mac ip src-mac
```

arp restricted-forwarding enable

Use **arp restricted-forwarding enable** to enable ARP restricted forwarding.

Use **undo arp restricted-forwarding enable** to disable ARP restricted forwarding.

Syntax

arp restricted-forwarding enable

undo arp restricted-forwarding enable

Default

ARP restricted forwarding is disabled.

Views

VLAN view

Predefined user roles

network-admin

Examples

Enable ARP restricted forwarding in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] arp restricted-forwarding enable
```

display arp detection

Use **display arp detection** to display the VLANs that are enabled with ARP attack detection.

Syntax

display arp detection

Views

Any view

Predefined user roles

network-admin

network-operator

Examples

Display the VLANs that are enabled with ARP attack detection.

```
<Sysname> display arp detection
ARP detection is enabled in the following VLANs:
1-2, 4-5
```

Related commands

arp detection enable

display arp detection statistics attack-source

Use **display arp detection statistics attack-source** to display statistics for ARP attack sources.

Syntax

display arp detection statistics attack-source slot *slot-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its ID. If you do not specify a member device, this command displays ARP attack source statistics for the master device.

Examples

Display statistics for ARP attack sources on slot 1.

```
<Sysname> display arp detection statistics attack-source slot 1
Interface             VLAN  MAC address    IP address      Number     Time
```

```
GE1/0/1                1      0005-0001-0001 10.1.1.14       24          17:09:56
03-27-2017
```

Table 3 Command output

Field	Description
Interface	Receiving interface of ARP attack packets.
VLAN	VLAN to which ARP attack packets belong.
MAC address	Sender MAC address in ARP attack packets.
IP address	Sender IP address in ARP attack packets.
Number	Number of ARP attack packets dropped by ARP attack detection.
Time	The most recent time when ARP attack detection dropped an ARP attack packet.

Related commands

arp detection enable

display arp detection statistics packet-drop

Use **display arp detection statistics packet-drop** to display statistics for packets dropped by ARP attack detection.

Syntax

display arp detection statistics packet-drop [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command displays dropped packet statistics for all interfaces.

Usage guidelines

This command displays numbers of packets discarded by user validity check and ARP packet validity check on interfaces.

Examples

Display statistics for packets dropped by ARP attack detection.

```
<Sysname> display arp detection statistics packet-drop
State: U-Untrusted  T-Trusted
ARP packets dropped by ARP inspect checking:
Interface(State)            IP        Src-MAC   Dst-MAC   Inspect
GE1/0/1(U)                  40        0         0         78
GE1/0/2(U)                  0         0         0         0
```

```
GE1/0/3(T)                0          0          0          0
GE1/0/4(U)                0          0          30         0
```

Table 4 Command output

Field	Description
State	State of an interface: • **U**—ARP untrusted interface. • **T**—ARP trusted interface.
Interface(State)	Inbound interface of ARP packets. State specifies the port state, **trusted** or **untrusted**.
IP	Number of ARP packets discarded due to invalid sender and target IP addresses.
Src-MAC	Number of ARP packets discarded due to invalid source MAC address.
Dst-MAC	Number of ARP packets discarded due to invalid destination MAC address.
Inspect	Number of ARP packets that failed to pass user validity check.

Related commands

`reset arp detection statistics packet-drop`

reset arp detection statistics attack-source

Use **`reset arp detection statistics attack-source`** to clear statistics for ARP attack sources.

Syntax

`reset arp detection statistics attack-source` [**`slot`** *`slot-number`*]

Views

User view

Predefined user roles

network-admin

Parameters

`slot` *`slot-number`*: Specifies an IRF member device by its ID. If you do not specify a member device, this command clears ARP attack source statistics for the master device.

Examples

Clear statistics for ARP attack sources.

```
<Sysname> reset arp detection statistics attack-source
```

Related commands

`arp detection enable`

`display arp detection statistics attack-source`

reset arp detection statistics packet-drop

Use **`reset arp detection statistics packet-drop`** to clear statistics for packets dropped by ARP attack detection.

Syntax

reset arp detection statistics packet-drop [**interface** *interface-type interface-number*]

Views

User view

Predefined user roles

network-admin

Parameters

interface *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command clears dropped packet statistics for all interfaces and all Ethernet service instances on the interfaces.

Examples

Clear statistics for packets dropped by ARP attack detection.

```
<Sysname> reset arp detection statistics packet-drop
```

Related commands

display arp detection statistics packet-drop

ARP scanning and fixed ARP commands

arp fixup

Use **arp fixup** to convert existing dynamic ARP entries to static ARP entries.

Use **undo arp fixup** to convert valid static ARP entries to dynamic ARP entries and delete invalid static ARP entries.

Syntax

arp fixup

undo arp fixup

Views

System view

Predefined user roles

network-admin

Usage guidelines

The ARP conversion is a one-time operation. You can use this command again to convert the dynamic ARP entries learned later to static.

The static ARP entries converted from dynamic ARP entries have the same attributes as the manually configured static ARP entries. Due to the device's limit on the total number of static ARP entries, some dynamic ARP entries might fail the conversion.

The static ARP entries after conversion can include the following entries:

- Existing dynamic and static ARP entries before conversion.
- New dynamic ARP entries learned during the conversion.

Dynamic ARP entries that are aged out during the conversion are not converted to static ARP entries.

To delete a static ARP entry changed from a dynamic one, use the **undo arp** *ip-address* [*vpn-instance-name*] command. To delete all such static ARP entries, use the **reset arp all** or **reset arp static** command.

Examples

Convert existing dynamic ARP entries to static ARP entries.

```
<Sysname> system-view
[Sysname] arp fixup
```

arp scan

Use **arp scan** to trigger an ARP scanning in an address range.

Syntax

arp scan [*start-ip-address* **to** *end-ip-address*] [**send-rate** *pps*]

Views

VLAN interface view

L3VE interface view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address of the scanning range.

end-ip-address: Specifies the end IP address of the scanning range. The end IP address must be higher than or equal to the start IP address.

send-rate *pps*: Specifies the rate at which the device sends ARP requests for ARP scanning, in pps. The value range for the *pps* argument is 10 to 1000, and the value must be a multiple of 10. If you do not set the rate, the device sends ARP requests to all IP addresses in the specified scanning range simultaneously.

Usage guidelines

ARP scanning automatically creates ARP entries for devices in the specified address range. IP addresses already in existing ARP entries are not scanned.

If the interface's primary and secondary IP addresses are in the address range, the sender IP address in the ARP request is the address on the smallest network segment.

If no address range is specified, the device learns ARP entries for devices on the subnet where the primary IP address of the interface resides. The sender IP address in the ARP requests is the primary IP address of the interface.

The start and end IP addresses must be on the same subnet as the primary IP address or secondary IP addresses of the interface.

ARP scanning will take some time. To stop an ongoing scan, press **Ctrl** + **C**. Dynamic ARP entries are created based on ARP replies received before the scan is terminated.

You can set the ARP packet sending rate if the scanning range has a large number of IP addresses. This setting can avoid high CPU usage and heavy network load caused by a burst of ARP traffic.

When you set the sending rate to a large value, the device might use a rate lower than the specified rate to ensure the device performance.

Examples

Configure the device to scan the neighbors on the network where the primary IP address of VLAN-interface 2 resides.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan
```

Configure the device to scan neighbors in an address range.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20
```

Configure the device to scan neighbors in an address range on VLAN-interface 2 and set the ARP packet sending rate to 10 pps.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] arp scan 1.1.1.1 to 1.1.1.20 send-rate 10
```

ARP gateway protection commands

arp filter source

Use **arp filter source** to enable ARP gateway protection for a gateway.

Use **undo arp filter source** to disable ARP gateway protection for a gateway.

Syntax

arp filter source *ip-address*

undo arp filter source *ip-address*

Default

ARP gateway protection is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies the IP address of a protected gateway.

Usage guidelines

You can enable ARP gateway protection for a maximum of eight gateways on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP gateway protection for the gateway with IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter source 1.1.1.1
```

ARP filtering commands

arp filter binding

Use **arp filter binding** to enable ARP filtering and configure an ARP permitted entry.

Use **undo arp filter binding** to remove an ARP permitted entry.

Syntax

arp filter binding *ip-address mac-address*

undo arp filter binding *ip-address*

Default

ARP filtering is disabled.

Views

Layer 2 Ethernet interface view

Layer 2 aggregate interface view

Predefined user roles

network-admin

Parameters

ip-address: Specifies a permitted sender IP address.

mac-address: Specifies a permitted sender MAC address.

Usage guidelines

If the sender IP and MAC addresses of an ARP packet match an ARP permitted entry, the ARP packet is permitted. If the sender IP and MAC addresses of an ARP packet do not match an ARP permitted entry, the ARP packet is discarded.

You can configure a maximum of eight ARP permitted entries on an interface.

You cannot configure both the **arp filter source** and **arp filter binding** commands on the same interface.

Examples

Enable ARP filtering and configure an ARP permitted entry.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] arp filter binding 1.1.1.1 0e10-0213-1023
```

ARP packet sender IP address checking commands

arp sender-ip-range

Use **arp sender-ip-range** to specify the sender IP address range for ARP packet checking.

Use **undo arp sender-ip-range** to restore the default.

Syntax

arp sender-ip-range *start-ip-address end-ip-address*

undo arp sender-ip-range

Default

No sender IP address range is specified for ARP packet checking.

Views

VLAN view

Predefined user roles

network-admin

Parameters

start-ip-address: Specifies the start IP address.

end-ip-address: Specifies the end IP address. The end IP address must be higher than or equal to the start IP address.

Usage guidelines

The gateway discards an ARP packet if its sender IP address is not within the allowed IP address range.

If you execute this command multiple times, the most recent configuration takes effect.

Examples

Specify the sender IP address range 1.1.1.1 to 1.1.1.20 for ARP packet checking in VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname–vlan2] arp sender-ip-range 1.1.1.1 1.1.1.20
```