14 Security Commands

About This Chapter

14.1 ACL Configuration Commands

14.1.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.1.2 acl ipv6 name

Function

The **acl ipv6 name** command creates a named ACL6 and enters the ACL6 view.

The **undo acl ipv6 name** command deletes a named ACL6.

By default, no named ACL6 is created.

Format

acl ipv6 name *acl6-name* [**advance** | **basic** | *acl6-number*] [**match-order** { **auto** | **config** }]

undo acl ipv6 name *acl6-name*

Parameters

Parameter	Description	Value
acl6-name	Specifies the name of an ACL6.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
advance	Indicates an advanced ACL6.	-
basic	Indicates a basic ACL6.	-
acl6-number	Specifies the number of an ACL6.	The value is an integer that ranges from 2000 to 3999. ● The value of a basic ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL6 ranges from 3000 to 3999.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. - **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. - **config**: indicates that ACL6 rules are matched based on the configuration order. The rule-id in an ACL6 rules does not indicate the priority of the rule. It indicates the rule ID and remains unchanged in auto and config mode switchover. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6s are mainly used in QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services for which packets need to be filtered.

Precautions

The Switch allocates a number to named ACL6s that have no specified number. The number allocated depends on the following:

- If only the type of a named ACL6 is specified, the number of the named ACL6 allocated by the Switch is the maximum value of the named ACL6 of the type.
- If the number and the type of a named ACL6 are not specified, the Switch considers the named ACL6 as the advanced ACL6 and allocates the maximum value as the number of the named ACL6.

After you create a named ACL6 by using the **acl ipv6 name** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6 name** *acl6-name* or **undo acl ipv6** *acl6-number* command to delete the ACL6.

When you delete an ACL6 that has been referenced by other services, the services will be interrupted. Therefore, before deleting an ACL6, ensure that the ACL6 is not in use.

Example

# Create basic ACL6 2001 named **test2**.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 name test2 2001
```

Related Topics

14.1.10 display acl ipv6

14.1.3 acl ipv6 (system view)

Function

The **acl ipv6** command creates a numbered ACL6 and enters the ACL6 view.

The **undo acl ipv6** command deletes a numbered ACL6.

By default, no numbered ACL6 is created.

Format

acl ipv6 [**number**] *acl6-number* [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | [**number**] *acl6-number* }

Parameters

Parameter	Description	Value
number	Indicates the number that identifies an ACL.	-

Parameter	Description	Value
acl6-number	Specifies an ACL6 number.	The value is an integer that ranges from 2000 to 3999. - The value of a basic ACL6 ranges from 2000 to 2999. - The value of an advanced ACL6 ranges from 3000 to 3999.
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. - **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. - **config**: indicates that ACL6 rules are matched based on the configuration order. The rule-id in an ACL6 rules does not indicate the priority of the rule. It indicates the rule ID and remains unchanged in auto and config mode switchover. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-
all	Indicates that all the configured ACL6s are deleted.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6 rules can be referenced by modules. ACL6s are applicable to QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services for which packets need to be filtered.

Precautions

After you create a named ACL6 using the **acl ipv6** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6** *acl6-number* command to delete the ACL6.

When you delete an ACL6 that has been referenced by other services, the services will be interrupted. Before deleting an ACL6, ensure that the ACL6 is not in use.

All ACL6s can be deleted on the device in one go, but this method is not recommended.

Example

# Create an advanced CL6 with the number of 3000.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3000
```

Related Topics

14.1.10 display acl ipv6

14.1.19 rule (basic ACL6 view)

14.1.17 rule (advanced ACL6 view)

14.1.4 acl name

Function

The **acl name** command creates a named ACL and enters the ACL view.

The **undo acl** command deletes a named ACL.

By default, no ACL is created.

Format

acl name *acl-name* [**advance** | **basic** | **link** | **ucl** | **user** | *acl-number*] [**match-order** { **auto** | **config** }] (Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support the **ucl** parameter.)

undo acl name *acl-name*

Parameters

Parameter	Description	Value
acl-name	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
advance	Indicates an advanced ACL.	-
basic	Indicates a basic ACL.	-
link	Indicates a Layer 2 ACL.	-
ucl	Indicates a user ACL.	-
user	Indicates a user-defined ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user-defined ACL ranges from 5000 to 5999. ● The number of a user ACL ranges from 6000 to 9999. **NOTE** Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support user ACL.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. ● **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services for which packets need to be filtered.

Precautions

After you create a named ACL by using the **acl name** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl name** *acl-name* or **undo acl** *acl-number* command to delete the ACL.

When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.

The device automatically allocates a number to the named ACLs that have no number specified. The number allocated depends on the following:

- If the type of a named ACL is specified, the number of the named ACL allocated by the device is the maximum value of the named ACL of the type.
- If the number and the type of a named ACL are not specified, the device considers the named ACL as the advanced ACL and allocates the maximum value as the number of the named ACL.

The Switch does not allocate the number to a named ACL repeatedly.

Example

# Create basic ACL 2001 named **test1**.

```
<HUAWEI> system-view
[HUAWEI] acl name test1 2001
```

Related Topics

14.1.9 display acl

14.1.5 acl (system view)

Function

The **acl** command creates an ACL with the specified number and enters the ACL view.

The **undo acl** command deletes a specified ACL.

By default, no ACL is created.

Format

acl [**number**] *acl-number* [**match-order** { **auto** | **config** }]

undo acl { [**number**] *acl-number* | **all** }

Parameters

Parameter	Description	Value
number	Specifies the number that identifies an ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user defined ACL ranges from 5000 to 5999. ● The number of a user ACL ranges from 6000 to 9999. **NOTE** Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support user ACL.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. ● **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-
all	Indicates that all ACLs are deleted.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services for which packets need to be filtered.

Precautions

- After you create an ACL using the **acl** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl** *acl-number* command to delete the ACL.
- When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.
- You are advised not to delete all ACLs because this operation may cause a service interruption.

Example

# Create an ACL numbered 2000.

```
<HUAWEI> system-view
[HUAWEI] acl number 2000
```

Related Topics

14.1.9 display acl

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

14.1.22 rule (user ACL view)

14.1.6 acl threshold-alarm

Function

The **acl threshold-alarm** command configures the alarm threshold percentage of ACL resource usage.

The **undo acl threshold-alarm** command restores the default alarm threshold percentage of ACL resource usage.

By default, the lower alarm threshold percentage is 70, and the upper alarm threshold percentage is 80.

Format

acl threshold-alarm { **upper-limit** *upper-limit* | **lower-limit** *lower-limit* } *

undo acl threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit*	Indicates the upper alarm threshold percentage of ACL resource usage.	The value is an integer that ranges from 1 to 100.
lower-limit *lower-limit*	Indicates the lower alarm threshold percentage of ACL resource usage.	The value is an integer that ranges from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the device runs ACL or ACL6 services for a period, the running ACL services occupy ACL resources. You can run the **acl threshold-alarm** command to set the alarm threshold percentage of ACL resources.

When the ACL resource usage (that is, the ratio of existing ACL entries to the maximum number of ACL entries supported by the device) is equivalent to or higher than the threshold, the device generates an alarm. When the ACL resource usage becomes equivalent to or lower than the lower threshold, the device generates a clear alarm.

Precautions

If you run the **acl threshold-alarm** command multiple times, only the latest configuration takes effect.

The upper threshold must be equivalent to or greater than the lower threshold.

Example

# Set the lower alarm threshold percentage to 30 and the upper alarm threshold percentage to 50.

```
<HUAWEI> system-view
[HUAWEI] acl threshold-alarm upper-limit 50 lower-limit 30
```

14.1.7 assign resource-template acl-mode

Function

The **assign resource-template acl-mode** command sets the ACL resource allocation mode.

The **undo assign resource-template acl-mode** command restores the default ACL resource allocation mode.

By default, the ACL resource allocation mode is dual-ipv4-ipv6.

NOTE

This command is supported only on the S5720HI.

Format

assign resource-template acl-mode { **dual-ipv4-ipv6** | **ipv4** | **l2** | **l2-ipv4** | **l2-ipv6** } [**slot** *slot-id*]

undo assign resource-template acl-mode [**slot** *slot-id*]

Parameters

Parameter	Description	Value
dual-ipv4-ipv6	Specifies the IPv4 and IPv6 ACL resource allocation mode.	-
ipv4	Specifies the IPv4 ACL resource allocation mode.	-
l2	Specifies the Layer 2 ACL resource allocation mode.	-
l2-ipv4	Specifies the Layer 2 IPv4 ACL resource allocation mode.	-
l2-ipv6	Specifies the Layer 2 IPv6 ACL resource allocation mode.	-

Parameter	Description	Value
slot *slot-id*	● Specifies the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured. If *slot-id* is not specified, usage of ACL resources in all the stack switches is displayed.	The value is determined based on the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

If the default number of ACLs for IPv4, IPv6, or Layer 2 services cannot meet service requirements, you can change the ACL resource allocation mode to increase the number of ACLs for the services. Before using this command to change the ACL resource allocation mode, consider the advantage and disadvantage of the change. For example, if the ACL resource allocation mode is changed from **dual-ipv4-ipv6** to **ipv4**, more ACLs are supported for IPv4 services, but the number of ACLs for IPv6 and Layer 2 services reduces to 0.

Table 14-1 ACL specifications in different resource allocation modes

Resource Allocation Mode	Maximum Number of IPv4 ACLs	Maximum Number of Layer 2+IPv4 ACLs	Maximum Number of IPv6 ACLs	Maximum Number of Layer 2+IPv6 ACLs	Maximum Number of Layer 2 ACLs	Total Number of ACLs
dual-ipv4-ipv6	16K	16K	8K	8K	16K	16K(IPV4)+8K(IPV6)
l2-ipv4	32K	32K	0	0	32K	32K
l2-ipv6	0	0	16K	16K	16K	16K
ipv4	64K	0	0	0	0	64K

Resource Allocation Mode	Maximum Number of IPv4 ACLs	Maximum Number of Layer 2+IPv4 ACLs	Maximum Number of IPv6 ACLs	Maximum Number of Layer 2+IPv6 ACLs	Maximum Number of Layer 2 ACLs	Total Number of ACLs
l2	0	0	0	0	64K	64K

Precautions

After configuring the ACL resource allocation mode, save the configuration, and restart the device for the configuration to take effect.

Example

# Change the ACL resource allocation mode to **IPv4**.

```
<HUAWEI> system-view
[HUAWEI] assign resource-template acl-mode ipv4
```

14.1.8 description

Function

The **description** command configures the description of an ACL.

The **undo description** command deletes the description of an ACL.

By default, no description is configured for an ACL.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Describes an ACL.	The value is a string of 1 to 127 case-sensitive characters with spaces supported.

Views

ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an ACL, for example, the usage or application scenario of the ACL. It is used to differentiate ACLs.

Prerequisites

The ACL to be described has been created.

Configuration Impact

The **description** command cannot be run in the ACL6 view.

If you run the **description** command multiple times in the same ACL view, only the latest configuration takes effect.

Example

# Configure the description of ACL 2100.

```
<HUAWEI> system-view
[HUAWEI] acl 2100
[HUAWEI-acl-basic-2100] description This acl is used in QoS policy
[HUAWEI-acl-basic-2100] display acl 2100
Basic ACL 2100, 0 rule
This acl is used in QoS policy
ACL's step is 5
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

14.1.3 acl ipv6 (system view)

14.1.9 display acl

Function

The **display acl** command displays the configuration of an ACL.

Format

display acl { *acl-number* | **name** *acl-name* | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of a numbered advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user-defined ACL ranges from 5000 to 5999. ● The number of a user ACL ranges from 6000 to 9999. **NOTE** Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support user ACL.
name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
all	Indicates all ACLs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display acl** command displays the ACL configuration.

Example

# Display configuration about the ACL named **test**.

```
<HUAWEI> display acl name test
Advanced ACL test 3999, 1 rule, match-order is auto
Acl's step is 5
 rule 5 permit ip destination 10.10.10.1 0
```

# Display the ACL configuration.

```
<HUAWEI> display acl all
 Total nonempty ACL number is 1

Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit ip dscp cs1
```

Table 14-2 Description of the **display acl** command output

Item	Description
Advanced ACL test 3999, 1 rule, match-order is auto	Advanced ACL 3999 named **test** that matches in the automatic order and contains one rule.
Acl's step is 5	The ACL's step is 5. To set the step between ACL rule IDs, run the **step** command.
rule 5 permit ip destination 10.10.10.1 0	Rule 5 that matches packets whose source IP address is 10.10.10.1. To modify an advanced ACL rule, run the **rule (advanced ACL view)** command.
Total nonempty ACL number is 1	One ACL contains rules.
Advanced ACL 3000, 1 rule	Advanced ACL 3000 contains one rule.
rule 5 permit ip dscp cs1	Rule 5 that matches packets with DSCP priorities. To modify an advanced ACL rule, run the **rule (advanced ACL view)** command.

Related Topics

14.1.5 acl (system view)

14.1.8 description

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

14.1.22 rule (user ACL view)

14.1.25 step

14.1.10 display acl ipv6

Function

The **display acl ipv6** command displays the configuration of a specific ACL6 or all ACL6s.

Format

display acl ipv6 { *acl6-number* | **name** *acl6-name* | **all** }

Parameters

Parameter	Description	Value
acl6-number	Specifies an ACL6 number.	The value is an integer that ranges from 2000 to 3999. The ACL6 with a number ranging from 2000 to 2999 is a basic ACL6 and the ACL6 with a number ranging from 3000 to 3999 is an advanced ACL6.
name *acl6-name*	Displays the ACL6 with a specified name.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
all	Displays the configurations of all ACL6s.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display acl ipv6** command displays the ACL6 configuration.

Example

# Display the configuration about the ACL6 with the number of 2000.

```
<HUAWEI> display acl ipv6 2000

Basic IPv6 ACL 2000, 2 rules
 rule 1 permit source 4::/64
 rule 0 deny source 3::/64
```

# Display the ACL6 configuration.

```
<HUAWEI> display acl ipv6 all
 Total nonempty acl6 number is 1

Basic IPv6 ACL 2000, 2 rules
 rule 1 permit source 4::/64
 rule 0 deny source 3::/64
```

Table 14-3 Description of the **display acl ipv6** command output

Item	Description
Total nonempty acl6 number is 1	One ACL6 contains rules.
Basic IPv6 ACL 2000, 2 rules	ACL6 2000, which is a basic ACL6 and has two rules.
rule 0 deny source 3::/64	ACL6 rule 0, which denies packets with the source IPv6 address 3::/64. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.
rule 1 permit source 4::/64	ACL6 rule 1, which permits packets with the source IPv6 address 4::/64. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.

Related Topics

14.1.3 acl ipv6 (system view)

14.1.19 rule (basic ACL6 view)

14.1.17 rule (advanced ACL6 view)

14.1.11 display acl resource

Function

The **display acl resource** command displays information about ACL resources.

Format

display acl resource [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays device information about ACL resources. *slot-id* specifies the stack ID.	The value is an integer. The value range depends on the configuration of a device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

ACL resources are related to hardware chips. The following are types of ACL resources:

- ACL entries: Each ACL entry stores an ACL rule.
- Meter/Car: a traffic control table used to limit the traffic rate. The meter/car must be used with ACL entries.
- Counter: a traffic counter table used to collect traffic statistics. The counter must be used with ACL entries.

If ACL configuration fails, all the ACL resources on the device may have been used up. You can run the **display acl resource** command to check whether there are available ACL resources (including ACL4 and ACL6).

Precautions

- After ACL is applied to the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, the ACL resources are applied to both incoming and outgoing traffic. For example, if a traffic policy is applied to only the incoming traffic, the **Outbound-ACL** value and **Inbound-ACL** value in the **display acl resource** command output are the same.
- On the S5720-EI, S6720-EI, and S6720S-EI, ACL resources are divided in slice mode. Each slice contains a certain number of ACL resources. Different types of services apply for different slices when ACLs are applied. When ACL resource insufficiency is displayed while ACL resources are applied to a service, but the **Free** field shows there are still free ACL resources, this indicates that ACL resources in the slice occupied by the service are insufficient, and new slices cannot be obtained. The free resources in the **Free** field are ACL resources in the slice occupied by other services.

Example

# Display information about ACL resources on the Slot 0 (S5700LI is used as an example).

```
<HUAWEI> display acl resource slot 0
Slot  0
GigabitEthernet0/0/1 to GigabitEthernet0/0/10
                Vlan-ACL    Inbound-ACL    Outbound-ACL    Router-
ACL
-------------------------------------------------------------------------
  Rule Used            0          71           71         10
  Rule Free         1024         421          421        522
  Rule Total        1024         492          492        532

  Meter Used           0           0            0          0
  Meter Free           0         172          128          0
  Meter Total          0         172          128          0
```

```
 Counter Used           0          0          0         0
 Counter Free           0        172        128         0
 Counter Total          0        172        128         0
------------------------------------------------------------------------
```

# Display information about ACL resources on the Slot 0 (S6720LI is used as an example).

```
<HUAWEI> display acl resource slot 0
Slot  0
XGigabitEthernet0/0/1 to XGigabitEthernet0/0/24
40GE0/0/1
40GE0/0/2
                Vlan-ACL    Inbound-ACL    Outbound-ACL   Reserved-ACL
------------------------------------------------------------------------
 Rule Used              0         30          30        124
 Rule Free            512       2018        2018        388
 Rule Total           512       2048        2048        512

 Meter Used             0          0           0         0
 Meter Free             0       1536        2048         0
 Meter Total            0       1536        2048         0

 Counter Used           0          0           0         0
 Counter Free           0       1536        2048         0
 Counter Total          0       1536        2048         0
------------------------------------------------------------------------
```

# Display information about ACL resources on the Slot 0. (S5720HI is used as an example)

```
<HUAWEI> display acl resource slot 0
Slot  0
GigabitEthernet0/0/1 to GigabitEthernet0/0/48
XGigabitEthernet0/0/1 to XGigabitEthernet0/0/4
                 Used         Free        Total
--------------------------------------------------------------------------
 ACL Unallocated   -            -          20480
 ACL Allocated     147          365          511
   Vlan    ACL     1            -            -
   Sec     ACL     146          -            -

 EXT Unallocated   -            -          8192
 EXT Allocated     0            0          0

 Car              260         32508       32768
 Counter          144         65392       65536
--------------------------------------------------------------------------
```

# Display information about ACL resources on the Slot 0. (S5720EI is used as an example)

```
<HUAWEI> display acl resource slot 0
Slot  0
GigabitEthernet0/0/1 to GigabitEthernet0/0/48
XGigabitEthernet0/0/1 to XGigabitEthernet0/0/4
                Used         Free        Total
-------------------------------------------------------------------------
 VACL            8           2040        2048

 IACL Unallocated -            -           3072
 IACL Allocated   -            -           1024
   Srv    ACL     10          502         512
   Sec    ACL     348         164         512

 EACL Unallocated -            -           1024
 EACL Allocated   -            -           0

 Ingress Meter    36          4060        4096
```

```
Egress  Meter    0           1024         1024
Ingress Counter  155           3941         4096
Egress  Counter  0           1024         1024

Ingress UDF      0           8           8
------------------------------------------------------------------------------
```

Table 14-4 Description of the **display acl resource** command output

Item	Description
Slot	Stack ID.
GigabitEthernet 0/0/1 to GigabitEthernet 0/0/x XGigabitEthernet 0/0/1 to XGigabitEthernet 0/0/x	Interface to which an ACL is applied.
Vlan-ACL	Inbound ACL resources delivered before Layer 2 forwarding process starts. ● For the services related to VLAN translation, for example, VLAN mapping (configured by using the **port vlan-mapping vlan map-vlan** command) and VLAN stacking (configured by using the **port vlan-stacking** command), the device delivers Vlan-ACL resources. ● When a traffic policy is applied to the **inbound** direction and bound to a traffic behavior containing a VLAN-related action (except **remark 8021p**), for example, if the action in a traffic behavior is to remark the VLAN tag on VLAN packets (configured by using the **remark vlan-id** command), the device delivers Vlan-ACL resources. This applies to the S5720HI.
Inbound-ACL	Inbound ACL resources delivered after Layer 3 forwarding process is complete.Generally, the device delivers Inbound-ACL resources in the following situation: ● The ACL is applied to a service irrelevant to direction, for example, a user group. ● The traffic policy is applied to the inbound direction and contains a traffic behavior irrelevant to VLAN.

Item	Description
Outbound-ACL	ACL resources in outbound direction. The device delivers Outbound-ACL resources when the traffic policy applied to the outbound direction contains a traffic behavior which is not **mirroring to observe-port**. If the traffic behavior contained in the traffic policy is **mirroring to observe-port**, the device delivers Inbound-ACL resources.
Router-ACL	ACL resources used for route forwarding. **NOTE** This field is displayed only when hardware-based Layer 3 forwarding is enabled for IPv4 packets on an S2750EI, S5700-10P-LI-AC, or S5700-10P-PWR-LI-AC.
Reserved-ACL	ACL resources reserved for CPCAR.
Rule Used	Number of used ACL rules.
Rule Free	Number of free ACL rules.
Rule Total	Total number of ACL rules.
Meter Used	Number of used rate limiting resources.
Meter Free	Number of idle rate limiting resources.
Meter Total	Total number of rate limiting resources.
Counter Used	Number of used counters.
Counter Free	Number of free counters.
Counter Total	Total number of counters, including those for collecting statistics on traffic policies, VLAN traffic, VLANIF interface traffic, and packets sent to the CPU.
Car	Traffic monitoring resources.
Counter	Traffic statistics collection resources.
Used	Number of used resources.
Free	Number of free resources.
Total	Total number of resources.
ACL Unallocated	Unallocated common ACL resources.

Item	Description
ACL Allocated	Number of ACL resources: ● Vlan ACL: ACL resources used by VLAN. ● Ingress ACL: Resources used by inbound traffic policy, ACL-based simplified traffic policy, and IPSG. ● Egress ACL: Resources used by outbound traffic policy and ACL-based simplified traffic policy. ● Ingress UCL: Resources used by traffic from user terminals to switch. ● Egress UCL: Resources used by traffic from switch to user terminals. ● Srv ACL: Resources used by inbound and outbound iPCA and voice VLAN. ● Sec ACL: Inbound secure ACL resources.
EXT Unallocated	Unallocated extended ACL resources.
EXT Allocated	Number of extended ACL resources: ● Ingress ACL: Resources used by inbound traffic policy and ACL-based simplified traffic policy. ● Egress ACL: Resources used by outbound traffic policy and ACL-based simplified traffic policy.
VACL	Inbound ACL resources delivered before Layer 2 forwarding process starts.
IACL Unallocated	Unallocated inbound ACL resources.
IACL Allocated	Inbound ACL resources are allocated, including: ● L2 ACL: ACL resources of L2 type. ● IPv4 ACL: ACL resources of IPv4 type. ● IPv6 ACL: ACL resources of IPv6 type. ● L2IPv4 ACL: ACL resources of L2 IPv4 type. ● L2IPv6 ACL: ACL resources of L2 IPv6 type. ● UDF ACL: user-defined ACL resources. ● Srv ACL: ACL resources of service type. ● Sec ACL: ACL resources of security type. ● Ext ACL: extended ACL resources.

Item	Description
EACL Unallocated	Unallocated outbound ACL resources.
EACL Allocated	Outbound ACL resources are allocated, including: ● L2 ACL: ACL resources of L2 type. ● IPv4 ACL: ACL resources of IPv4 type. ● IPv6 ACL: ACL resources of IPv6 type. ● L2IPv4 ACL: ACL resources of L2 IPv4 type. ● L2IPv6 ACL: ACL resources of L2 IPv6 type. ● UDF ACL: user-defined ACL resources. ● Srv ACL: ACL resources of service type. ● Ext ACL: extended ACL resources.
Ingress Meter	Inbound rate limiting resources.
Egress Meter	Outbound rate limiting resources.
Ingress Counter	Inbound statistics collection resources.
Egress Counter	Outbound statistics collection resources.
Ingress UDF	Inbound user-defined ACL resources.

Related Topics

14.1.5 acl (system view)

14.1.12 display snmp-agent trap feature-name acle all

Function

The **display snmp-agent trap feature-name acle all** command displays the status of all traps on the ACL module.

Format

display snmp-agent trap feature-name acle all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the trap function of a specified feature is enabled, you can run the **display snmp-agent trap feature-name acle all** command to check the status of all traps of ACL. You can use the **snmp-agent trap enable feature-name acle** command to enable the trap function of ACL.

Prerequisites

SNMP has been enabled. See **snmp-agent**.

Example

# Display all the traps of the ACL module.

```
<HUAWEI>display snmp-agent trap feature-name acle all
------------------------------------------------------------------------------
Feature name: ACLE
Trap number : 4
------------------------------------------------------------------------------
Trap name                         Default switch status   Current switch status
hwAclResTotalCountExceedTrap      on                      on
hwAclResTotalCountExceedClearTrap
                                  on                      on
hwAclResThresholdExceedTrap       on                      on
hwAclResThresholdExceedClearTrap
                                  on                      on
```

Table 14-5 Description of the **display snmp-agent trap feature-name acle all** command output

Item	Description
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.

Item	Description
Trap name	Trap name. Traps of the ACL module include: ● hwAclResTotalCountExceedTrap: indicates the Huawei-property trap sent when the ACL resource usage on the device reaches 100%. ● hwAclResTotalCountExceedClearTrap: indicates the Huawei-property trap sent when the ACL resource usage on the device reaches 100%, and then falls below 100% and stays below 100% for a period of time. ● hwAclResThresholdExceedTrap: indicates the Huawei-property trap sent when the ACL resource usage on the device exceeds the upper alarm threshold (percentage). ● hwAclResThresholdExceedClearTrap: indicates the Huawei-property trap sent when the ACL resource usage on the device falls below the lower alarm threshold (percentage).
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

14.1.24 snmp-agent trap enable feature-name acle

14.1.13 display time-range

Function

The **display time-range** command displays the configuration and status of the current time range.

Format

display time-range { **all** | *time-name* }

Parameters

Parameter	Description	Value
all	Indicates all the configured time ranges.	-
time-name	Specifies the name of a time range during which ACL rules take effect.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To specify a time range during which ACL rules take effect, run the **time-range** command and reference the time range name when you configure an ACL.

Before using a time range to filter data packets, run the **display time-range** command to view the time range configuration to avoid duplicate time ranges.

NOTE

The device updates the status of ACLs with a delay of about 30 seconds. The **display time-range** command adopts the current time range to determine the status of ACLs; therefore, you may find that the ACL using an active time range is inactive. This is normal.

Example

# Display the configuration and status of all time ranges.

```
<HUAWEI> display time-range all
Current time is 14:48:13 10-17-2012 Wednesday

Time-range : abc (Active)
from 23:23 2012/9/9 to 23:59 2012/12/31
Total time-range number is 1
```

Table 14-6 Description of the **display time-range** command output

Item	Description
Current time is 14:48:13 10-17-2012 Wednesday	The current time is Wednesday 14:48:13 10-17-2012.

Item	Description
Time-range:abc (Active)	The time range is named **abc** and is active. The time range can be: - Active. - Inactive.
from 23:23 2012/9/9 to 23:59 2012/12/31	Time range abc is from 23:23 2012/9/9 to 23:59 2012/12/31.
Total time-range number	The total time-range number.

Related Topics

14.1.26 time-range

14.1.14 reset acl counter

Function

The **reset acl counter** command clears statistics about ACLs.

Format

reset acl counter { **name** *acl-name* | *acl-number* | **all** }

Parameters

Parameter	Description	Value
name *acl-name*	Specifies the name of an ACL whose statistics need to be cleared.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.

Parameter	Description	Value
acl-number	Specifies the number of an ACL whose statistics need to be cleared.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of a numbered advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user-defined ACL ranges from 5000 to 5999. ● The number of a user ACL ranges from 6000 to 9999. **NOTE** Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support user ACL.
all	Clears all the ACL statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL statistics generated in a certain period, run the **reset acl counter** command to clear existing statistics and start statistics collection.

NOTICE

After the **reset acl counter** command is executed, the system does not prompt you the statistics deletion.

Before using the **reset acl counter** command, determine whether you intend to clear ACL statistics.

Follow-up Procedure

After running the **reset acl counter** command to clear the previous ACL statistics, you can use the **display acl match-counter** command in the diagnostic view to check ACL rules and statistics on the packets matching the ACL rules in the current period.

Example

# Clear statistics about ACL 2000.

```
<HUAWEI> reset acl counter 2000
```

Related Topics

14.1.9 display acl

14.1.15 reset acl ipv6 counter

Function

The **reset acl ipv6 counter** command clears the ACL6 statistics.

Format

reset acl ipv6 counter { **name** *acl6-name* | *acl6-number* | **all** }

Parameters

Parameter	Description	Value
name *acl6-name*	Specifies the name of an ACL6 whose statistics need to be cleared.	The value is a string of 1 to 64 case-sensitive characters without spaces. The value must start with a letter.
acl6-number	Specifies the number of an ACL6 whose statistics need to be cleared.	The value is an integer that ranges from 2000 to 3999. ● ACL6s numbered 2000 to 2999 are basic ACL6s. ● ACL6s numbered 3000 to 3999 are advanced ACL6s.
all	Clears all the ACL6 statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL6 statistics in a certain period, run the **reset acl ipv6 counter** command to clear existing statistics and start statistics collection.

NOTICE

Before using the **reset acl ipv6 counter** command, determine whether you intend to clear ACL6 statistics.

After the **reset acl ipv6 counter** command is executed, the system does not prompt you the statistics deletion.

Follow-up Procedure

After running the **reset acl ipv6 counter** command to clear the previous ACL statistics, you can use the **display acl ipv6** command to view ACL rules and statistics on the packets matching the ACL rules in the current period.

Example

# Clear the statistics about basic ACL6 2000.

```
<HUAWEI> reset acl ipv6 counter 2000
```

Related Topics

14.1.10 display acl ipv6

14.1.16 rule (advanced ACL view)

Function

The **rule** command adds or modifies an advanced ACL rule.

The **undo rule** command deletes an advanced ACL rule.

By default, no advanced ACL rule is configured.

Format

- When the parameter *protocol* is specified as the Internet Control Message Protocol (ICMP), the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **icmp-type** { *icmp-name* | *icmp-type* [*icmp-code*] } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **icmp-type**

{ *icmp-name* | *icmp-type* [*icmp-code*] } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as the Transmission Control Protocol (TCP), the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as the User Datagram Protocol (UDP), the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as another protocol rather than GRE, IGMP, IP, IPINIP, or OSPF, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | { **fragment** | **first-fragment** } | **logging** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | **ttl-expired** | **vpn-instance** *vpn-instance-name*] *

- To delete an advanced ACL rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | { { **precedence** | **tos** } * | **dscp** } | { **fragment** | **first-fragment** } | **logging** | **icmp-type** | **source** | **source-port** | **tcp-flag** | **time-range** | **ttl-expired** | **vpn-instance**] *

NOTE

- The S2750, S5700LI, and S5700S-LI do not support **tos**.
- Only the S5720EI, S6720S-EI, and S6720EI support **ttl-expired**.
- The **vpn-instance** parameter is supported only when a software-based ACL is applied to the S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720EI, or S6720S-EI. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S1720, S2700, S5700, and S6720 V200R011C10 Configuration Guide - Security* ACL Configuration - ACL Fundamentals.
- Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support **first-fragment**.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-

Parameter	Description	Value
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
gre	Indicates that the protocol type is GRE. The value 47 indicates the GRE protocol.	-
igmp	Indicates that the protocol type is IGMP. The value 2 indicates the IGMP protocol.	-
ip	Indicates that the protocol type is IP.	-
ipinip	Indicates that the protocol type is IPINIP. The value 4 indicates the IPINIP protocol.	-
ospf	Indicates that the protocol type is OSPF. The value 89 indicates the OSPF protocol.	-
protocol-number	Indicates the protocol type expressed by name or number. **NOTE** Parameters in an ACL vary with the protocol type. The combination of **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } and **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } is applicable to TCP and UDP only.	The value expressed by number is an integer that ranges from 1 to 255.

Parameter	Description	Value
destination { *destination-address destination-wildcard* | **any** }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. - *destination-address*: specifies the destination IP address of data packets. - *destination-wildcard*: specifies the wildcard mask of the destination IP address. - **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 or the value of *destination-wildcard* is 255.255.255.255.	*destination-address*: The value is in dotted decimal notation. *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
icmp-type { *icmp-name* | *icmp-type* [*icmp-code*] }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. - *icmp-name*: specifies the name of ICMP packets. - *icmp-type*: specifies the type of ICMP packets. - *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. **Table 14-8** lists the mapping between ICMP names and ICMP types and codes.

Parameter	Description	Value
source { *source-address source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. ● *source-address*: specifies the source IP address of packets. ● *source-wildcard*: specifies the wildcard mask of the source IP address. ● **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address*: The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-

Parameter	Description	Value
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value is a string of 1 to 32 characters.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: ● **eq** *port*: equivalent to the destination port number. ● **gt** *port*: greater than the destination port number. ● **1t** *port*: smaller than the destination port number. ● **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: ● **eq** *port*: equivalent to the source port number. ● **gt** *port*: greater than the source port number. ● **1t** *port*: smaller than the source port number. ● **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.
dscp *dscp*	Specifies the value of a Differentiated Services Code Point (DSCP). **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value is an integer or a name. ● The value ranges from 0 to 63 when it is an integer. ● When it is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.

Parameter	Description	Value
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. ● The value can be 0, 1, 2, 4, or 8 when it is an integer. ● When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 14-7** describes the mapping between ToS names and values.
precedence *precedence*	Indicates that packets are filtered based on the precedence field. *precedence* specifies the precedence value.	The value ranges from 0 to 7. The values 0 to 7 correspond to *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network*.
fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments.	-
first-fragment	Indicates that the rule is valid for only initial fragments. If this parameter is specified, the rule is valid for only initial fragments.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: ● An ACL-based simplified traffic policy is configured and the **traffic-filter** and **traffic-secure** commands reference ACLs. ● MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GFR, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, **deny** must be specified for the **logging** parameter to take effect.	-
ttl-expired	Matches packets with the TTL value 1. If this keyword is not specified, the ACL rule matches packets with any TTL value.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** If the **vpn-instance** parameter is not specified, the switch matches packets from both public and private networks against ACL.	The value must be an existing VPN instance name.

Table 14-7 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 14-8 Mapping between ICMP names and ICMP types and codes

icmp-name	icmp-type	icmp-code
Echo	8	0
Echo-reply	0	0
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0
Information-request	15	0
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0

Views

Advanced ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An advanced ACL matches packets based on information such as source and destination IP addresses, source and destination port numbers, and protocol types.

The **rule** command defines the time range and flexibly configures the time ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. (If a simplified traffic policy references a specified rule in an ACL, this command does not take effect.) Before deleting a rule, ensure that the rule is not being referenced.

The parameter **fragment** cannot be set together with **source-port**, **destination-port**, **icmp-type**, and **tcp-flag**; otherwise, the following error message is displayed:

```
Error: The fragment cannot be configured together with the source-port, destination-port, icmp-type and
tcp-flag.
```

Example

# Add a rule to ACL 3000 to filter ICMP packets.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 1 permit icmp
```

# Delete a rule from ACL 3000.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] undo rule 1
```

# Add a rule to ACL 3000 to filter IGMP packets.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 2 permit igmp
```

# Add a rule to ACL 3000 to filter packets with DSCP priorities.

```
<HUAWEI> system-view
[HUAWEI] acl 3000
[HUAWEI-acl-adv-3000] rule 3 permit ip dscp cs1
```

# Add a rule to ACL 3001 to filter all the IP packets sent from hosts at 10.9.0.0 to hosts at 10.38.160.0.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule permit ip source 10.9.0.0 0.0.255.255 destination 10.38.160.0 0.0.0.255
```

# Add a rule to ACL 3001 to filter the packets with source UDP port number 128 from 10.9.8.0 to 10.38.160.0.

```
<HUAWEI> system-view
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule permit udp source 10.9.8.0 0.0.0.255 destination 10.38.160.0 0.0.0.255
destination-port eq 128
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

14.1.9 display acl

14.1.25 step

14.1.17 rule (advanced ACL6 view)

Function

The **rule** command adds or modifies an advanced ACL6 rule.

The **undo rule** command deletes an advanced CL6 rule.

By default, no advanced ACL6 rule is created.

Format

- When **protocol** is set to TCP, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **tcp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { **tcp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-*

length | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When **protocol** is set to UDP, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **udp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { **udp** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When **protocol** is set to ICMPv6, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { **icmpv6** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **icmp6-type** { *icmp6-type-name* | *icmp6-type* [*icmp6-code*] } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { **icmpv6** | *protocol-number* } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **icmp6-type** { *icmp6-type-name* | *icmp6-type* [*icmp6-code*] } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When **protocol** is set to other protocols, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **ipv6** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **gre** | **ipv6** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | *destination-ipv6-address* **postfix** *postfix-length* | **any** } | { { **precedence** *precedence* | **tos** *tos* } * | **dscp** *dscp* } | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- To delete an advanced ACL6 rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | **routing** [**routing-type** *routing-type*] | { **fragment** | **first-fragment** } | **icmp6-type** | **logging** | { { **precedence** | **tos** } * | **dscp** } | **routing** | **source** | **source-port** | **tcp-flag** | **time-range** | **vpn-instance**] *

NOTE

- The **vpn-instance** parameter is supported only when a software-based ACL is applied to the S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720EI, or S6720S-EI. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S1720, S2700, S5700, and S6720 V200R011C10 Configuration Guide - Security* ACL Configuration - ACL Fundamentals.
- Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support **destination**, **routing** [**routing-type** *routing-type*] and **first-fragment**.
- Only the S5730SI, S6720SI, S5720EI, S5720HI, S6720EI, and S6720S-EI support **dscp**, **precedence**, and **tos**.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, a rule is created using the ID and ordered based on the configured sequence. ● If the rule ID is not specified, the device allocates an ID to the new rule. By default, the step of ACL6 is 1 and cannot be changed. Therefore, the device allocates IDs at an interval of 1 to ACL6 rules.	The value is an integer that ranges from 0 to 2047.
deny	Indicates to drop packets conforming to certain conditions.	-
permit	Indicates to forward packets conforming to certain conditions.	-
tcp	Specifies the protocol type is TCP.	-
udp	Specifies the protocol type is UDP.	-
icmpv6	Specifies the protocol type is ICMPv6.	-
protocol-number	Specifies the protocol type that is expressed as a name or a number.	The value ranges from 1 to 255. The protocol type expressed as a name can be GRE, ICMPv6, IPv6, OSPF, TCP, and UDP.

Parameter	Description	Value
destination { *destination-ipv6-address prefix-length* | *destination-ipv6-address/ prefix-length* | **any** }	Indicates the destination address and prefix of a packet.	*destination-ipv6-address* is expressed in hexadecimal notation. The value of *prefix-length* is an integer that ranges from 1 to 128. You can also use **any** to represent any destination address.
destination *destination-ipv6-address* **postfix** *postfix-length*	Indicates the destination address and the length of destination address postfix.	*destination-ipv6-address* indicates the destination address and is expressed in hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.
dscp *dscp*	Specifies the Differentiated Services Code Point (DSCP) value. **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value of *dscp* can be an integer or a name. When the value is an integer, the value ranges from 0 to 63. When the value is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
routing [**routing-type** *routing-type*]	Specifies the IPv6 header in ACL6. The *routing-type* parameter specifies the routing-type field in the IPv6 header.	The value of *routing-type* is an integer that ranges from 0 to 255.
fragment	Indicates that the rule is valid for only non-first fragmented packets.	-
first-fragment	Indicates that the rule is valid for only initial fragmented packets.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: ● An ACL-based simplified traffic policy is configured and the **traffic-filter** command references ACLs. ● MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GFR, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, **deny** must be specified for the **logging** parameter to take effect.	-
precedence *precedence*	Indicates that the packets are filtered according to the precedence field.	**precedence** can be expressed as a name or a number. The value ranges from 0 to 7.
source { *source-ipv6-address prefix-length* | *source-ipv6-address/ prefix-length* | **any** }	Indicates the source address and prefix of a packet.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128. You can also use **any** to represent any source address.

Parameter	Description	Value
source *source-ipv6-address* **postfix** *postfix-length*	Indicates the source address and the length of source address postfix.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: ● **eq** *port*: equivalent to the destination port number. ● **gt** *port*: greater than the destination port number. ● **1t** *port*: smaller than the destination port number. ● **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: ● **eq** *port*: equivalent to the source port number. ● **gt** *port*: greater than the source port number. ● **1t** *port*: smaller than the source port number. ● **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.
icmp6-type { *icmp6-type-name* | *icmp6-type* [*icmp6-code*] }	Indicates that the type and code of ICMPv6 packets, which is effective only when the packet protocol is ICMP. If this parameter is not specified, all ICMP packets are matched.	*icmp6-type*: indicates the type of ICMP messages. The value ranges from 0 to 255. *icmp6-code*: indicates the type of ICMP messages. The value ranges from 0 to 255. The value of *icmp6-type-name* and the corresponding ICMP-Type and ICMP-Code are as **Table 14-10**.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Specifies the type of the SYN Flag in the TCP packet header is ack(010000).	-

Parameter	Description	Value
established	Specifies the type of the SYN Flag in the TCP packet header is ack(010000) or rst(000100).	-
fin	Specifies the type of the SYN Flag in the TCP packet header is fin(000001).	-
psh	Specifies the type of the SYN Flag in the TCP packet header is psh(001000).	-
rst	Specifies the type of the SYN Flag in the TCP packet header is rst(000100).	-
syn	Specifies the type of the SYN Flag in the TCP packet header is syn(000010).	-
urg	Specifies the type of the SYN Flag in the TCP packet header is urg(100000).	-
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.

Parameter	Description	Value
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. ● The value ranges from 0 to 15 when it is an integer. ● When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 14-9** describes the mapping between ToS names and values.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** If the **vpn-instance** parameter is not specified, the switch matches packets from both public and private networks against ACL.	The value must be an existing VPN instance name.

Table 14-9 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 14-10 Values of *icmp6-type-name* and the corresponding ICMP-Type and ICMP-Code

icmp6-type-name	icmp-type	icmp-code
Redirect	137	0
Echo	128	0
Echo-reply	129	0
Err-Header-field	4	0

icmp6-type-name	icmp-type	icmp-code
Frag-time-exceeded	3	1
Hop-limit-exceeded	3	0
Host-admin-prohib	1	1
Host-unreachable	1	3
Neighbor-advertisement	136	0
Neighbor-solicitation	135	0
Network-unreachable	1	0
Packet-too-big	2	0
Port-unreachable	1	4
Router-advertisement	134	0
Router-solicitation	133	0
Unknown-ipv6-opt	4	2
Unknown-next-hdr	4	1

Views

Advanced ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Advanced ACL6s classify data packets based on the source IP address, destination IP address, source port number, destination port number, and protocol type.

The **rule** command defines the time range and flexibly configures the time ACL6 rules take effect.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.

When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.

The parameter **fragment** cannot be set together with **source-port**, **destination-port**, **icmp6-type**, and **tcp-flag**.

Example

# Add a rule to ACL6 3000 to deny the packets with the destination UDP port number that is greater than 128 from fc00:1::1 to fc00:3::1.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 3000
[HUAWEI-acl6-adv-3000] rule deny udp source fc00:1::1 64 destination fc00:3::1 64 destination-port gt
128
```

Related Topics

14.1.3 acl ipv6 (system view)

14.1.2 acl ipv6 name

14.1.10 display acl ipv6

14.1.18 rule (basic ACL view)

Function

The **rule** command adds or modifies a basic ACL rule.

The **undo rule** command deletes a basic ACL rule.

By default, no rule is configured for a basic ACL.

Format

rule [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **fragment** | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

NOTE

The **vpn-instance** parameter is supported only when a software-based ACL is applied to the S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720EI, or S6720S-EI. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S1720, S2700, S5700, and S6720 V200R011C10 Configuration Guide - Security* ACL Configuration - ACL Fundamentals.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match a rule.	-

Parameter	Description	Value
source { *source-address source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. - *source-address*: specifies the source IP address of packets. - *source-wildcard*: specifies the wildcard mask of the source IP address. - **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address* : The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** If the **vpn-instance** parameter is not specified, the switch matches packets from both public and private networks against ACL.	The value must be an existing VPN instance name.
fragment	Indicates that the rule is valid for only non-first fragmented packets. If **fragment** is contained, the rule is valid for non-first fragmented packets and invalid for non-fragmented packets and first fragmented packet. **NOTE** Rules that do not contain **fragment** are valid for all the packets.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: ● An ACL-based simplified traffic policy is configured and the **traffic-filter** and **traffic-secure** commands reference ACLs. ● MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GFR, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, **deny** must be specified for the **logging** parameter to take effect.	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value is a string of 1 to 32 characters.

Views

Basic ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL matches packets based on information such as source IP addresses, fragment flags, and time ranges.

The **rule** command defines the time range and flexibly configures the time ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.

Example

# Add a rule in ACL 2001 to permit the packets from 192.168.32.1.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule permit source 192.168.32.1 0
```

# Delete rule 5 from ACL 2001.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] undo rule 5
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

14.1.9 display acl

14.1.25 step

14.1.19 rule (basic ACL6 view)

Function

The **rule** command adds or modifies basic ACL6 rules.

The **undo rule** command deletes a basic CL6 rule.

By default, there is no basic ACL6 rule.

Format

rule [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule { **deny** | **permit** } [**fragment** | **logging** | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | *source-ipv6-address* **postfix** *postfix-length* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

NOTE

The **vpn-instance** parameter is supported only when a software-based ACL is applied to the S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720EI, or S6720S-EI. For usage scenarios of software-based ACLs, see "**ACL Implementations**" in the *S1720, S2700, S5700, and S6720 V200R011C10 Configuration Guide - Security* ACL Configuration - ACL Fundamentals.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, a rule is created using the ID and ordered based on the configured sequence. ● If the rule ID is not specified, the device allocates an ID to the new rule. By default, the step of ACL6 is 1 and cannot be changed. Therefore, the device allocates IDs at an interval of 1 to ACL6 rules.	The value is an integer that ranges from 0 to 2047.
deny	Indicates to drop packets conforming to certain conditions.	-
permit	Indicates to forward packets conforming to certain conditions.	-
fragment	Indicates that the rule is valid for only non-first fragmented packets.	-

Parameter	Description	Value
logging	Logs IP information of packets that match the rule. **NOTE** The **logging** parameter takes effect for incoming packets in either of the following scenarios: ● An ACL-based simplified traffic policy is configured and the **traffic-filter** command references ACLs. ● MQC is configured, the traffic behavior is set to **permit** or **deny**, and the **traffic-policy** command references ACLs. In addition, for the S1720GFR, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, **deny** must be specified for the **logging** parameter to take effect.	-
source { *source-ipv6-address prefix-length* | *source-ipv6-address/ prefix-length* }	Indicates the source address and prefix of a packet.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128.
source *source-ipv6-address* **postfix** *postfix-length*	Indicates the source address and the length of source address postfix.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *postfix-length* is an integer that ranges from 1 to 64.
any	Indicates any source address.	-

Parameter	Description	Value
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** If the **vpn-instance** parameter is not specified, the switch matches packets from both public and private networks against ACL.	The value must be an existing VPN instance name.

Views

Basic ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL6 matches packets based on information such as source IP addresses, fragment flags, and time ranges.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.

Example

# Add a rule for the ACL6 with a number of 2000 to prohibit the passing of packets from the source fc00:1::1/64.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule deny source fc00:1::1/64
```

Related Topics

14.1.3 acl ipv6 (system view)

14.1.2 acl ipv6 name

14.1.10 display acl ipv6

14.1.20 rule (layer 2 ACL view)

Function

The **rule** command adds or modifies a Layer 2 ACL rule.

The **undo rule** command deletes a Layer 2 ACL rule.

By default, there is no rule in the related Layer 2 ACL view.

Format

rule [*rule-id*] { **permit** | **deny** } [[**ether-ii** | **802.3** | **snap**] | **l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **cvlan-id** *cvlan-id* [*cvlan-id-mask*] | **cvlan-8021p** *802.1p-value* | **double-tag** | **time-range** *time-name*] *

undo rule { **permit** | **deny** } [[**ether-ii** | **802.3** | **snap**] | **l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **cvlan-id** *cvlan-id* [*cvlan-id-mask*] | **cvlan-8021p** *802.1p-value* | **double-tag** | **time-range** *time-name*] *

undo rule *rule-id*

NOTE

The S1720GFR, S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, and S5700S-LI do not support **cvlan-id** *cvlan-id* [*cvlan-id-mask*], **cvlan-8021p** *802.1p-value*, and **double-tag**.

The S1720X, S1720X-E, S6720LI, S5730SI, S5730S-EI, S6720S-LI, S6720SI, and S6720S-SI do not support **cvlan-8021p** *802.1p-value*.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule overwrites the old rule. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match a rule.	-
permit	Permits the packets that match a rule.	-

Parameter	Description	Value
ether-ii | **802.3** | **snap**	Indicates the encapsulation format of a packet that matches the rule. - *ether-ii*: specifies the Ethernet II encapsulation. - *802.3*: specifies the 802.3 encapsulation. - *snap*: specifies the SNAP encapsulation. **NOTE** - On the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, or S5700S-LI, when the ACL matching the encapsulation format **ether-ii** or **snap** is configured, the ACL matches the packets encapsulated with both Ethernet II and SNAP, including IPv4 and IPv6 packets. - On the S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, or S6720S-SI, when the ACL matching the encapsulation format **ether-ii** or **snap** is configured, the ACL matches the IPv6 packets encapsulated with Ethernet II and SNAP, but matches the IPv4 packets encapsulated with either **ether-ii** or **snap**.	-

Parameter	Description	Value
l2-protocol *type-value* [*type-mask*]	Indicates the type of a Layer 2 protocol. This parameter corresponds to the Ethernet type of Ethernet_II frames and the type-code domain of Ethernet_SNAP frames. ● *type-value*: specifies the type value of a Layer 2 protocol. ● *type-mask*: specifies the type mask of a Layer 2 protocol.	*type-value* can be a hexadecimal number of 3 to 6 bits that ranges from 0x0000 to 0xFFFF or the following protocol name: ● ARP: corresponding to 0x0806 ● IP: corresponding to 0x0800 ● IPv6: corresponding to 0x86dd ● MPLS: corresponding to 0x8847 ● RARP: corresponding to 0x8035 The default value of *type-mask* is 0xffff.
destination -mac *dest-mac-address* [*dest-mac-mask*]	Specifies the destination MAC address of packets that matches ACL rules. ● *dest-mac-address* specifies the destination MAC address of packets. ● *dest-mac-mask* specifies the mask of the destination MAC address of packets.	*dest-mac-address* and *dest-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *dest-mac-mask* is ffff-ffff-ffff. You can obtain the required destination MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.
source-mac *source-mac-address* [*source-mac-mask*]	Specifies the source MAC address of packets that matches ACL rules. ● *source-mac-address* specifies the source MAC address of packets. ● *source-mac-mask* specifies the mask of the source MAC address of packets. If this parameter is not specified, the mask is ffff-ffff-ffff.	*source-mac-address* and *source-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *source-mac-mask* is ffff-ffff-ffff. You can obtain the required source MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.

Parameter	Description	Value
vlan-id *vlan-id* [*vlan-id-mask*]	Indicates the outer VLAN ID contained in a packet that matches the rule. ● *vlan-id*: specifies the number of the VLAN ID. ● *vlan-id-mask*: specifies the mask of the VLAN ID.	The value of *vlan-id* is an integer ranging from 1 to 4094. The value of the *vlan-id-mask* is a hexadecimal number ranging from 0x0 to 0xFFF. The default value is 0xFFF.
8021p *802.1p-value*	Indicates the 802.1p priority in the outer VLAN tag of a packet that matches the rule.	The value is an integer ranging from 0 to 7.
cvlan-id *cvlan-id* [*cvlan-id-mask*]	Indicates the inner VLAN ID of a packet that matches the rule. ● *cvlan-id*: specifies the number of the inner VLAN ID. ● *cvlan-id-mask*: specifies the mask of the inner VLAN ID.	The value of *cvlan-id* is an integer ranging from 1 to 4094. The value of the *cvlan-id-mask* is a hexadecimal number ranging from 0x0 to 0xFFF. The default value is 0xFFF.
cvlan-8021p *802.1p-value*	Indicates the 802.1p priority in the inner VLAN tag of a packet that matches the rule.	The value is an integer ranging from 0 to 7.
double-tag	Indicates that only packets with double tags match the rule.	-
time-range *time-name*	Defines the time range during which an ACL rule is valid. *time-name* specifies the name of a time range. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value of *time-name* is a string of 1 to 32 characters.

Views

layer 2 ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 ACL matches packets based on Layer 2 information of the packets, such as source MAC addresses, destination MAC addresses, and Layer 2 protocol types.

The **rule** command defines the time range and flexibly configures the time when the ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists, the new rule overwrites the old rule no matter whether the rules conflict.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.

Example

# Add a rule to ACL 4001 to match packets with the destination MAC address being 0000-0000-0001, source MAC address being 0000-0000-0002, and the value of the Layer 2 protocol type being 0x0800.

```
<HUAWEI> system-view
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-protocol 0x0800
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

14.1.9 display acl

14.1.25 step

14.1.21 rule (user-defined ACL view)

Function

The **rule** command adds and modifies a rule in the related UCL view.

The **undo rule** command deletes an ACL rule.

By default, there is no rule in the related advanced UCL view.

Format

rule [*rule-id*] { **deny** | **permit** } [[**l2-head** | **ipv4-head** | **ipv6-head** | **l4-head**] { *rule-string rule-mask offset* } &<1-8> | **time-range** *time-name*] *

undo rule { **deny** | **permit** } [[**l2-head** | **ipv4-head** | **ipv6-head** | **l4-head**] { *rule-string rule-mask offset* } &<1-8> | **time-range** *time-name*] *

undo rule *rule-id*

NOTE

The S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support &<1-8> and **ipv6-head**.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule overwrites the old rule. If the specified rule ID does not exist, the Switch creates a new rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the Switch allocates an ID to the new rule. The rule IDs are sorted in ascending order. The Switch automatically allocates IDs according to the step. The step is set by using the **14.1.25 step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match a rule.	-
permit	Permits the packets that match a rule.	-

Parameter	Description	Value
l2-head | **ipv4-head** | **ipv6-head** | **l4-head**	Indicates the position from which the offset starts. ● **l2-head**: indicates that the offset begins from the Layer 2 header. ● **ipv4-head**: indicates that the offset begins from the IPv4 header. ● **ipv6-head**: indicates that the offset begins from the IPv6 header. ● **l4-head**: indicates that the offset begins from the Layer 4 header.	-
rule-string	Specifies the customized rule string.	The value is a string of 3 to 10 characters. The string is in hexadecimal notation. The maximum length of the string is 4 bytes. **NOTE** The **rule** command in the user-defined ACL view matches four bytes each time. When the matching field length is smaller than four bytes, add 0 to the field.
rule-mask	Specifies the mask of the rule string.	The value is a string of 3 to 10 characters. The string is in hexadecimal notation. The maximum length of the string is 4 bytes. When the mask bit of the customized character string is 1, the ACL matches the bit. When the mask bit of the customized character string is 0, the ACL does not match the bit.
offset	Specifies the value of the offset.	The value is an integer, in bytes. The value of the offset varies with the offset position. ● For **l2-head**, the value of *offset* is **4N+2**. N is an integer starting from 0. ● For other offset positions, the value of *offset* is **4N**. N is an integer starting from 0.

Parameter	Description	Value
time-range *time-name*	Defines the time range during which an ACL rule takes effect. *time-name* specifies the name of the time range during which an ACL rule takes effect.	The value is a string of 1 to 32 characters.

Views

User-defined ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user-defined ACL defines rules by setting the offset position and value of the packet. The user-defined ACL is applicable to matching rules of a traffic classifier.

The **rule** command defines the time range and flexibly configures the time when the ACL rules take effect.

NOTE

The user-defined ACL is applicable to only the incoming traffic.

Prerequisites

An ACL must be created before the rule is configured.

Precautions

- If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule. To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result will be incorrect.
- To change the offset in a user-defined ACL rule, delete and reconfigure the ACL rule.
- The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Use this command with caution, especially when you delete an ACL rule that has been referenced.
- When specifying an ACL rule to match offset bytes in the Layer 2 header on the S5730SI, S5730S-EI, S6720-56C-PWH-SI-AC, or S6720-56C-PWH-SI, add a tag first if the ACL rule will be applied on a GE electrical interface through which packets having no tag pass.

Example

# Add a rule in ACL 5001 to match the four bytes following the 14 offset bytes from the Layer 2 header. The string of the ACL rule is **0x0180C200**.

```
<HUAWEI> system-view
[HUAWEI] acl 5001
[HUAWEI-acl-user-5001] rule permit l2-head 0x0180C200 0xFFFFFFFF 14
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

14.1.9 display acl

14.1.25 step

14.1.22 rule (user ACL view)

Function

The **rule** command configures a user ACL rule.

The **undo rule** command deletes a user ACL rule.

By default, no user ACL rule is configured.

NOTE

Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.

Format

- When the parameter *protocol* is specified as the ICMP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **icmp-type** { *icmp-name* | *icmp-type* [*icmp-code*] } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **icmp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **icmp-type** { *icmp-name* | *icmp-type* [*icmp-code*] } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as the TCP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address* *destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule { **deny** | **permit** } { *protocol-number* | **tcp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **established** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as the UDP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **udp** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- When the parameter *protocol* is specified as the GRE, IGMP, IP, IPINIP, or OSPF, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

  undo rule { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**source** { { *source-address source-wildcard* | **any** } | { **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } * | **destination** { { { *destination-address destination-wildcard* | **any** } | { **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

- To delete an ACL rule, run:
  undo rule *rule-id*

NOTE

The S5720EI, S6720S-EI, and S6720EI do not support **destination** { **fqdn** *fqdn-name* }, **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* }, and **vpn-instance** *vpn-instance-name*.

Only the S5720HI supports the **source** and **destination** parameters in [**source**] **ucl-group** and [**destination**] **ucl-group**.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-

Parameter	Description	Value
permit	Permits the packets that match the rule.	-
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
gre	Indicates that the protocol type is GRE. The value 47 indicates the GRE protocol.	-
igmp	Indicates that the protocol type is IGMP. The value 2 indicates the IGMP protocol.	-
ip	Indicates that the protocol type is IP.	-
ipinip	Indicates that the protocol type is IPINIP. The value 4 indicates the IPINIP protocol.	-
ospf	Indicates that the protocol type is OSPF. The value 89 indicates the OSPF protocol.	-
protocol-number	Indicates the protocol type expressed by number.	The value expressed by number is an integer that ranges from 1 to 255.

Parameter	Description	Value
source { { *source-address source-wildcard* | **any** } | { [**source**] **ucl-group** { *source-ucl-group-index* | **name** *source-ucl-group-name* } } } *	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. ● *source-address*: specifies the source IP address of packets. ● *source-wildcard*: specifies the wildcard mask of the source IP address. ● **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 and the value of *source-wildcard* is 255.255.255.255. ● **ucl-group** *source-ucl-group-index*: specifies the ID of the UCL group to which the source IP address of packets belongs. ● **ucl-group name** *source-ucl-group-name*: specifies the name of the UCL group to which the source IP address of packets belongs.	● *source-address*: The value is in dotted decimal notation. ● *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1. ● The value of *source-ucl-group-name* must be the name of an existing UCL group. ● *source-ucl-group-index* is an integer that ranges from 0 to 48 for S5720EI, S6720S-EI, and S6720EI, 0 to 64000 for the other models. ● When the value of *source-ucl-group-index* is 0, the source address of packet matching the ACL rule is beyond the UCL group range.

Parameter	Description	Value
destination { { { *destination-address* *destination-wildcard* | **any** } | { [**destination**] **ucl-group** { *destination-ucl-group-index* | **name** *destination-ucl-group-name* } } } * | **fqdn** *fqdn-name* }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. - *destination-address*: specifies the destination IP address of data packets. - *destination-wildcard*: specifies the wildcard mask of the destination IP address. - **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 and the value of *destination-wildcard* is 255.255.255.255. - **ucl-group** *destination-ucl-group-index*: specifies the ID of the UCL group to which the destination IP address of packets belongs. - **ucl-group name** *destination-ucl-group-name*: specifies the name of the UCL group to which the destination IP address of packets belongs. - **fqdn** *fqdn-name*: specifies the name of a domain. The precise matching and fuzzy matching (using *) are supported. In fuzzy matching, the fuzzy domain name and full domain name cannot include each	- *destination-address*: The value is in dotted decimal notation. - *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1. - *destination-ucl-group-index* is an integer that ranges from 0 to 48 for S5720EI, S6720S-EI, and S6720EI, 0 to 64000 for the other models. - When the value of *destination-ucl-group-index* is 0, the destination address of packet matching the ACL rule is beyond the UCL group range. - The value of *fqdn-name* is a string of 1 to 64 characters.

Parameter	Description	Value
	other. For example, if **www.abc.com** has been configured on the device, ***.abc.com** cannot be configured, but ***.aaa.com** can be configured. Similarly, if ***.abc.com** has been configured on the device, ***.www.abc.com** cannot be configured, but **www.aaa.com** can be configured. This parameter is available for only wireless users.	
icmp-type { *icmp-name* | *icmp-type* [*icmp-code*] }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. - *icmp-name*: specifies the name of ICMP packets. - *icmp-type*: specifies the type of ICMP packets. - *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. **NOTE** **Table 14-11** lists the mapping between ICMP names and ICMP types and codes.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: ● **eq** *port*: equal operator. ● **gt** *port*: greater than operator. ● **1t** *port*: smaller than operator. ● **range** *port-start port-end*: within the range.*port-start* specifies the start port number.*port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: ● **eq** *port*: equal operator. ● **gt** *port*: greater than operator. ● **1t** *port*: smaller than operator. ● **range** *port-start port-end*: within the range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. ● When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port* ● When the value is expressed as a number, it ranges from 0 to 65534 in **gt** *port* ● When the value is expressed as a number, it ranges from 1 to 65535 in **lt** *port* The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-

Parameter	Description	Value
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL cannot be bound to the specified time range.	The value is a string of 1 to 32 characters.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance on the inbound interface.	The value must be an existing VPN instance name.

Table 14-11 Mapping between ICMP names and ICMP types and codes

icmp-name	icmp-type	icmp-code
Echo	8	0
Echo-reply	0	0
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0
Information-request	15	0

icmp-name	icmp-type	icmp-code
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0

Views

User ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user ACL defines rules to filter IPv4 packets based on the source IP addresses or source User Control List (UCL) groups, destination IP addresses or destination UCL groups, IP protocol types, ICMP types, TCP source/destination port numbers, UDP source/destination port numbers, and time ranges.

Currently, the user ACL can only be applied to the UCL groups of the NAC feature. To control the network access rights of users based on user groups, you can perform the following operations: configure a UCL group, associate user ACL rules with the UCL group so that the ACL rules apply to all users in the user group, configure packet filtering based on user ACL to make the ACL take effect, and then apply the UCL group to the AAA service scheme.

Prerequisites

If the **ucl-group name** *source-ucl-group-name* or **ucl-group name** *destination-ucl-group-name* parameter is configured for a rule, the source and destination UCL groups must have been created by the **13.4.195 ucl-group** command.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. (If a simplified traffic policy references a specified rule in an ACL, this command does not take effect.) Before deleting a rule, ensure that the rule is not being referenced.

Example

# Add a rule to ACL 6000 to reject all the IP packets sent from UCL group group1 to network segment 10.9.9.0/24.

```
<HUAWEI> system-view
[HUAWEI] ucl-group 1 name group1
[HUAWEI] acl 6000
[HUAWEI-acl-ucl-6000] rule deny ip source ucl-group name group1 destination 10.9.9.0 0.0.0.255
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

14.1.9 display acl

14.1.23 rule description

Function

The **rule description** command configures the description of an ACL rule.

The **undo rule description** command deletes the description of an ACL rule.

By default, no description is configured for an ACL rule.

Format

rule *rule-id* **description** *description*

undo rule *rule-id* **description**

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule.	• ACL view: The value is an integer that ranges from 0 to 4294967294. • ACL6 view: The value is an integer that ranges from 0 to 2047.

Parameter	Description	Value
description *description*	Specifies the description of an ACL rule. You can configure the description to record an ACL rule in detail.	The value is a character string and contains a maximum of 127 characters.

Views

ACL view, ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

The *rule-id* parameter identifies a rule, but cannot describe the meaning and usage of the rule. The description with a character string can be used to solve the problem.

Prerequisites

The ACL rule has been created. If the ACL rule does not exist, the system displays an error message when you run this command.

Precautions

If the **rule description** command is run repeatedly, the latest configuration takes effect.

After you run the **undo rule** *rule-id* command, the rule and rule description are deleted.

Example

# Configure the description for rule 5 in acl 2001, which permits the packets from 192.168.32.1.

```
<HUAWEI> system-view
[HUAWEI] acl 2001
[HUAWEI-acl-basic-2001] rule 5 permit source 192.168.32.1 0
[HUAWEI-acl-basic-2001] rule 5 description permit 192.168.32.1
[HUAWEI-acl-basic-2001] display acl 2001
Basic ACL 2001, 1 rule
Acl's step is 5
 rule 5 permit source 192.168.32.1 0
 rule 5 description permit 192.168.32.1
```

Related Topics

14.1.18 rule (basic ACL view)

14.1.16 rule (advanced ACL view)

14.1.20 rule (layer 2 ACL view)

14.1.21 rule (user-defined ACL view)

14.1.17 rule (advanced ACL6 view)

14.1.19 rule (basic ACL6 view)

14.1.9 display acl

14.1.10 display acl ipv6

14.1.24 snmp-agent trap enable feature-name acle

Function

The **snmp-agent trap enable feature-name acle** command enables the trap function for the ACL module.

The **undo snmp-agent trap enable feature-name acle** command disables the trap function for the ACL module.

By default, the trap function is enabled for the ACL module.

Format

snmp-agent trap enable feature-name acle [**trap-name** { **hwaclresthresholdexceedcleartrap** | **hwaclresthresholdexceedtrap** | **hwaclrestotalcountexceedcleartrap** | **hwaclrestotalcountexceedtrap** }]

undo snmp-agent trap enable feature-name acle [**trap-name** { **hwaclresthresholdexceedcleartrap** | **hwaclresthresholdexceedtrap** | **hwaclrestotalcountexceedcleartrap** | **hwaclrestotalcountexceedtrap** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwaclresthresholdexceedcleartrap	Enables the device to send a Huawei-property trap sent when the ACL resource usage on the device falls below the lower alarm threshold (percentage).	-
hwaclresthresholdexceedtrap	Enables the device to send a Huawei-property trap sent when the ACL resource usage on the device exceeds the upper alarm threshold (percentage).	-

Parameter	Description	Value
hwaclrestotalcountexceedcleartrap	Enables the device to send a Huawei-property trap sent when the ACL resource usage on the device reaches 100%, and then falls below 100% and stays below 100% for a period of time.	-
hwaclrestotalcountexceedtrap	Enables the device to send a Huawei-property trap sent when the ACL resource usage on the device reaches 100%.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the trap function is enabled, the device generates traps during running and sends traps to the NMS through SNMP. When the trap function is not enabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

Example

# Enable the hwaclresthresholdexceedtrap for ACL.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name acle trap-name hwaclresthresholdexceedtrap
```

Related Topics

14.1.12 display snmp-agent trap feature-name acle all

14.1.25 step

Function

The **step** command sets the step between ACL rule IDs.

The **undo step** command restores the default step between ACL rule IDs.

By default, the step between ACL rule IDs is 5.

Format

step *step*

undo step

Parameters

Parameter	Description	Value
step	Specifies the step between ACL rule IDs.	The value is an integer that ranges from 1 to 20.

Views

ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The step is the difference between rule IDs when the system automatically assigns rule IDs. For example, if the ACL step value is set to 5, rules are numbered 5, 10, 15, and so on.

To add a rule between existing rules, you need to reset the step. For example, an ACL in **config** mode contains three rules with IDs being 5, 10, and 15. To insert a new rule after rule 5 (the first rule), run the **rule 7** *xxxx* command to insert rule 7.

If the step value is changed, ACL rule IDs are arranged automatically. For example, if the original rule IDs are 5, 10, and 15, the rule IDs become 2, 4, and 6 after you change the step value to 2.

NOTE

The **undo step** command can be used to realign ACL rule IDs immediately based on the default step. For example, ACL rule group 3001 contains four rules with IDs being 1, 3, 5, and 7, and the step is 2. After the **undo step** command is executed, the rule IDs become 5, 10, 15, and 20 and the step value is restored to 5.

Prerequisites

An ACL has been created by running the **acl** command.

Precautions

The ACL6 does not support the step.

Example

# Set the step between rules in ACL 3101 to 2.

```
<HUAWEI> system-view
[HUAWEI] acl 3101
[HUAWEI-acl-adv-3101] step 2
```

Related Topics

14.1.5 acl (system view)

14.1.4 acl name

14.1.26 time-range

Function

The **time-range** command sets a time range.

The **undo time-range** command deletes a time range.

By default, no time range is set.

Format

time-range *time-name* { *start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1* *date1* [**to** *time2 date2*] }

undo time-range *time-name* [*start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*]]

Parameters

Parameter	Description	Value
time-name	Specifies the name of a time range.	The value is a string of case-sensitive characters without spaces and must begin with a letter. The value ranges from 1 to 32. To avoid confusion, do not use "all" as the name of a time range.
start-time	Specify the start time of a time range.	The format is hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59.

Parameter	Description	Value
end-time	Specify the end time of a time range.	The format is hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59.
days	Specifies the date on which the time range takes effect.	The value can be one of the following: ● The numbers 0 to 6 indicate that the time range takes effect from Sunday to Saturday. The number 0 refers to Sunday. ● A weekday includes Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. ● The value "Daily" indicates that the time range takes effect during the seven days in a week. ● The value "off-day" indicates that the time range takes effect on weekends including Saturday and Sunday. ● The value "Working-day" indicates that the time range takes effect in five days from Monday to Friday.

Parameter	Description	Value
from *time1 date1*	Specifies the time for the time range to take effect.	*time1* is in the format of hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59. *date1* is in the format of yyyy/mm/dd. ● *yyyy* specifies the year. The value is an integer that ranges from 1970 to 2099. ● *mm* specifies the month. The value is an integer that ranges from 1 to 12. ● *dd* specifies the day. The value is an integer that ranges from 1 to 31.
to *time2 date2*	Specifies the end of a time range.	The formats *time2* and *date2* are the same as those of the start time. The end time must be later than the start time. If the end time is not set, the device takes the maximum value allowed by the system.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If some services or functions need to be started at intervals or periodically, you can run the **time-range** command to set the time range. When configuring ACL or ACL6 rules, you can reference the names of time ranges.

The time range is classified into the following types:

- Relative time range (periodic time range): It is specified by *start-time* and *end-time*. The weekday when the time range takes effect is determined by *days*.
- Absolute time range: It is specified by **from** and **to**. The absolute time range can be used to limit the periodic time range.

You can set the same name for multiple time ranges to describe a special period. If multiple time ranges have the same name, the periodic time ranges are ORed, and a periodic time range and a definite time range are ANDed. For example, three time ranges are set with the same name **test**:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** takes effect at 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in the year 2010.

Precautions

There may be a time difference of no more than 10 seconds between the configured time range and the time range that actually takes effect.

Example

# Set a time range named **test** that takes effect from 2010-01-01 00:00 to 2010-12-31 23:59.

```
<HUAWEI> system-view
[HUAWEI] time-range test from 0:0 2010/1/1 to 23:59 2010/12/31
```

# Set a time range named **test** that takes effect at 8:00-18:00 from Monday to Friday.

```
<HUAWEI> system-view
[HUAWEI] time-range test 8:00 to 18:00 working-day
```

# Set a time range named **test** that takes effect from 14:00 to 18:00 on every Saturday and Sunday.

```
<HUAWEI> system-view
[HUAWEI] time-range test 14:00 to 18:00 off-day
```

Related Topics

14.1.13 display time-range

14.2 Local Attack Defense Configuration Commands

14.2.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.2.2 auto-defend attack-packet sample

Function

The **auto-defend attack-packet sample** command sets the packet sampling ratio for attack source tracing.

The **undo auto-defend attack-packet sample** command restores the default packet sampling ratio.

By default, the packet sampling ratio is 5. That is, one packet is sampled in every 5 packets.

Format

auto-defend attack-packet sample *sample-value*

undo auto-defend attack-packet sample

Parameters

Parameter	Description	Value
sample-value	Specifies the packet sampling ratio for attack source tracing.	The value is an integer that ranges from 1 to 1024.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attack source tracing samples packets to identify attacks. Errors may occur in attack packet identification or packet rate calculation. A proper packet sampling ratio can reduce errors. A small sampling ratio makes the attack source tracing result accurate, but increases CPU usage. For example, when the sampling ratio is set to 1, every packet is sampled. The attack source tracing result is accurate, but the CPU usage is high because every packet is resolved.

The **auto-defend attack-packet sample** command sets the sampling ratio. You can set a proper value based on the requirements of attack source tracing precision and CPU usage.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

When a smaller attack source tracing threshold is used, the sampling ratio has greater impact on the attack source tracing result.

Example

# Set the sampling ratio for attack source tracing in the attack defense policy named **test** to 2.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend attack-packet sample 2
```

Related Topics

14.2.24 cpu-defend policy

14.2.3 auto-defend enable

14.2.3 auto-defend enable

Function

The **auto-defend enable** command enables automatic attack source tracing.

The **undo auto-defend enable** command disables automatic attack source tracing.

By default, attack source tracing is enabled.

Format

auto-defend enable

undo auto-defend enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of attack packets may attack the device CPU. Attack source tracing enables the device to trace attack sources and send logs or alarms to notify the administrator so that the administrator can take measures to defend against the attacks. By default, logs are sent to notify the administrator if attack source tracing is enabled.

After automatic attack source tracing is enabled, the device traces the source of the specified packets sent to the CPU. The packet type can be set using the **14.2.6 auto-defend protocol** command.

Precautions

Attack source tracing configured in an attack defense policy takes effect only when the attack defense policy is applied in the system view.

If the system software of a switch in a version earlier than V200R009C00 is upgraded to V200R009C00 or later version, an **undo auto-defend enable** configuration is automatically generated.

Example

# Enable attack source tracing in the attack defense policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
```

Related Topics

14.2.24 cpu-defend policy

14.2.4 auto-defend action

Function

The **auto-defend action** command enables attack source **punish** function and specifies a **punish** action.

The **undo auto-defend action** command disables the attack source **punish** function.

By default, the attack source **punish** function is disabled.

Format

auto-defend action { **deny** [**timer** *time-length*] | **error-down** }

undo auto-defend action

Parameters

Parameter	Description	Value
deny	Discards packets sent from an attack source.	-
timer *time-length*	Specifies the period during which packets sent from an identified attack source are discarded.	The value ranges from 1 to 86400, in seconds. The default value is 300.
error-down	Shuts down an interface that receives attack packets.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The **auto-defend action** command is applied to taking attack source **punish** actions. The device discards the packets sent from the identified source or shuts down the interface receiving attack packets.

NOTE

If the auto-defend action is set to shutdown, run the **error-down auto-recovery cause auto-defend interval** *interval-value* command to set a recovery delay before the device is attacked. This command is invalid for the interface in error-down state.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend action** command multiple times, only the latest configuration takes effect.

After the auto-defend action is set to **deny**, the device discards packets when being attacked. The configuration result can be verified using the **display auto-defend attack-source** command.

The device does not take **punish** actions on attack sources of whitelist users.

Attack source tracing configured in an attack defense policy takes effect only when the attack defense policy is applied in the system view.

NOTICE

If the device shuts down the interface that receives the attack packets, services of authorized users on the interface are interrupted. Exercise caution when you configure the device to shut down the interface.

Example

# Configure the device to discard packets from the identified source every 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend action deny timer 10
Info: This configuration may cause packet loss.
```

Related Topics

14.2.3 auto-defend enable

14.2.24 cpu-defend policy

14.2.29 display auto-defend attack-source

4.2.22 error-down auto-recovery

14.2.5 auto-defend alarm enable

Function

The **auto-defend alarm enable** command enables the event reporting function for attack source tracing.

The **undo auto-defend alarm enable** command disables the event reporting function for attack source tracing.

By default, the event reporting function for attack source tracing is disabled.

Format

auto-defend alarm enable

undo auto-defend alarm enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of packets of a specified protocol from an attack source exceeds the threshold in a specified period, the device reports an event to the administrator so that the administrator can take measures to protect the device.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Follow-up Procedure

Run the **auto-defend threshold** command to set the event reporting threshold for attack source tracing.

Example

# Enable the event reporting function in the attack defense policy **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend alarm enable
```

Related Topics

14.2.24 cpu-defend policy

14.2.3 auto-defend enable

14.2.6 auto-defend protocol

Function

The **auto-defend protocol** command specifies the types of protocol packets that the device monitors in attack source tracing.

The **undo auto-defend protocol** command deletes specified types of protocol packets that the device monitors in attack source tracing.

By default, the device traces sources of 8021X, ARP, DHCP, ICMP, IGMP, TCP, Telnet in attack source tracing.

Format

auto-defend protocol { **all** | { **8021x** | **arp** | **dhcp** | **icmp** | **igmp** | **tcp** | **telnet** | **ttl-expired** | **udp** }* }

undo auto-defend protocol { **8021x** | **arp** | **dhcp** | **icmp** | **igmp** | **tcp** | **telnet** | **ttl-expired** | **udp** }*

Parameters

Parameter	Description	Value
all	Configures the device to trace sources of 8021X, ARP, DHCP, ICMP, IGMP, TCP, Telnet, TTL-expired, and UDP packets in attack source tracing.	-
8021x	Adds 8021X packets to the list of traced packets or deletes 8021X packets from the list.	-
arp	Adds Address Resolution Protocol (ARP) packets to the list of traced packets or deletes ARP packets from the list.	-
dhcp	Adds Dynamic Host Configuration Protocol (DHCP) packets to the list of traced packets or deletes DHCP packets from the list.	-

Parameter	Description	Value
icmp	Adds Internet Control Message Protocol (ICMP) packets to the list of traced packets or deletes ICMP packets from the list.	-
igmp	Adds Internet Group Management Protocol (IGMP) packets to the list of traced packets or deletes IGMP packets from the list.	-
tcp	Adds Transmission Control Protocol (TCP) packets to the list of traced packets or deletes TCP packets from the list.	-
telnet	Adds Telnet packets to the list of traced packets or deletes Telnet packets from the list.	-
ttl-expired	Adds packets with the TTL value of 1 to the list of traced packets or deletes these packets from the list.	-
udp	Adds User Datagram Protocol (UDP) packets to the list of traced packets or deletes UDP packets from the list.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The

auto-defend protocol command is applied to the packet parsing phase. When an attack occurs, you cannot identify the type of attack packets. The **auto-defend protocol** command allows you to flexibly specify the types of traced packets.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

- If you run this command multiple times, only the latest configuration takes effect.
- If a packet type is specified, when the device is attacked and the attack source is traced, you can run the **display auto-defend attack-source** command to view attack source information.
- The attack source tracing function of local attack defense is valid to only IPv4 packets.

Example

# Delete IGMP and TTL-expired packets from the list of traced packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] undo auto-defend protocol igmp ttl-expired
```

Related Topics

14.2.3 auto-defend enable

14.2.24 cpu-defend policy

14.2.29 display auto-defend attack-source

14.2.7 auto-defend threshold

Function

The **auto-defend threshold** command sets the checking threshold and event reporting thresholdfor attack source tracing.

The **undo auto-defend threshold** command restores the default checking threshold and event reporting threshold for attack source tracing.

By default, the checking threshold and event reporting threshold for attack source tracing is 60 pps.

Format

auto-defend threshold *threshold*

undo auto-defend threshold

Parameters

Parameter	Description	Value
threshold	Specifies the checking threshold and event reporting threshold for attack source tracing.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack source tracing is enabled, you can set the checking threshold and event reporting threshold for attack source tracing. When the number of sent protocol packets from an attack source in a specified period exceeds the checking threshold, the device traces and logs the attack source.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend threshold** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

After the **auto-defend enable** command is executed, the device traces the attack source based on the default threshold even if the **auto-defend threshold** command is not used.

Example

# Set the checking threshold and event reporting threshold for attack source tracing in the attack defense policy named **test** to 200 pps.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend threshold 200
```

Related Topics

14.2.24 cpu-defend policy

14.2.3 auto-defend enable

14.2.8 auto-defend trace-type

Function

The **auto-defend trace-type** command configures an attack source tracing mode.

The **undo auto-defend trace-type** command deletes an attack source tracing mode.

By default, attack source tracing is based on source IP addresses and source MAC addresses.

Format

auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

undo auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

Parameters

Parameter	Description	Value
source-mac	Configures attack source tracing based on source MAC addresses so that the device classifies and collects statistics based on the source MAC address and identifies the attack source.	-
source-ip	Configures attack source tracing based on source IP addresses so that the device classifies and collects statistics based on the source IP address and identifies the attack source.	-
source-portvlan	Configures attack source tracing based on source ports +VLANs so that the device classifies and collects statistics based on the source port and VLAN and identifies the attack source.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling attack source tracing, you can specify one or more attack source tracing modes. The device then uses the specified modes to trace attack sources.

The device supports the following attack source tracing modes:

- Source IP address-based tracing: defends against Layer 3 attack packets.
- Source MAC address-based tracing: defends against Layer 2 attack packets with a fixed source MAC address.

- Source port+VLAN based tracing: defends against Layer 2 attack packets with different source MAC addresses.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

Table 14-12 lists the attack source tracing modes supported for different types of packets.

Table 14-12 Attack source tracing modes supported for different types of packets

Packet Type	Attack Source Tracing Mode
802.1X	Based on source MAC addresses and based on source ports+VLANs
ARP, DHCP, IGMP, ND, DHCPv6, MLDv6	Based on source MAC addresses, based on IP addresses, and based on source ports+VLANs
ICMP, TTL-expired, Telnet, TCP, UDP	Based on source IP addresses and based on source ports+VLANs

If you run this command multiple times, only the latest configuration takes effect.

A switch supports different numbers if attack source tracing modes for different protocol packets. For details, see the default modes described above.

After the attack source tracing function is enabled on the device, you can run the **display auto-defend attack-source** command to view attack source tracing information if an attack occurs.

When the attack source tracing mode is **source-ip** and action is **error-down**, if multiple interfaces receive the attack packets with the same source IP address and the packet rate exceeds the threshold, the switch shuts down only one interface, and then checks packet rate again. If the packet rate is still higher than the threshold, the switch shuts down another interface. The switch repeats the operations until the packet rate falls below the threshold.

Example

# Configure attack source tracing based on source MAC addresses.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] undo auto-defend trace-type source-ip source-portvlan
```

Related Topics

14.2.24 cpu-defend policy

14.2.29 display auto-defend attack-source

14.2.9 auto-defend whitelist

Function

The **auto-defend whitelist** command configures an attack source tracing whitelist. The switch does not trace the source of users in the whitelist.

The **undo auto-defend whitelist** command deletes an attack source tracing whitelist.

By default, no whitelist is configured for attack source tracing. If any of the following conditions is met, however, the switch uses the condition as the whitelist matching rule, regardless of whether attack source tracing is enabled. After attack source tracing is enabled, the switch does not perform attack source tracing for the packets matching such rules.

- If an application uses the TCP protocol and has set up a TCP connection with the switch, the switch will not consider TCP packets with the matching source IP address as attack packets. If no TCP packets match a source IP address within 1 hour, the rule that specifies this source IP address will be aged out.
- If an interface has been configured as a DHCP trusted interface using the **dhcp snooping trusted** command, the switch will not consider DHCP packets received from this interface as attack packets.
- If an interface has been configured as a MAC forced forwarding (MFF) network-side interface using the **mac-forced-forwarding network-port** command, the switch will not consider ARP packets received from this interface as attack packets.

For the preceding conditions, the switch supports a maximum of 16 whitelist matching rules based on source IP addresses and interfaces, and a maximum of 8 whitelist matching rules based on source IP addresses of TCP packets.

Format

auto-defend whitelist *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* }

undo auto-defend whitelist *whitelist-number* [**acl** *acl-number* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
whitelist-number	Specifies the number of a whitelist.	The value is an integer that ranges from 1 to 16.

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL referenced by a whitelist.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs
interface *interface-type interface-number*	Specifies the interface to which the whitelist is applied. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attack source tracing helps locate and punish sources of denial of service (DoS) attacks. If some users do not need to be traced regardless of whether an attack occurs, run the **auto-defend whitelist** command to configure a whitelist for users.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

Before referencing an ACL in a whitelist, create the ACL and configure rules.

If the ACL referenced by the whitelist specifies some protocols, ensure that packets of these protocols can be traced. You can run the **display auto-defend configuration** command to view the protocols supported by attack source tracing. If a protocol is not supported by attack source tracing, you can run the **auto-defend protocol** command to configure attack source tracing to support the protocol.

Example

# Add source IP addresses 10.1.1.1 and 10.1.1.2 to the attack source tracing whitelist.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
```

```
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.2 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend whitelist 1 acl 2000
```

Related Topics

14.1.5 acl (system view)

14.2.3 auto-defend enable

14.2.6 auto-defend protocol

14.2.24 cpu-defend policy

14.2.30 display auto-defend configuration

14.2.10 auto-port-defend aging-time

Function

The **auto-port-defend aging-time** command configures the aging time for port attack defense.

The **undo auto-port-defend aging-time** command restores the default aging time for port attack defense.

By default, the aging time for port attack defense is 300 seconds.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

auto-port-defend aging-time *time*

undo auto-port-defend aging-time [*time*]

Parameters

Parameter	Description	Value
aging-time *time*	Specifies the aging time for port attack defense.	The value is an integer that ranges from 30 to 86400, and must be a multiple of 10. The unit is second.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a device with port attack defense function enabled detects an attack on a port, the device traces the source and limits the rate of the attack packets on the port within the aging time (T seconds). When the aging time expires, the device calculates the protocol packet rate on the port again. If the rate is still above the protocol rate threshold, the device keeps tracing the source and limits the rate of the attack packets; otherwise, the device stops the operations.

If the aging time is too short, the device frequently starts packet rate detection on ports, which consumes CPU resources. If the aging time is too long, protocol packets cannot be promptly processed by the CPU, which affects services. Therefore, you need to run the **auto-port-defend aging-time** command to set an appropriate aging time according to the CPU usage and service status.

Prerequisites

The port attack defense function has been enabled using the **14.2.12 auto-port-defend enable** command.

Precautions

If you run the **auto-port-defend aging-time** command multiple times in the same attack defense policy view, only the latest configuration takes effect.

Example

# Set the aging time in the attack defense policy **test** view to 350 seconds.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend aging-time 350
```

Related Topics

14.2.24 cpu-defend policy

14.2.12 auto-port-defend enable

14.2.11 auto-port-defend alarm enable

Function

The **auto-port-defend alarm enable** command enables the report of port attack defense events.

The **undo auto-port-defend alarm enable** command disables the report of port attack defense events.

By default, port attack defense events are not reported.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

auto-port-defend alarm enable

undo auto-port-defend alarm enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a port undergoes a DoS attack, the malicious attack packets sent from this port to the CPU occupy bandwidth. As a result, the CPU cannot process the protocol packets sent from other ports, and services are interrupted. In this situation, you can enable the report of port attack defense events. When the rate of protocol packets on a port exceeds the check threshold, the switch reports an event to notify the network administrator, so that the administrator can promptly take measures to protect the switch.

Prerequisites

The port attack defense function has been enabled using the **auto-port-defend enable** command.

Follow-up Procedure

Run the **auto-port-defend protocol** { **all** | **arp-request** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** } **threshold** *threshold* command to set the threshold for protocol packet check in port attack defense.

Example

# Enable the report of port attack defense events in the attack defense policy **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend alarm enable
```

Related Topics

14.2.24 cpu-defend policy

14.2.3 auto-defend enable

14.2.14 auto-port-defend protocol threshold

14.2.12 auto-port-defend enable

Function

The **auto-port-defend enable** command enables the port attack defense function.

The **undo auto-port-defend enable** command disables the port attack defense function.

By default, the port attack defense function is enabled.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

auto-port-defend enable

undo auto-port-defend enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker initiates a DoS attack on a port, the malicious attack packets sent from this port to the CPU occupy bandwidth. As a result, the CPU cannot process the protocol packets sent from other ports, and services are interrupted.

The port attack defense function effectively limits the number of packets sent to the CPU, and prevents DoS attacks aiming at the CPU.

This function is enabled by default. If the number of packets received by a port within one second exceeds the protocol rate threshold, the device considers that an attack occurs on the port. Then the device traces the source and limits the rate of attack packets, and records an attack log to avoid impact on other ports.

Precautions

After the port attack defense function is enabled in an attack defense policy, the attack defense policy must be applied in the system view.

Example

# Enable the port attack defense function in the attack defense policy **test** view.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
```

Related Topics

14.2.24 cpu-defend policy

14.2.13 auto-port-defend protocol

Function

The **auto-port-defend protocol** command specifies the types of protocol packets to which port attack defense is applied.

The **undo auto-port-defend protocol** command cancels port attack defense for certain types of protocol packets.

By default, port attack defense is applicable to ARP Request, ARP Reply, DHCP, ICMP, IGMP, and IP fragment packets.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

auto-port-defend protocol { **all** | { **arp-request** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** }* }

undo auto-port-defend protocol { **arp-request** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** }*

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support icmp and ip-fragment packets.

Parameters

Parameter	Description	Value
all	Applies port attack defense to ARP Request, ARP Reply, DHCP, ICMP, IGMP, and IP fragment packets.	-
arp-request	Applies port attack defense to ARP Request packets or cancels port attack defense for ARP Request packets.	-

Parameter	Description	Value
arp-reply	Applies port attack defense to ARP Reply packets or cancels port attack defense for ARP Reply packets.	-
dhcp	Applies port attack defense to DHCP packets or cancels port attack defense for DHCP packets.	-
icmp	Applies port attack defense to ICMP packets or cancels port attack defense for ICMP packets.	-
igmp	Applies port attack defense to IGMP packets or cancels port attack defense for IGMP packets.	-
ip-fragment	Applies port attack defense to IP fragment packets or cancels port attack defense for IP fragment packets.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device calculates the rate of all protocol packets, including ARP Request, ARP Reply, DHCP, ICMP, IGMP, and IP fragment packets, received by a port, and traces the source and limits the rate of attack packets. If the packets exceeding protocol rate threshold contain only a few attack packets, you can run the **undo auto-port-defend protocol** command to cancel port attack defense for unneeded protocol types. If the device limits the rate of too many protocols, services are affected.

Prerequisites

The port attack defense function has been enabled using the **14.2.12 auto-port-defend enable** command.

Precautions

If you run this command multiple times in the same attack defense policy view, only the latest configuration takes effect.

After port attack defense is applied to a type of protocol packets, the **14.2.32 display auto-port-defend attack-source** command can display the attack source tracing information if the port is attacked by the specified protocol packets.

Example

# In the attack defense policy **test**, cancel port attack defense for ARP Reply packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] undo auto-port-defend protocol arp-reply
```

Related Topics

14.2.12 auto-port-defend enable

14.2.24 cpu-defend policy

14.2.32 display auto-port-defend attack-source

14.2.14 auto-port-defend protocol threshold

Function

The **auto-port-defend protocol threshold** command sets the protocol packet rate threshold for port attack defense.

The **undo auto-port-defend protocol threshold** command restores the default protocol packet rate threshold for port attack defense.

The following table lists the default rate thresholds for different protocols.

Packet Type	Rate Threshold
arp-request	60 pps for the S5720EI, S6720S-EI, and S6720EI, 120 pps for the S5720HI, and 30 pps for other switch models
arp-reply	60 pps for the S5720EI, S6720S-EI, and S6720EI, 120 pps for the S5720HI, and 30 pps for other switch models
dhcp	60 pps for the S5720EI, S6720S-EI, and S6720EI, 120 pps for the S5720HI, and 30 pps for other switch models

Packet Type	Rate Threshold
icmp	120 pps for the S5720HI and 60 pps for other switch models
igmp	120 pps for the S5720HI and 60 pps for other switch models
ip-fragment	30 pps

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

auto-port-defend protocol { **all** | **arp-request** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** } **threshold** *threshold*

undo auto-port-defend protocol { **all** | **arp-request** | **arp-reply** | **dhcp** | **icmp** | **igmp** | **ip-fragment** } **threshold** [*threshold*]

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support icmp and ip-fragment packets.

Parameters

Parameter	Description	Value
all	Sets the rate thresholds for ARP Request, ARP Reply, DHCP, ICMP, IGMP, and IP fragment packets.	-
arp-request	Specifies the rate threshold for ARP Request packets.	-
arp-reply	Specifies the rate threshold for ARP Reply packets.	-
dhcp	Specifies the rate threshold for DHCP packets.	-
icmp	Specifies the rate threshold for ICMP packets.	-
igmp	Specifies the rate threshold for IGMP packets.	-
ip-fragment	Specifies the rate threshold for IP fragment packets.	-

Parameter	Description	Value
threshold *threshold*	Specifies the protocol rate threshold.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port attack defense is enabled on a port, the device calculates the rate of affected protocol packets received by the port. If the packet rate exceeds the protocol rate threshold, the device considers that an attack occurs. Then the device traces the source and limits the rate of attack packets on the port, and records a log. The device moves the packets within the protocol rate limit (CPCAR in attack defense policies) to the low-priority queue, and then sends them to the CPU. The device discards the excess packets.

You need to set an appropriate rate threshold for port attack defense according to service requirements. If the CPU fails to process many protocol packets promptly after port attack defense is enabled, set a large packet rate threshold. If the CPU is busy processing the packets of a protocol, set a small rate threshold for this protocol to avoid impact on other services.

Prerequisites

The port attack defense function has been enabled using the **14.2.12 auto-port-defend enable** command.

Precautions

If you run the **auto-port-defend protocol threshold** command multiple times in the same attack defense policy view, only the latest configuration takes effect.

Example

# In the attack defense policy **test**, set the rate threshold for ARP Request packets to 40 pps.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend protocol arp-request threshold 40
```

Related Topics

14.2.12 auto-port-defend enable

14.2.24 cpu-defend policy

14.2.15 auto-port-defend sample

Function

The **auto-port-defend sample** command sets the protocol packet sampling ratio for port attack defense.

The **undo auto-defend attack-packet sample** command restores the default protocol packet sampling ratio for port attack defense.

By default, the protocol packet sampling ratio for port attack defense is 5. That is, one packet is sampled when every 5 packets are received.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

auto-port-defend sample *sample-value*

undo auto-port-defend sample [*sample-value*]

Parameters

Parameter	Description	Value
sample *sample-value*	Specifies the protocol packet sampling ratio for port attack defense.	The value is an integer that ranges from 1 to 1024.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device with port attack defense enabled identifies attacks by analyzing sampled packets. There may be errors in attack packet identification or packet rate calculation. Errors influence the attack defense effect. An appropriate sampling ratio helps you control attack defense accuracy.

A small sampling ratio improves attack defense accuracy, but consumes more CPU resources. When the sampling ratio is set to 1, the device analyzes every packet. The attack packets can be detected quickly, but CPU usage becomes high and services are affected. Therefore, make a balance between the attack defense requirement and CPU usage to decide a sampling ratio.

Prerequisites

The port attack defense function has been enabled using the **14.2.12 auto-port-defend enable** command.

Precautions

If the protocol packet rate threshold for port attack defense is set to a small value, the attack identification error caused by packet sampling ratio is large.

Example

# Set the protocol packet sampling ratio to 4 in the attack defense policy **test** view.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend sample 4
```

Related Topics

14.2.12 auto-port-defend enable

14.2.24 cpu-defend policy

14.2.16 auto-port-defend whitelist

Function

The **auto-port-defend whitelist** command configures a whitelist for port attack defense.

The **undo auto-port-defend whitelist** command deletes a whitelist for port attack defense.

By default, no whitelist is configured for port attack defense. After a port is configured as a DHCP trusted port using the **dhcp snooping trusted** command, the device automatically delivers whitelist matching rules regardless of whether the port attack defense function is enabled. A maximum of 16 rules based on source IP addresses and interfaces can be delivered. The device will not perform port attack defense actions on the DHCP packets received on interfaces.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

auto-port-defend whitelist *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* }

undo auto-port-defend whitelist *whitelist-number* [**acl** *acl-number* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
whitelist-number	Specifies the number of the whitelist configured for port attack defense.	The value is an integer that ranges from 1 to 16.
acl *acl-number*	Specifies the number of the ACL applied to the whitelist.	The value of *acl-number* is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs
interface *interface-type interface-number*	Specifies the type and number of the interface to which the whitelist is applied. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The port attack defense function is enabled by default on the device, so the device calculates protocol packet rates on all interfaces, and traces the source and limits the rate of attack packets. In some services, network-side interfaces need to receive a lot of valid protocol packets. You should add these interfaces or network nodes connecting to these interfaces to the whitelist. The device does not trace the source or limit the rate of protocol packets received by the interfaces in the whitelist.

Prerequisites

The port attack defense function has been enabled using the **14.2.12 auto-port-defend enable** command.

Precautions

To define the whitelist using an ACL, you must create an ACL and configure rules for the ACL.

Before configuring an ACL whitelist for some protocols, ensure that the port attack defense function supports these protocols. Use the **14.2.13 auto-port-defend protocol** command to specify the protocols to which port attack defense is applied.

Example

# In the attack defense policy **test**, configure a whitelist that references an ACL. The ACL permits the packets from the users with IP addresses 10.1.1.1 and 10.1.1.2.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] rule permit source 10.1.1.2 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend whitelist 1 acl 2000
```

# In the attack defense policy **test**, add interface GE0/0/1 to the whitelist for port attack defense.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend whitelist 1 interface gigabitethernet 0/0/1
```

Related Topics

14.1.5 acl (system view)

14.2.12 auto-port-defend enable

14.2.13 auto-port-defend protocol

14.2.24 cpu-defend policy

14.2.17 blacklist

Function

The **blacklist** command configures a blacklist.

The **undo blacklist** command deletes a blacklist.

By default, no blacklist is configured.

Format

IPv4 blacklist:

blacklist *blacklist-id* **acl** *acl-number1*

undo blacklist *blacklist-id*

IPv6 blacklist:

blacklist *blacklist-id* **acl ipv6** *acl-number2*

undo blacklist *blacklist-id*

NOTE

Only the S6720EI, S6720S-EI, S5720HI, and S5720EI support the IPv6 blacklist.

Blacklist that discards the packets matching ACL rules in the forwarding chip:

blacklist *blacklist-id* **acl** *acl-number3* **hard-drop**

undo blacklist *blacklist-id*

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support the blacklist that discards the packets matching ACL rules in the forwarding chip.

Parameters

Parameter	Description	Value
blacklist-id	Specifies the ID of a blacklist.	The value is an integer that ranges from 1 to 8.
acl *acl-number1*	Specifies the number of an Access Control List (ACL) referenced by a blacklist.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs
acl ipv6 *acl-number2*	Specifies the ACL matching the IPv6 blacklist.	The value of *acl-number2* is an integer that ranges from 3000 to 3999.
acl *acl-number3*	Specifies the ACL matching the IPv4 blacklist.	The value of *acl-number3* is an integer that ranges from 3000 to 3999.
hard-drop	Discards the packets matching the blacklist in the forwarding chip.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

To defend against malicious packet attacks, the device uses ACLs to add users with the specific characteristic into a blacklist and discards the packets from the users in the blacklist. In addition, for S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, packets matching the IPv4 blacklist are sent to the CPU first, and then discarded. To discard the packets directly without sending them to the CPU, you can run the **blacklist** *blacklist-id* **acl** *acl-number3* **hard-drop** command. This function can reduce impact of malicious packets on the CPU usage, and applies to only IPv4 packets.

An attack defense policy can contain a maximum of eight blacklists (including IPv4 and IPv6 blacklists and the blacklist that discards the packets matching ACL rules).

Example

# Specify ACL 2001 as the rule of blacklist 2.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist 2 acl 2001
Info: This configuration may cause packet loss.
```

# Apply ACL 3001 to IPv6 blacklist 3.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist 3 acl ipv6 3001
Info: This configuration may cause packet loss.
```

# Apply ACL 3006 to blacklist 5 to discard the packets matching ACL 3006 in the forwarding chip.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist 5 acl 3006 hard-drop
Info: This configuration may cause packet loss.
```

Related Topics

14.1.5 acl (system view)

14.2.24 cpu-defend policy

14.2.18 car (attack defense policy view)

Function

The **car** command sets the rate limit for packets sent to the CPU.

The **undo car** command restores the default rate limit for packets sent to the CPU.

By default, the CIR value for user-defined flows is 64 kbit/s. You can run the **display cpu-defend configuration** command to check the CAR values for protocol packets.

Format

car { **packet-type** *packet-type* | **user-defined-flow** *flow-id* } **cir** *cir-value* [**cbs** *cbs-value*]

undo car { **packet-type** *packet-type* | **user-defined-flow** *flow-id* }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the type of packets.	The supported packet type depends on the device.
user-defined-flow *flow-id*	Specifies the ID of the user-defined flow. **NOTE** Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support this parameter.	The value is an integer that ranges from 1 to 8.
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer. ● The value of **packet-type** *packet-type* varies according to packet types. The value range can be displayed after you press ? following the command. ● The value of **user-defined-flow** *flow-id* ranges from 8 to 4096, in kbit/s. **NOTE** The minimum value that can take effect for different models may be greater than the configurable minimum value. If the configured value is smaller than the minimum value that can take effect, the minimum value that can take effect will be used. You can run the **display cpu-defend applied command** to view the value that actually takes effect.
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer. ● The value of **packet-type** *packet-type* varies according to packet types. The value range can be displayed after you press ? following the command. ● The value of **user-defined-flow** *flow-id* ranges from 10000 to 800000, in bytes.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch has default CAR values for each type of protocol packet. You can adjust CAR values for specified types of protocol packets based on services and network environment.

After an attack defense policy is created, you can limit the rate of protocol packets using the policy:

- Reduce the CAR values in the following situation: When a network undergoes an attack, reduce the CAR values of the corresponding protocol, to reduce impact on the system CPU.
- Increase the CAR values in the following situation: When service traffic volume on the network increases, a large number of protocol packets need to be sent to the CPU. Increase the CAR values of the corresponding protocols to meet service requirements.

NOTICE

Improper CPCAR settings will affect services on your network. If you need to adjust CPCAR settings, you are advised to contact technical support personnel for help.

Precautions

If you run the **deny** command, and then the **car** command, the **car** command takes effect; if you run the **car** command, and then the **deny** command, the **deny** command takes effect.

NOTE

When the actual and configured rates of packets sent to the CPU are large, the CPU usage may be high and the performance may deteriorate. In the worst situation, the stack breaks.

On an S1720GFR, S2750, S5700LI, or S5700S-LI running a version earlier than V200R007C00, if CPCAR is configured for DHCPv6 reply packets, the following situations occur after the version is upgraded to V200R007C00 or later:

- If only the CPCAR for DHCPv6 reply packets is configured before the upgrade, the switch automatically changes the CPCAR value for DHCPv6 reply packets to be the same as the CPCAR value for DHCP client packets after the version is upgraded to V200R007C00 or later.
- If the CPCAR values for both DHCP client and DHCPv6 reply packets are configured before the upgrade, the switch reserves only the CPCAR for DHCP client packets after the version is upgraded to V200R007C00 or later.

The S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI switches use the CAR values configured for FIB-hit packets to limit the rate of ND packets destined for the MAC address of the local switch.

The S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI limit rates of BPDU, CDP, LNP, and VCMP packets by using the CPCAR configured by the **car packet-type bpdu-tunnel cir** *cir-value* [**cbs** *cbs-value*] command.

Example

# Set the rate limit in the attack defense policy named **test** for ARP Reply packets: set the CIR value to 64 kbit/s and the CBS value to 33000 bytes.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] car packet-type arp-reply cir 64 cbs 33000
Warning: Improper parameter settings may affect stable operating of the system. Use this command under
assistance of Huawei engineer
s. Continue? [Y/N]:y
```

Related Topics

14.2.24 cpu-defend policy

14.2.27 deny

14.2.40 display cpu-defend policy

14.2.37 display cpu-defend configuration

14.2.19 cpu-defend application-apperceive enable

Function

The **cpu-defend application-apperceive enable** command enables active link protection (ALP). After the ALP is enabled, the CAR values of protocol packets set using **linkup-car** can take effect.

The **undo cpu-defend application-apperceive enable** command disables ALP.

By default, ALP is enabled on FTP, HTTPS, IKE, IPSEC-ESP, SSH, TELNET, and TFTP packets and disabled on BGP and OSPF packets.

NOTE

After hardware-based Layer 3 forwarding is enabled for IPv4 packets on an S2750EI, S5700-10P-LI-AC, or S5700-10P-PWR-LI-AC, this command is not supported.

Format

cpu-defend application-apperceive [**bgp** | **ftp** | **https** | **ike** | **ipsec-esp** | **ospf** | **ssh** | **telnet** | **tftp**] **enable**

undo cpu-defend application-apperceive [**bgp** | **ftp** | **https** | **ike** | **ipsec-esp** | **ospf** | **ssh** | **telnet** | **tftp**] **enable**

NOTE

- Only the S5730SI, S5730S-EI, S5720EI, S5720HI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **bgp** parameter.
- Only the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S5720EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **ike** parameter.
- Only the S2720EI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S5720EI, S5720HI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **ipsec-esp** parameter.
- Only the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5730SI, S5730S-EI, S5720EI, S5720HI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **ospf** parameter.

Parameters

Parameter	Description	Value
bgp	Enables ALP on BGP packets.	-
ftp	Enables ALP on FTP packets.	-
https	Enables ALP on HTTPS packets.	-
ike	Enables ALP on IKE packets.	-
ipsec-esp	Enables ALP on IPSEC-ESP packets.	-
ospf	Enables ALP on OSPF packets.	-
ssh	Enables ALP on SSH packets.	-
telnet	Enables ALP on TELNET packets.	-
tftp	Enables ALP on TFTP packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default CAR value of BGP, FTP, HTTPS, OSPF, IKE, IPSEC-ESP, SSH, TFTP, or TELNET protocol is small. When a switch uses these protocols to transfer files or set up connections with other hosts or devices, the number of protocol packets sharply increases in a short period. When the packet rate exceeds the limit, the protocol packets are dropped. The switch may also undergo attacks of other protocols. This affects data transmission and causes service interruption.

You can run the **cpu-defend application-apperceive** command to enable ALP, ensuring normal operation of BGP, FTP, HTTPS, OSPF, IKE, IPSEC-ESP, SSH, TFTP, or TELNET services when attacks occur. When a connection is set up, the switch sends packets at the rate of the CPCAR value configured using the **linkup-car** command. The CPCAR value can be set as required.

Precautions

To enable the ALP function for a certain protocol, run the **cpu-defend application-apperceive enable** command to enable ALP globally. For example, before enabling ALP for the TFTP protocol, run the **cpu-defend application-apperceive enable** command, and then the **cpu-defend application-apperceive tftp enable** command to make the configuration take effect.

Before running the **linkup-car** command, you are advised to run the **display cpu-defend configuration** command to check the CIR value supported by the current protocol or displayed CIR value.

Example

# Enable ALP on BGP packets and set the CIR value to 256 kbit/s.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] linkup-car packet-type bgp cir 256
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend application-apperceive enable
[HUAWEI] cpu-defend application-apperceive bgp enable
```

Related Topics

14.2.37 display cpu-defend configuration

14.2.46 linkup-car

14.2.20 cpu-defend dynamic-car enable

Function

The **cpu-defend dynamic-car enable** command enables a switch to dynamically adjust the default CIR value for protocol packets.

The **undo cpu-defend dynamic-car enable** command disables a switch from dynamically adjusting the default CIR value for protocol packets.

By default, dynamic adjustment of the default CIR value is enabled globally, but the switch is disabled from dynamically adjusting the default CIR value for ARP protocol packets.

NOTE

Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI support this command.

Format

cpu-defend dynamic-car [**arp**] **enable**

undo cpu-defend dynamic-car [**arp**] **enable**

Parameters

Parameter	Description	Value
arp	Enables the switch to dynamically adjust the default CIR value for ARP protocol packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A fixed default CIR value may not adapt to dynamic requirements on rate limiting for protocol packets. The **cpu-defend dynamic-car enable** command enables a switch to dynamically adjust the default CIR value for protocol packets.

If the default CIR value for a protocol has never been changed, the switch dynamically adjusts the default CIR value for the protocol packets based on service scale (for example, number of dynamic ARP entries) and CPU usage to meet various service requirements. For details, see **Table 14-13**.

Table 14-13 Default CPCAR adjustment for ARP packets

Number of ARP Entries	Adjusted Default CPCAR
Fewer than or equal to 512	Unchanged
More than 512 and fewer than or equal to 1024	128 kbit/s (remain unchanged if the default CIR is larger than 128 kbit/s)
More than 1024 and fewer than or equal to 3072	256 kbit/s
More than 3072 and fewer than or equal to 4096	512 kbit/s
More than 4096512	512 kbit/s

NOTE

When the number of entries increases, the CIR value is automatically increased. If the CPU is overloaded, the CIR value is decreased.

Precautions

The switch dynamically adjusts the default CIR value for ARP protocol packets only when the function is enabled globally and on ARP protocol packets.

The default CIR value dynamically adjusted only takes effect when the CIR value of the protocol packet is not manually changed.

After the default CPCAR setting is modified for ARP, only the CIR value for ARP reply and ARP request packets is adjusted.

Example

# Enable the switch to dynamically adjust the default CIR value for ARP protocol packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend dynamic-car enable
[HUAWEI] cpu-defend dynamic-car arp enable
```

14.2.21 cpu-defend host-car

Function

The **cpu-defend host-car** command specifies the packet type to which the user-level rate limiting is applied.

By default, the user-level rate limiting can apply to ARP Request, ARP Reply, ND, DHCP Request, DHCPv6 Request, and 8021x packets, but does not apply to IGMP packets.

NOTE

Only the S5720HI supports this command.

Format

cpu-defend host-car { { **arp** | **dhcp-request** | **dhcpv6-request** | **igmp** | **nd** | **8021x** | **https-syn** } * | **all** }

Parameters

Parameter	Description	Value
arp	Applies user-level rate limiting to ARP packets.	-
dhcp-request	Applies user-level rate limiting to DHCP Request packets.	-

Parameter	Description	Value
dhcpv6-request	Applies user-level rate limiting to DHCPv6 Request packets.	-
igmp	Applies user-level rate limiting to IGMP packets.	-
nd	Applies user-level rate limiting to ND packets.	-
8021x	Applies user-level rate limiting to 8021x packets.	-
https-syn	Applies user-level rate limiting to HTTPS-SYN packets.	-
all	Applies user-level rate limiting to ARP, DHCP Request, DHCPv6 Request, IGMP, ND, 8021x, and HTTPS-SYN packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch limits the rates of the ARP, ND, DHCP Request, DHCPv6 Request, and 8021x packets received from user MAC addresses, and discards excessive packets when the packet rates exceed the rate limit. If you need to limit the rate of only IGMP and HTTPS-SYN packets or packets of the specified types, specify the packet type.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- If the command is run multiple times, the user-level rate limiting applies to the packet type specified in the last command. For example, if the command specifying ARP and DHCP Request packets is run, and then the **cpu-defend host-car arp** command is run, the user-level rate limiting applies to only ARP packets.
- After the **cpu-defend host-car all** command is run, the configuration file displays **cpu-defend host-car 8021x arp dhcp-request dhcpv6-request igmp nd**.

Example

# Apply user-level rate limiting to ARP, DHCP Request, DHCPv6 Request, IGMP, and ND packets.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend host-car arp dhcp-request dhcpv6-request igmp nd
```

14.2.22 cpu-defend host-car enable

Function

The **cpu-defend host-car enable** command enables the user-level rate limiting.

The **undo cpu-defend host-car enable** command disables the user-level rate limiting.

By default, the user-level rate limiting is enabled.

NOTE

Only the S5720HI supports this command.

Format

cpu-defend host-car enable

undo cpu-defend host-car enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User-side hosts are prone to virus attacks. Infected hosts may send a large number of protocol packets to network devices, causing a high CPU usage and degraded performance on the devices and affecting services. You can configure the user-level rate limiting to resolve this problem. User-level rate limiting identifies users by user MAC addresses and limits the rates of specified packets (ARP, ND, DHCP Request, DHCPv6 Request, IGMP, 802.1X, and HTTPS-SYN packets) for both wired and wireless users. By default, the threshold for each user MAC address is 10 pps.

The user-level rate limiting is more precise than CPCAR (based on device) and port attack defense (based on interface) because it is user-specific and has little impact on online users.

Precautions

- It is recommended that you disable user-level rate limiting on the network-side interfaces of an access switch and a gateway switch. The user-level rate limiting is enabled on interfaces by default.
- In the user-level rate limiting, the system performs a hash calculation for the source MAC addresses of specified packets, and places the packets into

different buckets. Therefore, multiple users may share the rate limit. When traffic volume is heavy, packets may be dropped. If you confirm that these users are authorized, run the **cpu-defend host-car mac-address** *mac-address* command to increase the rate threshold for the specified MAC addresses.

Example

# Disable the user-level rate limiting.

```
<HUAWEI> system-view
[HUAWEI] undo cpu-defend host-car enable
```

14.2.23 cpu-defend host-car pps

Function

The **cpu-defend host-car pps** command sets the rate limit for the user-level rate limiting.

The **undo cpu-defend host-car pps** command restores the default rate limit for the user-level rate limiting.

By default, the rate limit for the user-level rate limiting is 10 pps.

NOTE

Only the S5720HI supports this command.

Format

cpu-defend host-car [**mac-address** *mac-address* | **car-id** *car-id*] **pps** *pps-value*

undo cpu-defend host-car { **mac-address** *mac-address* | **car-id** *car-id* }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Sets the rate limit for the specified MAC address.	The value is in the H-H-H format. H is a hexadecimal number of 1 to 4 digits.
car-id *car-id*	Sets the rate limit for the specified bucket.	The value is an integer that ranges from 0 to 8191.
pps *pps-value*	Indicates the rate limit.	The value is an integer that ranges from 1 to 128.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

User-level rate limiting identifies users by user MAC addresses and limits the rates of specified packets (ARP, ND, DHCP Request, DHCPv6 Request, IGMP, 802.1X, and HTTPS-SYN packets) for both wired and wireless users. By default, the user-level rate limit is 10 pps. You can set a rate limit based on user.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- If the rate limit is too high, attacks cannot be prevented and CPU may be overloaded.
- If both the **cpu-defend host-car mac-address** *mac-address* **pps** *pps-value* and **cpu-defend host-car pps** *pps-value* commands are run, the rate limit for the specified MAC address is determined by the former command, and the rate limit for other MAC addresses is determined by the latter command.
- The user-level rate limiting performs a hash calculation for the source MAC addresses of specified packets, and places the packets into different buckets. When two user MAC addresses are mapped to the same bucket index, the two users share the same rate limit (in pps mode). If the two users modify the rate limit for the bucket simultaneously, the setting will be overwritten. To avoid this situation, the rate limit for the specified MAC address cannot be set upon hash conflict.
- When the **cpu-defend host-car mac-address** *mac-address* **pps** *pps-value* and **cpu-defend host-car pps** *pps-value* commands are run to configure the rate limit for multiple MAC addresses, the settings are displayed in the alphabetic order in the configuration file.

Example

# Set the rate limit for MAC address 000a-000b-000c to 20 pps.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend host-car mac-address 000a-000b-000c pps 20
```

14.2.24 cpu-defend policy

Function

The **cpu-defend policy** command creates an attack defense policy and displays the attack defense policy view.

The **undo cpu-defend policy** command deletes an attack defense policy.

By default, the **default** attack defense policy exists on the device and is applied to the device. The **default** attack defense policy cannot be deleted or modified.

Format

cpu-defend policy *policy-name*

undo cpu-defend policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy.	The value is a string of 1 to 31 case-insensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of packets including malicious attack packets are sent to the CPU on a network. If excess packets are sent to the CPU, the CPU usage becomes high and CPU performance deteriorates. The attack packets affect services and may even cause system breakdown. To solve the problem, create an attack defense policy and configure CPU attack defense and attack source tracing in the attack defense policy.

Precautions

The device supports a maximum of 13 attack defense policies, including the **default** attack defense policy. The **default** attack defense policy is generated in the system by default and is applied to the device. The **default** attack defense policy cannot be deleted or modified. The other 12 policies can be created, modified, and deleted.

The configuration in a user-defined attack defense policy overrides the configuration in the **default** attack defense policy. If no parameter is set in the user-defined attack defense policy, the configuration in the **default** attack defense policy is used.

When the **default** attack defense policy is used, protocol packets sent to the CPU are limited based on the default CIR value.

Example

# Create an attack defense policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test]
```

Related Topics

14.2.40 display cpu-defend policy

14.2.25 cpu-defend-policy

Function

The **cpu-defend-policy** command applies an attack defense policy.

The **undo cpu-defend-policy** command cancels the application of an attack defense policy.

By default, the **default** attack defense policy is applied to the switch.

Format

The stack-incapable models support the following commands:

cpu-defend-policy *policy-name* **global**

undo cpu-defend-policy { *policy-name* **global** | **global** }

Other models support the following format:

cpu-defend-policy *policy-name* [**global**]

undo cpu-defend-policy [*policy-name*] [**global**]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy. ● If the **global** keyword is specified, the attack defense policy is applied to the switching chip. ● If the **global** keyword is not specified, the attack defense policy is applied to the CPU. Only the attack defense policies that limit the rates of packets sent to the CPU can be applied to the CPU. Other types of attack defense policies are not applicable to the CPU, so configuring such policies cannot protect the CPU.	The attack defense policy must already exist.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, you must apply the policy in the system view. Otherwise, the attack defense policy does not take effect.

Prerequisites

An attack defense policy has been created by using the **14.2.24 cpu-defend policy** command.

Example

# Apply the attack defense policy named **test** to all devices.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend-policy test global
```

Related Topics

14.2.24 cpu-defend policy

14.2.26 cpu-defend trap drop-packet

Function

The **cpu-defend trap drop-packet** command enables alarm reporting for packet loss caused by CPCAR exceeding.

The **undo cpu-defend trap drop-packet** command restores the default configuration.

By default, the system does not report alarms for packet loss caused by CPCAR exceeding.

NOTE

Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support this command.

Format

cpu-defend trap drop-packet

undo cpu-defend trap drop-packet

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the CPU, a switch limits the rate of protocol packets sent to the CPU based on the CPCAR. If the rate of protocol packets exceeds the CPCAR, excess protocol packets are dropped. As a result, the corresponding service may not run normally. To quickly detect packet loss caused by CPCAR exceeding, you can use this command to enable alarm reporting for this event. After this function is enabled, the switch checks for packet loss caused by CPCAR at 10-minute intervals. If the switch finds that the number of dropped packets of a protocol increases, the switch reports a packet loss alarm.

Precautions

After this alarm reporting function is enabled, the switch reports packet loss alarms based on protocol types. That is, if the rates of packets of multiple protocols exceed the CPCAR values set for these protocols, the switch reports an alarm for each protocol.

Example

# Enable alarm reporting for packet loss caused by CPCAR exceeding.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend trap drop-packet
```

14.2.27 deny

Function

The **deny** command configures the device to discard packets sent to the CPU.

The **undo deny** command restores the default action taken for the packets sent to the CPU.

By default, the device does not discard packets sent to the CPU. Instead, the device limits the rate of packets sent to the CPU and user-defined flows using the default rate. You can check the CAR values of each type of packets using the **display cpu-defend configuration** command.

Format

deny { **packet-type** *packet-type* | **user-defined-flow** *flow-id* }

undo deny { **packet-type** *packet-type* | **user-defined-flow** *flow-id* }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the type of the packet to be discarded.	The supported packet type depends on the device.

Parameter	Description	Value
user-defined-flow *flow-id*	Specifies the ID of the user-defined flow to be discarded. **NOTE** Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support this parameter.	The value is an integer that ranges from 1 to 8.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, if the device receives attack packets of a specified type or a large number of packets sent to the CPU, run the **deny** command to configure the device to discard packets of the specified type sent to the CPU.

Precautions

If you run the **deny** command, and then the **car** command, the **car** command takes effect; if you run the **car** command, and then the **deny** command, the **deny** command takes effect. After the **undo deny** command is executed, the default action for packets sent to the CPU is restored, that is, CIR and CBS actions are performed.

To configure the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, or S6720S-SI, switch to discard BPDU, CDP, LNP, and VCMP packets, run the **deny packet-type bpdu-tunnel** command.

Example

# Configure the drop action taken for ARP Reply packets to be sent to the CPU in the attack defense policy **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] deny packet-type arp-reply
```

Related Topics

14.2.24 cpu-defend policy

14.2.18 car (attack defense policy view)

14.2.40 display cpu-defend policy

14.2.28 description (attack defense policy view)

Function

The **description** command configures the description of an attack defense policy.

The **undo description** command deletes the description of an attack defense policy.

By default, no description is configured for an attack defense policy.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the content of a description.	It is a string of 1 to 63 case-sensitive characters with spaces.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an attack defense policy, for example, the usage or application scenario of the attack defense policy. The description is used to differentiate attack defense policies.

Precautions

If you run the **description** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

Example

# Configure the description **defend_arp_attack** for the attack defense policy named **test**.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] description defend_arp_attack
```

Related Topics

14.2.24 cpu-defend policy

14.2.29 display auto-defend attack-source

Function

The **display auto-defend attack-source** command displays the attack sources.

Format

display auto-defend attack-source [**history** [**begin** *begin-date begin-time*] [**slot** *slot-id*] | [**slot** *slot-id*] [**detail**]]

Parameters

Parameter	Description	Value
history	Displays the history attack source information. If **history** is not specified, all existing attack source information is displayed.	-
begin *begin-date begin-time*	Specifies the start time.	*begin-date* is in the format YYYY/MM/DD. *begin-time* is in the format HH:MM:SS. The value of YYYY/MM/DD ranges from 2000/1/1 to 2099/12/31. The value of HH:MM:SS ranges from 00:00:00 to 23:59:59.
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.

Parameter	Description	Value
detail	Displays detailed information about the attack sources, including the type of attack packets. If **detail** is not specified, brief information about the attack sources is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display auto-defend attack-source** command displays the attack sources.

In a stack, the attack source list can be saved on each member switch. The **display auto-defend attack-source slot** *slot-id* command displays the attack source list on the specified member switch.

Example

# Display the attack source list.

```
<HUAWEI> display auto-defend attack-source
 Attack Source User Table (slot 0):
 ---------------------------------------------------------------------------
 MacAddress       InterfaceName             Vlan:Outer/Inner    TotalPackets
 ---------------------------------------------------------------------------
 0000-c103-0102   GigabitEthernet0/0/1        100               1395
 ---------------------------------------------------------------------------
 Total: 1

 Attack Source Port Table (slot 0):
 ----------------------------------------------------------
 InterfaceName             Vlan:Outer/Inner    TotalPackets
 ----------------------------------------------------------
 GigabitEthernet0/0/1        100               605
 ----------------------------------------------------------
 Total: 1

 Attack Source IP Table (slot 0):
 --------------------------------------------------------------------
 IPAddress                                 TotalPackets
 --------------------------------------------------------------------
 2:2:2:2:2:2:2:2                            1395
 --------------------------------------------------------------------
 Total: 1
```

# Display detailed information about the attack source list.

```
<HUAWEI> display auto-defend attack-source detail
 Attack Source User Table (slot 0):
 ---------------------------------------------------
 MAC Address                  0000-c103-0102
 Interface                  GigabitEthernet0/0/1
 VLAN: Outer/Inner              100
   ARP:                    1580
 Total                     1580
 ---------------------------------------------------
 Total: 1

 Attack Source Port Table (slot 0):
 ---------------------------------------------------
 Interface                  GigabitEthernet0/0/1
 VLAN: Outer/Inner              100
   ARP:                    790
 Total                     790
 ---------------------------------------------------
 Total: 1

 Attack Source IP Table (slot 0):
 --------------------------------------------------------------------------
 IP address                 2:2:2:2:2:2:2:2
   ARP:                    1580
 Total                     1580
  --------------------------------------------------------------------------
 Total: 1
```

Table 14-14 Description of the **display auto-defend attack-source** command output

Item	Description
Attack Source User Table (slot 0)	Source tracing information of device, which is distinguished according to the attack user.
Attack Source Port Table (slot 0)	Source tracing information of device, which is distinguished according to the attacked interface. **NOTE** The device does not support attack source tracing based on source interfaces and VLANs for Layer 3 Ethernet interfaces. Therefore, this field does not contain the attack source tracing information of Layer 3 Ethernet interfaces.
Attack Source IP Table (slot 0)	Source tracing information of device, which is distinguished according to the attacked interface.
IPAddress	User IP address.
MacAddress	MAC address of the user.
InterfaceName	Name of the interface that initiates the attack.
Interface	Name of the interface that initiates the attack.
Vlan:Outer/Inner	ID of the VLAN that an interface belongs to. **Outer** indicates the outer VLAN ID and **Inner** indicates the inner VLAN ID. **NOTE** This field displays - for the attack source tracing entries of Layer 3 Ethernet interfaces.

Item	Description
TotalPackets	Total number of packets received by the device.

# Display history attack source information.

```
<HUAWEI> display auto-defend attack-source history

 S : start time
 E : end time

 Attack History User Table (slot 0):
 ---------------------------------------------------------------------------
 AttackTime          MacAddress     IFName       Vlan:O/I  Protocol   PPS
 ---------------------------------------------------------------------------
 S:2016-09-08 07:36:15 0000-c103-0102 GE0/0/1       100      ARP         40
 E:-
 ---------------------------------------------------------------------------
 Total: 1

 Attack History Port Table (slot 0):
 ------------------------------------------------------------
 AttackTime          IFName       Vlan:O/I  Protocol   PPS
 ------------------------------------------------------------
 S:2016-09-08 07:36:37 GE0/0/1       100      ARP         40
 E:-
 ------------------------------------------------------------
 Total: 1

 Attack History IP Table (slot 0):
 -------------------------------------------------------------------------
 AttackTime          IPAddress                          Protocol
 PPS
 -------------------------------------------------------------------------
 S:2016-09-08 07:36:15 2:2:2:2:2:2:2:2                      ARP
 E:-
 40
 -------------------------------------------------------------------------
 Total: 1
```

Table 14-15 Description of the display auto-defend attack-source history command output

Item	Description
Attack History User Table (slot 0)	Information about attack sources on the device, which is distinguished according to attackers.
Attack History Port Table (slot 0)	Information about attack sources on the device, which is distinguished according to attacked interfaces.
Attack History IP Table (slot 0)	Information about attack sources on the device, which is distinguished according to attacked source IP addresses.
AttackTime	Attack time. ● S indicates start time. ● E indicates end time. If the attack is not ended when you display history attack source information, this field displays -.

Item	Description
MacAddress	User MAC address.
IPAddress	User IP address.
IFName	Name of the interface that initiates the attack.
Vlan:O/I	ID of the VLAN that an interface belongs to. The value O indicates the outer VLAN ID and the value I indicates the inner VLAN ID.
Protocol	Attack type.
PPS	Highest rate of attack packets.

Related Topics

14.2.24 cpu-defend policy

14.2.3 auto-defend enable

14.2.30 display auto-defend configuration

Function

The **display auto-defend configuration** command displays the attack source tracing configuration.

Format

display auto-defend configuration [**cpu-defend policy** *policy-name*]

Parameters

Parameter	Description	Value
cpu-defend policy *policy-name*	Displays the attack source tracing configuration of a specified attack defense policy. ● If this parameter is specified, the configuration of the specified attack defense policy is displayed. ● If this parameter is not specified, the configurations of all attack defense policies are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After attack source tracing is configured in an attack defense policy, you can run the **display auto-defend configuration** command to view the attack source tracing configuration.

Example

# Display the attack source tracing configuration.

```
<HUAWEI> display auto-defend configuration
 ----------------------------------------------------------------------------
 Name  : test
 Related slot : <0>
 auto-defend                      : enable
 auto-defend attack-packet sample : 5
 auto-defend threshold            : 60 (pps)
 auto-defend alarm                : enable
 auto-defend trace-type           : source-mac source-ip
 auto-defend protocol             : arp icmp dhcp igmp ttl-expired tcp telnet
 auto-defend action               : deny (Expired time : 300 s)
 auto-defend whitelist 1          : acl number 2002
 ----------------------------------------------------------------------------
```

Table 14-16 Description of the **display auto-defend configuration** command output

Item	Description
Name	Name of an attack defense policy.
Related slot	ID of the stack to which the attack defense policy is applied.
auto-defend	Whether attack source tracing is enabled. To enable attack source tracing, run the **14.2.3 auto-defend enable** command.
auto-defend attack-packet sample	Packet sampling ratio for attack source tracing. To set the packet sampling ratio for attack source tracing, run the **14.2.2 auto-defend attack-packet sample** command.
auto-defend threshold	Checking threshold for attack source tracing. To set the checking threshold for attack source tracing, run the **14.2.7 auto-defend threshold** command.
auto-defend alarm	Whether the alarm function for attack source tracing is enabled. To enable the alarm function for attack source tracing, run the **14.2.5 auto-defend alarm enable** command.
auto-defend trace-type	Attack source tracing mode: ● source-mac: indicates attack source tracing based on source MAC addresses. ● source-ip: indicates attack source tracing based on source IP addresses. ● source-portvlan: indicates attack source tracing based on source ports+VLANs. To configure the attack source tracing mode, run the **14.2.8 auto-defend trace-type** command.
auto-defend protocol	Type of traced packets. To specify the types of protocol packets that the device monitors in attack source tracing, run the **14.2.6 auto-defend protocol** command.
auto-defend action	Action taken on the attack source. The value can be: ● deny (Expired time: 300s): indicates that the device discards all attack packets in 300s. ● error-down: indicates that the inbound interfaces of attack packets are shut down. To configure the **punish** action, run the **14.2.4 auto-defend action** command.
auto-defend whitelist 1	Whitelist for attack source tracing. For related commands, see **14.2.9 auto-defend whitelist**.

Related Topics

14.2.24 cpu-defend policy

14.2.4 auto-defend action

14.2.5 auto-defend alarm enable

14.2.2 auto-defend attack-packet sample

14.2.3 auto-defend enable

14.2.6 auto-defend protocol

14.2.8 auto-defend trace-type

14.2.7 auto-defend threshold

14.2.31 display auto-defend whitelist

Function

The **display auto-defend whitelist** command displays information about the attack source tracing whitelist.

Format

display auto-defend whitelist [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- On a standalone switch without the stacking function configured, this parameter specifies a slot ID. - In a stack system, this parameter specifies a stack ID.	Set the value according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the whitelist for attack source tracing is configured or when you locate faults on network, run the **display auto-defend whitelist** command to verify whitelist information. If no whitelist is configured, the command displays no whitelist information.

Example

# Display information about the attack source tracing whitelist on the switch.

```
<HUAWEI> display auto-defend whitelist
 Protocol      Interface              IP                ACL      Status
-----------------------------------------------------------------------------
   DHCP          GE0/0/1               --                --       auto
   DHCP          GE0/0/2               --                --       auto
```

Table 14-17 Description of the **display auto-defend whitelist** command output

Item	Description
Protocol	Protocol type of the packets excluded from attack source tracing.
Interface	Interface on which inbound packets are excluded from attack source tracing.
IP	Source IP address of the packets excluded from attack source tracing. If not source IP address is specified in the whitelist rule, this field displays --.
ACL	ACL number specified in a manually configured whitelist rule. If the whitelist rule is automatically delivered, this field displays --.
Status	Type of the whitelist rule, which can be: ● **auto**: An automatically delivered whitelist rule is triggered by services. ● **manual**: You can run the **auto-defend whitelist** *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* } command in the attack defense policy view to manually configure an attack source tracing whitelist.

14.2.32 display auto-port-defend attack-source

Function

The **display auto-port-defend attack-source** command displays source tracing information on interfaces.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

display auto-port-defend attack-source [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- The value indicates the slot ID if stacking is not configured. - The value indicates the stack ID when stack is configured. If **slot** *slot-id* is not specified, the source tracing information on the interfaces of the master device (stack configured) or local device (stack not configured) is displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The source tracing information helps you locate attack sources.

Example

# Display the source tracing information on the interfaces of the device.

```
<HUAWEI> display auto-port-defend attack-source
Attack source table on slot 0:
Total : 1
-------------------------------------------------------------------------------
Interface   Vlan Protocol     Expire(s)  PacketRate(pps)  LastAttackTime
-------------------------------------------------------------------------------
GE0/0/1     NA   arp-request  297        12               2013-07-06 17:36:54
-------------------------------------------------------------------------------
```

Table 14-18 Description of the display auto-defend attack-source command output

Item	Description
Attack source table on slot 0	Source tracing information on the interfaces of device.
Total	Number of source tracing records.
Interface	Name of the attacked interface.
Vlan	VLAN ID in attack packets. If the device does not support checking on VLAN IDs in attack packets, this field displays NA.
Protocol	Attack packet type.
Expire(s)	Remaining time of the aging time for port attack defense. **NOTE** If the **Expire(s)** field of an entry displays 0, this entry will be deleted after a certain period (a maximum of 10 seconds).
PacketRate(pps)	Rate of the last received attack packet.
LastAttackTime	Time when the last attack packet is received.

Related Topics

14.2.24 cpu-defend policy

14.2.12 auto-port-defend enable

14.2.33 display auto-port-defend configuration

Function

The **display auto-port-defend configuration** command displays the configuration of port attack defense.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

display auto-port-defend configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the configuration of port attack defense, use this command.

Example

# Display the configuration of port attack defense on the local device.

```
<HUAWEI> display auto-port-defend configuration
-------------------------------------------------------------------------------
 Name  : test
 Related slot : 0
 Auto-port-defend                          : enable
 Auto-port-defend sample                   : 5
 Auto-port-defend aging-time               : 300 second(s)
 Auto-port-defend arp-request threshold : 50 pps(enable)
 Auto-port-defend arp-reply threshold   : 50 pps(enable)
 Auto-port-defend dhcp threshold        : 50 pps(enable)
 Auto-port-defend icmp threshold        : 50 pps(enable)
 Auto-port-defend igmp threshold        : 50 pps(enable)
 Auto-port-defend ip-fragment threshold : 50 pps(enable)
 Auto-port-defend alarm                    : disable
-------------------------------------------------------------------------------
```

Table 14-19 Description of the display auto-port-defend configuration command output

Item	Description
Name	Name of an attack defense policy.
Related slot	ID of the stack to which the attack defense policy is applied.In a non-stack environment, this field indicates that the attack defense policy is applied to the local device.
Auto-port-defend	Whether port attack defense is enabled. To enable the port attack defense function, run the **14.2.12 auto-port-defend enable** command.
Auto-port-defend sample	Sampling ratio for protocol packets. To set this parameter, run the **14.2.15 auto-port-defend sample** command.
Auto-port-defend aging-time	Aging time for port attack defense. To set this parameter, run the **14.2.10 auto-port-defend aging-time** command.

Item	Description
Auto-port-defend arp-request threshold	Whether port attack defense is applied to ARP Request packets and rate threshold. To set this parameter, run the **14.2.13 auto-port-defend protocol arp-request** and **auto-port-defend protocol arp-request threshold** *threshold* commands.
Auto-port-defend arp-reply threshold	Whether port attack defense is applied to ARP Reply packets and rate threshold. To set this parameter, run the **14.2.13 auto-port-defend protocol arp-reply** and **auto-port-defend protocol arp-reply threshold** *threshold* commands.
Auto-port-defend dhcp threshold	Whether port attack defense is applied to DHCP packets and rate threshold. To set this parameter, run the **14.2.13 auto-port-defend protocol dhcp** and **auto-port-defend protocol dhcp threshold** *threshold* commands.
Auto-port-defend icmp threshold	Whether port attack defense is applied to ICMP packets and rate threshold. To set this parameter, run the **14.2.13 auto-port-defend protocol icmp** and **auto-port-defend protocol icmp threshold** *threshold* commands.
Auto-port-defend igmp threshold	Whether port attack defense is applied to IGMP packets and rate threshold. To set this parameter, run the **14.2.13 auto-port-defend protocol igmp** and **auto-port-defend protocol igmp threshold** *threshold* commands.
Auto-port-defend ip-fragment threshold	Whether port attack defense is applied to IP fragments and rate threshold. To set this parameter, run the **14.2.13 auto-port-defend protocol ip-fragment** and **auto-port-defend protocol ip-fragment threshold** *threshold* commands.
Auto-port-defend alarm	Whether the report of port attack defense events is enabled. To set this parameter, run the **14.2.11 auto-port-defend alarm enable** command.

Related Topics

14.2.10 auto-port-defend aging-time

14.2.12 auto-port-defend enable

14.2.13 auto-port-defend protocol

14.2.14 auto-port-defend protocol threshold

14.2.15 auto-port-defend sample

14.2.24 cpu-defend policy

14.2.34 display auto-port-defend statistics

Function

The **display auto-port-defend statistics** command displays packet statistics on port attack defense.

NOTE

Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.

Format

display auto-port-defend statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- The value indicates the slot ID if stacking is not configured. - The value indicates the stack ID when stack is configured. If **slot** *slot-id* is not specified, packet statistics on the master device (stack configured) or local device (stack not configured) are displayed.	The value depends on the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view statistics on the packets discarded and accepted in the port attack defense service, use this command. The statistics help you understand protocol packet processing status and promptly adjust the attack defense policy.

Example

# Display packet statistics on the interfaces of the device.

```
<HUAWEI> display auto-port-defend statistics
Statistics on MPU:
-------------------------------------------------------------------------------
Protocol     Vlan Queue Cir(Kbps)  Pass(Packet/Byte)  Drop(Packet/
Byte)
-------------------------------------------------------------------------------
icmp        NA   2     256        23095             3
                          NA                NA
-------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 14-20 Description of the display auto-port-defend statistics command output

Item	Description
Statistics on MPU	Packet statistics on the interfaces of the device.
Protocol	Attack packet type.
Vlan	VLAN ID in attack packets. If the device does not support checking on VLAN IDs in attack packets, this field displays NA.
Queue	Queue from which attack packets are sent.
Cir(Kbps)	Protocol rate limit (CPCAR in attack defense policies). To configure a CIR value, run the **car** **packet-type** *packet-type* **cir** *cir-value* command in the attack defense policy view.
Pass(Packet/Byte)	Number and bytes of attack packets that pass through the device. The value 23095 indicates the number of accepted packets. Value **NA** indicates that the device does not support byte statistics collection.
Drop(Packet/Byte)	Number and bytes of attack packets discarded by the device. The value 3 indicates the number of discarded packets. Value **NA** indicates that the device does not support byte statistics collection.

Related Topics

14.2.51 reset auto-port-defend statistics

14.2.35 display auto-port-defend whitelist

Function

The **display auto-port-defend whitelist** command displays information about the interface attack defense whitelist.

NOTE

The S1720GFR, S2750EI, S5700LI, and S5700S-LI do not support this command.

Format

display auto-port-defend whitelist [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	- Specifies a slot ID if stacking is not configured. - Specifies a stack ID in a stack.	Set the value according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the whitelist for port attack defense is configured or when you locate faults on network, run the **display auto-port-defend whitelist** command to verify whitelist information. If no whitelist is configured, the command displays no whitelist information.

Example

# Display information about the interface attack defense whitelist.

```
<HUAWEI> display auto-port-defend whitelist
 Protocol      Interface              IP               ACL      Status
-------------------------------------------------------------------------------
   --          Eth-Trunk0             --               --       auto
   --          GE0/0/1              --                --       manual
   --            --               --            2000      manual
```

Table 14-21 Description of the **display auto-port-defend whitelist** command output

Item	Description
Protocol	Protocol type of packets free from the interface attack defense action. If no packet protocol type is specified in the whitelist rule, this field displays --.
Interface	Interface free from the attack defense action. If the whitelist is configured based on ACL rules, this field displays --.
IP	Source IP address of packets free from the interface attack defense action. If the whitelist is configured based on interfaces or automatically delivered, this field displays --.
ACL	ACL number specified in a manually configured whitelist rule.
Status	Type of the whitelist rule, which can be: ● **auto**: An automatically delivered whitelist rule is triggered by services. ● **manual**: You can run the **auto-port-defend whitelist** *whitelist-number* { **acl** *acl-number* | **interface** *interface-type interface-number* } command in the attack defense policy view to configure a whitelist for port attack defense.

14.2.36 display cpu-defend applied

Function

The **display cpu-defend applied** command displays the actual CAR values for the protocol packets delivered to the chip.

Format

display cpu-defend applied [**packet-type** *packet-type*] { **mcu** | **slot** *slot-id* | **all** }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device.
mcu	Indicates the main control board. **NOTE** Only the stack-capable models support the **mcu** parameter.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if a stack is configured.	The value must be set according to the device configuration.
all	Indicates all switches in a stack if stacking is enabled, or the switch itself if stacking is disabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The actual CAR values may be different from the configured CAR values. The possible causes are as follows:

- The CIR value specified in the **car** **packet-type** *packet-type* **cir** *cir-value* [**cbs** *cbs-value*] command is a consecutive range. However, the actual CIR value is discrete, depending on chip granularity. For example, if the CIR value range is set to 65 to 128 with the granularity 64 kbit/s, the actual CIR value may be 64 or 128, which depends on product models.
- The configured CIR value exceeds the chip capacity and the upper threshold. For example, the CIR value is set to 10000, but the chip does not support CIR value 1000. Then the actual CIR value cannot reach 10000.

You can run the **display cpu-defend applied** command to view the actual CAR values for protocol packets.

NOTE

When too much output information is to be displayed, specify the **begin**, **exclude**, or **include** parameter to display only the required information.

Example

# Display the actual CAR values for ARP Request messages sent from the switch.

```
<HUAWEI> display cpu-defend applied packet-type arp-request slot 0
Applied Car on slot 0:
----------------------------------------------------------------------------
Packet Type        Cir(Kbps)    Cbs(Byte) Applied Cir(Kbps) Applied Cbs(Byte)
----------------------------------------------------------------------------
arp-request              65        10000              128            10000
----------------------------------------------------------------------------
```

Table 14-22 Description of the **display cpu-defend applied** command output

Item	Description
Applied Car on slot 0	CAR value for protocol packets sent by a specified stack.
Packet Type	Packet type.
Cir(Kbps)	Configured committed information rate (CIR), in kbit/s. To set the CIR value, run the **14.2.18 car (attack defense policy view)** and **14.2.46 linkup-car** commands.
Cbs(Byte)	Configured committed burst size (CBS) value, in bytes. To set the CBS value, run the **14.2.18 car (attack defense policy view)** and **14.2.46 linkup-car** commands.
Applied Cir(Kbps)	Actual CIR value on the chip, in kbit/s.
Applied Cbs(Byte)	Actual CBS value on the chip, in bytes.

Related Topics

14.2.18 car (attack defense policy view)

14.2.46 linkup-car

14.2.37 display cpu-defend configuration

Function

The **display cpu-defend configuration** command displays CAR configurations.

Format

The stack-incapable models support the following commands:

display cpu-defend configuration [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]

Other models support the following format:

display cpu-defend configuration [**packet-type** *packet-type*] { **all** | **slot** *slot-id* | **mcu** }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device.
all	Indicates all devices.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.
mcu	Indicates the main control board.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cpu-defend configuration** command to view the rate limit of protocol packets sent to the CPU. By default, the rate limit of protocol packets in the **default** policy is displayed.

In a stack, you can run the **cpu-defend-policy global** command to bind all switches to the same attack defense policy. Then you can run the **display cpu-defend configuration all** command to view the same CAR configuration of all switches in the stack.

Example

# Display the CAR configurations.

```
<HUAWEI> display cpu-defend configuration all
Car configurations on mainboard.
----------------------------------------------------------------------
Packet Name         Status     Cir(Kbps)   Cbs(Byte)
----------------------------------------------------------------------
arp-miss            Enabled         64       12032
arp-reply           Enabled        256       48128
arp-request          Enabled        256       48128
bgp                Enabled        384       72192
bgp4plus             Enabled        256       48128
dhcpv6-reply         Enabled        256       48128
dhcpv6-request       Enabled        256       48128
dns                Enabled         64       12032
fib-hit            Enabled         64       12032
fib-miss            Enabled         64       12032
ftp               Enabled        512       96256
hop-limit           Enabled         64       12032
http               Enabled        512       96256
https              Enabled        512       96256
hw-tacacs           Enabled        128       24064
icmp               Enabled        128       24064
icmpv6              Enabled         64       12032
igmp               Enabled        256       48128
isis              Enabled        256       48128
mdns-relay          Enabled        256       48128
mld                Enabled        256       48128
mpls-fib-hit         Enabled        256       48128
mpls-ldp            Enabled        512       96256
mpls-one-label       Enabled        128       24064
mpls-ping           Enabled        128       24064
mpls-rsvp           Enabled        128       24064
mpls-ttl-expired     Enabled        128       24064
mpls-vccv-ping       Enabled        128       24064
nac-arp-reply        Enabled        128       24064
nac-arp-request      Enabled        128       24064
nac-nd              Enabled         64       12032
nd                 Enabled        128       24064
ntp                Enabled        128       24064
ospf               Enabled        384       72192
ospfv3              Enabled        384       72192
pim                Enabled        256       48128
pimv6               Enabled        128       24064
portal             Enabled        128       24064
radius             Enabled        128       24064
rip               Enabled        256       48128
ripng              Enabled        256       48128
snmp                Enabled        128       24064
ssh                Enabled        128       24064
tcp                Enabled         64       12032
telnet             Enabled        128       24064
ttl-expired         Enabled         64       12032
vrrp               Enabled        128       24064
vrrp6              Enabled        128       24064
----------------------------------------------------------------------

Linkup Information:
--------------------------------------------------------------------------------
Packet Name : ftp
Cir(Kbps)/Cbs(Byte) : 4096/770048
SIP(SMAC) : 10.1.2.1
DIP(DMAC) : 10.1.3.1
Port(S/C) : 42372/22
--------------------------------------------------------------------------------
Car configurations on slot 0.
----------------------------------------------------------------------
Packet Name         Status     Cir(Kbps)   Cbs(Byte)  Queue  Port-Type
```

```
----------------------------------------------------------------------
8021x              Disabled        128      24064     3         NA
arp-mff            Disabled         64      12032     3         NA
arp-miss           Enabled          64      12032     3         NA
arp-reply          Enabled         128      24064     3        UNI
arp-request        Enabled         128      24064     3        UNI
bfd                Disabled         64      12032     5        NNI
bgp                Enabled         256      48128     5         NA
bgp4plus           Enabled         128      24064     5         NA
bpdu-tunnel        Disabled         64      12032     5         NA
cdp                Disabled        128      24064     5         NA
dhcp-client        Enabled         512      96256     3        NNI
dhcp-server        Enabled         512      96256     3        UNI
dhcpv6-reply       Enabled         256      48128     3        NNI
dhcpv6-request     Enabled         256      48128     3        UNI
dldp               Disabled        128      24064     5         NA
dns                Enabled          64      12032     5         NA
easy-operation     Disabled        128      24064     3         NA
eoam-1ag           Disabled        256      48128     5         NA
eoam-1ag-lblt      Disabled        128      24064     5         NA
eoam-3ah           Disabled         64      12032     5         NA
erps-port          Disabled         64      12032     5         NA
fib-hit            Enabled          64      12032     3         NA
fib-miss           Disabled         64      12032     3        UNI
ftp                Enabled          64      12032     3         NA
gre-keepalive      Enabled          64      12032     5         NA
gvrp               Disabled        128      24064     5         NA
hop-limit          Enabled          64      12032     2        NNI
http               Enabled          64      12032     3         NA
https              Enabled          64      12032     3         NA
hw-tacacs          Enabled          64      12032     3        NNI
icmp               Enabled         128      24064     3        UNI
icmp-ttl-expired   Disabled          0          0     3        UNI
icmpv6             Enabled          64      12032     3        NNI
igmp               Enabled         128      24064     3         NA
ipsec-ah           Disabled        256      48128     5         NA
ipsec-esp          Disabled        256      48128     5         NA
isis               Disabled        256      48128     5        NNI
lacp               Disabled        128      24064     7         NA
ldt                Enabled          64      12032     5         NA
lldp               Disabled        128      24064     5         NA
lnp                Enabled         128      24064     5         NA
loopbacktest       Disabled         64      12032     5         NA
mad                Disabled        128      24064     5         NA
mdns-relay         Disabled        256      48128     5         NA
mld                Disabled        128      24064     3        NNI
mpls-fib-hit       Enabled         128      24064     5         NA
mpls-ldp           Enabled         256      48128     5         NA
mpls-one-label     Enabled         128      24064     3         NA
mpls-ping          Enabled          64      12032     5         NA
mpls-rsvp          Enabled         128      24064     5         NA
mpls-ttl-expired   Enabled         128      24064     5         NA
mpls-vccv-ping     Disabled        128      24064     3         NA
nac-arp-reply      Disabled         64      12032     3         NA
nac-arp-request    Disabled         64      12032     3         NA
nac-dhcp           Disabled        256      48128     3         NA
nac-dhcpv6         Disabled        256      48128     3         NA
nac-nd             Disabled         64      12032     3         NA
nd                 Enabled          64      12032     5        UNI
ntdp               Enabled         128      24064     5         NA
ntp                Enabled          64      12032     5        NNI
ospf               Disabled        256      48128     5        NNI
ospf-hello         Disabled        256      48128     5        NNI
ospfv3             Disabled        256      48128     5        NNI
pim                Enabled         128      24064     5        NNI
pimv6              Disabled         64      12032     5        NNI
portal             Enabled          64      12032     3        NNI
pppoe              Disabled        128      24064     3         NA
radius             Enabled          64      12032     3        NNI
```

```
rip              Disabled       128      24064      5        NNI
ripng             Disabled       256      48128      5        NNI
rrpp              Disabled       64      12032      5        NA
sep-global          Disabled       128      24064      5        NA
sep-port           Disabled       128      24064      5        NA
smart-link          Disabled       64      12032      5        NA
snmp              Enabled       128      24064      3        NNI
ssh              Enabled       64      12032      5        NNI
stp              Disabled       64      12032      5        NA
tcp              Enabled       64      12032      3        NA
telnet            Enabled       64      12032      5        NA
ttl-expired         Enabled       64      12032      2        NA
udp-helper          Disabled       64      12032      3        NA
vbst              Disabled       64      12032      5        NA
vbst-trunk          Disabled       64      12032      5        NA
vcmp              Enabled       128      24064      3        NA
vpls-igmp          Disabled       64      12032      3        NA
vrrp              Disabled       64      12032      5        NA
vrrp6             Disabled       64      12032      5        NA
y1731             Disabled       256      48128      5        NA
-----------------------------------------------------------------------

Linkup Information:
---------------------------------------------------------------------------------
Packet Name : ftp
Cir(Kbps)/Cbs(Byte) : 4096/770048
SIP(SMAC) : 10.1.2.1
DIP(DMAC) : 10.1.3.1
Port(S/C) : 42372/22
---------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 14-23 Description of the **display cpu-defend configuration** command output

Item	Description
Car configurations on slot 0	CAR configuration of a stack with a specified ID.
Car configurations on mainboard	CAR configurations on the device.
Packet Name	Packet type.
Status	Protocol packet status: ● Enabled ● Disabled
Cir(Kbps)	Committed Information Rate (CIR), in kbit/s. To set the CIR value, run the **14.2.18 car (attack defense policy view)** and **14.2.46 linkup-car** commands.

Item	Description
Cbs(Byte)	Committed burst size (CBS), in bytes. To configure the CBS value, run the **14.2.18 car (attack defense policy view)** and **14.2.46 linkup-car** commands.
Queue	Queue that protocol packets are sent to.
Port-Type	Port type. The value can be UNI, NNI, or ENI. To configure the port type, run the **14.2.47 port type** and **14.2.48 port-type** commands.
Linkup Information	Information about the protocol connection. **NOTE** This information is displayed only when association of protocols is triggered.
SIP(SMAC)	Source IP address or source MAC address.
DIP(DMAC)	Destination IP address or destination MAC address.
Port(S/C)	Source/Destination port number.

14.2.38 display cpu-defend dynamic-car history-record

Function

The **display cpu-defend dynamic-car history-record** command displays historical records on dynamic adjustment of the default CIR value of protocol packets.

NOTE

Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI support this command.

Format

display cpu-defend dynamic-car history-record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the default CIR value is set, you can run this command to view the historical records of adjustment.

The historical records show the CIR value change from the original CIR value to the specified CIR value. The granularity of the CIR value is 64 kbit/s.

Example

# Display the historical records on dynamic adjustment of the default CIR value of protocol packets.

```
<HUAWEI> display cpu-defend dynamic-car history-record
 Global status : Enable
 -----------------------------------------------------------------------------
 Time                 Protocol    Packet-type     Slot  CIR(Kbps)   Status
 -----------------------------------------------------------------------------
 2012-08-24 11:28:10  arp         arp-reply        0      128         Success
 2012-08-24 11:28:08  arp         arp-request      0      128         Success
 2012-08-24 11:27:37  arp         arp-reply        0      64          Success
 2012-08-24 11:27:37  arp         arp-request      0      64          Success
-----------------------------------------------------------------------------
```

Table 14-24 Description of the display cpu-defend dynamic-car history-record command output

Item	Description
Global status	The device is enabled to dynamically adjust the default CIR value of protocol packets. To enable the device to dynamically adjust the default CIR value of protocol packets, run the **14.2.20 cpu-defend dynamic-car enable** command.
Time	Timestamps of the default CIR value of protocol packets that is dynamically adjusted.
Protocol	Protocol name. To configure a protocol, run the **cpu-defend dynamic-car** [**arp**] command.
Packet-type	Packet type.
Slot	ID of the stack where the default CIR value is dynamically adjusted. The value indicates the slot ID if stacking is not configured.

Item	Description
CIR(Kbps)	Dynamically adjusted default CIR value, in kbit/s. If the default CIR value restores to the original default CIR value, N/A is displayed. **NOTE** When the rate of sending packets to the CPU is too large, the CPU becomes overloaded. The device restores the original default CIR value for protocol packets and this field is displayed as N/A.
Status	Result of dynamic adjustment. The value can be: ● success: indicates that the adjustment succeeds. ● fail: indicates that the adjustment fails. ● conflict: indicates that the adjusted default CIR value conflicts the configured CIR value. The CIR value configured by users takes effect.

Related Topics

14.2.20 cpu-defend dynamic-car enable

14.2.52 reset cpu-defend dynamic-car history-record

14.2.39 display cpu-defend host-car statistics

Function

The **display cpu-defend host-car statistics** command displays the number of packets discarded in user-level rate limiting.

NOTE

Only the S5720HI supports this command.

Format

display cpu-defend host-car [**mac-address** *mac-address*] **statistics** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Indicates the number of discarded packets from the specified MAC address.	-
slot *slot-id*	Indicates the number of packets discarded by the specified slot.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the number of packets discarded in the user-level rate limiting, run this command.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- If the number of discarded packets is 0, the index is not displayed.

Example

# Display the number of packets discarded in the user-level rate limiting.

```
<HUAWEI> display cpu-defend host-car statistics
slot 0
car-id                    car-drop
-------------------------------------------
3192                        740385
3347                             7
4133                        529474
4471                        529477
5075                        529476
5836                        529474
6046                       1001218
```

Table 14-25 Description of the display cpu-defend host-car statistics command output

Item	Description
slot	Slot ID.
car-id	Bucket ID for rate limiting.
car-drop	Number of dropped packets whose rate exceeds the CAR. To configure the CAR value, run the **cpu-defend host-car** [**mac-address** *mac-address* | **car-id** *car-id*] **pps** *pps-value* command.

14.2.40 display cpu-defend policy

Function

The **display cpu-defend policy** command displays the attack defense policy configuration.

Format

display cpu-defend policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specified attack defense policy. ● If *policy-name* is specified, information about the specified attack defense policy is displayed. ● If *policy-name* is not specified, information about all attack defense policies is displayed.	The attack defense policy must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an attack defense policy is created, you can run the **display cpu-defend policy** command to view the stack ID that the attack defense policy is applied to and configurations of the attack defense policy.

Example

# Display information about all attack defense policies.

```
<HUAWEI> display cpu-defend policy
  -----------------------------------------------------------------
 Name  : default
 Related slot : <3>
  -----------------------------------------------------------------
 Name  : test
 Description : defend_arp_attack
 Related slot : <mcu>
```

# Display information about the attack defense policy named **test**.

```
<HUAWEI> display cpu-defend policy test
 Description : defend_arp_attack
 Related slot : <0>
 Configuration :
   Blacklist 1 ACL number : 2001
   Car packet-type arp-request : CIR(128)  CBS(24064)
   Deny packet-type arp-reply
   Port-type eni packet-type arp-request
   Linkup-car packet-type  ftp : CIR(5000)  CBS(940000)
```

Table 14-26 Description of the display cpu-defend policy command output

Item	Description
Name	Name of an attack defense policy. To configure an attack defense policy, run the **14.2.24 cpu-defend policy** command.
Description	Description of an attack defense policy. To configure a description for an attack defense policy, run the **14.2.28 description (attack defense policy view)** command.
Related slot	Slot ID or stack ID that an attack defense policy is applied to. When mcu is displayed, it indicates the main control board.
Blacklist 1 ACL number	Number of an ACL defined in blacklist 1. To configure a blacklist, run the **14.2.17 blacklist** command.
Car packet-type arp-request	CIR values of ARP Request packets. To set the CIR values for ARP Request packets, run the **14.2.18 car (attack defense policy view)** command.
Deny packet-type arp-reply	ARP Reply packets are discarded. To configure the device to discard ARP Reply packets, run the **14.2.27 deny** command.
Port-type eni packet-type arp-request	ARP Request packets are sent to the CPU through ENI ports.
Linkup-car packet-type ftp	CIR values of FTP packets after an FTP connection is set up. To set the CIR values of FTP packets after an FTP connection is set up, run the **14.2.46 linkup-car** and **14.2.19 cpu-defend application-apperceive enable** commands.

Related Topics

14.2.17 blacklist

14.2.18 car (attack defense policy view)

14.2.19 cpu-defend application-apperceive enable

14.2.24 cpu-defend policy

14.2.27 deny

14.2.28 description (attack defense policy view)

14.2.46 linkup-car

14.2.41 display cpu-defend port-type

Function

The **display cpu-defend port-type** command displays physical interfaces of Network-Network Interface (NNI), User-Network Interface (UNI), and Enhanced Network Interface (ENI) types.

NOTE

Only the S5720EI, S6720S-EI, and S6720EI support this command.

Format

display cpu-defend port-type slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	• This parameter specifies the slot ID if stacking is not configured. • This parameter specifies the stack ID if a stack is configured.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After specifying interfaces types for sending protocol packets using the **port type** { **uni** | **eni** | **nni** } and **port-type** { **uni** | **eni** | **nni** } **packet-type** *type* commands, you can run the **display cpu-defend port-type** command to view types of interfaces on the device.

Example

# Display interface types in stack 0.

```
<HUAWEI> display cpu-defend port-type slot 0
 Uni Port :
 Eni Port :
 Nni Port :GigabitEthernet0/0/1-22
```

Table 14-27 Description of the display cpu-defend port-type command output

Item	Description
Uni Port	The interface is a user-side interface on the device.
Eni Port	The interface is an interface connected to another switch or user.
Nni Port	The interface is a network-side interface on the device.

Related Topics

14.2.48 port-type

14.2.47 port type

14.2.42 display cpu-defend rate

Function

The **display cpu-defend rate** command displays the rate of sending protocol packets to the CPU.

NOTE

Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.

Format

display cpu-defend rate [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device.
all	Indicates all switches in a stack if stack is enabled, or the switch itself if stack is disabled.	-

Parameter	Description	Value
slot *slot-id*	- This parameter specifies the slot ID if stacking is not configured. - This parameter specifies the stack ID if stack is enabled.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cpu-defend rate** command to view the rate of sending protocol packets to the CPU when checking the configuration of an attack defense policy. In this way, you can determine which type of protocols may attack the CPU based on the rate.

NOTE

To ensure normal operation of other services and protect the CPU, the rate of incremental protocol packets is calculated only in a specified period after you run the **display cpu-defend rate** command and displayed on the terminal. After you run this command, a message is displayed to wait for a while.

Example

# Display the rate of ARP Reply packets sent from the switch to the CPU.

```
<HUAWEI> display cpu-defend rate packet-type arp-reply slot 0
Info: Please wait for a moment....
Cpu-defend rate on slot 0:
-----------------------------------------------------------------------------
Packet Type          Pass(bps)    Drop(bps)       Pass(pps)       Drop(pps)
-----------------------------------------------------------------------------
arp-reply              49504       86496             91            159
-----------------------------------------------------------------------------
```

Table 14-28 Description of the **display cpu-defend rate** command output

Item	Description
Packet Type	Packet type.
Pass(bps)	Number of forwarded bits within one second.
Drop(bps)	Number of discarded bits within one second.

Item	Description
Pass(pps)	Number of forwarded packets within one second.
Drop(pps)	Number of discarded packets within one second.

14.2.43 display cpu-defend statistics

Function

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU.

NOTE

Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.

Format

display cpu-defend statistics [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
packet-type *packet-type*	Displays statistics on the specified type of protocol packets. *packet-type* specifies the packet type. ● If *packet-type* is specified, statistics on the specified type of protocol packets are displayed. ● If *packet-type* is not specified, statistics on all protocol packets are displayed.	The supported packet type depends on the device.
all	This parameter indicates all switches in a stack if stacking is enabled, or the switch itself if stacking is disabled. If **all** and **slot** are not specified, the CAR statistics on the master switch are cleared.	-

Parameter	Description	Value
slot *slot-id*	• This parameter specifies the slot ID if stacking is not configured. • This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU, including the number of forwarded and discarded packets. This helps the network administrator configure attack defense policies.

Precautions

If **all** and **slot** are not specified, the CAR statistics on the master switchin a stack are displayed.

Example

# Display statistics on packets on the switch.

```
<HUAWEI> display cpu-defend statistics
 Statistics on slot 0:
-------------------------------------------------------------------------------
Packet Type         Pass(Packet/Byte)   Drop(Packet/Byte)  Last-dropping-time
-------------------------------------------------------------------------------
arp-miss                          0                  0  -
                              0                  0
arp-reply                         0                  0  -
                              0                  0
arp-request                       0                  0  -
                              0                  0
dns                               0                  0  -
                              0                  0
eoam-3ah                          0                  0  -
                              0                  0
fib-hit                           0                  0  -
                              0                  0
ftp                               0                  0  -
                              0                  0
hw-tacacs                         0                  0  -
......
```

# Display CAR statistics on ARP Reply packets of the switch.

```
<HUAWEI> display cpu-defend statistics packet-type arp-reply
 Statistics on slot 0:
-------------------------------------------------------------------------------
Packet Type         Pass(Packet/Byte)   Drop(Packet/Byte)  Last-dropping-time
-------------------------------------------------------------------------------
arp-reply                 3625354          5612376421  2013-09-26 12:05:37
                      377036776         583687147k
-------------------------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 14-29 Description of the **display cpu-defend statistics** command output

Item	Description
Statistics on slot 0	CAR statistics on protocol packets sent by a specified switch or stack.
Packet Type	Packet type.
Pass(Packet/Byte)	Number of forwarded packets or bytes.
Drop(Packet/Byte)	Number of discarded packets or bytes. **NOTE** When the length exceeds 11 digits, the end of the value is displayed as k, indicating that the value is multiplied by 1000. When the length exceeds 14 digits, the end of the value is displayed as m, indicating that the value is multiplied by 1000000. When the length exceeds 17 digits, the end of the value is displayed as g, indicating that the value is multiplied by 1000000000.
Last-dropping-time	Last time statistics about dropped packets were collected.

Related Topics

14.2.54 reset cpu-defend statistics

14.2.44 display snmp-agent trap feature-name securitytrap all

Function

The **display snmp-agent trap feature-name securitytrap all** command displays the status of all traps on the security module.

Format

display snmp-agent trap feature-name securitytrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the trap function of a specified feature is enabled, you can run the **display snmp-agent trap feature-name securitytrap all** command to check the status of all traps of security. You can use the **snmp-agent trap enable feature-name securitytrap** command to enable the trap function of security.

Prerequisites

SNMP has been enabled. See **snmp-agent**.

Example

# Display all the traps of the security module.

```
<HUAWEI>display snmp-agent trap feature-name securitytrap all
------------------------------------------------------------------------------
Feature name: SECURITYTRAP
Trap number : 28
------------------------------------------------------------------------------
Trap name                       Default switch status   Current switch status
hwStrackUserInfo                  on                      on
hwStrackIfVlanInfo                on                      on
hwStrackSrcIpInfo                 on                      on
hwXQoSStormControlTrap            on                      on
hwXQoSStormControlTrapExt         on                      on
hwARPSGatewayConflict             on                      on
hwARPSEntryCheck                  on                      on
hwARPSPacketCheck                 on                      on
hwARPSDaiDropALarm                on                      on
hwARPGlobalSpeedLimitALarm        on                      on
hwARPIfSpeedLimitALarm            on                      on
hwARPVlanSpeedLimitALarm          on                      on
hwARPMissGlobalSpeedLimitALarm    on                      on
hwARPMissIfSpeedLimitALarm        on                      on
hwARPMissVlanSpeedLimitALarm      on                      on
hwARPSIPSpeedLimitALarm           on                      on
hwARPSMACSpeedLimitALarm          on                      on
hwARPMissSIPSpeedLimitALarm       on                      on
hwArpIfRateLimitBlockALarm        on                      on
hwIPSGDropALarm                   on                      on
hwICMPGlobalDropALarm             on                      on
hwICMPIfDropALarm                 on                      on
hwStrackDenyPkt                   on                      on
hwStrackErrorDown                 on                      on
hwDefendCpcarDropPkt              on                      on
hwMACsecFailNotify                on                      on
hwStrackPortAtk                   on                      on
hwStrackUserAbnormal              on                      on
```

Table 14-30 Description of the display snmp-agent trap feature-name securitytrap all command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.

Item	Specification
Trap name	Trap name. The ACL module uses the following Huawei-property traps: ● hwStrackUserInfo: sent when attack source tracing detects a user-based attack. ● hwStrackIfVlanInfo: sent when attack source tracing detects an attack initiated from an interface. ● hwStrackSrcIpInfo: sent when attack source tracing detects a source IP address-based attack. ● hwXQoSStormControlTrap: sent when storm control detects a port status change. ● hwXQoSStormControlTrapExt: sent when the interface state machine changes. ● hwARPSGatewayConflict: sent when the device receives an ARP packet of which the source IP address is the same as gateway IP address. ● hwARPSEntryCheck: sent when the device detects an attack packet used to modify an ARP entry. ● hwARPSPacketCheck: sent when the device detects an invalid ARP packet. ● hwARPSDaiDropALarm: sent when the number of ARP packets discarded by DAI reaches the alarm threshold. ● hwARPGlobalSpeedLimitALarm: sent when the rate of ARP packets received by the device reaches the alarm threshold. ● hwARPIfSpeedLimitALarm: sent when the rate of ARP packets received by an interface reaches the alarm threshold. ● hwARPVlanSpeedLimitALarm: sent when the rate of ARP packets in a VLAN reaches the alarm threshold. ● hwARPMissGlobalSpeedLimitALarm: sent when the rate of ARP Miss messages on the device exceeds the threshold and the number of discarded ARP Miss messages exceeds the alarm threshold. ● hwARPMissIfSpeedLimitALarm: sent when the rate of ARP Miss messages on an interface reaches the alarm threshold. ● hwARPMissVlanSpeedLimitALarm: sent when the rate of ARP Miss messages in a VLAN exceeds the threshold and the number of discarded ARP Miss messages exceeds the alarm threshold.

Item	Specification
	● hwARPSIPSpeedLimitALarm: sent when the rate of ARP packets from a source IP address exceeds the alarm threshold. ● hwARPSMACSpeedLimitALarm: sent when the rate of ARP packets from a source MAC address exceeds the alarm threshold. ● hwARPMissSIPSpeedLimitALarm: sent when the rate of ARP Miss messages from a source IP address exceeds the alarm threshold. ● hwArpIfRateLimitBlockALarm: sent when the rate of ARP packets received by the device exceeds the threshold and ARP packets are discarded on interfaces within block period. ● hwIPSGDropALarm: sent when the number of IP packets discarded by IPSG reaches the alarm threshold. ● hwICMPGlobalDropALarm: sent when the rate of global ICMP packets reaches the alarm threshold. ● hwICMPIfDropALarm: sent when the rate of ICMP packets on an interface reaches the alarm threshold. ● hwStrackDenyPkt: sent when the device detects an attack source and discards the packets from this attack source. ● hwStrackErrorDown: sent when the device detects an attack source and sets the port status of the attack source to error-down. ● hwDefendCpcarDropPkt: sent when packets are dropped because the rate of protocol packets sent to the CPU exceeds the CPCAR value. ● hwMACsecFailNotify: sent when MACsec configuration on an interface is invalid. ● hwStrackPortAtk: sent when an interface is attacked by protocol packets and port attack defense is started. ● hwStrackUserAbnormal: sent when the rate of packets received by an LPU exceeds the normal rate.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.

Item	Specification
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

14.2.55 snmp-agent trap enable feature-name securitytrap

14.2.45 host-car disable

Function

The **host-car disable** command disables user-level rate limiting on interfaces.

The **undo host-car disable** command enables user-level rate limiting on interfaces.

By default, user-level rate limiting is enabled on all interfaces.

NOTE

Only the S5720HI supports this command.

Format

host-car disable

undo host-car disable

Parameters

None

Views

GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the switch performs user-level rate limiting on the users connecting to all interfaces. If you are sure that the users connecting to an interface are secure, you can disable user-level rate limiting on this interface.

Precautions

- Before using this command, run the **cpu-defend host-car enable** command to enable user-level rate limiting.
- After user-level rate limiting is disabled on an interface, the switch does not limit the rate of packets received from the specified user MAC address and cannot protect the interface against attacks. In addition, the packets of the same type sent from other users may be affected.

Example

# Disable user-level rate limiting on the interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] host-car disable
```

14.2.46 linkup-car

Function

The **linkup-car** command sets the CPCAR value for packets of a protocol connection, including the Committed Information Rate (CIR) and Committed Burst Size (CBS).

The **undo linkup-car** command restores the default CPCAR rate limit.

Table 14-31 lists the default CIR and CBS values for the setup of BGP, FTP, HTTPS, IKE, IPSEC-ESP, OSPF, SSH, TELNET, and TFTP connections.

Format

linkup-car packet-type { **bgp** | **ftp** | **https** | **ike** | **ipsec-esp** | **ospf** | **ssh** | **telnet** | **tftp** } **cir** *cir-value* [**cbs** *cbs-value*]

undo linkup-car packet-type { **bgp** | **ftp** | **https** | **ike** | **ipsec-esp** | **ospf** | **ssh** | **telnet** | **tftp** }

NOTE

- Only the S5730SI, S5730S-EI, S5720EI, S5720HI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **bgp** parameter.
- Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support the **https** parameter.
- Only the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S5720EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **ike** parameter.
- Only the S2720EI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S5720EI, S5720HI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **ipsec-esp** parameter.
- Only the S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S5720LI, S5720S-LI, S5730SI, S5730S-EI, S5720EI, S5720HI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support the **ospf** parameter.

Parameters

Parameter	Description	Value
bgp	Indicates that the protocol type is BGP.	-
ftp	Indicates that the protocol type is FTP.	-
https	Indicates that the protocol type is HTTPS.	-
ike	Indicates that the protocol type is IKE.	-
ipsec-esp	Indicates that the protocol type is IPSEC-ESP.	-
ospf	Indicates the protocol type is OSPF.	-
ssh	Indicates the protocol type is SSH.	-
telnet	Indicates the protocol type is TELNET.	-
tftp	Indicates the protocol type is TFTP.	-
cir *cir-value*	Specifies the CIR value.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.
cbs *cbs-value*	Specifies the CBS value.	The value is an integer that ranges from 10000 to 4294967295, in bytes.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default CPCAR value of BGP, FTP, HTTPS, OSPF, IKE, IPSEC-ESP, SSH, TFTP, or TELNET protocol is small. When a switch uses these protocols to transfer files or set up connections with other hosts or devices, the number of protocol packets sharply increases in a short period. When the packet rate exceeds the limit, the protocol packets are dropped. The switch may also undergo attacks of other protocols. This affects data transmission and causes service interruption.

You can run the **cpu-defend application-apperceive** command to enable active link protection, ensuring normal operation of BGP, FTP, HTTPS, OSPF, IKE, IPSEC-ESP, SSH, TFTP, or TELNET services when attacks occur. When a connection is set up, the switch sends packets at the rate of the CPCAR value configured using the **linkup-car** command. The CPCAR value can be set as required.

Follow-up Procedure

Run the **cpu-defend application-apperceive** **bgp enable** command or **cpu-defend application-apperceive** **ospf enable** common to enable ALP to enable the rate limit set using the **linkup-car** command. By default, ALP is enabled on FTP, HTTPS, IKE, IPSEC-ESP, TFTP, SSH, and TELNET packets and disabled on BGP and OSPF packets.

Precautions

You are advised to run the **display cpu-defend configuration** command to check the CIR value supported by the protocol being used before running the **linkup-car** command to set the rate limit.

BGP and OSPF are disabled when the configuration is initialized. You can set the rate limit using the **car** command before the protocols are enabled and the **linkup-car** command after connections are set up and ALP is enabled.

You can set a shared CPCAR value for packets of FTP, SSH, TFTP connections on S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI. For example, the **linkup-car packet-type ftp cir** *cir-value* [**cbs** *cbs-value*] command specifies the CPCAR value for FTP packets when an FTP connection is set up, and also specifies the CPCAR value for packets of SSH, TFTP connections.

Table 14-31 Default CIR and CBS values

Product	CIR	CBS
S1720GFR, S2750EI, S5700LI, S5700S-LI, S5710-X-LI	• FTP, SSH, TFTP: 1024 kbit/s • TELNET: 64 kbit/s	• FTP, SSH, TFTP: 192512 bytes • TELNET: 12032 bytes
S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S5720LI, S5720S-LI, S6720LI, S6720S-LI	• FTP, SSH, TFTP: 1024 kbit/s • OSPF: 512 kbit/s • TELNET: 64 kbit/s	• FTP, SSH, TFTP: 192512 bytes • OSPF: 96256 bytes • TELNET: 12032 bytes

Product	CIR	CBS
S5720SI, S5720S-SI	● FTP, SSH, TFTP: 1024 kbit/s ● IKE: 64 kbit/s ● IPSEC-ESP: 320 kbit/s ● TELNET: 64 kbit/s	● FTP, SSH, TFTP: 192512 bytes ● IKE: 12032 bytes ● IPSEC-ESP: 60160 bytes ● TELNET: 12032 bytes
S2720EI	● FTP, SSH, TFTP: 1024 kbit/s ● IKE: 64 kbit/s ● IPSEC-ESP: 320 kbit/s ● OSPF: 512 kbit/s ● TELNET: 64 kbit/s	● FTP, SSH, TFTP: 192512 bytes ● IKE: 12032 bytes ● IPSEC-ESP: 60160 bytes ● OSPF: 96256 bytes ● TELNET: 12032 bytes
S5730SI, S5730S-EI, S6720SI, S6720S-SI	● BGP: 1024 kbit/s ● FTP, SSH, TFTP: 1536 kbit/s ● IKE: 64 kbit/s ● IPSEC-ESP: 4096 kbit/s ● OSPF: 512 kbit/s ● TELNET: 64 kbit/s	● BGP: 192512 bytes ● FTP, HTTPS, SSH, TFTP: 288768 bytes ● IKE: 12032 bytes ● IPSEC-ESP: 770048 bytes ● OSPF: 96256 bytes ● TELNET: 12032 bytes
S5720EI, S6720EI, S6720S-EI	● BGP: 1024 kbit/s ● FTP, HTTPS, SSH, TFTP: 1536 kbit/s ● IKE: 64 kbit/s ● IPSEC-ESP: 4096 kbit/s ● OSPF: 512 kbit/s ● TELNET: 64 kbit/s	● BGP: 192512 bytes ● FTP, HTTPS, SSH, TFTP: 288768 bytes ● IKE: 12032 bytes ● IPSEC-ESP: 770048 bytes ● OSPF: 96256 bytes ● TELNET: 12032 bytes
S5720HI	● BGP: 1024kbit/s ● FTP, HTTPS, SSH, TFTP: 1536kbit/s ● IPSEC-ESP: 800kbit/s ● OSPF: 512kbit/s ● TELNET: 64kbit/s	● BGP: 192512bytes ● FTP, HTTPS, SSH, TFTP: 288768bytes ● IPSEC-ESP: 150400bytes ● OSPF: 96256bytes ● TELNET: 12032bytes

Example

# Set the CIR and CBS for sending packets of FTP connections to 1000 kbit/s and 100000 bytes.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] linkup-car packet-type ftp cir 1000 cbs 100000
```

Related Topics

14.2.24 cpu-defend policy

14.2.37 display cpu-defend configuration

14.2.19 cpu-defend application-apperceive enable

14.2.47 port type

Function

The **port type** command configures the interface type. The interface type can be Network Network Interface (NNI), User Network Interface (UNI), or Enhanced Network Interface (ENI).

The **undo port type** command cancels the configuration.

By default, the interface type is NNI.

NOTE

Only the S5720EI, S6720S-EI, and S6720EI support this command.

Format

port type { **uni** | **eni** | **nni** }

undo port type

Parameters

Parameter	Description	Value
uni	Indicates that the interface is a user-side interface on the device.	-
eni	Indicates that the interface is connected to another switch or user. An ENI supports all protocols that are supported by an UNI.	-
nni	Indicates that the interface is a network-side interface on the device. An NNI supports all protocol packets.	-

Views

40GE interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, protocol packets that can be sent to the CPU are controlled by an ACL. If protocol packets are sent to the device, packets received by interfaces cannot be differentiated.

If an interface is attacked and the user disables the device to send packets, packets cannot be sent from other interfaces, affecting communications of the device. If an interface is attacked and the user does not disable the device to send packets, attack packets occupy resources and valid packets cannot be sent.

For example, OSPF is enabled on an interface and OSPF packets are sent to the device. If a non-OSPF interface is attacked, attack packets will occupy resources and valid OSPF packets cannot be forwarded. As a result, OSPF negotiation becomes slow or fails.

The **port type** command specifies the interface types according to the interface location. Interfaces of different types support different protocols and send only the packets of the supported protocols to the CPU. This reduces the workload of the CPU and provides flexible ways to protect the CPU.

Precautions

If you run the **port type** command multiple times, only the latest configuration takes effect.

Follow-up Procedure

This command differentiates packets from different types of interfaces so that the attack packets are denied and valid packets are forwarded. If an attack occurs, you can run the **14.2.27 deny** command to discard packets of a specified type or run the **14.2.18 car (attack defense policy view)** command to limit the rate of a specified type of protocol packets.

Example

# Configure GE0/0/1 as an NNI.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port type nni
```

Related Topics

14.2.48 port-type

14.2.27 deny

14.2.18 car (attack defense policy view)

14.2.48 port-type

Function

The **port-type** command maps interfaces to protocol types. The type can be User Network Interface (UNI), Enhanced Network Interface (ENI), or Network Network Interface (NNI).

The **undo port-type** command cancels the configuration.

By default, the type of interface sending protocol packets to the CPU is displayed using the **display cpu-defend configuration** command.

NOTE

Only the S5720EI, S6720S-EI, and S6720EI support this command.

Format

port-type { **uni** | **eni** | **nni** } **packet-type** *packet-type*

undo port-type [**uni** | **eni** | **nni**] **packet-type** *packet-type*

Parameters

Parameter	Description	Value
uni	Indicates that the interface is a user-side interface on the device.	-
eni	Indicates that the interface is connected to another switch or user. An ENI supports all protocols that are supported by an UNI.	-
nni	Indicates that the interface is a network-side interface on the device. An NNI supports all protocol packets.	-
packet-type *packet-type*	Specifies the protocol supported by an interface type. A protocol is mapped to only one interface type.	The supported packet type depends on the device.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, protocol packets that can be sent to the CPU are controlled by an ACL. If protocol packets are sent to the device, packets received by interfaces cannot be differentiated.

If an interface is attacked and the user disables the device to send packets, packets cannot be sent from other interfaces, affecting communications of the device. If an interface is attacked and the user does not disable the device to send packets, attack packets occupy resources and valid packets cannot be sent.

The **port-type** command maps interfaces to protocol types. The **14.2.47 port type** command specifies the interface types according to port locations. By using the two commands, the interfaces send only the packets of the supported protocols. This reduces the workload of CPU and provides ways to flexibly protect the CPU.

NOTE

Protocol packets are not supported by the UNI, ENI, or NNI interfaces. These protocol packets are sent to the CPU for processing from any interface on the device.

Procedure

After you run the **14.2.47 port type** command to configure interface types, run the **port-type** command to specify the protocols supported by the interfaces and the method to process the protocol packets.

Precautions

If you run the **port-type** command multiple times, only the latest configuration takes effect because a protocol is mapped to only one interface type.

Follow-up Procedure

This command differentiates packets from different types of interfaces so that the attack packets are denied and valid packets are forwarded. If an attack occurs, you can run the **14.2.27 deny** command to discard a specified type of packets. When receiving packets of the type, the interfaces discard these packets. You can also run the **14.2.18 car (attack defense policy view)** command to limit the rate of attack packets of a specified type.

Example

# Configure UNI interfaces to send ARP Reply packets to the CPU.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] port-type uni packet-type arp-reply
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend-policy test global
```

Related Topics

14.2.18 car (attack defense policy view)

14.2.24 cpu-defend policy

14.2.27 deny

14.2.37 display cpu-defend configuration

14.2.47 port type

14.2.49 reset auto-defend attack-source

Function

The **reset auto-defend attack-source** command clears information about attack sources.

Format

reset auto-defend attack-source [**history**] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
history	Deletes history attack source information. If **history** is not specified, all existing attack source information is deleted.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stacking is enabled. If **slot** *slot-id* is not specified, information about attack sources is cleared.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the latest attack source information on the device, run the **reset auto-defend attack-source** command to delete the existing attack source information, wait for a period, and run the **display auto-defend attack-source** command.

To delete history attack source information, run the **reset auto-defend attack-source history** command.

Precautions

After the **reset auto-defend attack-source** command is run, information about attack sources is cleared and cannot be restored.

Example

# Delete existing attack source information on the device.

```
<HUAWEI> system-view
[HUAWEI] reset auto-defend attack-source
```

Related Topics

14.2.29 display auto-defend attack-source

14.2.50 reset auto-defend attack-source trace-type

Function

The **reset auto-defend attack-source trace-type** command clears the counter of packets traced after attack source tracing based on source MAC addresses, source IP addresses, or source ports+VLANs is configured.

Format

reset auto-defend attack-source trace-type { **source-mac** [*mac-address*] | **source-ip** [*ipv4-address*] | **source-portvlan** [**interface** *interface-type interface-number* **vlan-id** *vlan-id* [**cvlan-id** *cvlan-id*]] } [**slot** *slot-id*]

Parameters

Parameter	Description	Value
source-mac [*mac-address*]	Clears the counter of packets traced after attack source tracing based on source MAC addresses is configured. If *mac-address* is specified, the counter of traced packets sent from the specified MAC address is cleared.	The value of *mac-address* is in H-H-H format. An H contains 1 to 4 hexadecimal numbers.
source-ip [*ipv4-address*]	Clears the counter of packets traced after attack source tracing based on source IP addresses is configured. If an ip-address is specified, the counter of traced packets sent from the specified IP address is cleared.	The value of *ipv4-address* is in dotted decimal notation.

Parameter	Description	Value
source-portvlan [**interface** *interface-type interface-number* **vlan-id** *vlan-id* [**cvlan-id** *cvlan-id*]]	Clears the counter of packets traced after attack source tracing based on source ports+VLANs is configured. If a port or VLAN is specified, the counter of traced packets sent from the specified port or VLAN is cleared. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. ● **vlan-id** *vlan-id* specifies the ID of the VLAN. ● **cvlan-id** *cvlan-id* specifies the inner VLAN ID in a QinQ packet.	*vlan-id* is an integer that ranges from 1 to 4094. *cvlan-id* is an integer that ranges from 1 to 4094.
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stack is enabled.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view information about attack sources in a specified period, run the **reset auto-defend attack-source** command to clear existing information about attack sources and run the **display auto-defend attack-source** command. However, the **reset auto-defend attack-source** clears information about all attack sources. You can run the **reset auto-defend attack-source trace-type** command to clear information about specified attack sources.

Precautions

After the **reset auto-defend attack-source trace-type** command is run, information about attack sources is cleared and cannot be restored.

Example

# Clear the counter of traced packets sent from IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] reset auto-defend attack-source trace-type source-ip 10.1.1.1
```

Related Topics

14.2.29 display auto-defend attack-source

14.2.49 reset auto-defend attack-source

14.2.51 reset auto-port-defend statistics

Function

The **reset auto-port-defend statistics** command deletes packet statistics on port attack defense.

NOTE

Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.

Format

reset auto-port-defend statistics [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
all	Deletes packet statistics of port attack defense on the interfaces of all stacked switches in a stack environment or on all interfaces of the local switch in a non-stack environment. If **all** or **slot** *slot-id* is not specified, packet statistics on the master device (stack configured) or local device (stack not configured) are deleted.	-
slot *slot-id*	• The value indicates the slot ID if stacking is not configured. • The value indicates the stack ID when stack is configured.	The value depends on the device configuration.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before viewing packet statistics of port attack defense in a certain period, delete existing packet statistics, and then run the **14.2.34 display auto-port-defend statistics** command to collect the latest statistics.

Precautions

The deleted packet statistics cannot be restored.

Example

# Delete packet statistics on the interfaces of the device.

```
<HUAWEI> reset auto-port-defend statistics
```

Related Topics

14.2.34 display auto-port-defend statistics

14.2.52 reset cpu-defend dynamic-car history-record

Function

The **reset cpu-defend dynamic-car history-record** command clears history records on dynamic adjustment of the default CIR value of protocol packets.

NOTE

Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720S-EI, and S6720EI support this command.

Format

reset cpu-defend dynamic-car history-record

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **reset cpu-defend dynamic-car history-record** command to clear the previous records and run the **display cpu-defend dynamic-car history-record** command to view the history records on dynamic adjustment of the default CIR value of protocol packets in a specified period.

Precautions

The **reset cpu-defend dynamic-car history-record** command clears history records on dynamic adjustment of the default CIR value of protocol packets and the records cannot be restored.

Example

# Clear the history records on dynamic adjustment of the default CIR value of protocol packets.

```
<HUAWEI> reset cpu-defend dynamic-car history-record
```

Related Topics

14.2.38 display cpu-defend dynamic-car history-record

14.2.53 reset cpu-defend host-car statistics

Function

The **reset cpu-defend host-car statistics** command clears packet statistics in the user-level rate limiting.

NOTE

Only the S5720HI supports this command.

Format

reset cpu-defend host-car [**mac-address** *mac-address*] **statistics** [**slot** *slot-id*]

Parameters

Parameter	Description	Value
mac-address *mac-address*	Clears statistics on the packets from the specified MAC address.	-
slot *slot-id*	Clears packet statistics on the specified slot.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Before viewing the latest packet statistics in the user-level rate limiting, run this command to clear existing packet statistics.

NOTICE

Packet statistics cannot be restored after they are deleted. Exercise caution when you use the command.

Example

# Clear packet statistics in user-level rate limiting.

```
<HUAWEI> reset cpu-defend host-car statistics
```

14.2.54 reset cpu-defend statistics

Function

The **reset cpu-defend statistics** command clears statistics on packets sent to the CPU.

NOTE

Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.

Format

reset cpu-defend statistics [**packet-type** *packet-type*] [**all** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the protocol type of packets. *packet-type* specifies the packet type. • If **packet-type** *packet-type* is specified, the statistics on the specified type of protocol packets are cleared. • If **packet-type** *packet-type* is not specified, the statistics on all protocol packets are cleared.	The supported packet type depends on the device.

Parameter	Description	Value
all	This parameter indicates all switches in a stack if stacking is enabled, or the switch itself if stack is disabled. If **all** and **slot** are not specified, the CAR statistics on the master switch in a stack are cleared.	-
slot *slot-id*	● This parameter specifies the slot ID if stacking is not configured. ● This parameter specifies the stack ID if stacking is enabled.	The value must be set according to the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view statistics on the packets sent to the CPU in a specified period, run the **reset cpu-defend statistics** command to clear existing statistics and run the **display cpu-defend statistics** command.

Precautions

The deleted packet statistics cannot be restored.

Example

# Clear statistics on BGP packets sent to the CPU.

```
<HUAWEI> reset cpu-defend statistics packet-type bgp slot 0
```

Related Topics

14.2.18 car (attack defense policy view)

14.2.43 display cpu-defend statistics

14.2.55 snmp-agent trap enable feature-name securitytrap

Function

The **snmp-agent trap enable feature-name securitytrap** command enables the trap function for the security module.

The **undo snmp-agent trap enable feature-name securitytrap** command disables the trap function for the security module.

By default, the trap function is enabled for the security module.

Format

snmp-agent trap enable feature-name securitytrap [**trap-name** { **hwarpglobalspeedlimitalarm** | **hwarpifratelimitblockalarm** | **hwarpifspeedlimitalarm** | **hwarpmissglobalspeedlimitalarm** | **hwarpmissifspeedlimitalarm** | **hwarpmisssipspeedlimitalarm** | **hwarpmissvlanspeedlimitalarm** | **hwarpsdaidropalarm** | **hwarpsentrycheck** | **hwarpsgatewayconflict** | **hwarpsipspeedlimitalarm** | **hwarpsmacspeedlimitalarm** | **hwarpspacketcheck** | **hwarpvlanspeedlimitalarm** | **hwdefendcpcardroppkt** | **hwicmpglobaldropalarm** | **hwicmpifdropalarm** | **hwipsgdropalarm** | **hwmacsecfailnotify** | **hwstrackdenypkt** | **hwstrackerrordown** | **hwstrackifvlaninfo** | **hwstrackportatk** | **hwstracksrcipinfo** | **hwstrackuserabnormal** | **hwstrackuserinfo** | **hwxqosstormcontroltrap** | **hwxqosstormcontroltrapext** }]

undo snmp-agent trap enable feature-name securitytrap [**trap-name** { **hwarpglobalspeedlimitalarm** | **hwarpifratelimitblockalarm** | **hwarpifspeedlimitalarm** | **hwarpmissglobalspeedlimitalarm** | **hwarpmissifspeedlimitalarm** | **hwarpmisssipspeedlimitalarm** | **hwarpmissvlanspeedlimitalarm** | **hwarpsdaidropalarm** | **hwarpsentrycheck** | **hwarpsgatewayconflict** | **hwarpsipspeedlimitalarm** | **hwarpsmacspeedlimitalarm** | **hwarpspacketcheck** | **hwarpvlanspeedlimitalarm** | **hwdefendcpcardroppkt** | **hwicmpglobaldropalarm** | **hwicmpifdropalarm** | **hwipsgdropalarm** | **hwmacsecfailnotify** | **hwstrackdenypkt** | **hwstrackerrordown** | **hwstrackifvlaninfo** | **hwstrackportatk** | **hwstracksrcipinfo** | **hwstrackuserabnormal** | **hwstrackuserinfo** | **hwxqosstormcontroltrap** | **hwxqosstormcontroltrapext** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwarpglobalspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP packets received by the device reaches the alarm threshold.	-

Parameter	Description	Value
hwarpifratelimitblockalarm	Enables the Huawei-property trap sent when the rate of ARP packets received by the device exceeds the threshold and ARP packets are discarded on interfaces within block period.	-
hwarpifspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP packets received by an interface reaches the alarm threshold.	-
hwarpmissglobalspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP Miss messages on the device exceeds the threshold and the number of discarded ARP Miss messages exceeds the alarm threshold.	-
hwarpmissifspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP Miss messages on an interface reaches the alarm threshold.	-
hwarpmisssipspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP Miss messages from a source IP address exceeds the alarm threshold.	-
hwarpmissvlanspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP Miss messages in a VLAN exceeds the threshold and the number of discarded ARP Miss messages exceeds the alarm threshold.	-

Parameter	Description	Value
hwarpsdaidropalarm	Enables the Huawei-property trap sent when the number of ARP packets discarded by DAI reaches the alarm threshold.	-
hwarpsentrycheck	Enables the Huawei-property trap sent when the device detects an attack packet used to modify an ARP entry.	-
hwarpsgatewayconflict	Enables the Huawei-property trap sent when the device receives an ARP packet of which the source IP address is the same as gateway IP address.	-
hwarpsipspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP packets from a source IP address exceeds the alarm threshold.	-
hwarpsmacspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP packets from a source MAC address exceeds the alarm threshold.	-
hwarpspacketcheck	Enables the Huawei-property trap sent when the device detects an invalid ARP packet.	-
hwarpvlanspeedlimitalarm	Enables the Huawei-property trap sent when the rate of ARP packets in a VLAN reaches the alarm threshold.	-
hwdefendcpcardroppkt	Enables the Huawei-property trap sent when packets are dropped because the rate of protocol packets sent to the CPU exceeds the CPCAR value.	-

Parameter	Description	Value
hwicmpglobaldropalarm	Enables the Huawei-property trap sent when the rate of global ICMP packets reaches the alarm threshold.	-
hwicmpifdropalarm	Enables the Huawei-property trap sent when the rate of ICMP packets on an interface reaches the alarm threshold.	-
hwipsgdropalarm	Enables the Huawei-property trap sent when the number of IP packets discarded by IPSG reaches the alarm threshold.	-
hwmacsecfailnotify	Enables the Huawei-property trap sent when MACsec configuration on an interface is invalid.	-
hwstrackdenypkt	Enables the Huawei-property trap sent when the device detects an attack source and discards the packets from this attack source.	-
hwstrackerrordown	Enables the Huawei-property trap sent when the device detects an attack source and sets the port status of the attack source to error-down.	-
hwstrackifvlaninfo	Enables the Huawei-property trap sent when attack source tracing detects an attack initiated from an interface.	-
hwstrackportatk	Enables the Huawei-property trap sent when an interface is attacked by protocol packets and port attack defense is started.	-

Parameter	Description	Value
hwstracksrcipinfo	Enables the Huawei-property trap sent when attack source tracing detects a source IP address-based attack.	-
hwstrackuserabnormal	Enables the Huawei-property trap sent when the rate of packets received by an LPU exceeds the normal rate.	-
hwstrackuserinfo	Enables the Huawei-property trap sent when attack source tracing detects a user-based attack.	-
hwxqosstormcontrol-trap	Enables the Huawei-property trap sent when storm control detects a port status change.	-
hwxqosstormcontrol-trapext	Enables the Huawei-property trap sent when the interface state machine changes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the trap function is enabled, the device generates traps during running and sends traps to the NMS through SNMP. When the trap function is not enabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

Example

# Enable the hwStrackUserInfo trap of the security module.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name securitytrap trap-name hwStrackUserInfo
```

Related Topics

14.2.44 display snmp-agent trap feature-name securitytrap all

14.2.56 user-defined-flow

Function

The **user-defined-flow** command configures a user-defined flow.

The **undo user-defined-flow** command deletes a user-defined flow.

By default, no user-defined flow is configured.

NOTE

Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support this command.

Format

user-defined-flow *flow-id* **acl** *acl-number*

undo user-defined-flow *flow-id*

Parameters

Parameter	Description	Value
flow-id	Specifies the ID of the user-defined flow.	The value is an integer that ranges from 1 to 8.
acl *acl-number*	Specifies the number of an Access Control List (ACL). The ACL referenced by a user-defined flow on the device can be a basic ACL, an advanced ACL, or a Layer 2 ACL.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When unknown attacks occur on the network, you can run the **user-defined-flow** command to bind an ACL rule with a user-defined flow. Then you can run the **car** **user-defined-flow** *flow-id* **cir** *cir-value* [**cbs** *cbs-value*] command to limit the rate of flows with the specific characteristic or run the **deny** **user-defined-flow** *flow-id* command to discard these flows.

Precautions

If an ACL containing the deny action is applied to the user-defined flow, packets matching the ACL are discarded.

Example

# Specify ACL 2001 as the rule of user-defined flow 2.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] user-defined-flow 2 acl 2001
```

Related Topics

14.1.5 acl (system view)

14.2.24 cpu-defend policy

14.3 Attack Defense Configuration Commands

14.3.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.3.2 anti-attack abnormal enable

Function

The **anti-attack abnormal enable** command enables defense against malformed packet attacks.

The **undo anti-attack abnormal enable** command disables defense against malformed packet attacks.

The **anti-attack abnormal disable** command disables defense against malformed packet attacks.

By default, defense against malformed packet attacks is enabled.

Format

anti-attack abnormal enable

undo anti-attack abnormal enable

anti-attack abnormal disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The malformed packet attack is to send malformed IP packets to the system. If such an attack occurs, the system may break down when processing the malformed IP packets. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack abnormal enable** command to enable defense against malformed packets.

The device detects malformed packets after defense against malformed packets is enabled.

The device directly discards packets of the following types:

- Flood attacks from IP null payload packets
- Attacks from IGMP null payload packets
- LAND attacks
- Smurf attacks

- Attacks from packets with invalid TCP flag bits

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including malformed packets.

Example

# Enable defense against malformed packet attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack abnormal enable
```

Related Topics

14.3.3 anti-attack enable

14.3.3 anti-attack enable

Function

The **anti-attack enable** command enables defense against all attack packets.

The **undo anti-attack enable** command disables defense against all attack packets.

The **anti-attack disable** command disables defense against all attack packets.

By default, defense against all attack packets is enabled.

Format

anti-attack enable

undo anti-attack enable

anti-attack disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different types of attacks on a network cause high device usage or system breakdown, affecting network services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack enable** command to enable defense against all attack packets.

Precautions

Running the **anti-attack enable** command is equivalent to running all of the following commands:

- **anti-attack abnormal enable**
- **anti-attack fragment enable**
- **anti-attack tcp-syn enable**
- **anti-attack udp-flood enable**
- **anti-attack icmp-flood enable**

Example

# Enable defense against all attack packets.

```
<HUAWEI> system-view
[HUAWEI] anti-attack enable
```

Related Topics

14.3.2 anti-attack abnormal enable

14.3.4 anti-attack fragment enable

14.3.8 anti-attack tcp-syn enable

14.3.10 anti-attack udp-flood enable

14.3.6 anti-attack icmp-flood enable

14.3.4 anti-attack fragment enable

Function

The **anti-attack fragment enable** command enables defense against packet fragment attacks.

The **undo anti-attack fragment enable** command disables defense against packet fragment attacks.

The **anti-attack fragment disable** command disables defense against packet fragment attacks.

By default, defense against packet fragment attacks is enabled.

Format

anti-attack fragment enable

undo anti-attack fragment enable

anti-attack fragment disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends error packet fragments to a device, the device consumes a large number of resources to process the error packet fragments, affecting normal services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack fragment enable** command to enable defense against packet fragment attacks.

The device detects error packet fragments after defense against error packet fragments is enabled. If the device detects error packet fragments, the device limits the rate of these fragments to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including packet fragments.

Example

# Enable defense against packet fragment attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack fragment enable
```

Related Topics

14.3.3 anti-attack enable

14.3.5 anti-attack fragment car

Function

The **anti-attack fragment car** command sets the rate limit of packet fragments.

The **undo anti-attack fragment car** command restores the rate limit of packet fragments.

By default, the rate limit of packet fragments is 155000000 bit/s.

Format

anti-attack fragment car cir *cir*

undo anti-attack fragment car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of packet fragments.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against packet fragment attacks is enabled, run the **anti-attack fragment car** command to set the rate limit of packet fragments. If the rate of received packet fragments exceeds the rate limit, the device discards excess packet fragments to ensure that the device CPU works properly.

Prerequisites

Defense against packet fragment attacks has been enabled using the **anti-attack fragment enable** command.

Example

# Set the rate limit of packet fragments to 8000 bit/s.

```
<HUAWEI> system-view
[HUAWEI] anti-attack fragment enable
[HUAWEI] anti-attack fragment car cir 8000
```

Related Topics

14.3.6 anti-attack icmp-flood enable

14.3.6 anti-attack icmp-flood enable

Function

The **anti-attack icmp-flood enable** command enables defense against ICMP flood attacks.

The **undo anti-attack icmp-flood enable** command disables defense against ICMP flood attacks.

The **anti-attack icmp-flood disable** command disables defense against ICMP flood attacks.

By default, defense against ICMP flood attacks is enabled.

Format

anti-attack icmp-flood enable

undo anti-attack icmp-flood enable

anti-attack icmp-flood disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of ICMP request packets to the target host in a short time, the target host is busy with these ICMP request packets. As a result, the target host is overloaded and cannot process normal services. To prevent ICMP flood attacks, run the **anti-attack icmp-flood enable** command to enable defense against ICMP flood attacks.

The device detects ICMP flood attack packets after defense against ICMP flood attacks is enabled. If the device detects ICMP flood attack packets, the device limits the rate of these ICMP flood attack packets to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including ICMP flood attack packets.

Example

# Enable defense against ICMP flood attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack icmp-flood enable
```

Related Topics

14.3.7 anti-attack icmp-flood car

14.3.3 anti-attack enable

14.3.7 anti-attack icmp-flood car

Function

The **anti-attack icmp-flood car** command sets the rate limit of ICMP flood attack packets.

The **undo anti-attack icmp-flood car** command restores the default rate limit of ICMP flood attack packets.

By default, the rate limit of ICMP flood attack packets is 155000000 bit/s.

Format

anti-attack icmp-flood car cir *cir*

undo anti-attack icmp-flood car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of ICMP flood attack packets.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against ICMP flood attacks is enabled, run the **anti-attack icmp-flood car** command to set the rate limit of ICMP flood attack packets. If the rate of received ICMP flood attack packets exceeds the rate limit, the device discards excess ICMP flood attack packets to ensure that its CPU works properly.

Prerequisites

Defense against ICMP flood attacks has been enabled using the **anti-attack icmp-flood enable** command.

Example

# Set the rate limit of ICMP flood attack packets to 8000 bit/s.

```
<HUAWEI> system-view
[HUAWEI] anti-attack icmp-flood enable
[HUAWEI] anti-attack icmp-flood car cir 8000
```

Related Topics

14.3.6 anti-attack icmp-flood enable

14.3.8 anti-attack tcp-syn enable

Function

The **anti-attack tcp-syn enable** command enables defense against TCP SYN flood attacks.

The **undo anti-attack tcp-syn enable** command disables defense against TCP SYN flood attacks.

The **anti-attack tcp-syn disable** command disables defense against TCP SYN flood attacks.

By default, defense against TCP SYN flood attacks is enabled.

Format

anti-attack tcp-syn enable

undo anti-attack tcp-syn enable

anti-attack tcp-syn disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An attacker sends a SYN packet to a target host to initiate a TCP connection but does not respond to the SYN-ACK sent from the target host. If the target host receives no ACK packet from the attacker, it keeps waiting for the ACK packet. A half-open connection is formed. The attacker keeps sending SYN packets, so many half-open connections are set up on the target host. This wastes a large number of resources. To prevent TCP SYN flood attacks, run the **anti-attack tcp-syn enable** command to enable defense against TCP SYN flood attacks.

The device detects TCP SYN flood attack packets after defense against TCP SYN flood attacks is enabled. If the device detects TCP SYN flood attack packets, the device limits the rate of these TCP SYN flood attack packets to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including TCP SYN flood attack packets.

Example

# Enable defense against TCP SYN flood attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack tcp-syn enable
```

Related Topics

14.3.9 anti-attack tcp-syn car

14.3.3 anti-attack enable

14.3.9 anti-attack tcp-syn car

Function

The **anti-attack tcp-syn car** command sets the rate limit at which TCP SYN packets are received.

The **undo anti-attack tcp-syn car** command restores the default rate limit at which TCP SYN packets are received.

By default, the rate limit at which TCP SYN packets are received is 155000000 bit/s.

Format

anti-attack tcp-syn car cir *cir*

undo anti-attack tcp-syn car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) at which TCP SYN packets are received.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against TCP SYN flood attacks is enabled, run the **anti-attack tcp-syn car** command to set the rate limit at which TCP SYN packets are received. If the rate of received TCP SYN attack packets exceeds the rate limit, the device discards excess TCP SYN flood attack packets to ensure that the device CPU works properly.

Prerequisites

Defense against TCP SYN flood attacks has been enabled using the **anti-attack tcp-syn enable** command.

Example

# Set the rate limit at which TCP SYN packets are received to 8000 bit/s.

```
<HUAWEI> system-view
[HUAWEI] anti-attack tcp-syn enable
[HUAWEI] anti-attack tcp-syn car cir 8000
```

Related Topics

14.3.8 anti-attack tcp-syn enable

14.3.10 anti-attack udp-flood enable

Function

The **anti-attack udp-flood enable** command enables defense against UDP flood attacks.

The **undo anti-attack udp-flood enable** command disables defense against UDP flood attacks.

The **anti-attack udp-flood disable** command disables defense against UDP flood attacks.

By default, defense against UDP flood attacks is enabled.

Format

anti-attack udp-flood enable

undo anti-attack udp-flood enable

anti-attack udp-flood disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of UDP packets to the target host in a short time, the target host is busy with these UDP packets. As a result, the target host is overloaded and cannot process normal services. To prevent UDP flood attacks, run the **anti-attack udp-flood enable** command to enable defense against UDP flood attacks.

The device detects UDP flood attack packets after defense against UDP flood attacks is enabled. The device directly discards UDP flood attack packets.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including UDP flood attack packets.

Example

# Enable defense against UDP flood attacks.

```
<HUAWEI> system-view
[HUAWEI] anti-attack udp-flood enable
```

Related Topics

14.3.3 anti-attack enable

14.3.11 display anti-attack statistics

Function

The **display anti-attack statistics** command displays statistics about attack packets of a specified type.

If no parameter is specified, the **display anti-attack statistics** command displays statistics about attack packets of all types.

Format

display anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood**]

Parameters

Parameter	Description	Value
abnormal	Displays statistics about malformed packets.	-
fragment	Displays statistics about defense against packet fragments.	-
tcp-syn	Displays statistics about defense against TCP SYN flood attacks.	-
udp-flood	Displays statistics about defense against UDP flood attacks.	-
icmp-flood	Displays statistics about defense against ICMP flood attacks.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display anti-attack statistics** command displays statistics on attack packets of the following types: malformed packet attack, packet fragment attack, TCP SYN flood attack, UDP flood attack, ICMP flood attack.

Example

# Display attack defense statistics.

```
<HUAWEI> display anti-attack statistics
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum       DropPacketNum        PassPacketNum
            (H)        (L)        (H)        (L)        (H)        (L)
-------------------------------------------------------------------------------
URPF         0          0          0          0          0          0
Abnormal     0          0          0          0          0          0
Fragment     0          0          0          0          0          0
Tcp-syn      0          58         0          0          0          58
Udp-flood    0          0          0          0          0          0
Icmp-flood   0          0          0          0          0          0
-------------------------------------------------------------------------------
```

Table 14-32 Description of the display anti-attack statistics command output

Item	Description
Packets Statistic Information	Attack defense statistics.
AntiAtkType	Attack defense type: ● URPF: URPF check (The device does not support this parameter.) ● Abnormal: defense against malformed packets ● Fragment: defense against packet fragments ● Tcp-syn: defense against TCP SYN flood attacks ● Udp-flood: defense against UDP flood attacks ● Icmp-flood: defense against ICMP flood attacks
TotalPacketNum	Total number of packets.
DropPacketNum	Number of discarded packets.
PassPacketNum	Number of forwarded packets.
(H)	Highest-order bit display.
(L)	Lowest-order bit display.

Related Topics

14.3.12 reset anti-attack statistics

14.3.12 reset anti-attack statistics

Function

The **reset anti-attack statistics** command clears attack defense statistics.

Format

reset anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood**]

Parameters

Parameter	Description	Value
abnormal	Clears statistics about defense against malformed packets.	-
fragment	Clears statistics about defense against packet fragments.	-
tcp-syn	Clears statistics about defense against TCP SYN flood attacks.	-
udp-flood	Clears statistics about defense against UDP flood attacks.	-
icmp-flood	Clears statistics about defense against ICMP flood attacks.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If no attack defense is specified, statistics about all types of attack defense are cleared.

NOTICE

The cleared statistics cannot be restored. Exercise caution when you use the command.

Example

# Clear statistics about defense against malformed packets.

```
<HUAWEI> reset anti-attack statistics abnormal
```

Related Topics

14.3.11 display anti-attack statistics

14.4 MFF Configuration Commands

14.4.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.4.2 display mac-forced-forwarding

Function

The **display mac-forced-forwarding** command displays the MFF configuration.

Format

display mac-forced-forwarding { **network-port** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
network-port	Displays network interface information.	-
vlan *vlan-id*	Displays the MFF configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mac-forced-forwarding** command displays the MFF network interface information and MFF configuration in a specified VLAN.

NOTE

When the **user-bind static** command is executed to configure a static binding entry for a non-DHCP user, at least **ip-address** and **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*] must be specified. In this case, the MFF entry that has the same IP address and VLAN ID as the static binding entry can be deleted when the static binding entry is deleted.

Example

# Display information about the MFF network interface.

```
<HUAWEI> display mac-forced-forwarding network-port
-------------------------------------------------------------------------------
VLAN ID                 Network-ports
-------------------------------------------------------------------------------
VLAN 10                 GigabitEthernet0/0/1
                    GigabitEthernet0/0/2
                    GigabitEthernet0/0/3
VLAN 100                 GigabitEthernet0/0/4
                    GigabitEthernet0/0/5
```

Table 14-33 Description of the display mac-forced-forwarding network-port command output

Item	Description
VLAN ID	ID of the VLAN that the network interface belongs to.
Network-ports	Network interface.

# Display the MFF configuration in VLAN 100.

```
<HUAWEI> display mac-forced-forwarding vlan 100
[Vlan 100] MFF host total count = 3
-------------------------------------------------------------------------------
Servers        192.168.1.2
             192.168.1.3
-------------------------------------------------------------------------------
User IP        User MAC            Gateway IP        Gateway MAC
-------------------------------------------------------------------------------
192.168.1.10   0001-0001-0001     192.168.1.254    0002-0002-0001
192.168.1.11   0001-0001-0002     192.168.1.254    0002-0002-0001
192.168.1.12   0001-0001-0003     192.168.1.252    0002-0002-0003
-------------------------------------------------------------------------------
```

Table 14-34 Description of the display mac-forced-forwarding vlan command output

Item	Description
MFF host total count	Number of users in VLAN 100.
Servers	IP addresses of servers in VLAN 100.
User IP	IP addresses of users in VLAN 100.
User MAC	MAC addresses of users in VLAN 100.
Gateway IP	Gateway IP address.
Gateway MAC	Gateway MAC address.

Related Topics

14.4.5 mac-forced-forwarding enable

14.4.6 mac-forced-forwarding gateway-detect

14.4.9 mac-forced-forwarding network-port

14.4.11 mac-forced-forwarding server

14.4.12 mac-forced-forwarding static-gateway

14.4.13 mac-forced-forwarding user-detect transparent

14.4.3 mac-forced-forwarding arp-trigger

Function

The **mac-forced-forwarding arp-trigger** command enables an EAN to add or update an MFF entry when receiving an ARP packet from a user.

The **mac-forced-forwarding arp-trigger** command disables an EAN from adding or updating an MFF entry when receiving an ARP packet from a user.

By default, the EAN does not add or update an MFF entry when receiving an ARP packet from a user.

Format

mac-forced-forwarding arp-trigger

undo mac-forced-forwarding arp-trigger

Parameters

N/A

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a data center, users and virtual machine (VM) servers are isolated at Layer 2 on EAN devices using MFF. If a VM connects to another EAN and does not send DHCP request packets after migrating between servers, the backup binding table may exist on the new EAN device and the original EAN may still reserve the MFF entry. This cannot ensure security of Layer 2 isolation and Layer 3 communication between users and servers. Run the **mac-forced-forwarding arp-trigger** command on the new EAN to enable it to check binding entries when receiving an ARP packet from the user. If an entry matches the user, the EAN updates the MFF entry. If no entry matches the user, the EAN adds a new entry. The EAN broadcasts the ARP packet to all network interfaces when receiving the first ARP packet regardless of whether the user entry exists.

Prerequisite

MFF has been enabled in the system view and VLAN view using the **mac-forced-forwarding enable** command.

Example

# Enable the EAN to add or update the MFF entries when receiving an ARP packet from a user in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding arp-trigger
```

Related Topics

14.4.5 mac-forced-forwarding enable

14.4.4 mac-forced-forwarding dumb-terminal-compatible

Function

The **mac-forced-forwarding dumb-terminal-compatible** command configures a device to forward the ARP packets from the gateway to dumb terminals.

The **undo mac-forced-forwarding dumb-terminal-compatible** command disables a device from forwarding the ARP packets from the gateway to dumb terminals.

By default, a device does not forward the ARP packets from gateway to dumb terminals.

Format

mac-forced-forwarding dumb-terminal-compatible

undo mac-forced-forwarding dumb-terminal-compatible

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MFF device connects to dumb terminals (which do not actively send ARP request packets or send ARP request packets at a long interval), the MFF device must transparently transmit the ARP packets from gateway to dumb terminals after the MFF entries are aged out; otherwise, the user ARP entries on gateway are aged out and user services are interrupted. Therefore, when the MFF device connects to dumb terminals, the MFF device needs to be configured to transparently transmit the ARP packets from gateway to dumb terminals.

Prerequisites

Global MFF has been enabled using the **14.4.5 mac-forced-forwarding enable** command.

Precautions

After the MFF device is configured to transparently transmit ARP packets to dumb terminals, run the **14.4.12 mac-forced-forwarding static-gateway** command to configure an IP address for the static gateway; otherwise, this function does not take effect.

After this function is enabled, the MFF device searches the static binding table when receiving ARP request packets from the gateway (configured using the **14.11.12 user-bind static** command):

- If the outbound interface is found in the static binding table, the device forwards the ARP request packets through this interface.
- If the outbound interface is not found in the static binding table, the device broadcasts the ARP request packets in the VLAN. In this situation, all users in the VLAN can receive the ARP packets.

Example

# Configure a device to transparently transmit ARP packets from gateway to dumb terminals in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mac-forced-forwarding enable
[HUAWEI] vlan 100
```

```
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding dumb-terminal-compatible
```

Related Topics

14.4.5 mac-forced-forwarding enable

14.4.5 mac-forced-forwarding enable

Function

The **mac-forced-forwarding enable** command enables MFF.

The **undo mac-forced-forwarding enable** command disables MFF.

By default, MFF is disabled.

Format

mac-forced-forwarding enable

undo mac-forced-forwarding enable

Parameters

None

Views

System view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Many networks require that the gateway monitor data traffic and isolate users. MFF isolates users at Layer 2 and connects users at Layer 3 on the same network segment. MFF enables traffic to be forwarded through the gateway. This implements traffic monitoring and accounting and ensures network security.

Precautions

You can run the **mac-forced-forwarding enable** command in the VLAN view and perform other configurations only after you enable MFF globally in the system view.

After MFF is disabled in the system view, other MFF configurations are automatically deleted.

MFF cannot be enabled in a VLAN where the super VLAN or VLANIF interface is configured.

MFF cannot be enabled in a sub-VLAN where the super VLAN and VLANIF interface are configured.

The MFF function is implemented based on ARP proxy, whereas the EAI function is implemented based on ARP request packet forwarding. Therefore, the two functions conflict with each other. If you have enabled both MFF and EAI in the same VLAN, the MFF function takes effect.

NOTE

When you enable MFF, if ACL resources are insufficient, the MFF function does not take effect.

MFF cannot be configured in the super-VLAN.

When DHCP relay is configured in a super VLAN, MFF cannot be enabled in its sub-VLANs.

Example

# Enable MFF in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] mac-forced-forwarding enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
```

Related Topics

14.4.2 display mac-forced-forwarding

14.4.6 mac-forced-forwarding gateway-detect

Function

The **mac-forced-forwarding gateway-detect** command enables timed gateway detection and sets the gateway detection interval.

The **undo mac-forced-forwarding gateway-detect** command disables timed gateway detection.

By default, timed gateway detection is enabled and the default gateway detection interval is 30s.

Format

mac-forced-forwarding gateway-detect [**interval** *interval-time*]

undo mac-forced-forwarding gateway-detect

Parameters

Parameter	Description	Value
interval *interval-time*	Indicates the gateway detection interval.	The value is an integer that ranges from 30 to 17280, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a practical network, services may be interrupted for a long time because the MFF-enabled device cannot immediately detect the gateway MAC address change. Timed gateway detection can solve this problem. After the detection function is enabled (enabled by default), the MFF-enabled device scans recorded gateway information every *interval-time* seconds. For each gateway recorded, the MFF-enabled device uses user information to construct an ARP request packet and sends it to the network interface. The MFF-enabled device then learns the gateway MAC address from the ARP reply packet. If the gateway MAC address changes, the MFF-enabled device immediately updates the gateway information and broadcasts gratuitous ARP packets to users. Users can update the gateway address.

Prerequisites

MFF has been enabled in a VLAN using the **mac-forced-forwarding enable** command.

Precautions

When detecting multiple gateway addresses, the MFF-enabled device sends an ARP reply packet with the first gateway address by default.

After MFF is enabled, timed gateway detection does not take effect if no ARP request packet is received from the user or gateway or if no user is authorized by the DHCP server to access the network.

If a gateway fails, traffic between users will be blocked. To avoid this situation, the device considers a gateway invalid if it does not receive a response from the gateway after five detection attempts. The device then deletes the MAC address entry of the invalid gateway.If the gateway detection interval is changed during a detection, the number of detection times is accumulated.

Example

# Enable timed gateway detection in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mac-forced-forwarding enable
[HUAWEI-vlan10] mac-forced-forwarding gateway-detect
```

Related Topics

14.4.2 display mac-forced-forwarding

14.4.5 mac-forced-forwarding enable

14.4.7 mac-forced-forwarding igmp-query discard

Function

The **mac-forced-forwarding igmp-query discard** command configures an MFF-enabled device to discard the IGMP Query messages from users when both MFF and IGMP snooping are enabled in a VLAN.

The **undo mac-forced-forwarding igmp-query discard** command disables an MFF-enabled device from discarding the IGMP Query messages from users when both MFF and IGMP snooping are enabled in a VLAN.

By default, an MFF-enabled device does not discard the IGMP Query messages from users when both MFF and IGMP snooping are enabled in a VLAN.

Format

mac-forced-forwarding igmp-query discard

undo mac-forced-forwarding igmp-query discard

Parameters

None.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

After MFF and IGMP snooping are enabled in a VLAN, the IGMP Query messages are broadcast in the VLAN. To prevent IGMP Query message broadcasting, use the **mac-forced-forwarding igmp-query discard** command.

Example

# Configure an MFF-enabled device to discard the IGMP Query messages from users in VLAN10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mac-forced-forwarding igmp-query discard
```

14.4.8 mac-forced-forwarding ipv6-isolate

Function

The **mac-forced-forwarding ipv6-isolate** command configures the user-side inbound interface on a device to discard IPv6 packets.

The **undo mac-forced-forwarding ipv6-isolate** command disables a device from discarding IPv6 packets from users.

By default, the user-side inbound interface on a device does not discard IPv6 packets from users.

Format

mac-forced-forwarding ipv6-isolate

undo mac-forced-forwarding ipv6-isolate

Parameters

None.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **mac-forced-forwarding ipv6-isolate** command is used, the user-side inbound interface on a device discards the IPv6 packets from users to prevent IPv6 packets from being broadcast on the VLAN. If the device does not discard IPv6 packets, users can learn the MAC addresses of each other, which makes MFF user isolation function invalid.

Prerequisites

The MFF function has been enabled in the system view and the VLAN view.

The VLAN contains at least one network-side interface.

Example

# Configure the user-side inbound interface on a device to discard IPv6 packets from users.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding ipv6-isolate
```

Related Topics

14.4.5 mac-forced-forwarding enable

14.4.9 mac-forced-forwarding network-port

Function

The **mac-forced-forwarding network-port** command configures an interface as a network interface.

The **undo mac-forced-forwarding network-port** command restores the interface to be a user interface.

By default, an interface is a user interface.

Format

mac-forced-forwarding network-port

undo mac-forced-forwarding network-port

Parameters

None

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make MFF in a VLAN effective, ensure that at least one network interface belongs to the VLAN. Therefore, configure network interfaces for MFF.

The interface that is connected to the gateway and other network devices is configured as a network interface.

Precautions

MFF has been enabled in the system view using the **mac-forced-forwarding enable** command. Regardless of whether MFF is enabled in the VLAN that an interface belongs to, the interface can be configured as a network interface.

Multiple interfaces can be configured as network interfaces.

Example

# Configure GE0/0/1 as a network interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] mac-forced-forwarding network-port
Info: This operation may take a few seconds. Please wait for a moment.....
```

Related Topics

14.4.2 display mac-forced-forwarding

14.4.5 mac-forced-forwarding enable

14.4.10 mac-forced-forwarding network-port-arp-trigger

Function

The **mac-forced-forwarding network-port-arp-trigger** command enables the network interface on an EAN to delete an MFF entry when the network port receives an ARP packet.

The **undo mac-forced-forwarding network-port-arp-trigger** command disables the network interface on an EAN from deleting an MFF entry when the network port receives an ARP packet.

By default, the network interface on an EAN does not delete the MFF entry when receiving an ARP packet.

Format

mac-forced-forwarding network-port-arp-trigger

undo mac-forced-forwarding network-port-arp-trigger

Parameters

N/A

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a data center, users and VM servers are isolated at Layer 2 on EAN devices using MFF. If a VM connects to another EAN after migrating between servers, and the binding table on the original EAN is not aged out, the original EAN considers the VM an MFF host. If an attacker accesses users or sends ARP request packets using the IP address and MAC address of the VM, the original EAN allows the request. Attacks are not defended. After you run the **mac-forced-forwarding network-port-arp-trigger** command on the original EAN, the original EAN determines that the VM has migrated to another EAN and deletes the MFF entry mapping the VM when receiving ARP packets from this VM.

Prerequisites

MFF has been enabled in the system view and VLAN view using the **mac-forced-forwarding enable** command.

Example

# Enable the network interface on an EAN to delete an MFF entry when receiving an ARP packet.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding network-port-arp-trigger
```

Related Topics

14.4.5 mac-forced-forwarding enable

14.4.11 mac-forced-forwarding server

Function

The **mac-forced-forwarding server** command configures the IP address for a server on the MFF network.

The **undo mac-forced-forwarding server** command deletes the configured IP address of a server.

By default, no IP address is configured for servers.

Format

mac-forced-forwarding server *server-ip* &<1–10>

undo mac-forced-forwarding server { *server-ip* | **all** }

Parameters

Parameter	Description	Value
server-ip	Specifies the IP address for a server.	The value is in dotted decimal notation. **NOTE** This IP address must be a class A, B, or C address. If the IP address is a class A address, it cannot be in the format 0.x.x.x.
all	Specifies IP addresses for all servers.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to the gateway, application servers such as the DHCP, multicast, or another server may be deployed on a network. You can configure IP addresses for application servers and set a list of accessible application servers on the MFF-enabled device.

- When a network interface on the MFF-enabled device receives an ARP request from a specified application server, the MFF-enabled device responds with the user MAC address by default. The packets sent from the server to the user are directly forwarded without passing through the gateway.
- If the MFF-enabled device is configured to transparently transmit ARP request packets, the device responds with the gateway MAC address. The packets sent from the server to the user are forwarded through the gateway.

Prerequisites

MFF has been enabled in a VLAN using the **mac-forced-forwarding enable** command.

Precautions

When the number of configured servers reaches the upper limit 10, run the **undo mac-forced-forwarding server** { *server-ip* | **all** } command to delete unneeded servers before you configure new servers.

NOTE

This command is required only when the application servers and clients are in the same VLAN.

Example

# Configure IP address 192.168.1.2 for a server in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding server 192.168.1.2
```

Related Topics

14.4.2 display mac-forced-forwarding

14.4.5 mac-forced-forwarding enable

14.4.12 mac-forced-forwarding static-gateway

Function

The **mac-forced-forwarding static-gateway** command configures a static gateway IP address in a VLAN.

The **undo mac-forced-forwarding static-gateway** command cancels the configuration.

By default, no static gateway IP address is configured in a VLAN.

Format

mac-forced-forwarding static-gateway *ip-address* &<1-16>

undo mac-forced-forwarding static-gateway { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the static gateway IP address in a VLAN. A maximum of 16 static gateway IP addresses in a VLAN can be specified in this command.	The value is in dotted decimal notation. **NOTE** This IP address must be a class A, B, or C address. If the IP address is a class A address, it cannot be in the format 0.x.x.x.
all	Deletes all static gateway IP addresses in the VLAN.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The static gateway is applicable when users are configured with static IP addresses. These users cannot dynamically obtain gateway information through DHCP packets. In this case, configure a static gateway address for each VLAN. After you run the **mac-forced-forwarding static-gateway** command, the users that are not authorized by the DHCP server can use the static gateway address to access the network. The users that are authorized by the DHCP server can still access the original gateway.

Prerequisites

Global MFF has been enabled using the **mac-forced-forwarding enable** command.

Precautions

If a static gateway IP address is changed, users will fail to access the network. The MAC address in the ARP table on the client belongs to the old gateway. After a new gateway is configured, the ARP entry on client is not updated immediately (that is, the MAC address in ARP table is not updated to the new gateway's MAC address). Therefore, the user cannot access the network.

Example

# Configure static gateway IP address 10.1.1.10 in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] mac-forced-forwarding enable
[HUAWEI-vlan100] mac-forced-forwarding static-gateway 10.1.1.10
```

Related Topics

14.4.2 display mac-forced-forwarding

14.4.5 mac-forced-forwarding enable

14.4.13 mac-forced-forwarding user-detect transparent

Function

The **mac-forced-forwarding user-detect transparent** command enables transparent transmission of ARP request packets.

The **undo mac-forced-forwarding user-detect transparent** command disables transparent transmission of ARP request packets.

By default, transparent transmission of ARP request packets is disabled.

Format

mac-forced-forwarding user-detect transparent

undo mac-forced-forwarding user-detect transparent

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MFF networking, if the gateway performs accounting for users based on the online duration, the gateway must know whether a user is online at a specified moment. By default, the MFF-enabled device sends ARP reply packets in response to ARP request packets sent from the gateway. The MFF-enabled device can always send ARP reply packets as long as the MFF entry is not aged out. As a result, the gateway always considers users online even if they have gone offline.

To solve this problem, configure the MFF-enabled device to transparently transmit ARP request packets sent from the gateway to the user. Then the MFF-enabled device does not respond to the ARP packets. If the gateway does not receive the ARP reply packet from a user, the gateway considers that the user has gone offline. The gateway can monitor the user status in a timely manner and correctly perform accounting.

Prerequisites

Global MFF has been enabled using the **mac-forced-forwarding enable** command.

Precautions

In other scenarios, use the default configuration.

Example

# Enable transparent transmission of ARP request packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] mac-forced-forwarding enable
[HUAWEI-vlan10] mac-forced-forwarding user-detect transparent
```

Related Topics

14.4.2 display mac-forced-forwarding

14.4.5 mac-forced-forwarding enable

14.5 Traffic Suppression and Storm Control Configuration Commands

14.5.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.5.2 broadcast-suppression (interface view)

Function

The **broadcast-suppression** command sets the maximum traffic rate of broadcast packets that can pass through an interface.

The **undo broadcast-suppression** command restores the default maximum traffic rate of broadcast packets that can pass through an interface.

By default, the rate of broadcast packets is suppressed by bandwidth percentage, and the percentage rate limit is 10%.

Format

broadcast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* }(Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support **cir** *cir-value* [**cbs** *cbs-value*].)

undo broadcast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **4.1.15 display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer. It ranges from 0 to 80 for 40GE interfaces and 0 to 100 for other types of interfaces.

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer. For an Ethernet interface, the value ranges from 0 to 100000; for a GE interface, the value ranges from 0 to 1000000; for a MultiGE interface, the value ranges form 0 to X, X indicates the negotiated bandwidth; for an XGE interface, the value ranges from 0 to 10000000; for a 40GE interface, the value ranges from 0 to 40000000; for a port group, the value ranges from 0 to 100000000, in kbit/s. **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: ● Ethernet interface: 0 to 148810 ● GE interface: 0 to 1488100 ● MultiGE interface: 0 to X. X indicates the negotiated bandwidth ● XGE interface: 0 to 14881000 ● 40GE interface: 0 to 59524000 ● Port group: 0 to 148810000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **broadcast-suppression** command to set the threshold of broadcast traffic that an interface allows to pass through. When the broadcast traffic rate reaches the rate limit, the system discards excess broadcast packets to control the traffic rate in a proper range.

Precautions

If the rate limit in bit/s is set for a type of packets on an interface, the rate limit in pps cannot be set for other types of packets on the same interface. In a similar manner, if the rate limit in pps is set for a type of packets on an interface, the rate limit in bit/s cannot be set for other types of packets on the same interface.

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet rate limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

Example

# Set the broadcast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] broadcast-suppression packets 100000
```

Related Topics

14.5.5 display flow-suppression interface

14.5.9 multicast-suppression (interface view)

14.5.16 unicast-suppression (interface view)

14.5.3 broadcast-suppression block outbound

Function

The **broadcast-suppression block outbound** command blocks outgoing broadcast packets on an interface.

The **undo broadcast-suppression block outbound** command unblocks outgoing broadcast packets on an interface.

By default, an interface does not block outgoing broadcast packets.

Format

broadcast-suppression block outbound

undo broadcast-suppression block outbound

Parameters

None

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

After an interface receives a broadcast packet, it broadcasts the packet to all users in the same VLAN. This may cause information leak. For example, if an unauthorized user is connected to an interface in a VLAN, an unauthorized user obtains a host's address from broadcast packets and uses the address to attack the host. To prevent information leak, use the **broadcast-suppression block outbound** command to block outgoing broadcast packets on an interface if users connected to the interface do not need to receive broadcast packets. For example, if users on an interface seldom change and require high security, you can use this command on the interface.

Precautions

The **broadcast-suppression block outbound** command is applicable only to interfaces on which users do not need to receive broadcast packets. This command will affect network operations if it is used on an interface where users need to receive broadcast packets.

Traffic suppression can be configured for incoming and outgoing packets on an interface, and the configurations are independent of each other. On an interface, you can use the **broadcast-suppression** command to limit the rate of incoming broadcast packets and use the **broadcast-suppression block outbound** command to block outgoing broadcast packets.

Example

# Block outgoing broadcast packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] broadcast-suppression block outbound
```

Related Topics

14.5.2 broadcast-suppression (interface view)

14.5.9 multicast-suppression (interface view)

14.5.10 multicast-suppression block outbound

14.5.16 unicast-suppression (interface view)

14.5.17 unicast-suppression block outbound

14.5.4 broadcast-suppression (VLAN view)

Function

The **broadcast-suppression** command sets the rate limit for broadcast packets in a VLAN.

The **undo broadcast-suppression** command cancels broadcast packets suppression in a VLAN.

By default, broadcast packets are not suppressed in a VLAN.

Format

broadcast-suppression *threshold-value*

undo broadcast-suppression

Parameters

Parameter	Description	Value
threshold-value	Specifies the rate limit of broadcast packets.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

After you run the **broadcast-suppression** command, the device limits the rate of broadcast packets based on the configured rate limit. If the rate limit is exceeded, the device discards excess broadcast packets.

Example

# Set the rate limit to 1000 kbit/s for broadcast packets in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] broadcast-suppression 1000
```

14.5.5 display flow-suppression interface

Function

The **display flow-suppression interface** command displays the traffic suppression configuration on an interface.

Format

display flow-suppression interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can display the traffic suppression for broadcast, unknown multicast, and unknown unicast packets on the interface, including rate limiting mode and rate limit value.

Example

# Display the traffic suppression configuration on GE0/0/1.

```
<HUAWEI> display flow-suppression interface gigabitethernet 0/0/1
 storm type          rate mode    set rate value
-------------------------------------------------------------------------------
 unknown-unicast     percent      percent: 90%
 multicast           percent      percent: 90%
 broadcast           percent      percent: 90%

-------------------------------------------------------------------------------
```

Table 14-35 Description of the display flow-suppression interface command output

Item	Description
storm type	Traffic type. Broadcast traffic, unknown multicast traffic, and unknown unicast traffic can be suppressed.
rate mode	Type of the rate limit. ● pps: packet mode ● percent: percentage mode
set rate value	Configured rate limit. The rate can be set by the following commands: ● **broadcast-suppression** ● **multicast-suppression** ● **unicast-suppression**

Related Topics

14.5.2 broadcast-suppression (interface view)

14.5.9 multicast-suppression (interface view)

14.5.16 unicast-suppression (interface view)

14.5.6 display storm-control

Function

The **display storm-control** command displays information about storm control on an interface.

Format

display storm-control [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can display the storm control for broadcast, unknown multicast, and unknown unicast packets on the interface, such as packet mode, storm control action, and packet status.

Example

# Display information about storm control on GE0/0/1.

```
<HUAWEI> display storm-control interface gigabitethernet 0/0/1
PortName     Type      Rate       Mode Action   Punish-  Trap Log Int Last-
                 (Min/Max)             Status              Punish-Time
-------------------------------------------------------------------------------
GE0/0/1      Multicast 1000      Pps  Block    Normal   Off  On  90  -
                  /2000
GE0/0/1      Broadcast 1000      Pps  Block    Normal   Off  On  90  -
                  /2000
GE0/0/1      Unicast   1000      Pps  Block    Normal   Off  On  90  -
                  /2000
```

Table 14-36 Description of the display storm-control command output

Item	Description
PortName	Interface name.
Type	Packet type. ● Broadcast packets ● Unknown Multicast packets ● Unknown Unicast packets To configure the type of packets on which storm control is performed, run the **storm-control** command.
Rate	● Min: lower rate threshold ● Max: upper rate threshold To configure the rates, run the **storm-control** command.

Item	Description
Mode	Storm control mode. - Kbps: CIR in kbit/s - Pps: packets in pps - %: percentage in % To configure the storm control mode, run the **storm-control** command.
Action	Storm control action. - Block: blocks packets. - Err-down: shuts down the interface. - None: No action is configured. To configure a storm control action, run the **storm-control action** command.
Punish-Status	Status of the interface. - Block: When the rate of receiving packets is greater than the value of **MaxRate** and the storm control action is **block**, the status of the interface is **block**. - Normal: Packets are normally forwarded. - Err-down: When the rate of receiving packets is greater than the value of **MaxRate** and the storm control action is **error-down**, the status of the interface is **error-down**.
Trap	Whether the alarm function for storm control is enabled. - on: The alarm function for storm control is enabled. - off: The alarm function for storm control is disabled. To configure the alarm function for storm control, run the **storm-control enable trap** command.
Log	Whether the log function for storm control is enabled. - on: The log function for storm control is enabled. - off: The log function for storm control is disabled. To configure the alarm function for storm control, run the **storm-control enable log** command.
Int	Interval for detecting storms, in seconds. The default value is 5.
Last-Punish-Time	Last time storm control is performed.

Related Topics

14.5.11 storm-control

14.5.12 storm-control action

14.5.13 storm-control enable

14.5.14 storm-control interval

14.5.7 icmp rate-limit

Function

The **icmp rate-limit** command sets the rate threshold of ICMP packets.

The **undo icmp rate-limit** command restores the default rate threshold of ICMP packets.

By default, the rate limits of ICMP packets in the system and on an interface depend on the product model. The value is 128 on the S6720EI, S6720S-EI, S5720HI, and S5720EI, and 190 on the other models, in pps.

Format

icmp rate-limit { **total** | **interface** *interface-type interface-number1* [**to** *interface-number2*] } **threshold** *threshold-value*

undo icmp rate-limit { **total** | **interface** *interface-type interface-number1* [**to** *interface-number2*] }

Parameters

Parameter	Description	Value
total	Specifies the total rate threshold in the system.	-

Parameter	Description	Value
interface *interface-type interface-number1* **to** *interface-number2*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● **to** *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces.	-
threshold *threshold-value*	Specifies the rate threshold of ICMP packets.	The value ranges from 0 to 1000, in pps. **NOTE** The value 0 indicates that the rate of ICMP packets is not limited.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

A network often undergoes ICMP packet attacks. If a switch receives a large number of broadcast ICMP request packets on user-side interfaces, these packets are sent to the switch CPU for processing. Then the CPU usage becomes high, affecting other services on the switch. You can use the **icmp rate-limit** command to prevent the switch from being attacked by ICMP packets.

After the rate limit function is configured for ICMP packets on an interface, the system automatically discards excess ICMP packets when the number of ICMP packets sent by an interface every second exceeds the rate threshold.

Precautions

Before setting the rate threshold of ICMP packets, use the **14.5.8 icmp rate-limit enable** command to enable the rate limit function for ICMP packets.

Example

# Set the rate threshold of ICMP packets on GE0/0/1 to GE0/0/5 to 20 pps.

```
<HUAWEI> system-view
[HUAWEI] icmp rate-limit interface gigabitethernet 0/0/1 to 0/0/5 threshold 20
```

Related Topics

14.5.8 icmp rate-limit enable

14.5.8 icmp rate-limit enable

Function

The **icmp rate-limit enable** command enables the traffic suppression function for ICMP packets.

The **undo icmp rate-limit enable** command disables the traffic suppression function for ICMP packets.

By default, the traffic suppression function for ICMP packets is disabled.

Format

icmp rate-limit enable

undo icmp rate-limit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Attackers may send a large number of ICMP packets to attack a network. If the device sends all the received ICMP packets to the CPU for processing, a lot of CPU usage resources are occupied and other services may be abnormal. To prevent ICMP packet attacks, you can configure the device to suppress ICMP packets.

Before configuring traffic suppression for ICMP packets on an interface, run the **undo icmp-reply fast** command to disable the ICMP reply fast function.

Example

# Enable the traffic suppression function for ICMP packets.

```
<HUAWEI> system-view
[HUAWEI] icmp rate-limit enable
```

Related Topics

14.5.7 icmp rate-limit

14.5.9 multicast-suppression (interface view)

Function

The **multicast-suppression** command sets the maximum traffic volume of unknown multicast packets that can pass through an interface.

The **undo multicast-suppression** allows all unknown multicast packets to pass.

By default, unknown multicast packets are not suppressed.

Format

multicast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* } (Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support **cir** *cir-value* [**cbs** *cbs-value*].)

undo multicast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **4.1.15 display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer. It ranges from 0 to 80 for 40GE interfaces and 0 to 100 for other types of interfaces.

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer. For an Ethernet interface, the value ranges from 0 to 100000; for a GE interface, the value ranges from 0 to 1000000; for a MultiGE interface, the value ranges form 0 to X, X indicates the negotiated bandwidth; for an XGE interface, the value ranges from 0 to 10000000; for a 40GE interface, the value ranges from 0 to 40000000; for a port group, the value ranges from 0 to 100000000, in kbit/s. **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: ● Ethernet interface: 0 to 148810 ● GE interface: 0 to 1488100 ● MultiGE interface: 0 to X. X indicates the negotiated bandwidth ● XGE interface: 0 to 14881000 ● 40GE interface: 0 to 59524000 ● Port group: 0 to 148810000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an increasing number of unknown multicast packets are transmitted on a network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **multicast-suppression** command to set the threshold of unknown multicast traffic that an interface allows to pass through. When the unknown multicast traffic volume exceeds the threshold, the system discards the excess unknown multicast packets to control the traffic volume of unknown multicast packets to a proper range.

Precautions

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

Example

# Set the maximum unknown multicast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-suppression packets 100000
```

Related Topics

14.5.2 broadcast-suppression (interface view)

14.5.5 display flow-suppression interface

14.5.16 unicast-suppression (interface view)

14.5.10 multicast-suppression block outbound

Function

The **multicast-suppression block outbound** command configures an interface to block outgoing unknown multicast packets.

The **undo multicast-suppression block outbound** command cancels the configuration.

By default, outgoing unknown multicast packets are not blocked on an interface.

Format

multicast-suppression block outbound

undo multicast-suppression block outbound

Parameters

None

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface receives unknown multicast packets, the interface broadcasts the packets to all users in the same VLAN. This may cause information leak. For example, if an unauthorized user is connected to an interface in a VLAN, the unauthorized user obtains the host address in unknown multicast packets by listening to unknown multicast packets and uses the host address to attack the host. To prevent information leak, use the **multicast-suppression block outbound** command to block outgoing unknown multicast packets on an interface if users connected to the interface do not need to receive unknown multicast packets.

Precautions

The **multicast-suppression block outbound** command is applicable only to interfaces where users do not need to receive unknown multicast packets. This command will affect network operations if it is used on an interface where users need to receive unknown multicast packets.

Traffic suppression can be configured for incoming and outgoing packets on an interface, and the configurations are independent of each other. On an interface, you can use the **multicast-suppression** command to limit the rate of incoming unknown multicast packets and use the **multicast-suppression block outbound** command to block outgoing unknown multicast packets.

Example

# Block outgoing unknown multicast packets onGE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] multicast-suppression block outbound
```

Related Topics

14.5.2 broadcast-suppression (interface view)

14.5.3 broadcast-suppression block outbound

14.5.9 multicast-suppression (interface view)

14.5.16 unicast-suppression (interface view)

14.5.17 unicast-suppression block outbound

14.5.11 storm-control

Function

The **storm-control** command enables storm control for broadcast packets, unknown multicast packets, and unknown unicast packets on an interface.

The **undo storm-control** command disables storm control.

By default, storm control is disabled on interfaces.

Format

storm-control { **broadcast** | **multicast** | **unicast** } **min-rate** *min-rate-value* **max-rate** *max-rate-value*

storm-control { **broadcast** | **multicast** | **unicast** } **min-rate cir** *min-rate-value-cir* **max-rate cir** *max-rate-value-cir* (Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.)

storm-control { **broadcast** | **multicast** | **unicast** } **min-rate percent** *min-rate-value-percent* **max-rate percent** *max-rate-value-percent* (Only the S5720EI, S5720HI, S6720S-EI, and S6720EI support this command.)

undo storm-control { **broadcast** | **multicast** | **unicast** | **all-packets** }

Parameters

Parameter	Description	Value
broadcast	Enables storm control for broadcast packets.	-
multicast	Enables storm control for unknown multicast packets.	-
unicast	Enables storm control for unknown unicast packets.	-

Parameter	Description	Value
min-rate *min-rate-value*	Specifies the lower threshold in packet rate limit mode. If the value of *min-rate-value* is specified, packets received by an interface are forwarded when the rate of receiving packets is smaller than the value of *min-rate-value* in storm detection.	The value is an integer, in pps. The value range is as follows: ● Ethernet interface: 1 to 148810 ● GE interface: 1 to 1488100 ● MultiGE interface: 1 to X. X indicates the negotiated bandwidth ● XGE interface: 1 to 14881000 ● 40 GE interface: 1 to 59524000 ● Port group: 1 to 148810000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group.

Parameter	Description	Value
min-rate cir *min-rate-value-cir*	Specifies the lower threshold in byte rate limit mode. If the value of *min-rate-value-cir* is specified, packets received by an interface are forwarded when the rate of receiving packets is smaller than the value of *min-rate-value-cir* in storm detection.	The value is an integer, in kbit/s. The value range is as follows: ● Ethernet interface: 1 to 100000 ● GE interface: 1 to 1000000 ● XGE interface: 1 to 10000000 ● 40 GE interface: 1 to 40000000 ● Port group: 1 to 100000000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group.
min-rate percent *min-rate-value-percent*	Specifies the lower threshold in percentage rate limit mode. If the value of *min-rate-value-percent* is specified, packets received by an interface are forwarded when the rate of receiving packets is lower than the value of *min-rate-value-percent* in storm detection.	The value is an integer, in percentage. The value ranges from 1 to 100.

Parameter	Description	Value
max-rate *max-rate-value*	Specifies the upper threshold in packet rate limit mode. Storm control is performed on an interface when the rate of receiving packets on the interface is greater than the value of *max-rate-value* in storm detection.	The value is an integer, in pps. The value range is as follows: ● Ethernet interface: 1 to 148810 ● GE interface: 1 to 1488100 ● MultiGE interface: 1 to X. X indicates the negotiated bandwidth ● XGE interface: 1 to 14881000 ● 40 GE interface: 1 to 59524000 ● Port group: 1 to 148810000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group.

Parameter	Description	Value
max-rate cir *max-rate-value-cir*	Specifies the upper threshold in byte rate limit mode. If the value of *max-rate-value-cir* is specified, storm control is performed on an interface when the rate of receiving packets on the interface is greater than the value of *max-rate-value-cir* in storm detection.	The value is an integer, in kbit/s. The value range is as follows: ● Ethernet interface: 1 to 100000 ● GE interface: 1 to 1000000 ● XGE interface: 1 to 10000000 ● 40 GE interface: 1 to 40000000 ● Port group: 1 to 100000000 **NOTE** The given value range for port groups is the maximum one. The actually delivered value range depends on the minimum value range allowed by member interfaces in a port group.
max-rate percent *max-rate-value-percent*	Specifies the upper threshold in percentage rate limit mode. If the value of *max-rate-value-percent* is specified, storm control is performed on an interface when the rate of receiving packets on the interface is greater than the value of *max-rate-value-percent* in storm detection.	The value is an integer, in percentage. The value ranges from 1 to 100.
all-packets	Disables storm control for all the broadcast packets, unknown multicast packets, and unknown unicast packets.	-

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the average rate of receiving packets on an interface is greater than the value of *max-rate-value*, *max-rate-value-cir*, or *max-rate-value-percent* in storm detection, storm control is performed on the packets.

NOTE

The storm detection interval can be set using the **14.5.14 storm-control interval** command.

Storm control actions include **block** and **shutdown**, which can be configured using the **14.5.12 storm-control action** command. If the action is **block** on an interface, packets on the interface are unblocked when the rate of receiving packets on the interface is smaller than the value of *min-rate-value*, *min-rate-value-cir* or *min-rate-value-percent*; if the action is **shutdown** on an interface, run the **undo shutdown** command to enable the interface.

Precautions

When detecting unicast packets, a switch does not distinguish unknown unicast packets from known unicast packets. The packet rate detected is the sum of the rates of unknown and known unicast packets. When the storm control action is block, the switch blocks only the unknown unicast packets. This rule also applies to multicast packets.

You cannot configure storm control and traffic suppression simultaneously on an interface. For example, if you configure traffic suppression for broadcast packets on an interface, then you cannot configure storm control for broadcast packets simultaneously on the interface.

After storm control is configured on an interface, the device does not check the VLAN IDs of packets when performing check on the packets. That is, the device performs storm control on all the packets no matter whether the VLANs of the packets are allowed by the interface.

Example

# Perform storm control on broadcast packets received on GE0/0/1. In the storm detection interval, perform storm control on packets when the rate of receiving packets on an interface is greater than 8000 pps and forward packets when the rate of receiving packets on an interface is smaller than 5000 pps.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control broadcast min-rate 5000 max-rate 8000
```

Related Topics

14.5.6 display storm-control

14.5.12 storm-control action

14.5.13 storm-control enable

14.5.14 storm-control interval

14.5.12 storm-control action

Function

The **storm-control action** sets the storm control action to **error-down** or **block**.

The **undo storm-control action** command cancels the configuration.

By default, no storm control action is configured.

Format

storm-control action { **block** | **error-down** }

undo storm-control action

Parameters

Parameter	Description	Value
block	Blocks packets.	-
error-down	Shuts down an interface.	-

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

You can control data packets and prevent flooding by running the **storm-control action** command to configure a storm control action and the **storm-control** command to set the upper and lower thresholds.

In a storm detection interval, when the average rate of receiving broadcast packets, unknown multicast packets, and unknown unicast packets is greater than the value of the specified upper threshold, packets are blocked or the interface is shut down.

If the storm control action on an interface is **block**, the interface is restored when the traffic falls below the lower threshold.

If the storm control action is **error-down**, the interface can be recovered using either of the following methods:

- Manual recovery (after an Error-Down event occurs):

If a few interfaces need to be recovered, run the **shutdown** and **undo shutdown** commands in the interface view. Alternatively, run the **restart** command in the interface view to restart the interfaces.

- Automatic recovery (before an Error-Down event occurs):

  If a large number of interfaces need to be recovered, manual recovery is time consuming and some interfaces may be omitted. To avoid this problem, run the **error-down auto-recovery** **cause storm-control interval** *interval-value* command in the system view to enable automatic interface recovery and set the recovery delay time. Run the **display error-down recovery** command to view information about automatic interface recovery.

  NOTE

  This method does not take effect on interfaces that are already in Error-Down state. It is effective only on interfaces that enter the Error-Down state after this configuration is complete.

Precautions

When detecting unicast packets, a switch does not distinguish unknown unicast packets from known unicast packets. The packet rate detected is the sum of the rates of unknown and known unicast packets. When the storm control action is block, the switch blocks only the unknown unicast packets. This rule also applies to multicast packets.

Example

# Configure the storm control action is **error-down** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control action error-down
Info: This configuration may cause port shutdown.
```

Related Topics

14.5.6 display storm-control

14.5.11 storm-control

14.5.13 storm-control enable

14.5.14 storm-control interval

14.5.13 storm-control enable

Function

The **storm-control enable** command configures the system to record logs or report traps during storm control.

The **undo storm-control enable** command configures the system not to record logs or report traps during storm control.

By default, the system does not record logs or report traps.

Format

storm-control enable { **log** | **trap** }

undo storm-control enable { **log** | **trap** }

Parameters

Parameter	Description	Value
log	Enables the log function.	-
trap	Enables the trap function.	-

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After storm control is configured, the switch monitors the broadcast, unknown multicast, and unknown unicast packets received on an interface. When the packet rate within a detection interval exceeds the upper limit, the switch executes the storm control action (block packets or shut down the interface) on the interface. This may affect services. You can configure the log or trap for storm control so that the administrator can quickly take actions to protect the switch.

- After the logging function is enabled for storm control, the storm control log information is recorded in the **STORMCTRL** log of the SECE module.
- After the trap function is enabled for storm control, the trap is SECE_1.3.6.1.4.1.2011.5.25.32.4.1.14.1 hwXQoSStormControlTrap.

Example

# Enable the trap reporting function during storm control on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control broadcast min-rate 3000 max-rate 5000
[HUAWEI-GigabitEthernet0/0/1] storm-control action block
[HUAWEI-GigabitEthernet0/0/1] storm-control enable trap
```

Related Topics

14.5.6 display storm-control

14.5.11 storm-control

14.5.12 storm-control action

14.5.14 storm-control interval

14.5.14 storm-control interval

Function

The **storm-control interval** command sets the storm detection interval.

The **undo storm-control interval** command restores the default storm detection interval.

By default, the storm detection interval is 5s.

Format

storm-control interval *interval-value*

undo storm-control interval

Parameters

Parameter	Description	Value
interval-value	Specifies the storm detection interval.	The value is an integer that ranges from 1 to 180, in seconds. The default value is 5s.

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Before using the **storm-control interval** command to set the storm detection interval, run the **14.5.11 storm-control** command in the interface view to configure storm control. Otherwise, the storm detection interval does not take effect.

Example

# Configure storm control and set the storm detection interval to 10 seconds on GE0/0/1.Block broadcast packets when the rate of receiving broadcast packets is greater than 5000 pps and forward the packets when the rate of receiving broadcast packets is smaller than 3000 pps in 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
```

```
[HUAWEI-GigabitEthernet0/0/1] storm-control broadcast min-rate 3000 max-rate 5000
[HUAWEI-GigabitEthernet0/0/1] storm-control action block
[HUAWEI-GigabitEthernet0/0/1] storm-control interval 10
```

Related Topics

14.5.6 display storm-control

14.5.11 storm-control

14.5.12 storm-control action

14.5.13 storm-control enable

14.5.15 suppression mode

Function

The **suppression mode** command sets the global traffic suppression mode.

The **undo suppression mode** command restores the default traffic suppression mode.

By default, the global traffic suppression mode is **packets**.

NOTE

Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support this command.

Format

suppression mode { **by-packets** | **by-bits** }

undo suppression mode

Parameters

Parameter	Description	Value
by-packets	Sets the traffic suppression mode to **packets**.	-
by-bits	Sets the traffic suppression mode to **bits**.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default traffic suppression mode on an interface is **packets**. To precisely control traffic rate, run the **suppression mode** command in the system view to set the traffic suppression mode to **bits**.

Precautions

If the **packets** mode has been set on an interface and the **bits** mode is set in the system view, the device automatically converts the traffic rate values and suppresses traffic based on **bits**. For example, if the maximum rate of broadcast packets allowed by a GE interface is set to 1000 pps, the device converts the traffic rate value as follows: 1000 x 84 x 8 = 672000 bits = 672 Kbit. In the preceding formula, 84 is the average length of packets (including the 64-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

If the traffic suppression mode set in the system view is **packets**, the **cir** parameter cannot be specified when you set the maximum traffic rate on an interface.

If the traffic suppression mode set in the system view is **bits**, the **packets** parameter cannot be specified when you set the maximum traffic rate on an interface.

Example

# Set the traffic suppression mode to **by-bits**.

```
<HUAWEI> system-view
[HUAWEI] suppression mode by-bits
Warning: All Interface supression mode will be changed. Continue? [Y/N]:y
```

Related Topics

14.5.2 broadcast-suppression (interface view)

14.5.9 multicast-suppression (interface view)

14.5.16 unicast-suppression (interface view)

14.5.16 unicast-suppression (interface view)

Function

The **unicast-suppression** command sets the maximum traffic volume of unknown unicast packets that can pass through an interface.

The **undo unicast-suppression** allows all unknown unicast packets to pass.

By default, unknown unicast packets are not suppressed.

Format

unicast-suppression { *percent-value* | **cir** *cir-value* [**cbs** *cbs-value*] | **packets** *packets-per-second* } (Only the S1720GFR, S1720GW, S1720GWR, S1720X, S1720GW-E, S1720GWR-E, S1720X-E, S2720EI, S2750EI, S5720SI, S5720S-SI, S5710-X-LI, S5720LI, S5720S-LI, S5700LI, S5700S-LI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI support **cir** *cir-value* [**cbs** *cbs-value*].)

undo unicast-suppression

Parameters

Parameter	Description	Value
percent-value	Specifies the percentage of bandwidth occupied by broadcast packets on an interface. If loopback detection is enabled on an interface, the interface rate is set by user. If loopback detection is not enabled on an interface, the interface rate is automatically negotiated. You can run the **4.1.15 display this interface** command in the interface view to check the interface rate (value of the **Speed** field).	The value is an integer. It ranges from 0 to 80 for 40GE interfaces and 0 to 100 for other types of interfaces.

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through. **NOTE** Traffic suppression based on **cir** is more precise than that based on **packets**. To specify the **cir** parameter, ensure that the traffic suppression mode set in the system view is **bits**.	The value is an integer. For an Ethernet interface, the value ranges from 0 to 100000; for a GE interface, the value ranges from 0 to 1000000; for a MultiGE interface, the value ranges form 0 to X, X indicates the negotiated bandwidth; for an XGE interface, the value ranges from 0 to 10000000; for a 40GE interface, the value ranges from 0 to 40000000; for a port group, the value ranges from 0 to 100000000, in kbit/s. **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1000000.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum size of traffic that can pass through.	The value is an integer that ranges from 10000 to 4294967295, in bytes. By default, the CBS value is 188 times the CIR value.

Parameter	Description	Value
packets *packets-per-second*	Specifies the number of packets transmitted per second. **NOTE** To specify the **packets** parameter, ensure that the traffic suppression mode set in the system view is **packets**.	The value is an integer and the value range is as follows: ● Ethernet interface: 0 to 148810 ● GE interface: 0 to 1488100 ● MultiGE interface: 0 to X. X indicates the negotiated bandwidth ● XGE interface: 0 to 14881000 ● 40GE interface: 0 to 59524000 ● Port group: 0 to 148810000 **NOTE** When an interface is configured with an optical module, the value range is determined by the rate of the optical module. For example, when an XGE interface is configured with a GE optical module, the value range is 0 to 1488100.

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an increasing number of unknown unicast packets are transmitted on the network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **unicast-suppression** command to set the threshold of unicast traffic that an interface allows to pass through. When the unknown unicast traffic rate exceeds the rate limit, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Precautions

Setting the bandwidth percentage is the same as setting the rate limit in pps. Take an interface of 1 Gbit/s as an example. If the bandwidth percentage is set to 50%, the device converts the bandwidth percentage to rate limit in pps as follows: (1000 x (50/100) x 1000 x 1000)/(84 x 8). In the preceding formula, 84 is the average length of packets (including the 60-byte packet body, 20-byte frame spacing, and 4-byte check information), and 8 is the number of bits in a byte.

NOTE

If a packet rate limit is configured for a type of packets on an interface, the percentage rate limit for other types of packets is converted into the packet rate limit.

Example

#Set the maximum unknown unicast packet rate to 100000 pps on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] unicast-suppression packets 100000
```

Related Topics

14.5.2 broadcast-suppression (interface view)

14.5.5 display flow-suppression interface

14.5.9 multicast-suppression (interface view)

14.5.17 unicast-suppression block outbound

Function

The **unicast-suppression block outbound** command configures an interface to block outgoing unknown unicast packets.

The **undo unicast-suppression block outbound** command cancels the configuration.

By default, an interface does not block outgoing unknown unicast packets.

Format

unicast-suppression block outbound

undo unicast-suppression block outbound

Parameters

None

Views

Ethernet interface view, 40GE interface view, GE interface view, XGE interface view, MultiGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface receives an unknown unicast packet, the interface broadcasts the packet to all users in the same VLAN. This may cause information leak. For example, if an unauthorized user is connected to an interface in a VLAN, the unauthorized user obtains a host's address from unknown unicast packets and uses the address to attack the host. To prevent information leak, use the **unicast-suppression block outbound** command to block unknown unicast packets on an interface if users connected to the interface do not need to receive broadcast packets. For example, if users on an interface seldom change and require high security, you can use this command on the interface.

Precautions

The **unicast-suppression block outbound** command is applicable only to interfaces where users do not need to receive unknown unicast packets. This command will affect network operations if it is used on an interface where users need to receive unknown packets.

Traffic suppression can be configured for incoming and outgoing packets on an interface, and the configurations are independent of each other. On an interface, use the **unicast-suppression** command to limit the rate of incoming unknown unicast packets and the **unicast-suppression block outbound** command to block outgoing unknown unicast packets.

Example

# Block outgoing multicast packets on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] unicast-suppression block outbound
```

Related Topics

14.5.2 broadcast-suppression (interface view)

14.5.3 broadcast-suppression block outbound

14.5.9 multicast-suppression (interface view)

14.5.10 multicast-suppression block outbound

14.5.16 unicast-suppression (interface view)

14.6 ARP Security Configuration Commands

14.6.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.6.2 arp anti-attack check user-bind alarm enable

Function

The **arp anti-attack check user-bind alarm enable** command enables the alarm function for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm enable** command disables the alarm function for ARP packets discarded by DAI.

By default, the alarm function for ARP packets discarded by DAI is disabled.

Format

arp anti-attack check user-bind alarm enable

undo arp anti-attack check user-bind alarm enable

Parameters

None

Views

Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DAI is enabled, if you want to receive an alarm when a large number of ARP packets are discarded by DAI, you can run the **arp anti-attack check user-bind alarm enable** command. After the alarm function is enabled, the device sends an alarm when the number of discarded ARP packets exceeds the threshold.

The alarm threshold is set by the **14.6.3 arp anti-attack check user-bind alarm threshold** command.

Prerequisites

DAI has been enabled on the interface using the **arp anti-attack check user-bind enable** command.

Example

# Enable the alarm function for ARP packets discarded by DAI on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
```

Related Topics

14.6.6 arp anti-attack check user-bind enable

14.6.3 arp anti-attack check user-bind alarm threshold

14.6.3 arp anti-attack check user-bind alarm threshold

Function

The **arp anti-attack check user-bind alarm threshold** command sets the alarm threshold for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm threshold** command restores the default alarm threshold for ARP packets discarded by DAI.

By default, the alarm threshold for ARP packets discarded by DAI is 100.

Format

arp anti-attack check user-bind alarm threshold *threshold*

undo arp anti-attack check user-bind alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the ARP packets discarded by DAI.	The value is an integer that ranges from 1 to 1000.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to set the alarm threshold for ARP packets discarded by DAI. After the alarm threshold is set, the device sends an alarm when the number of ARP packets discarded by DAI exceeds this threshold.

Prerequisites

DAI has been enabled using the **arp anti-attack check user-bind enable** command in the interface view, and the alarm function for ARP packets discarded by DAI has been enabled using the **arp anti-attack check user-bind alarm enable** command.

Precautions

The **arp anti-attack check user-bind alarm threshold** command takes effect in the system view only when DAI and the alarm function for ARP packets discarded by DAI are enabled on the interface. The global alarm threshold takes effect on all interfaces enabled with the two functions.

If the alarm thresholds are set in the interface view and system view, the alarm threshold configured in the interface view takes effect. If the alarm threshold on an interface is not configured, the global alarm threshold is used.

Example

# Set the alarm threshold for ARP packets discarded by DAI on GE0/0/1 to 200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind alarm threshold 200
```

Related Topics

14.6.6 arp anti-attack check user-bind enable

14.6.2 arp anti-attack check user-bind alarm enable

14.6.4 arp anti-attack check user-bind check-item (interface view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries on an interface.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and VLAN ID.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
vlan	Indicates that the device checks VLAN IDs in ARP packets.	-

Views

Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and VLAN ID of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, use the **arp anti-attack check user-bind check-item** command to configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled on the interface using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

Example

# Configure GE0/0/1 to check IP addresses in ARP packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind check-item ip-address
```

Related Topics

14.6.6 arp anti-attack check user-bind enable

14.6.5 arp anti-attack check user-bind check-item (VLAN view)

14.6.5 arp anti-attack check user-bind check-item (VLAN view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries in a VLAN.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and interface number.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-

Parameter	Description	Value
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
interface	Indicates that the device checks interface numbers in ARP packets.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled in the VLAN using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

Example

# Configure the device to check IP addresses in ARP packets from VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp anti-attack check user-bind enable
[HUAWEI-vlan100] arp anti-attack check user-bind check-item ip-address
```

Related Topics

14.6.6 arp anti-attack check user-bind enable

14.6.4 arp anti-attack check user-bind check-item (interface view)

14.6.6 arp anti-attack check user-bind enable

Function

The **arp anti-attack check user-bind enable** command enables DAI on an interface or in a VLAN. DAI enables the device to check ARP packets based on binding entries.

The **undo arp anti-attack check user-bind enable** command disables DAI on an interface or in a VLAN.

By default, DAI is disabled on an interface or in a VLAN.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

Parameters

None

Views

VLAN view, Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent MITM attacks and theft on authorized user information, run the **arp anti-attack check user-bind enable** command to enable DAI. When a device receives an ARP packet, it compares the source IP address, source MAC address, VLAN ID, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

You can enable DAI in the interface view or the VLAN view. When DAI is enabled in an interface view, the device checks all ARP packets received on the interface against binding entries. When DAI is enabled in the VLAN view, the device checks ARP packets received on interfaces belong to the VLAN based on binding entries.

Follow-up Procedure

Run the **14.6.4 arp anti-attack check user-bind check-item (interface view)** or **14.6.5 arp anti-attack check user-bind check-item (VLAN view)** command to configure check items for ARP packet check based on binding entries.

Precautions

When resources are sufficient, DAI can be enabled in a maximum of 10 VLANs.

Example

# Enable DAI on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack check user-bind enable
```

# Enable DAI in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp anti-attack check user-bind enable
```

Related Topics

14.6.4 arp anti-attack check user-bind check-item (interface view)

14.6.5 arp anti-attack check user-bind check-item (VLAN view)

14.6.7 arp anti-attack entry-check enable

Function

The **arp anti-attack entry-check enable** command enables ARP entry fixing.

The **undo arp anti-attack entry-check enable** command disables ARP entry fixing.

By default, ARP entry fixing is disabled.

Format

arp anti-attack entry-check { **fixed-mac** | **fixed-all** | **send-ack** } **enable**

undo arp anti-attack entry-check [**fixed-mac** | **fixed-all** | **send-ack**] **enable**

Parameters

Parameter	Description	Value
fixed-mac	Indicates ARP entry fixing in **fixed-mac** mode. When receiving an ARP packet, the device discards the packet if the MAC address does not match the MAC address in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry.	-
fixed-all	Indicates ARP entry fixing in **fixed-all** mode. When the MAC address, interface number, and VLAN ID of an ARP packet match those in the corresponding ARP entry, the device updates other information about the ARP entry.	-

Parameter	Description	Value
send-ack	Indicates ARP entry fixing in **send-ack** mode. When the device receives an ARP packet with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user.	-

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To defend against ARP address spoofing attacks, enable ARP entry fixing. The **fixed-mac**, **fixed-all**, and **send-ack** modes are applicable to different scenarios and are mutually exclusive:

- The **fixed-mac** mode applies to networks where user MAC addresses are unchanged but user access locations often change. When a user connects to a different interface on the device, the device updates interface information in the ARP entry of the user timely.
- The **fixed-all** mode applies to networks where user MAC addresses and user access locations are fixed.
- The **send-ack** mode applies to networks where user MAC addresses and user access locations often change.

Precautions

After ARP entry fixing is enabled, the function that updates ARP entries when MAC address entries change (configured by the **5.1.41 mac-address update arp** command) becomes invalid.

In **send-ack** mode, the device can record a maximum of 100 ARP entries in the ARP Request packets intended to trigger ARP entry modification.

If you run the **arp anti-attack entry-check enable** command in the system view, ARP entry fixing is enabled on all interfaces. If you run the **arp anti-attack entry-check enable** command in the interface view, ARP entry fixing is enabled on the specified interface.

If ARP entry fixing is enabled globally and on a VLANIF interface simultaneously, the configuration on the VLANIF interface takes precedence over the global configuration.

Example

# Enable ARP entry fixing and specify the **fixed-mac** mode.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack entry-check fixed-mac enable
```

Related Topics

14.6.36 display arp anti-attack configuration

14.6.8 arp anti-attack gateway-duplicate enable

Function

The **arp anti-attack gateway-duplicate enable** command enables ARP gateway anti-collision.

The **undo arp anti-attack gateway-duplicate enable** command disables ARP gateway anti-collision.

By default, ARP gateway anti-collision is disabled.

📖 NOTE

Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

arp anti-attack gateway-duplicate enable

undo arp anti-attack gateway-duplicate enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges the gateway address to send ARP packets with the source IP address being the IP address of the gateway on the LAN, ARP entries on hosts in the LAN record the incorrect gateway address. As a result, all traffic from user hosts to the gateway is sent to the attacker and the attacker intercepts user information. Communication of users is interrupted.

To prevent bogus gateway attacks, enable ARP gateway anti-collision on the gateway using the **arp anti-attack gateway-duplicate enable** command. The gateway considers that a gateway collision occurs when a received ARP packet meets either of the following conditions:

- The source IP address in the ARP packet is the same as the IP address of the VLANIF interface matching the physical inbound interface of the packet.
- The source IP address in the ARP packet is the virtual IP address of the inbound interface but the source MAC address in the ARP packet is not the virtual MAC address of the VRRP group.

The device generates an ARP anti-collision entry and discards the received packets with the same source MAC address and VLAN ID in a specified period. This function prevents ARP packets with the bogus gateway address from being broadcast in a VLAN.

Precautions

A maximum of 100 ARP anti-attack entries exist on the device at the same time. When the maximum number is exceeded, the device cannot prevent new ARP gateway collision attacks.

Example

# Enable ARP gateway anti-collision.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack gateway-duplicate enable
```

Related Topics

14.6.36 display arp anti-attack configuration

14.6.37 display arp anti-attack gateway-duplicate item

14.6.9 arp anti-attack log-trap-timer

Function

The **arp anti-attack log-trap-timer** command sets the interval for sending ARP alarms.

The **undo arp anti-attack log-trap-timer** command restores the default setting.

The default interval for sending alarms is 0, indicating that the device does not send ARP alarms.

Format

arp anti-attack log-trap-timer *time*

undo arp anti-attack log-trap-timer

Parameters

Parameter	Description	Value
time	Specifies the interval for sending ARP alarms.	The value is an integer that ranges from 0 to 1200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limiting on ARP packets based on source IP addresses is enabled, if the number of ARP packets the device receives per second exceeds the limit, the device discards the excess ARP packets. The device considers the excess ARP packets as potential attacks. The device sends ARP alarms indicating potential attacks to the NMS. To avoid excessive alarms when ARP attacks occur, reduce the alarm quantity by setting a proper interval for sending alarms.

Precautions

In the insecure environment, you are advised to extend the interval for sending ARP alarms. This prevents excessive ARP alarms. In the secure environment, you are advised to shorten the interval for sending ARP alarms. This facilitates fault rectification in real time.

After the interval is set, the device discards alarms generates in this interval; therefore, some faults cannot be rectified in real time.

The command takes effect only on the alarm for ARP rate limit based on source IP addresses (corresponding to **arp speed-limit source-ip**). The other ARP alarms are generated at a fixed interval of 5 seconds.

Example

# Set the interval for sending ARP alarms to 20 seconds.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack log-trap-timer 20
```

Related Topics

14.6.36 display arp anti-attack configuration

14.6.10 arp anti-attack packet-check

Function

The **arp anti-attack packet-check** command enables ARP packet validity check and specifies check items.

The **undo arp anti-attack packet-check** command disables ARP packet validity check.

By default, ARP packet validity check is disabled.

Format

arp anti-attack packet-check { **ip** | **dst-mac** | **sender-mac** } *

undo arp anti-attack packet-check [**ip** | **dst-mac** | **sender-mac**] *

Parameters

Parameter	Description	Value
ip	Indicates ARP packet validity check based on the IP address.	-
dst-mac	Indicates ARP packet validity check based on the destination MAC address.	-
sender-mac	Indicates ARP packet validity check based on the source MAC address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To avoid ARP attacks, you can use the **arp anti-attack packet-check** command to enable ARP packet validity check on an access device or a gateway to filters out ARP packets with invalid IP addresses or MAC addresses. The device checks validity of an ARP packet based on each or any combination of the following items:

- Source and destination IP addresses: The device checks the source and destination IP addresses in an ARP packet. If the source or destination IP address is all 0s, all 1s, or a multicast IP address, the device discards the packet as an invalid packet. The device checks both the source and destination IP addresses in an ARP Reply packet but checks only the source IP address in an ARP Request packet.
- Source MAC address: The device compares the source MAC address in an ARP packet with that in the Ethernet frame header. If they are the same, the packet is valid. If they are different, the device discards the packet.

- Destination MAC address: The device compares the destination MAC address in an ARP packet with that in the Ethernet frame header. If they are the same, the packet is valid. If they are different, the device discards the packet.

Precautions

Generally, packets with different source and destination MAC addresses in the ARP packet and Ethernet frame header are allowed by the ARP protocol. When an attack occurs, capture and analyze packets. If the attack is initiated by using inconsistent source or destination MAC addresses in the ARP packet and Ethernet frame header, enable ARP packet validity check based on the source or destination MAC address.

If you run the **arp anti-attack packet-check sender-mac** command multiple times, all the check items specified in these commands take effect.

Example

# Enable ARP packet validity check and configures the device to check the source MAC address in an ARP packet.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack packet-check sender-mac
```

Related Topics

14.6.36 display arp anti-attack configuration

14.6.11 arp anti-attack rate-limit

Function

The **arp anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP packets globally, in a VLAN, or on an interface, and enables the function of discarding all ARP packets received from the interface when the rate of ARP packets exceeds the limit on an interface.

The **undo arp anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP packets globally, in a VLAN, or on an interface, and allows the device to send ARP packets to the CPU again.

By default, a maximum of 100 ARP packets are allowed to pass per second, and the function of discarding all ARP packets received from the interface when the rate of ARP packets exceeds the limit is disabled.

Format

System view, VLAN view

arp anti-attack rate-limit packet *packet-number* [**interval** *interval-value*]

undo arp anti-attack rate-limit

Interface view

arp anti-attack rate-limit packet *packet-number* [**interval** *interval-value* | **block-timer** *timer*] *

undo arp anti-attack rate-limit

Parameters

Parameter	Description	Value
packet *packet-number*	Specifies the maximum rate of sending ARP packets, that is, the number of ARP packets allowed to pass through in the rate limiting duration.	The value is an integer that ranges from 1 to 16384. The default value is 100.
interval *interval-value*	Specifies the rate limiting duration of ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.
block-timer *timer*	Specifies the duration for blocking ARP packets.	The value is an integer that ranges from 5 to 864000, in seconds.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, run the **arp anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP packets globally, in a VLAN, or on an interface. In the rate limiting duration, if the number of received ARP packets exceeds the limit, the device discards the excess ARP packets.

If the parameter **block-timer** *timer* is specified, the device discards all ARP packets received in the duration specified by *timer*.

Prerequisites

Rate limit on ARP packets has been enabled globally, in a VLAN, or on an interface using the **arp anti-attack rate-limit enable** command.

Precautions

If the maximum rate and rate limiting duration are configured in the system view, VLAN view, and interface view at the same time, the device uses the configurations in the interface view, VLAN view, and system view in order.

The **arp anti-attack rate-limit packet** *packet-number* **block-timer** *timer* command can be configured on a maximum of 16 interfaces.

NOTE

The **arp anti-attack rate-limit** command takes effect only on ARP packets sent to the CPU for processing in **none-block** mode, and does not affect ARP packet forwarding by the chip. In **block** mode, the device discards subsequent ARP packets on an interface only when the number of ARP packets sent to the CPU exceeds the limit.

Example

# Configure Layer 2 interface GE0/0/1 to allow 200 ARP packets to pass through in 10 seconds, and configure GE0/0/1 to discard all ARP packets in 60 seconds when the number of ARP packets exceeds the limit.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit packet 200 interval 10 block-timer 60
```

# Configure Layer 3 interface GE0/0/1 to allow 200 ARP packets to pass through in 10 seconds, and configure GE0/0/1 to discard all ARP packets in 60 seconds when the number of ARP packets exceeds the limit.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit packet 200 interval 10 block-timer 60
```

Related Topics

14.6.14 arp anti-attack rate-limit enable

14.6.12 arp anti-attack rate-limit alarm enable

Function

The **arp anti-attack rate-limit alarm enable** command enables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

The **undo arp anti-attack rate-limit alarm enable** command disables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

By default, the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit is disabled.

Format

arp anti-attack rate-limit alarm enable

undo arp anti-attack rate-limit alarm enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, if you want the device to generate alarms for excessive discarded ARP packets, run the **arp anti-attack rate-limit alarm enable** command. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command.

Example

# Enable rate limit on ARP packets globally and enable the alarm function.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack rate-limit enable
[HUAWEI] arp anti-attack rate-limit alarm enable
```

# Enable rate limit for the ARP packets on Layer 2 interface GE0/0/1 and enable the alarm function.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
```

# Enable rate limit for the ARP packets on Layer 3 interface GE0/0/1 and enable the alarm function.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
```

Related Topics

14.6.14 arp anti-attack rate-limit enable

14.6.13 arp anti-attack rate-limit alarm threshold

14.6.13 arp anti-attack rate-limit alarm threshold

Function

The **arp anti-attack rate-limit alarm threshold** command sets the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.

The **undo arp anti-attack rate-limit alarm threshold** command restores the default alarm threshold.

By default, the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is 100.

Format

arp anti-attack rate-limit alarm threshold *threshold*

undo arp anti-attack rate-limit alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.	The value is an integer that ranges from 1 to 16384.

Views

System view, VLAN view, Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **arp anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp anti-attack rate-limit alarm enable** command.

Example

# Enable rate limit on ARP packets globally, enable the alarm function, and set the alarm threshold to 50.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack rate-limit enable
[HUAWEI] arp anti-attack rate-limit alarm enable
[HUAWEI] arp anti-attack rate-limit alarm threshold 50
```

# Enable rate limit for the ARP packets on Layer 2 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 50.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm threshold 50
```

# Enable rate limit for the ARP packets on Layer 3 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 50.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit alarm threshold 50
```

Related Topics

14.6.14 arp anti-attack rate-limit enable

14.6.12 arp anti-attack rate-limit alarm enable

14.6.14 arp anti-attack rate-limit enable

Function

The **arp anti-attack rate-limit enable** command enables rate limit on ARP packets.

The **undo arp anti-attack rate-limit enable** command disables rate limit on ARP packets.

By default, rate limiting on ARP packet is disabled.

Format

arp anti-attack rate-limit enable

undo arp anti-attack rate-limit enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The device has no sufficient CPU resource to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

You can run the **arp anti-attack rate-limit enable** command to enable rate limit on ARP packets. When the rate of ARP packets exceeds the limit, excess ARP packets are discarded. To set the rate limit and rate limiting duration of ARP packets, run the **arp anti-attack rate-limit** command.

After the optimized ARP reply function (disabled by default) is enabled using the **undo arp optimized-reply disable** command, rate limiting on ARP packets globally, in a VLAN, or on an Interface does not take effect.

Example

# Enable rate limit on ARP packets globally.

```
<HUAWEI> system-view
[HUAWEI] arp anti-attack rate-limit enable
```

# Enable rate limit for the ARP packets on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
```

# Enable rate limit for the ARP packets on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp anti-attack rate-limit enable
```

Related Topics

14.6.11 arp anti-attack rate-limit

14.6.15 arp trust source

Function

The **arp trust source** command enables ARP gateway protection for the specified IP address.

The **undo arp trust source** command disables ARP gateway protection for the specified IP address.

By default, ARP gateway protection is disabled.

Format

arp trust source *ip-address*

undo arp trust source { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the protected gateway IP address.	The value is in dotted decimal notation.
all	Disables ARP gateway protection for all IP addresses in the current view.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker poses as a gateway to send ARP packets, other users on the network consider the attacker to be a gateway, causing a communication interruption between authorized users and gateway. This situation will also happen if a user incorrectly sets the host IP address as the gateway address. To prevent such bogus gateway attacks, configure ARP gateway protection on the device's interfaces connected to the gateway. When the ARP packets from a gateway address reach a device:

- The interfaces with gateway protection enabled can receive and forward the ARP packets.
- The interfaces without gateway protection enabled discard the ARP packets.

Precautions

A maximum of 8 protected gateway addresses can be specified on each interface, and 32 can be specified on the entire device. If the same gateway IP address is specified on different interfaces, the system considers that multiple protected gateway IP addresses have been configured.

Example

# Enable ARP gateway protection on GE0/0/1 and set the protected gateway IP address to 10.10.10.1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp trust source 10.10.10.1
```

14.6.16 arp gratuitous-arp send enable

Function

The **arp gratuitous-arp send enable** command enables gratuitous ARP packet sending.

The **undo arp gratuitous-arp send enable** command disables gratuitous ARP packet sending.

By default, gratuitous ARP packet sending is disabled.

Format

arp gratuitous-arp send enable

undo arp gratuitous-arp send enable

Parameters

None

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges the gateway address to send ARP packets to other user hosts, ARP entries on the hosts record the incorrect gateway address. As a result, the gateway cannot receive data sent from the hosts. You can enable gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

By default, the device sends a gratuitous ARP packet every 60 seconds after this function is enabled. You can also set the interval using the **arp gratuitous-arp send interval** command.

Precautions

After you run the **arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is enabled on all VLANIF interfaces.

After you run the **undo arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is disabled on all VLANIF interfaces.

Example

# Enable gratuitous ARP packet sending on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp gratuitous-arp send enable
```

Related Topics

14.6.17 arp gratuitous-arp send interval

14.6.17 arp gratuitous-arp send interval

Function

The **arp gratuitous-arp send interval** command sets the interval for sending gratuitous ARP packets.

The **undo arp gratuitous-arp send interval** command restores the default interval for sending gratuitous ARP packets.

By default, the interval for sending gratuitous ARP packets is 60 seconds.

Format

arp gratuitous-arp send interval *interval-time*

undo arp gratuitous-arp send interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for sending gratuitous ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds.

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device sends a gratuitous ARP packet every 60 seconds after gratuitous ARP sending is enabled. You can set the interval for sending gratuitous ARP packets using the **arp gratuitous-arp send interval** command.

If you set the interval in the system view, the configuration takes effect on all VLANIF interfaces. If you set the interval in both the system view and VLANIF interface view, the configuration on the VLANIF interface takes precedence over the global configuration.

Prerequisites

Gratuitous ARP packet sending has been enabled using the **arp gratuitous-arp send enable** command.

Example

# Set the interval for sending gratuitous ARP packets to 100 seconds on VLANIF 10.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp gratuitous-arp send enable
[HUAWEI-Vlanif10] arp gratuitous-arp send interval 100
```

Related Topics

14.6.16 arp gratuitous-arp send enable

14.6.18 arp learning dhcp-trigger

Function

The **arp learning dhcp-trigger** command enables ARP learning triggered by DHCP.

The **undo arp learning dhcp-trigger** command disables ARP learning triggered by DHCP.

By default, ARP learning triggered by DHCP is disabled.

Format

arp learning dhcp-trigger

undo arp learning dhcp-trigger

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many DHCP users connect to a network device, the device needs to learn and maintain many ARP entries. This affects device performance.

To address this issue, configure ARP learning triggered by DHCP on the gateway. When the DHCP server allocates an IP address for a user, the gateway generates an ARP entry for the user based on the DHCP ACK packet received on the VLANIF interface.

Precautions

Before using this command, ensure that DHCP is enabled using the **dhcp enable** command.

When both VRRP and DHCP relay are configured on the network, neither the **dhcp snooping enable** command nor the **arp learning dhcp-trigger** command can be configured on the VRRP master and backup devices.

Example

# Enable ARP learning triggered by DHCP on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] vlan batch 100
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp learning dhcp-trigger
```

Related Topics

6.3.17 dhcp enable

14.6.19 arp learning disable

Function

The **arp learning disable** command disables an interface from learning dynamic ARP entries.

The **undo arp learning disable** command enables an interface to learn dynamic ARP entries.

By default, an interface is enabled to learn dynamic ARP entries.

Format

arp learning disable

undo arp learning disable

Parameters

None

Views

VLANIF interface view, VBDIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security and facilitate management, you can enable an interface to learn or disable an interface from learning dynamic ARP entries. You can also use the **14.6.21 arp learning strict (system view)** or **14.6.20 arp learning strict (interface view)** commands to strictly control ARP entry learning on an interface.

Precautions

If an interface is disabled from learning ARP entries, the network will be interrupted.

If an interface has learned some dynamic ARP entries, the system does not delete these entries after the interface is disabled from learning dynamic ARP entries. You can manually delete or reserve these learned dynamic ARP entries (deleted by the **6.2.43 reset arp** command).

Example

# Disable VLANIF10 from learning dynamic ARP entries.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp learning disable
```

14.6.20 arp learning strict (interface view)

Function

The **arp learning strict** command enables strict ARP learning on the interface.

The **undo arp learning strict** command restores the global configuration on the interface.

By default, strict ARP learning is disabled on the interface.

Format

arp learning strict { **force-enable** | **force-disable** | **trust** }

undo arp learning strict

Parameters

Parameter	Description	Value
force-enable	Indicates that strict ARP learning is enabled.	-
force-disable	Indicates that strict ARP learning is disabled.	-
trust	Indicates that the configuration of strict ARP learning is the same as the global configuration. **NOTE** The effect of the **trust** parameter is the same as the effect of the **undo arp learning strict** command.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself, but does not allow the device to learn the ARP entries for the ARP packets received from other devices. In this way, the device can defend against most ARP attacks.

Prerequisites

On an Ethernet interface works in Layer 2 mode. you need run **undo portswitch**, switch the interface to Layer 3 mode.

NOTE

Only the S5720EI, S5720HI and S6720EI/S6720S-EI support switching between Layer 2 and Layer 3 modes.

Precautions

The configuration on an interface takes precedence over the global configuration.

When ARP attacks occur on many interfaces of the device, you can run the **14.6.21 arp learning strict (system view)** command to enable strict ARP learning globally.

Example

# Enable strict ARP learning on VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] quit
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp learning strict force-enable
```

# Enable strict ARP learning on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp learning strict force-enable
```

Related Topics

14.6.21 arp learning strict (system view)

14.6.40 display arp learning strict

14.6.21 arp learning strict (system view)

Function

The **arp learning strict** command enables strict ARP learning.

The **undo arp learning strict** command disables strict ARP learning.

By default, strict ARP learning is disabled.

Format

arp learning strict

undo arp learning strict

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. In this way, the device can defend against most ARP attacks.

Precautions

The configuration on an interface takes precedence over the global configuration.

Example

# Enable strict ARP learning.

```
<HUAWEI> system-view
[HUAWEI] arp learning strict
```

Related Topics

14.6.20 arp learning strict (interface view)

14.6.40 display arp learning strict

14.6.22 arp optimized-reply disable

Function

The **arp optimized-reply disable** command disables the optimized ARP reply function.

The **undo arp optimized-reply disable** command enables the optimized ARP reply function.

By default, the optimized ARP reply function is enabled.

Format

arp optimized-reply disable

undo arp optimized-reply disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stack functions as an access gateway, the stack can receive a large number of ARP packets requesting for the stack's interface MAC address. If all these ARP Request packets are sent to the master switch, the CPU usage of the switch increases, and other services are affected.

To address the preceding problem, enable optimized ARP reply, which improves the switch's capability of defending against ARP flood attack. After this function is enabled, the stack performs the following operations:

- When receiving an ARP Request packet of which the destination IP address is the local interface address, the switch where the interface is located directly returns an ARP Reply packet.
- When a stack system receives an ARP Request packet of which the destination IP address is not the local interface address and intra-VLAN proxy ARP is enabled on the master switch, the switch where the interface is located checks whether the ARP Request packet meets the proxy condition. If so, the switch returns an ARP Reply packet. If not, the switch discards the packet.

NOTE

The optimized ARP reply function can be configured on a stand-alone fixed switch, but does not take effect.

By default, the optimized ARP reply function is enabled. After a device receives an ARP Request packet, the device checks whether an ARP entry corresponding to the source IP address of the ARP Request packet exists.

- If the corresponding ARP entry exists, the stack performs optimized ARP reply to this ARP Request packet.
- If the corresponding ARP entry does not exist, the stack does not perform optimized ARP reply to this ARP Request packet.

Precautions

- The optimized ARP reply function does not take effect for ARP Request packets with double VLAN tags.
- The optimized ARP reply function takes effect for ARP Request packets sent by wireless users.
- The optimized ARP reply function takes effect only for the ARP Request packets received by VLANIF interfaces. The optimized ARP reply function does not take effect for the ARP Request packets sent from the VLANIF interfaces of super VLANs and sub VLANs.
- The optimized ARP reply function does not take effect globally or on VLANIF interfaces after you run any of the following commands:
  - **ip address** *ip-address* { *mask* | *mask-length* } **sub**: configures secondary IP addresses for VLANIF interfaces.
  - **arp anti-attack gateway-duplicate enable**: enables the ARP gateway anti-collision function.

  - **arp ip-conflict-detect enable**: enables IP address conflict detection.
  - **arp anti-attack check user-bind enable**: enables dynamic ARP inspection.
  - **dhcp snooping arp security enable**: enables egress ARP inspection.
  - **arp over-vpls enable**: enables ARP proxy on the device located on a VPLS network.
  - **arp-proxy enable**: configures the routed ARP proxy function.
- After the optimized ARP reply function is enabled, the following functions become invalid:
  - ARP rate limiting based on source MAC addresses (configured using the **14.6.24 arp speed-limit source-mac** command)
  - ARP rate limiting based on source IP addresses (configured using the **14.6.25 arp speed-limit source-ip** command)
  - Global ARP rate limiting, ARP rate limiting in VLANs, as well as ARP rate limiting on interfaces (configured using the **14.6.14 arp anti-attack rate-limit enable** command)

Example

# Disable the optimized ARP reply function.

```
<HUAWEI> system-view
[HUAWEI] arp optimized-reply disable
```

Related Topics

14.6.41 display arp optimized-reply statistics

14.6.42 display arp optimized-reply status

14.6.23 arp over-vpls enable

Function

The **arp over-vpls enable** command enables ARP proxy on a device of a VPLS network.

The **undo arp over-vpls enable** command disables ARP proxy on a device of a VPLS network.

By default, ARP proxy is disabled on a device of a VPLS network.

NOTE

Only the S5720HI supports this command.

Format

arp over-vpls enable

undo arp over-vpls enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent bogus ARP packets at the PW side from being broadcast to the AC side on a VPLS network, enable ARP proxy over VPLS on a PE.

ARP packets at the PW side are sent to the CPU for processing.

- If the ARP packets are ARP Request packets and the destination IP addresses in the packets match DHCP snooping binding entries, the device constructs ARP Reply packets based on the DHCP snooping binding entries and sends them to the requester at the PW side.
- If the ARP packets are not ARP Request packets or the destination IP addresses in the packets match no DHCP snooping binding entry, the device forwards these ARP packets to the destination.

Precautions

Before using this command, ensure that DHCP snooping is enabled using the **dhcp snooping over-vpls enable** command.

Example

# Enable ARP proxy on a device of a VPLS network.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping over-vpls enable
[HUAWEI] arp over-vpls enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.23 dhcp snooping over-vpls enable

14.6.24 arp speed-limit source-mac

Function

The **arp speed-limit source-mac** command sets the maximum rate of ARP packets based on source MAC addresses.

The **undo arp speed-limit source-mac** command restores the default setting.

By default, the maximum rate of ARP packets from each source MAC address is set to 0, that is, the rate of ARP packets is not limited based on source MAC addresses.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

Format

arp speed-limit source-mac [*mac-address*] **maximum** *maximum*

undo arp speed-limit source-mac [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address. If this parameter is specified, the rate of ARP packets from the MAC address is limited. If this parameter is not specified, the rate of ARP packets from each MAC address is limited.	The value is in the H-H-H format. H is a hexadecimal number of 1 to 4 digits.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified MAC address.	The value ranges from 0 to 12288 for the S5720EI, from 0 to 45056 for the S6720EI/ S6720S-EI, from 0 to 61440 for the S5720HI, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed source MAC addresses but variable source IP addresses, the CPU is overloaded and ARP entries are exhausted. To prevent this problem, limit the rate of ARP packets based on source MAC addresses.

After the **arp speed-limit source-mac** command is run, the device collects statistics on ARP packets from a specified source MAC address. If the number of

ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source MAC address.

If the source MAC address is not specified, the rate of ARP packets from each MAC address is limited. If the rate of ARP packets from each source IP address is set using the **arp speed-limit source-ip** command at the same time and the rate is the same as that set using the **arp speed-limit source-mac** command, both commands take effect. When receiving ARP packets from a fixed source, the device limits the rate of these packets based on the maximum rate set by the **arp speed-limit source-mac** command.

After the optimized ARP reply function (disabled by default) is enabled using the **undo arp optimized-reply disable** command, rate limiting on ARP packets based on the source MAC address does not take effect.

Example

# Set the maximum rate of ARP packets from any source MAC address to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-mac maximum 100
```

# Set the maximum rate of ARP packets from a specified MAC address 0-0-1 to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-mac 0-0-1 maximum 50
```

Related Topics

14.6.25 arp speed-limit source-ip

14.6.36 display arp anti-attack configuration

14.6.25 arp speed-limit source-ip

Function

The **arp speed-limit source-ip** command sets the maximum rate of ARP packets based on the source IP address.

The **undo arp speed-limit source-ip** command restores the default setting.

By default, the device allows a maximum of 30 ARP packets from the same source IP address to pass through per second.

Format

arp speed-limit source-ip [*ip-address*] **maximum** *maximum*

undo arp speed-limit source-ip [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the rate of ARP packets from the IP address is limited. If this parameter is not specified, the rate of ARP packets from each IP address is limited.	The value is in dotted decimal notation.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified source IP address. **NOTE** If the rate of all ARP packets is limited, a large value is recommended because valid packets may be discarded if the value is small. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The integer form, in pps, is as follows: ● S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S5720LI, and S5720S-LI: 0 to 2048 ● S5720SI and S5720S-SI: 0 to 4096 ● S5720EI: 0 to 12288 ● S5720HI: 0 to 61440 ● S5730SI, S5730S-EI, S6720SI and S6720S-SI: 0 to 20000 ● S1720X, S1720X-E, S6720LI, and S6720S-LI: 0 to 8192 ● S6720EI and S6720S-EI: 0 to 96000 ● Other device: 0 to 256

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed IP addresses (for example, the ARP packets with the same source IP addresses but frequently changing MAC addresses or outbound interfaces), the CPU is overloaded and cannot process other services. To prevent this problem, limit the rate of ARP packets based on the source IP address.

After the **arp speed-limit source-ip** command is run, the device collects statistics on ARP packets based on the source IP address. If the number of ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source IP address.

When you confirm that the network is secure, set the rate limit to 0 to increase ARP learning speed. After the rate limit is set to 0, the device does not limit the ARP packet rate based on source IP addresses.

If the source IP address is not specified, the rate of ARP packets from each IP address is limited. If the rate of ARP packets from each source MAC address is set using the **14.6.24 arp speed-limit source-mac** command at the same time and the rate is the same as that set using the **arp speed-limit source-ip** command, both commands take effect. When receiving ARP packets from a fixed source, the device limits the rate of these packets based on the maximum rate set by the **14.6.24 arp speed-limit source-mac** command.

After the optimized ARP reply function (disabled by default) is enabled using the **undo arp optimized-reply disable** command, rate limiting on ARP packets based on the source IP address does not take effect.

Example

# Set the maximum rate of ARP packets from a source IP address to 100 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-ip maximum 100
```

# Set the maximum rate of ARP packets from a specified IP address 10.0.0.1 to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] arp speed-limit source-ip 10.0.0.1 maximum 50
```

Related Topics

14.6.24 arp speed-limit source-mac

14.6.36 display arp anti-attack configuration

14.6.26 arp validate(interface view)

Function

The **arp validate** command enables MAC address consistency check in an ARP packet on an interface. This function compares the source and destination MAC addresses in ARP packets with those in the Ethernet frame header.

The **undo arp validate** command disables MAC address consistency check in an ARP packet on an interface.

By default, MAC address consistency check in an ARP packet is disabled.

Format

arp validate { **source-mac** | **destination-mac** } *

undo arp validate { **source-mac** | **destination-mac** } *

Parameters

Parameter	Description	Value
source-mac	Indicates that the device compares the source MAC address in a received ARP packet with that in the Ethernet frame header.	-
destination-mac	Indicates that the device compares the destination MAC address in a received ARP packet with that in the Ethernet frame header.	-

Views

Ethernet interface view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view, VE interface view

Default Level

2: Configuration level

Usage Guidelines

The MAC address consistency check function for ARP packets prevents attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header. This function is usually configured on gateways.

After the **arp validate** command is run, the gateway checks the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

When using this command, note the following points:

- If **source-mac** is specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks only the source MAC address consistency.
- If **destination-mac** is specified:
  - When receiving an ARP Request packet, the device does not check the destination MAC address consistency because the ARP Request packet is broadcast.

  - When receiving an ARP Reply packet, the device checks the destination MAC address consistency.
- If **source-mac** and **destination-mac** are specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks the source and destination MAC address consistency.

Example

# Enable MAC address consistency check in an ARP packet on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp validate source-mac destination-mac
```

# Enable MAC address consistency check in an ARP packet on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp validate source-mac destination-mac
```

14.6.27 arp-fake expire-time

Function

The **arp-fake expire-time** command sets the aging time of temporary ARP entries.

The **undo arp-fake expire-time** command restores the default aging time of temporary ARP entries.

By default, the aging time of temporary ARP entries is 3 seconds.

Format

arp-fake expire-time *expire-time*

undo arp-fake expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of temporary ARP entries.	The value is an integer that ranges from 1 to 36000, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, VLANIF interface view, VBDIF interface view, VE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

- In the aging time of temporary ARP entries:
  - Before receiving an ARP reply packet, the device discards the IP packets matching the temporary ARP entry and does not generate ARP Miss messages.
  - After receiving an ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
- When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages and temporary ARP entries are repeatedly generated

When a device undergoes an ARP Miss attack, you can run the **arp-fake expire-time** command to extend the aging time of temporary ARP entries to reduce the frequency of triggering ARP Miss messages and minimize the impact on the device.

Example

# Set the aging time of temporary ARP entries to 10 seconds on VLANIF10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp-fake expire-time 10
```

# Set the aging time of temporary ARP entries to 10 seconds on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-fake expire-time 10
```

14.6.28 arp-limit

Function

The **arp-limit** command sets the maximum number of ARP entries that an interface can dynamically learn.

The **undo arp-limit** command deletes the maximum number of ARP entries that an interface can dynamically learn.

By default, the maximum number of ARP entries that an interface can dynamically learn is the same as the number of ARP entries supported by the device.

Format

VLANIF interface, VBDIF interface, VE sub-interface, Layer 3 interface, and Ethernet sub-interface:

arp-limit maximum *maximum*

undo arp-limit

VE sub-interface, Layer 2 interface and port group:

arp-limit vlan *vlan-id1* [**to** *vlan-id2*] **maximum** *maximum*

undo arp-limit vlan *vlan-id1* [**to** *vlan-id2*]

NOTE

Only the S5720EI, S5720HI and S6720EI/S6720S-EI support Layer 3 interfaces and sub-interfaces.

Only the S5720HI supports VE sub-interfaces.

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a VLAN from which the maximum number of ARP entries an interface can dynamically learn is limited. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If **to** *vlan-id2* is not specified, the device limits the maximum number of ARP entries an interface dynamically learns from the VLAN *vlan-id1*. If **to** *vlan-id2* is specified, the device limits the maximum number of ARP entries an interface dynamically learns from	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

Parameter	Description	Value
	each VLAN from *vlan-id1* to *vlan-id2*.	
maximum *maximum*	Specifies the maximum number of ARP entries that an interface can dynamically learn.	The value is an integer that ranges as follows: ● S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, S2720EI, S5720LI and S5720S-LI: from 1 to 2048 ● S5720SI and S5720S-SI: from 1 to 4096 ● S5720EI: from 1 to 16384 ● S5720HI: from 1 to 61440 ● S5730SI, S5730S-EI, S6720SI and S6720S-SI: from 1 to 20000 ● S1720X, S1720X-E, S6720LI, and S6720S-LI: from 1 to 8192 ● S6720EI and S6720S-EI: from 1 to 96000 ● Other devices: from 1 to 256

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent ARP entries from being exhausted by ARP attacks from a host connecting to an interface on the device, set the maximum number of ARP entries that the interface can dynamically learn. When the number of the ARP entries learned by a specified interface reaches the maximum number, no dynamic ARP entry can be added.

Precautions

If the number of ARP entries learned by an interface exceeds the maximum number, the device neither learns new ARP entries nor clears the learned ARP entries. Instead, the device asks users to delete the excess ARP entries.

If the **arp-limit vlan** *vlan-id1* **to** *vlan-id2* **maximum** *maximum* command is run more than once, the following situations are available:

- If **maximum** *maximum* is the same in multiple command instances, all configurations take effect. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 35 to 40 maximum 200** command are run, both configurations take effect. If the VLAN ranges specified in multiple command instances are overlapping, the system automatically merges the VLAN ranges. For example, if the **arp-limit vlan 50 to 80 maximum 200** command and then the **arp-limit vlan 70 to 100 maximum 200** command are run, both configurations take effect, and the system merges the configurations into **arp-limit vlan 50 to 100 maximum 200**.
- If **maximum** *maximum* is different in multiple command instances, the latest configuration overrides the previous one for the same VLAN range. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 15 to 25 maximum 300** command are run, the system automatically divides the configurations into **arp-limit vlan 10 to 14 maximum 200**, **arp-limit vlan 15 to 25 maximum 300**, and **arp-limit vlan 26 to 30 maximum 200**.

Example

# Configure that VLANIF 10 can dynamically learn a maximum of 20 ARP entries.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] quit
[HUAWEI] interface vlanif 10
[HUAWEI-Vlanif10] arp-limit maximum 20
```

# Configure that Layer 3 interface GE0/0/1 can dynamically learn a maximum of 20 ARP entries.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-limit maximum 20
```

# Configure that Layer 2 interface GE0/0/1 can dynamically learn a maximum of 20 ARP entries corresponding to VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-limit vlan 10 maximum 20
```

Related Topics

14.6.44 display arp-limit

14.6.29 arp-miss anti-attack rate-limit

Function

The **arp-miss anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP Miss messages globally, in a VLAN, or on an interface.

The **undo arp-miss anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP Miss messages globally, in a VLAN, or on an interface.

By default, the device can process a maximum of 100 ARP Miss messages per second.

NOTE

Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

arp-miss anti-attack rate-limit packet *packet-number* [**interval** *interval-value*]

undo arp-miss anti-attack rate-limit

Parameters

Parameter	Description	Value
packet *packet-number*	Specifies the maximum rate of ARP Miss messages, that is, the number of ARP Miss messages the device processes in the rate limiting duration.	The value is an integer that ranges from 1 to 16384. The default value is 100.
interval *interval-value*	Specifies the rate limiting duration of ARP Miss messages.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, you can set maximum rate and rate limiting duration of ARP Miss messages globally, in a VLAN, or on an interface. If the number of ARP Miss messages triggered by IP packets in the rate limiting duration exceeds the limit, the device does not process the excess ARP Miss packets and discards the IP packets triggering the excess ARP Miss messages.

Prerequisites

Rate limit on ARP Miss messages has been enabled globally, in a VLAN, or on an interface using the **arp-miss anti-attack rate-limit enable** command.

Precautions

If rate limit on ARP Miss messages is configured in the system view, VLAN view, and interface view, the device uses the configurations in the interface view, VLAN view, and system view in order.

Example

# Configure the device to process a maximum of 200 ARP Miss messages triggered by IP packets from Layer 2 interface GE0/0/1 in 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit packet 200 interval 10
```

# Configure the device to process a maximum of 200 ARP Miss messages triggered by IP packets from Layer 3 interface GE0/0/1 in 10 seconds.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit packet 200 interval 10
```

Related Topics

14.6.32 arp-miss anti-attack rate-limit enable

14.6.30 arp-miss anti-attack rate-limit alarm enable

Function

The **arp-miss anti-attack rate-limit alarm enable** command enables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

The **undo arp-miss anti-attack rate-limit alarm enable** command disables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

By default, the alarm function is disabled.

NOTE

Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

arp-miss anti-attack rate-limit alarm enable

undo arp-miss anti-attack rate-limit alarm enable

Parameters

None

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, if you want that the device can generate alarms to notify the network administrator of a large number of discarded excess ARP Miss messages, run the **arp-miss anti-attack rate-limit alarm enable** command. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp-miss anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command.

Example

# Enable the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
```

# Enable the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
```

Related Topics

14.6.29 arp-miss anti-attack rate-limit

14.6.31 arp-miss anti-attack rate-limit alarm threshold

14.6.32 arp-miss anti-attack rate-limit enable

14.6.31 arp-miss anti-attack rate-limit alarm threshold

Function

The **arp-miss anti-attack rate-limit alarm threshold** command sets the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss packets exceeds the limit.

The **undo arp-miss anti-attack rate-limit alarm threshold** command restores the default alarm threshold.

By default, the alarm threshold for ARP Miss packets discarded is 100.

NOTE

Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

arp-miss anti-attack rate-limit alarm threshold *threshold*

undo arp-miss anti-attack rate-limit alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.	The value is an integer that ranges from 1 to 16384, in pps.

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **arp-miss anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp-miss anti-attack rate-limit alarm enable** command.

Example

# Enable rate limit on ARP Miss messages globally, enable the alarm function, and set the alarm threshold to 200.

```
<HUAWEI> system-view
[HUAWEI] arp-miss anti-attack rate-limit enable
[HUAWEI] arp-miss anti-attack rate-limit alarm enable
[HUAWEI] arp-miss anti-attack rate-limit alarm threshold 200
```

# Enable rate limit on ARP Miss messages on Layer 2 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm threshold 200
```

# Enable rate limit on ARP Miss messages on Layer 3 interface GE0/0/1, enable the alarm function, and set the alarm threshold to 200.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm enable
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit alarm threshold 200
```

Related Topics

14.6.29 arp-miss anti-attack rate-limit

14.6.30 arp-miss anti-attack rate-limit alarm enable

14.6.32 arp-miss anti-attack rate-limit enable

14.6.32 arp-miss anti-attack rate-limit enable

Function

The **arp-miss anti-attack rate-limit enable** command enables rate limit on ARP Miss messages globally, in a VLAN, or on an interface.

The **undo arp-miss anti-attack rate-limit enable** command disables rate limit on ARP Miss messages globally, in a VLAN, or on an interface.

By default, rate limit on ARP Miss messages is disabled globally, in a VLAN, or on an interface.

NOTE

Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

arp-miss anti-attack rate-limit enable

undo arp-miss anti-attack rate-limit enable

Parameters

None

Views

System view, VLAN view, GE interface view, 40GE interface view, XGE interface view, MultiGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device, that is, if the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route, the device triggers a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the CPU for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, configure rate limit on ARP Miss messages globally, in a VLAN, or on an interface. The device collects statistics on ARP Miss messages. If the number of ARP Miss messages generated within the rate limiting duration exceeds the threshold (the maximum number of ARP Miss messages), the gateway discards the IP packets triggering the excess ARP Miss messages.

Follow-up Procedure

Run the **arp-miss anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP Miss messages.

Example

# Enable rate limit on ARP Miss messages on Layer 2 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
```

# Enable rate limit on ARP Miss messages on Layer 3 interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] arp-miss anti-attack rate-limit enable
```

Related Topics

14.6.29 arp-miss anti-attack rate-limit

14.6.33 arp-miss speed-limit source-ip

Function

The **arp-miss speed-limit source-ip** command sets the maximum number of ARP Miss messages based on source IP addresses and specifies the mode for processing ARP Miss packets.

The **undo arp-miss speed-limit source-ip** command restores the default setting.

By default, the device processes a maximum of 30 ARP Miss messages triggered by IP packets from the same source IP address per second.

If the number of ARP Miss messages triggered by IP packets from the same source IP address per second exceeds the limit, the device discards the excess ARP Miss messages, that is, the device discards the excess ARP Miss packets. The device then uses the **block** mode to discard all ARP Miss packets from the source IP address within 5 minutes by default.

NOTE

Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

arp-miss speed-limit source-ip *ip-address* [**mask** *mask*] **maximum** *maximum* [**none-block** | **block timer** *timer*] (The S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI do not support [**none-block** | **block timer** *timer*].)

arp-miss speed-limit source-ip maximum *maximum*

undo arp-miss speed-limit source-ip [*ip-address* [**mask** *mask*]]

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the maximum number of ARP Miss messages triggered by packets from this IP address is limited. If this parameter is not specified, the maximum number of ARP Miss messages triggered by packets from each IP address is limited.	The value is in dotted decimal notation.
mask *mask*	Specifies the mask of the IP address. If this parameter is specified, the maximum number of ARP Miss messages triggered by packets from IP addresses in the network segment is limited.	The value is an integer that ranges from 1 to 32.

Parameter	Description	Value
maximum *maximum*	Specifies the maximum number of ARP Miss messages based on the source IP address. **NOTE** If the maximum number of ARP Miss messages triggered by packets from each IP address is limited, a large value is recommended for this parameter because a small value may cause discarding of valid packets. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The value is an integer that ranges from 0 to 4096 for the S5720SI and S5720S-SI, 0 to 16384 for the S5720EI, and from 0 to 61440 for the S5720HI, 0 to 8192 for the S6720LI and S6720S-LI, 0 to 20000 for the S5730SI, S5730S-EI, S6720SI and S6720S-SI, 0 to 96000 for the S6720EI and S6720S-EI. If the value is 0, the maximum number of ARP Miss messages is not limited based on the source IP address.
none-block	Indicates that ARP Miss packets are processed in **none-block** mode. If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the CPU of the device discards the excess ARP Miss messages, that is, the CPU discards the excess ARP Miss packets.	-
block timer *timer*	Indicates that ARP Miss packets are processed in **block** mode. If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device discards the excess ARP Miss messages and delivers an ACL to enable the chip to discard all packets that are sent from this source IP address within the period specified by *timer*. When the period specified by *timer* expires, the ACL ages out and the chip does not discard ARP Miss packets from the source IP address and sends them to the CPU for processing.	The value ranges from 5 to 864000, in seconds. The default value is 5 minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device considers that an attack is initiated from the source IP address. If the ARP Miss message processing mode is set to **block**, the device discards excess ARP Miss packets from this source IP address and delivers an ACL to discard all subsequent packets sent from this source IP address. If the ARP Miss message processing mode is set to **none-block**, the device only discards excess ARP Miss packets.

The administrator can use the **arp-miss speed-limit source-ip** command to set the maximum number of ARP Miss packets and specify the mode for processing ARP Miss packets based on the actual network environment.

If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device considers that an attack is initiated from the source IP address. The administrator can use the **arp-miss speed-limit source-ip** command to set the maximum number of ARP Miss messages that the device can process within a specified duration, protecting the system resources and ensuring proper running of other services.

Precautions

You can set the maximum number of ARP Miss messages for a maximum of 512 IP addresses.

If the ARP Miss packet processing mode is set to **none-block**, the device discards ARP Miss packets triggering excess ARP Miss messages to reduce CPU load. The non-block action can cause a high CPU usage, and the block action uses ACL resources. The default ARP Miss packet processing mode is recommended.

In the process of setting the maximum number of ARP Miss messages based on source IP addresses, if the ARP Miss packet processing mode is not specified, the device use the default processing mode **block**.

When the maximum number of ARP Miss packets exceeds the limit, the delivered ACL discards only the ARP Miss packets from the source IP address. Other packets can still be sent to the CPU.

A maximum of 16 ACLs can be delivered to the chip to discard ARP Miss packets from a specified IP address or network segment. When the device delivers 16 ACLs and all ACLs do not age out, and the number of ARP Miss packets from other IP addresses or network segments per second exceeds the limit, the device does not deliver any ACL to discard all subsequent packets and the CPU discards excess ARP packets.

NOTE

The S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI cannot deliver ACLs to discard ARP Miss packets.

Example

# Set the maximum number of ARP Miss messages triggered by each source IP address per second to 60.

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip maximum 60
```

# Set the maximum number of ARP Miss messages triggered by the IP address 10.0.0.1 per second to 100, and set the maximum number of ARP Miss messages triggered by other source IP addresses per second to 60.

```
<HUAWEI> system-view
[HUAWEI] arp-miss speed-limit source-ip maximum 60
[HUAWEI] arp-miss speed-limit source-ip 10.0.0.1 maximum 100
```

Related Topics

14.6.36 display arp anti-attack configuration

14.6.34 display arp anti-attack arpmiss-record-info

Function

The **display arp anti-attack arpmiss-record-info** command displays information recorded by the device when rate limit on ARP Miss messages is triggered.

NOTE

Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

display arp anti-attack arpmiss-record-info [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Displays the IP address of discarded ARP Miss packets.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After rate limit on ARP Miss messages is triggered, the device discards excess ARP Miss messages. You can run this command to view information recorded by the device when rate limit on ARP Miss messages is triggered. The information helps locate and rectify faults.

The device can record a maximum of 256 records about rate limit on ARP Miss messages. If a new round of rate limit on ARP Miss messages is triggered when the number of records reaches 256, the device takes the following actions:

1. If the source IP address of the attacker already exists in a record, the device updates the block time in the record using the discarding time of the new ARP Miss message.
2. If the source IP address of the attacker does not exist in any record, the device deletes the first record and adds a new record for this attacker.

Example

# Display information recorded by the device when rate limit on ARP Miss messages is triggered.

```
<HUAWEI> display arp anti-attack arpmiss-record-info
Interface    IP address      Attack time         Block time         Aging-time
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
The number of record(s) in arp-miss table is 0
```

Table 14-37 Description of the display arp anti-attack arpmiss-record-info command output

Item	Description
Interface	Interface where ARP Miss packets are discarded.
IP address	Source IP address of discarded ARP Miss packets.
Attack time	First time when rate limit on ARP Miss messages is triggered, that is, time when the number of ARP Miss messages exceeds the limit.
Block time	Last time when the device discards the ARP Miss messages of the attacker.
Aging-time	Period during which the device discards ARP Miss packets. If the ARP Miss packet processing mode is set to **none-block**, the values of **Block time** and **Aging-time** are both 0. If the ARP Miss packet processing mode is set to **block**, the value of **Aging-time** is configured by the **14.6.33 arp-miss speed-limit source-ip** command, and the default value is 5 seconds.

Related Topics

14.6.33 arp-miss speed-limit source-ip

14.6.35 display arp anti-attack configuration check user-bind

Function

The **display arp anti-attack configuration check user-bind** command displays the configuration of DAI in a VLAN or on an interface.

Format

display arp anti-attack configuration check user-bind [**vlan** [*vlan-id*] | **interface** [*interface-type interface-number*]]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays DAI configuration in the specified VLAN. If *vlan-id* is not specified, the DAI configurations in all VLANs are displayed.	*vlan-id* is an integer that ranges from 1 to 4094.
interface [*interface-type interface-number*]	Displays DAI on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If *interface-type interface-number* is not specified, the DAI configurations on all interfaces are displayed. If neither **vlan** [*vlan-id*] nor **interface** [*interface-type interface-number*] is specified, the DAI configurations in all VLANs and on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the configuration of DAI in a VLAN or on an interface, including whether the function is enabled, check items, whether the alarm function is enabled for discarded ARP packets, and alarm threshold.

Only after DAI and the alarm function are enabled, output of this command is displayed.

Example

# Display DAI configuration on GE0/0/1.

```
<HUAWEI> display arp anti-attack configuration check user-bind interface gigabitethernet 0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 50
 arp anti-attack check user-bind check-item ip-address
```

# Display ARP check configurations in all VLANs and on all interfaces.

```
<HUAWEI> display arp anti-attack configuration check user-bind
#
vlan 2
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind check-item ip-address
#
vlan 3
 arp anti-attack check user-bind enable
#
GigabitEthernet0/0/1
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 50
 arp anti-attack check user-bind check-item ip-address
#
```

Table 14-38 Description of the display arp anti-attack configuration check user-bind command output

Item	Description
arp anti-attack check user-bind enable	DAI has been enabled. You can run the **14.6.6 arp anti-attack check user-bind enable** command to enable DAI.
arp anti-attack check user-bind alarm enable	The alarm function for ARP packets discarded by DAI has been enabled. You can run the **14.6.2 arp anti-attack check user-bind alarm enable** command to enable the alarm function.

Item	Description
arp anti-attack check user-bind alarm threshold 50	Alarm threshold of discarded ARP packets matching no binding entry. You can run the **14.6.3 arp anti-attack check user-bind alarm threshold** command to set the alarm threshold.
arp anti-attack check user-bind check-item ip-address	Only the IP address is checked during ARP packet check based on binding entries. You can run the **14.6.4 arp anti-attack check user-bind check-item (interface view)** command or **14.6.5 arp anti-attack check user-bind check-item (VLAN view)** command to specify the check item for ARP packet check based on binding entries.

Related Topics

14.6.6 arp anti-attack check user-bind enable

14.6.4 arp anti-attack check user-bind check-item (interface view)

14.6.2 arp anti-attack check user-bind alarm enable

14.6.3 arp anti-attack check user-bind alarm threshold

14.6.5 arp anti-attack check user-bind check-item (VLAN view)

14.6.36 display arp anti-attack configuration

Function

The **display arp anti-attack configuration** command displays the ARP anti-attack configuration.

Format

display arp anti-attack configuration { **arp-rate-limit** | **arp-speed-limit** | **entry-check** | **arpmiss-rate-limit** | **arpmiss-speed-limit** | **gateway-duplicate** | **log-trap-timer** | **packet-check** | **all** } (Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support **arpmiss-rate-limit**, **arpmiss-speed-limit** and **gateway-duplicate**.)

Parameters

Parameter	Description	Value
arp-rate-limit	Displays the configuration of rate limit on ARP packets globally, in a VLAN, or on an interface.	-

Parameter	Description	Value
arp-speed-limit	Displays the configuration of rate limit on ARP packets based on the source IP address or source MAC address.	-
entry-check	Displays the ARP entry fixing mode.	-
arpmiss-rate-limit	Displays the configuration of rate limit on ARP Miss messages globally, in a VLAN, or on an interface.	-
arpmiss-speed-limit	Displays the configuration of rate limit on ARP Miss messages based on the source IP address.	-
gateway-duplicate	Displays whether gateway anti-collision is enabled.	-
log-trap-timer	Displays the interval for sending ARP alarms.	-
packet-check	Displays whether ARP packet validity check is enabled.	-
all	Displays all ARP anti-attack configurations.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After all ARP anti-attack functions are configured, you can run this command to check all configurations.

Example

# Display the configuration of rate limit on ARP packets based on the source IP address or source MAC address.

```
<HUAWEI> display arp anti-attack configuration arp-speed-limit
ARP speed-limit for source-MAC configuration:
MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 0
-------------------------------------------------------------------------------
The number of configured specified MAC address(es) is 0, spec is 512.

ARP speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
10.1.1.1            100
Others              0
-------------------------------------------------------------------------------
The number of configured specified IP address(es) is 1, spec is 512.
```

# Display the configuration of rate limit on ARP Miss messages based on the source IP address.

```
<HUAWEI> display arp anti-attack configuration arpmiss-speed-limit
 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
 -------------------------------------------------------------------------
 10.0.0.30/32        400
 Others              0
 -------------------------------------------------------------------------
 The number of configured specified IP address(es) is 1, spec is 512.
```

# Display the ARP entry fixing mode.

```
<HUAWEI> display arp anti-attack configuration entry-check
 ARP anti-attack entry-check mode:
 Vlanif      Mode
-------------------------------------------------------------------------------
 All         send-ack
-------------------------------------------------------------------------------
```

# Display all ARP anti-attack configurations.

```
<HUAWEI> display arp anti-attack configuration all
ARP anti-attack packet-check configuration:
-------------------------------------------------------------------------------
Sender-MAC checking function: disable
Dst-MAC checking function: disable
IP checking function: disable
-------------------------------------------------------------------------------

ARP gateway-duplicate anti-attack function: disabled

ARP anti-attack log-trap-timer: 0 second(s)
(The log and trap timer of speed-limit, default is 0 and means disabled.)

ARP anti-attack entry-check mode:
Vlanif      Mode
-------------------------------------------------------------------------------
All         disabled
-------------------------------------------------------------------------------

ARP rate-limit configuration:
-------------------------------------------------------------------------------
Global configuration:
Interface configuration:
  GigabitEthernet0/0/10 :
    arp anti-attack rate-limit enable
    arp anti-attack rate-limit packet 10 interval 1
VLAN configuration:
-------------------------------------------------------------------------------
```

```
ARP miss rate-limit configuration:
-------------------------------------------------------------------------------
Global configuration:
Interface configuration:
VLAN configuration:
-------------------------------------------------------------------------------

ARP speed-limit for source-MAC configuration:
MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 0
-------------------------------------------------------------------------------
The number of configured specified MAC address(es) is 0, spec is 512.

ARP speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 0
-------------------------------------------------------------------------------
The number of configured specified IP address(es) is 0, spec is 512.

ARP miss speed-limit for source-IP configuration:
IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
All                 500
-------------------------------------------------------------------------------
The number of configured specified IP address(es) is 0, spec is 512.
```

Table 14-39 Description of the display arp anti-attack configuration all command output

Item	Description
ARP anti-attack packet-check configuration	Whether ARP packet validity check is enabled. - **Sender-mac checking function** indicates that the source MAC address is checked. - **Dst-mac checking function** indicates that the destination MAC address is checked. - **Ip checking function** indicates that the IP address is checked. You can run the **14.6.10 arp anti-attack packet-check** command to enable ARP packet validity check.
ARP gateway-duplicate anti-attack function	Whether ARP gateway anti-collision is enabled. You can run the **14.6.8 arp anti-attack gateway-duplicate enable** command to enable ARP gateway anti-collision.
ARP anti-attack log-trap-timer	Interval for sending ARP alarms You can run the **14.6.9 arp anti-attack log-trap-timer** command to set the interval for sending ARP alarms.

Item	Description
ARP anti-attack entry-check mode	ARP entry fixing mode. **Vlanif** specifies the interface to which the ARP entry fixing mode is applied. The modes include: ● fixed-mac ● fixed-all ● send-ack ● disabled You can run the **14.6.7 arp anti-attack entry-check enable** command to set the ARP entry fixing mode.
ARP rate-limit configuration	Configuration of rate limit on ARP packets. ● **Global configuration** indicates the global configuration of rate limit on ARP packets. ● **Interface configuration** indicates the configuration of rate limit on ARP packets on an interface. ● **Vlan configuration** indicates the configuration of rate limit on ARP packets in a VLAN. You can run the **14.6.11 arp anti-attack rate-limit** command to configure rate limit on ARP packets.
ARP miss rate-limit configuration	Configuration of rate limit on ARP Miss messages. ● **Global configuration** indicates the global configuration of rate limit on ARP Miss messages. ● **Interface configuration** indicates the configuration of rate limit on ARP Miss messages on an interface. ● **Vlan configuration** indicates the configuration of rate limit on ARP Miss messages in a VLAN. You can run the **14.6.29 arp-miss anti-attack rate-limit** command to configure rate limit on ARP Miss messages.
ARP speed-limit for source-MAC configuration	Rate limit on ARP packets based on the source MAC address. You can run the **14.6.24 arp speed-limit source-mac** command to configure rate limit on ARP packets based on the source MAC address.
ARP speed-limit for source-IP configuration	Rate limit on ARP packets based on the source IP address. You can run the **14.6.25 arp speed-limit source-ip** command to configure rate limit on ARP packets based on the source IP address.

Item	Description
ARP miss speed-limit for source-IP configuration	Rate limit on ARP Miss messages based on source IP addresses. You can run the **14.6.33 arp-miss speed-limit source-ip** command to configure rate limit on ARP Miss messages based on the source IP address.
The number of configured specified MAC address(es) is 0, spec is 512.	Number (0) of the configured source MAC addresses based on which the rate of ARP packets or ARP Miss messages is limited, and the maximum value (512) allowed.
The number of configured specified IP address(es) is 1, spec is 512.	Number (1) of the configured source IP addresses based on which the rate of ARP packets or ARP Miss messages is limited, and the maximum value (512) allowed.
MAC-address	Rate limit on ARP packets based on a specified MAC address. ● **ALL** indicates all MAC addresses. ● **Others** indicates other MAC addresses except for the specified MAC address.
IP-address	Rate limit on ARP packets and ARP Miss messages based on a specified IP address. ● **ALL** indicates all IP addresses. ● **Others** indicates other IP addresses except for the specified IP address.
suppress-rate	Rate limit on ARP packets and ARP Miss messages. Value 0 indicates that the rate limit function is disabled for ARP packets and ARP Miss messages. You can run the **arp anti-attack rate-limit packet** *packet-number* command to configure the rate limit of ARP packets, and run the **arp-miss anti-attack rate-limit packet** *packet-number* command to configure the rate limit of ARP Miss messages.

14.6.37 display arp anti-attack gateway-duplicate item

Function

The **display arp anti-attack gateway-duplicate item** command displays ARP gateway anti-collision entries.

NOTE

Only the S5720HI, S5720EI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

display arp anti-attack gateway-duplicate item

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP gateway anti-collision is enabled, you can run this command to view ARP anti-collision entries.

Example

# Display ARP gateway anti-collision entries.

```
<HUAWEI> display arp anti-attack gateway-duplicate item
 Interface              IP address       MAC address      VLANID   Aging time
-------------------------------------------------------------------------------
 GigabitEthernet0/0/1    10.1.1.1         0000-0000-0002  2        150
 GigabitEthernet0/0/2    10.1.1.2         0000-0000-0004  2        170
-------------------------------------------------------------------------------
The number of record(s) in gateway conflict table is 2
```

Table 14-40 Description of the display arp anti-attack gateway-duplicate item command output

Item	Description
Interface	Inbound interface of ARP packets.
IP address	IP address of the gateway.
MAC address	Source MAC address of ARP packets.
VLANID	VLAN ID of ARP packets.
Aging time	Aging time of entries. The maximum value is 180 seconds. This parameter cannot be configured.

Related Topics

14.6.8 arp anti-attack gateway-duplicate enable

14.6.38 display arp anti-attack packet-check statistics

Function

The **display arp anti-attack packet-check statistics** command displays the statistics on invalid ARP packets that are filtered out during ARP packet validity check.

Format

display arp anti-attack packet-check statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP packet validity check is enabled, if you want to view the statistics on invalid ARP packets that are filtered out, you can run this command.

Example

# Display the statistics on invalid ARP packets that are filtered out in ARP packet validity check is displayed.

```
<HUAWEI> display arp anti-attack packet-check statistics
Number of ARP packet(s) checked:                    5
Number of ARP packet(s) dropped by sender-mac checking: 0
Number of ARP packet(s) dropped by dst-mac checking:    0
Number of ARP packet(s) dropped by src-ip checking:     2
Number of ARP packet(s) dropped by dst-ip checking:     0
```

Table 14-41 Description of the display arp anti-attack packet-check statistics command output

Item	Description
Number of ARP packet(s) checked	Number of ARP packets whose validity is checked.
Number of ARP packet(s) dropped by sender-mac checking	Number of invalid ARP packets that are filtered out because the source MAC address in the packet is different from that in the Ethernet frame header.

Item	Description
Number of ARP packet(s) dropped by dst-mac checking	Number of invalid ARP packets that are filtered out because the destination MAC address in the packet is different from that in the Ethernet frame header.
Number of ARP packet(s) dropped by src-ip checking	Number of invalid ARP packets with invalid source IP addresses that are filtered out.
Number of ARP packet(s) dropped by dst-ip checking	Number of invalid ARP packets with invalid destination IP addresses that are filtered out.

Related Topics

14.6.10 arp anti-attack packet-check

14.6.39 display arp anti-attack statistics check user-bind interface

Function

The **display arp anti-attack statistics check user-bind interface** command displays the statistics on discarded ARP packets matching no binding entry.

Format

display arp anti-attack statistics check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. Where, ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DAI and the alarm function are enabled, you can run this command to display the statistics on discarded ARP packets matching no binding entry.

Example

# Display the statistics on discarded ARP packets matching no binding entry on GE0/0/1.

```
<HUAWEI> display arp anti-attack statistics check user-bind interface gigabitethernet 0/0/1
 Dropped ARP packet number is 966
 Dropped ARP packet number since the latest warning is 605
```

Table 14-42 Description of the display arp anti-attack statistics check user-bind interface command output

Item	Description
Dropped ARP packet number is 966	Number of discarded ARP packets matching no DHCP snooping binding entry.
Dropped ARP packet number since latest warning is 605	Statistics on discarded ARP packets matching no DHCP snooping binding entry after the latest alarm is generated.

Related Topics

14.6.6 arp anti-attack check user-bind enable

14.6.4 arp anti-attack check user-bind check-item (interface view)

14.6.2 arp anti-attack check user-bind alarm enable

14.6.3 arp anti-attack check user-bind alarm threshold

14.6.40 display arp learning strict

Function

The **display arp learning strict** command displays strict ARP learning globally and on all interfaces.

Format

display arp learning strict

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After strict ARP learning is configured, you can run this command to check the configuration.

Example

# Display strict ARP learning globally and on all interfaces.

```
<HUAWEI> display arp learning strict
The global configuration:arp learning strict
 Interface                        LearningStrictState
------------------------------------------------------------
 Vlanif100                         force-disable
 Vlanif200                         force-enable
------------------------------------------------------------
 Total:2
 Force-enable:1
 Force-disable:1
```

Table 14-43 Description of the display arp learning strict command output

Item	Description
The global configuration	Global strict ARP learning. The value **arp learning strict** indicates that strict ARP learning has been enabled. If the parameter is left blank, strict ARP learning is disabled. You can run the **14.6.21 arp learning strict (system view)** command to enable strict ARP learning.
Interface	Interface name.
LearningStrictState	Strict ARP learning. ● The value **force-enable** indicates that strict ARP learning is enabled. ● The value **force-disable** indicates that strict ARP learning is disabled. You can run the **14.6.20 arp learning strict (interface view)** command to enable strict ARP learning.

Item	Description
Total	Total number of interfaces to which strict ARP learning is applied.
Force-enable	Number of the interfaces on which strict ARP learning is enabled.
Force-disable	Number of the interfaces on which strict ARP learning is disabled.

Related Topics

14.6.21 arp learning strict (system view)

14.6.20 arp learning strict (interface view)

14.6.41 display arp optimized-reply statistics

Function

The **display arp optimized-reply statistics** command displays statistics on optimized ARP Reply packets.

Format

display arp optimized-reply statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics on optimized ARP Reply packets after the optimized ARP reply function is enabled on the device.

Example

# Display statistics on optimized ARP Reply packets.

```
<HUAWEI> display arp optimized-reply statistics
Slot          Received          Processed            Dropped
-------------------------------------------------------------
0                  11                 9                  7
```

Table 14-44 Description of the display arp optimized-reply statistics command output

Item	Description
Slot	Stack ID.
Received	Number of ARP Request packets entering the processing procedure of the optimized ARP reply function.
Processed	Number of optimized ARP Reply packets.
Dropped	Number of ARP Request packets discarded.

Related Topics

14.6.22 arp optimized-reply disable

14.6.49 reset arp optimized-reply statistics

14.6.42 display arp optimized-reply status

Function

The **display arp optimized-reply status** command displays the status of the optimized ARP reply function.

Format

display arp optimized-reply status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the status of the optimized ARP reply function.

Example

# Check the status of the optimized ARP reply function.

```
<HUAWEI> display arp optimized-reply status
Current configuration:Disable
Actual         status:Inactive
Related configuration:
   arp optimized-reply disable
   arp anti-attack check user-bind enable
   arp anti-attack gateway-duplicate enable
```

Table 14-45 Description of the display arp optimized-reply status command output

Item	Description
Current configuration	Configuration of the optimized ARP reply function. ● Enable ● Disable To set this field, run the **14.6.22 arp optimized-reply disable** command.
Actual status	Status of the optimized ARP reply function. ● Active ● Inactive
Related configuration	Configuration that results in the invalid optimized ARP reply function. If the optimized ARP reply function has taken effect, this field is not displayed.

Related Topics

14.6.22 arp optimized-reply disable

14.6.43 display arp packet statistics

Function

The **display arp packet statistics** command displays the statistics on ARP packets.

Format

display arp packet statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate and rectify ARP faults, you can run this command to view the statistics on ARP packets.

This command displays the ARP packet statistics on the active switch in a stack system.

Example

# Display the statistics on ARP packets.

```
<HUAWEI> display arp packet statistics
ARP Pkt Received: sum 420066
ARP Received In Message-cache: sum 0
ARP-Miss Msg Received: sum 0
ARP Learnt Count: sum 5
ARP Pkt Discard For Limit: sum 0
ARP Pkt Discard For SpeedLimit: sum 0
ARP Pkt Discard For Proxy Suppress: sum 179578
ARP Pkt Discard For Other: sum 90347
ARP-Miss Msg Discard For SpeedLimit: sum 0
ARP Discard In Message-cache For SpeedLimit: sum 0
ARP-Miss Msg Discard For Other: sum 0
```

Table 14-46 Description of the display arp packet statistics command output

Item	Description
ARP Pkt Received	Number of the received ARP packets.
ARP Received In Message-cache	Number of ARP packets received within each second when a switch encapsulates multiple ARP request packets into one packet.
ARP-Miss Msg Received	Total number of ARP Miss messages triggered by ARP Miss packets sent to the CPU.
ARP Learnt Count	Times of ARP learning.
ARP Pkt Discard For Limit	Number of ARP packets discarded due to the ARP entry limit. To configure the maximum number of dynamic ARP entries that an interface can learn, run the **arp-limit** command.

Item	Description
ARP Pkt Discard For SpeedLimit	Number of ARP packets discarded when the number of ARP packets from a specified source IP address exceeds the limit. To configure a rate limit for ARP packets based on the source IP address, run the **arp speed-limit source-ip** command.
ARP Pkt Discard For Proxy Suppress	Number of packets discarded for the speed limit.
ARP Pkt Discard For Other	Number of the packets discarded due to other causes.
ARP-Miss Msg Discard For SpeedLimit	Number of ARP Miss messages discarded when the number of ARP Miss messages triggered by IP packets from a specified source IP address exceeds the limit.
ARP Discard In Message-cache For SpeedLimit	Number of ARP packets discarded due to software rate limit when a switch encapsulates multiple ARP request packets into one packet. To configure a rate limit for ARP Miss messages based on the source IP address, run the **arp-miss speed-limit source-ip** command.
ARP-Miss Msg Discard For Other	Number of the ARP Miss messages discarded due to other causes.

14.6.44 display arp-limit

Function

The **display arp-limit** command displays the maximum number of ARP entries that an interface can dynamically learn.

Format

display arp-limit [**interface** *interface-type interface-number*[*.subinterface-number*]] [**vlan** *vlan-id*]

NOTE

Only the S5720EI, S5720HI and S6720EI/S6720S-EI support sub-interface.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*[*.subinterface-number*]	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. ● *subinterface-number* specifies the sub-interface number.	-
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the maximum number of ARP entries that an interface can dynamically learn is set, you can run this command to check the configuration.

If **interface** *interface-type interface-number*[*.subinterface-number*] and **vlan** *vlan-id* are specified, you can view the maximum number of ARP entries that the specified interface can dynamically learn in the specified VLAN. If the two parameters are not specified, the maximum number of ARP entries that each interface can dynamically learn is displayed.

Example

# Display the number of ARP entries that each interface can dynamically learn.

```
<HUAWEI> display arp-limit
 Interface               LimitNum        VlanID          LearnedNum(Mainboard)
-------------------------------------------------------------------------
 Vlanif100               1000           0                0
 GigabitEthernet0/0/1    16384          10               0
 -------------------------------------------------------------------------
 Total:2
```

Table 14-47 Description of the display arp-limit command output

Item	Description
Interface	Interface name.
LimitNum	Maximum number of ARP entries that an interface can dynamically learn. To configure the maximum number of dynamic ARP entries that an interface can learn, run the **arp-limit** command.
VlanID	ID of the VLAN that the interface belongs to.
LearnedNum(Mainboard)	Number of ARP entries that an interface has learned.

Related Topics

14.6.28 arp-limit

14.6.45 display arp-miss speed-limit source-ip

Function

The **display arp-miss speed-limit source-ip** command displays the configuration of rate limit on ARP Miss message based on the source IP address.

NOTE

Only the S5720EI, S5720HI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI support this command.

Format

display arp-miss speed-limit source-ip

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP Miss rate limiting based on source IP address is configured, you can run this command to check the configuration.

Example

# Display the configuration of rate limit on ARP Miss messages based on the source IP address.

```
<HUAWEI> display arp-miss speed-limit source-ip
 Slot     SuppressType   SuppressValue
 ---------------------------------------------------
 0        ARP-miss       600
```

Table 14-48 Description of the display arp-miss speed-limit source-ip command output

Item	Description
Slot	- The value indicates the slot ID if stacking is not configured. - The value indicates the stack ID if stacking is configured.
SuppressType	Suppression type.
SuppressValue	Maximum rate of ARP Miss messages from a specified source IP address. To configure a rate limit for ARP Miss messages based on the source IP address, run the **arp-miss speed-limit source-ip** command.

Related Topics

14.6.33 arp-miss speed-limit source-ip

14.6.46 reset arp anti-attack packet-check statistics

Function

The **reset arp anti-attack packet-check statistics** command clears the statistics on invalid ARP packets that are filtered out during ARP packet validity check.

Format

reset arp anti-attack packet-check statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to clear existing statistics, and run the **display arp anti-attack packet-check statistics** command to view the statistics on follow-up invalid ARP packets that are filtered out.

Example

# Clear the statistics on invalid ARP packets that are filtered out in ARP packet validity check.

```
<HUAWEI> reset arp anti-attack packet-check statistics
```

14.6.47 reset arp anti-attack statistics check user-bind

Function

The **reset arp anti-attack statistics check user-bind** command clears the statistics on discarded ARP packets matching no binding entry.

Format

reset arp anti-attack statistics check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. Where, ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

User view, system view

Default Level

2: Configuration level

Usage Guidelines

After DAI is enabled and some ARP packets matching no binding entry are discarded, you can run this command to clear the statistics on the discarded ARP packets.

Example

# Clear the statistics on discarded ARP packets on GE0/0/1.

```
<HUAWEI> reset arp anti-attack statistics check user-bind interface gigabitethernet 0/0/1
```

Related Topics

14.6.6 arp anti-attack check user-bind enable

14.6.48 reset arp anti-attack statistics rate-limit

Function

The **reset arp anti-attack statistics rate-limit** command clears the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit.

Format

reset arp anti-attack statistics rate-limit

Parameters

None

Views

User view, system view

Default Level

2: Configuration level

Usage Guidelines

After rate limit on ARP packets is enabled globally, the device discards the excess packets when the rate of ARP packets exceeds the limit. You can run this command to clear the statistics on the discarded ARP packets.

Example

# Clear the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit.

```
<HUAWEI> reset arp anti-attack statistics rate-limit
```

Related Topics

14.6.14 arp anti-attack rate-limit enable

14.6.49 reset arp optimized-reply statistics

Function

The **reset arp optimized-reply statistics** command clears statistics on optimized ARP Reply packets.

Format

reset arp optimized-reply statistics [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID.	The value must be set according to the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To collect statistics on optimized ARP Reply packets on the device, you can run the **reset arp optimized-reply statistics** [**slot** *slot-id*] command to clear statistics on optimized ARP Reply packetsof the device.

Example

# Clears statistics on optimized ARP Reply packets.

```
<HUAWEI> reset arp optimized-reply statistics
```

Related Topics

14.6.41 display arp optimized-reply statistics

14.6.50 reset arp packet statistics

Function

The **reset arp packet statistics** command clears the statistics on ARP packets.

Format

reset arp packet statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display arp packet statistics** command to display the statistics on ARP packets. To obtain correct statistics, run the **reset arp packet statistics** command to clear existing statistics first.

The **reset arp packet statistics** command clears the ARP packet statistics on the active switch in a stack system.

Example

# Clear the statistics on all ARP packets.

```
<HUAWEI> reset arp packet statistics
```

14.7 Port Security Configuration Commands

14.7.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.7.2 display mac-address sec-config

Function

The **display mac-address sec-config** command displays secure static MAC address entries.

Format

display mac-address sec-config [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the secure static MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays the secure static MAC address entries on a specified interface.	-
verbose	Displays detailed information about secure static MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After secure static MAC address entries are configured by the command **port-security mac-address**, you can run the **display mac-address sec-config** command to check these entries.

Example

# Display all secure static MAC address entries.

```
<HUAWEI> display mac-address sec-config
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                   Learned-From        Type
-------------------------------------------------------------------------------
0022-0022-0033 100/-/-                      GE0/0/1            sec-config

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-49 Description of the display mac-address sec-config command output

Item	Description
MAC Address	Destination MAC address in a secure static MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or the ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. The value is **sec-config**, which indicates a secure static MAC address.

Related Topics

14.7.7 port-security mac-address

14.7.3 display mac-address security

Function

The **display mac-address security** command displays secure dynamic MAC address entries.

Format

display mac-address security [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays secure dynamic MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
interface-type interface-number	Displays secure dynamic MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about secure dynamic MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface by using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. The learned secure dynamic MAC address entries are deleted after the device restarts.

After configuring the port security function, you can run the **display mac-address security** command to check whether the learned secure dynamic MAC address entries are correct.

Follow-up Procedure

If the displayed secure dynamic MAC address entries are invalid, run the **undo mac-address security** command to delete secure dynamic MUX MAC address entries.

Precautions

If you run the **display mac-address security** command without parameters, all secure dynamic MAC address entries are displayed.

If the MAC address table does not contain any secure dynamic MAC address entry, no information is displayed.

When the device has a large number of secure dynamic MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

# Display all secure dynamic MAC address entries.

```
<HUAWEI> display mac-address security
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                    Learned-From        Type
-------------------------------------------------------------------------------
0022-0022-0033 100/-/-                        GE0/0/1             security
0000-0000-0001 200/-/-                        GE0/0/2             security

-------------------------------------------------------------------------------
Total items displayed = 2
```

# Display detailed information about all secure dynamic MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address security vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 0000-0000-0001           VLAN : 10
Learned-From: GE0/0/1              Type : security
Aging-Time  : 200s

-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-50 Description of the display mac-address security command output

Item	Description
MAC Address	Destination MAC address in a secure dynamic MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or the ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. The value is **security**, which indicates a secure dynamic MAC address.
Aging-Time	How soon a secure dynamic MAC address entry will be aged out.

Related Topics

5.1.13 display mac-address summary

5.1.14 display mac-address total-number

14.7.6 port-security enable

14.7.4 display mac-address sticky

Function

The **display mac-address sticky** command displays sticky VLAN MAC address entries.

Format

display mac-address sticky [**vlan** *vlan-id* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays sticky MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays sticky MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about sticky MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the switch stores MAC addresses of other devices. When forwarding an Ethernet frame, the switch searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

After port security is enabled on an interface by using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. The learned secure dynamic MAC address entries are deleted after the switch restarts. If the sticky MAC function is also enabled on the interface by using the **port-security mac-address sticky** command, secure dynamic MAC address entries change to sticky MAC address entries. Sticky MAC address entries are not deleted after the switch restarts.

To check the sticky MAC configuration or the learned sticky MAC address entries, run the **display mac-address sticky** command.

Follow-up Procedure

If the displayed sticky MAC address entries are invalid, run the **undo mac-address sticky** command to delete sticky MAC address entries.

Precautions

If you run the **display mac-address sticky** command without parameters, all sticky MAC address entries are displayed.

If the MAC address table does not contain any sticky MAC address, no information is displayed.

When the switch has a large number of sticky MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

# Display all sticky MAC address entries.

```
<HUAWEI> display mac-address sticky
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                       Learned-From        Type
-------------------------------------------------------------------------------
0022-0022-0033 100/-/-                         GE0/0/1           sticky
0000-0000-0001 200/-/-                         GE0/0/2           sticky

-------------------------------------------------------------------------------
Total items displayed = 2
```

# Display detailed information about all sticky MAC address entries in VLAN 10.

```
<HUAWEI> display mac-address sticky vlan 10 verbose
-------------------------------------------------------------------------------
MAC Address : 0000-0000-0001            VLAN : 10
Learned-From: GE0/0/1                   Type : sticky
```

```
-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-51 Description of the display mac-address sticky command output

Item	Description
MAC Address	MAC address in a sticky MAC address entry.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or the ID of the BD that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry. The value is **sticky**, which indicates a sticky MAC address.

Related Topics

5.1.13 display mac-address summary

5.1.14 display mac-address total-number

14.7.6 port-security enable

14.7.8 port-security mac-address sticky

14.7.5 port-security aging-time

Function

The **port-security aging-time** command sets the aging time of secure dynamic MAC addresses on an interface.

The **undo port-security aging-time** command restores the default configuration.

By default, secure dynamic MAC addresses will not be aged out.

Format

port-security aging-time *time* [**type** { **absolute** | **inactivity** }]

undo port-security aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time of secure dynamic MAC addresses.	The value is an integer that ranges from 1 to 1440, in minutes.
type	Specifies the type of the aging time.	The default type is **absolute**, indicating the absolute aging time.

Parameter	Description	Value
absolute	Indicates the absolute aging time. After the aging time of secure dynamic MAC addresses is set, the system calculates the lifetime of each MAC address every minute. If the lifetime of a MAC address plus 1 is greater than or equal to *time* minutes, the secure dynamic MAC address is aged immediately. If the lifetime is smaller than *time* minutes, the system determines whether to delete the secure dynamic MAC address after 1 minute.	-
inactivity	Indicates the relative aging time. After the relative aging time is set to *time* minutes, the system checks traffic from each secure dynamic MAC address every 1 minute. If no traffic is received from a secure dynamic MAC address, this MAC address is aged out after *time* minutes.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **port-security enable** command to enable port security on an interface, MAC address entries learned by the interface are saved in the MAC address table as secure dynamic MAC addresses. The learned secure dynamic MAC addresses will not be aged by default. When the number of learned MAC addresses reaches the limit, the interface cannot learn new MAC addresses.

If MAC addresses learned by an interface can be trusted only for a certain period, run the **port-security aging-time** command to set the aging time of secure dynamic MAC addresses on the interface. Then secure dynamic MAC addresses can be aged out and the interface can learn new MAC addresses.

Prerequisites

Port security is enabled on the interface.

Precautions

If the aging time of secure dynamic MAC addresses on an interface is shorter than the global aging time of dynamic MAC addresses, secure dynamic MAC addresses are aged out when the global aging time expires.

If you run the **port-security aging-time** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Set the aging time of secure dynamic MAC addresses on GE0/0/1 to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security aging-time 30
```

Related Topics

14.7.6 port-security enable

14.7.6 port-security enable

Function

The **port-security enable** command enables the port security function on an interface.

The **undo port-security enable** command disables the port security function on an interface.

By default, port security is disabled on an interface.

Format

port-security enable

undo port-security enable

Parameters

None

Views

GE interface view, Ethernet interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. By default, secure dynamic MAC addresses will not be aged out. If the aging time of secure dynamic MAC address entries is set, these entries will be aged out. After the device restarts, secure dynamic MAC address entries are lost and need to be relearned.You can also create secure static MAC addresses which do not age out.

Port security has the following functions:

- Prevent unauthorized guests from using their computers to connect to an enterprise network.
- Prevent employees of a company from moving their computers without permission.

Precautions

- The total number of MAC addresses on interfaces enabled with port security cannot exceed 4096. For example, if the numbers of MAC addresses learned on interfaces 1, 2, 3, and 4 are 1000 respectively, interface 5 can learn a maximum of 96 MAC addresses.
- The protection action, maximum number of learned secure MAC address entries, and secure static MAC addresses, sticky MAC function can be configured only after port security is enabled.
- Port security and MAC address limiting conflict on an interface; therefore, the **port-security enable** and **mac-limit maximum** commands cannot be used on the same interface.
- Port security and MUX VLAN conflict on an interface; therefore, the **port-security enable** and **port mux-vlan enable** commands cannot be used on the same interface.
- Port security and NAC conflict on an interface; therefore, the **port-security enable** and **mac-authen**, **dot1x enable**, or **authentication-profile** commands cannot be used on the same interface.
- Port security and generating snooping MAC entries conflict on an interface; therefore, the **port-security enable** and **user-bind ip sticky-mac** commands cannot be used on the same interface.
- If port security is enabled after MAC address learning is disabled using the **mac-address learning disable** command, the dynamic port security function does not take effect. If port security is enabled before MAC address learning is disabled on an interface, the device no longer learns MAC addresses on the

interface, but secure MAC addresses that have been learned are reserved (including secure static MAC addresses).

Example

# Enable port security on GigabitEthernet0/0/2.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] port-security enable
```

Related Topics

14.7.10 port-security protect-action

14.7.9 port-security max-mac-num

14.7.8 port-security mac-address sticky

14.7.5 port-security aging-time

14.7.7 port-security mac-address

Function

The **port-security mac-address** command configures a static secure MAC address.

The **undo port-security mac-address** command deletes a static secure MAC address.

By default, a static secure MAC address is not configured.

Format

port-security mac-address *mac-address* **vlan** *vlan-id*

undo port-security mac-address *mac-address* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a static secure MAC address.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits. The MAC address cannot be The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **port-security enable** command is used to configure port security, the learned MAC address becomes a dynamic secure MAC address.

When the interface becomes Down or the device is reset, static secure MAC addresses are not affected, and dynamic secure MAC addresses need to be learned again. Static secure MAC addresses are not aged out. Static secure MAC addresses have higher priority than dynamic secure MAC addresses.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

You can run the **port-security mac-address** *mac-address* **vlan** *vlan-id* command multiple times to configure multiple static secure MAC addresses.

The static secure MAC cannot be the virtual MAC address of the Virtual Router Redundancy Protocol (VRRP).

Example

# Configure a static secure MAC address on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security mac-address 286E-D488-B6FF vlan 10
```

Related Topics

14.7.6 port-security enable

14.7.8 port-security mac-address sticky

Function

The **port-security mac-address sticky** enables the sticky MAC function on an interface.

The **undo port-security mac-address sticky** disables the sticky MAC function on an interface.

By default, the sticky MAC function is disabled on an interface.

Format

port-security mac-address sticky [*mac-address* **vlan** *vlan-id*]

undo port-security mac-address sticky [*mac-address* **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a sticky MAC address entry. **NOTE** This parameter is not supported in the port group view.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. A MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Specifies the ID of a VLAN. **NOTE** This parameter is not supported in the port group view.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries.

After the sticky MAC function is enabled on an interface, the dynamic MAC addresses learned by the interface change to sticky MAC addresses. If the number of sticky MAC addresses does not reach the limit, the MAC addresses learned subsequently change to sticky MAC addresses. When the number of sticky MAC addresses reaches the limit, packets whose source MAC addresses do not match sticky MAC address entries are discarded. In addition, the system determines whether to send a trap message or shut down the interface according to the configured security protection action.

After enabling the sticky MAC function on an interface, you can run the **port-security mac-address sticky** *mac-address* **vlan** *vlan-id* command to manually configure a sticky MAC address entry.

The sticky MAC function has the following functions:

- Prevent non-employees from using their own computers to access the company intranet without the permission of the network administrator.
- Prevent employees from moving network devices or computers of the company without the permission of the network administrator.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

Running the **undo port-security mac-address sticky** command will convert the sticky MAC addresses on the interface into secure dynamic MAC addresses.

The configuration information is not displayed after you run the **port-security mac-address sticky** [*mac-address* **vlan** *vlan-id*] command to configure sticky MAC address entries.

If you run the **port-security mac-address sticky** [*mac-address* **vlan** *vlan-id*] command multiple times, multiple sticky MAC address entries are configured.

Sticky MAC can not be the virtual MAC address of the Virtual Router Redundancy Protocol (VRRP).

Example

# Enable the sticky MAC function on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security mac-address sticky
```

Related Topics

14.7.6 port-security enable

14.7.9 port-security max-mac-num

14.7.9 port-security max-mac-num

Function

The **port-security max-mac-num** command sets the maximum number of secure MAC addresses that can be learned on an interface.

The **undo port-security max-mac-num** command restores the default maximum number of secure MAC addresses that can be learned on an interface.

By default, only one MAC address can be learned on an interface.

Format

port-security max-mac-num *max-number*

undo port-security max-mac-num

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of secure MAC addresses that can be learned by an interface.	The value is an integer that ranges from 1 to 1024.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security on an interface, you can run the **port-security max-mac-num** command to limit the number of MAC addresses that the interface can learn. If the switch receives packets with a nonexistent source MAC address after the number of secure MAC addresses reaches the limit, the switch considers that the packets are sent from an unauthorized user, regardless of whether the destination MAC address of packets is valid, and takes the action configured using the **port-security protect-action** command on the interface. This prevents untrusted users from accessing these interfaces, improving security of the switch and the network.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

- The total number of MAC addresses on interfaces enabled with port security cannot exceed 4096. For example, if the numbers of MAC addresses learned on interfaces 1, 2, 3, and 4 are 1000 respectively, interface 5 can learn a maximum of 96 MAC addresses.
- If the sticky MAC function is disabled, *max-number* limits the number of secure dynamic MAC addresses learned by the interface and secure static MAC addresses configured manually.

- If the sticky MAC function is enabled, *max-number* limits the number of sticky MAC addresses learned by the interface, and sticky MAC addresses and secure static MAC addresses configured manually.
- If you run the **port-security max-mac-num** command multiple times in the same interface view, only the latest configuration takes effect.

Example

# Set the maximum number of MAC addresses that can be learned by GigabitEthernet0/0/1 to 5.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security max-mac-num 5
```

Related Topics

14.7.6 port-security enable

14.7.8 port-security mac-address sticky

14.7.10 port-security protect-action

Function

The **port-security protect-action** command configures the protection action to be used when the number of learned MAC addresses on an interface exceeds the upper limit or static MAC address flapping is detected.

The **undo port-security protect-action** command restores the default protection action.

The default action is **restrict**.

Format

port-security protect-action { **protect** | **restrict** | **shutdown** }

undo port-security protect-action

Parameters

Parameter	Description	Value
protect	● Discards packets with new source MAC addresses when the number of learned MAC addresses exceeds the limit. ● When static MAC address flapping occurs, the interface discards the packets with this MAC address.	-
restrict	● Discards packets with new source MAC addresses and sends a trap message when the number of learned MAC addresses exceeds the limit. ● When static MAC address flapping occurs, the interface discards the packets with this MAC address and sends a trap.	-
shutdown	● Set the interface status to error down and sends a trap message when the number of learned MAC addresses exceeds the limit. ● When static MAC address flapping occurs, the interface takes the error down action and sends a trap.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security, you can run the **port-security protect-action** command to configure the action performed on the interface when the number of learned MAC addresses on an interface exceeds the upper limit or static MAC address flapping is detected.

The default action **restrict** is recommended. If the action is set to **shutdown** on an interface connected to a downstream device, the interface discards packets from trusted MAC addresses. Select the **shutdown** action only when the interface is directly connected to a user terminal.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

The interface takes protection actions when detecting static MAC address flapping only after the **port-security static-flapping protect** command is executed.

If the action is set to **shutdown**, the interface takes the error down action when the number of learned MAC addresses exceeds the limit or static MAC address flapping is detected. In addition, the interface status will not be automatically recovered.

If you run the **port-security protect-action** command multiple times in the same interface view, only the latest configuration takes effect.

If both port security and traffic policy-based VLAN translation are configured on an interface of the S5720EI, S5720HI, S6720EI, and S6720S-EI, the interface can forward protocol packets with source MAC addresses out of the MAC address table when the number of learned MAC addresses exceeds the limit.

Example

# Set the protection action on GigabitEthernet0/0/1 to **protect**.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-security enable
[HUAWEI-GigabitEthernet0/0/1] port-security protect-action protect
```

Related Topics

14.7.6 port-security enable

14.7.8 port-security mac-address sticky

14.7.11 port-security static-flapping protect

Function

The **port-security static-flapping protect** command enables static MAC address flapping detection.

The **undo port-security static-flapping protect** command disables static MAC address flapping detection.

By default, static MAC address flapping detection is disabled.

Format

port-security static-flapping protect

undo port-security static-flapping protect

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Secure MAC addresses are also static MAC address. When an interface receives a packet of which the source MAC address exists in the static MAC table on another interface, the interface discards this packet. This affects customer services. For example, when PC 1 connects to GE0/0/1 where sticky MAC is enabled, the sticky MAC table of GE0/0/1 includes PC 1's MAC address. When PC 1 is disconnected from GE0/0/1 and connected to GE0/0/2, GE0/0/2 discards the packets from PC 1. In this situation, you can enable static MAC address flapping detection. Then the interface will take the configured action.

Precautions

Static MAC address flapping detection is supported only on the interfaces with port security enabled.

Example

# Enable static MAC address flapping detection.

```
<HUAWEI> system-view
[HUAWEI] port-security static-flapping protect
```

14.7.12 undo mac-address security

Function

The **undo mac-address security** command deletes secure MAC address entries. Secure MAC address entries include dynamic and static secure MAC address entries and sticky MAC address entries.

Format

undo mac-address { **sec-config** | **security** | **sticky** } [*interface-type interface-number* | **vlan** *vlan-id*] *

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the outbound interface in a secure MAC address entry to be deleted.	-
vlan *vlan-id*	Specifies the VLAN ID in a secure MAC address entry to be deleted.	The value is an integer that ranges from 1 to 4094.
sec-config	Deletes static secure MAC address entries.	-
security	Deletes dynamic secure MAC address entries, that is, MAC address entries learned by an interface enabled with port security.	-
sticky	Deletes sticky MAC address entries, that is, MAC address entries learned by an interface enabled with the sticky MAC function.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After port security is enabled on an interface, dynamic MAC address entries learned by the interface turn into secure MAC address entries. secure MAC address entries are not aged out. After the number of MAC address entries learned by an interface reaches the limit, the interface cannot learn new MAC address entries. Packets matching no MAC address entry are broadcast, wasting bandwidth resources. This command can delete useless secure MAC address entries to release the MAC address table space.

You can delete some of secure MAC address entries as required. For example:

- If you do not specify *interface-type interface-number*, the command deletes MAC address entries of the specified type on all interfaces.
- If you do not specify **vlan** *vlan-id*, the command deletes MAC address entries of the specified type in all VLANs.

Example

# Delete all static secure MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address sec-config
```

# Delete all dynamic secure MAC address entries on gigabitethernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address security gigabitethernet 0/0/1
```

# Delete all sticky MAC address entries.

```
<HUAWEI> system-view
[HUAWEI] undo mac-address sticky
```

Related Topics

5.1.53 undo mac-address

14.7.7 port-security mac-address

14.7.8 port-security mac-address sticky

14.8 DHCP Snooping Configuration Commands

14.8.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.8.2 arp dhcp-snooping-detect enable

Function

The **arp dhcp-snooping-detect enable** command enables association between the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) snooping.

The **undo arp dhcp-snooping-detect enable** command disables association between ARP and DHCP snooping.

By default, association between ARP and DHCP snooping is disabled.

Format

arp dhcp-snooping-detect enable

undo arp dhcp-snooping-detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP client sends a DHCP Release message to release its IP address, the DHCP snooping-enabled device immediately deletes the binding entry of the

DHCP client. If a DHCP client is abnormally disconnected and cannot send a DHCP Release message, the DHCP snooping-enabled device cannot immediately delete the binding entry of the DHCP client.

If association between ARP and DHCP snooping is enabled using this command and no ARP entry corresponding to the IP address in the DHCP snooping binding entry is found, the DHCP snooping-enabled device performs an ARP probe on the IP address. If no user is detected for consecutive four times, the DHCP snooping-enabled device deletes the DHCP snooping binding entry corresponding to the IP address. (The probe interval is 20 seconds, and the probe times and probe interval are fixed values and cannot be modified.) If the DHCP snooping-enabled device supports the DHCP relay function, this device then sends a DHCP Release message in place of the DHCP client to notify the DHCP server to release the IP address.

Prerequisites

Before association between the ARP and DHCP snooping is enabled, ensure that an IP address configured on the device is on the same network segment as the IP address of the client for ARP probe.

Example

# Enable association between ARP and DHCP snooping on the device.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] arp dhcp-snooping-detect enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.3 dhcp option82 append vendor-specific

Function

The **dhcp option82 append vendor-specific** command inserts the Sub9 suboption into Option 82.

The **undo dhcp option82 append vendor-specific** command restores the default configuration.

By default, Sub9 suboption is not inserted into the Option 82 field of DHCP messages.

Format

dhcp option82 append vendor-specific

undo dhcp option82 append vendor-specific

Parameters

None

Views

Interface view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **dhcp option82 append vendor-specific** command is run on a DHCP relay agent or DHCP snooping device, the device will insert the Sub9 suboption into the Option 82 field of a received DHCP message. When this DHCP message is forwarded to the DHCP server, the server obtains the DHCP client location information from the Sub9 suboption.

The Sub9 suboption has old and new formats. The old format contains the vendor ID, for example, hwid. The new format does not contain the vendor ID.

Both the **dhcp option82 append vendor-specific** and **14.8.8 dhcp option82 vendor-specific format** commands can insert the Sub9 into the Option 82 field of the DHCP message, except that the Sub9 formats are different:

- **dhcp option82 append vendor-specific**: inserts the Sub9 of the new format. The new format includes the location information such as the node identifier, node chassis ID, node slot ID, node port number, and user VLAN.
- **14.8.8 dhcp option82 vendor-specific format**: inserts the Sub9 of the old format. The old format includes the DHCP client information such as user IP address and device name.

Precautions

- When both the **dhcp option82 append vendor-specific** and **14.8.8 dhcp option82 vendor-specific format** commands are run, the **dhcp option82 append vendor-specific** command takes effect.
- The Sub9 suboption can be inserted into Option 82 only when the Sub9 format is the same as the DHCP packet format. If the formats are different:
  - If the **14.8.8 dhcp option82 vendor-specific format** command has been run, the Sub9 of the new format cannot be inserted into Option 82.
  - If the **dhcp option82 append vendor-specific** command has been run, whether the Sub9 of the old format can be inserted depends on the Option 82 insertion method (which is configured using the **14.8.4 dhcp option82 enable** command).
    - When the Option 82 insertion method is Insert, the Sub9 is not inserted.
    - When the Option 82 insertion method is Rebuild, the Sub9 is reconstructed and then inserted into Option 82.
- The total length of the Option 82 field cannot exceed 255 bytes.

Example

# Insert the Sub9 suboption into the Option 82 field of DHCP messages.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 append vendor-specific
```

14.8.4 dhcp option82 enable

Function

The **dhcp option82 enable** command enables a device to insert the Option 82 field to a DHCP message.

The **undo dhcp option82 enable** command disables a device from inserting the Option 82 field to a DHCP message.

By default, a device does not insert the Option 82 field to a DHCP message.

Format

In the interface view and port group view

dhcp option82 { **insert** | **rebuild** } **enable**

undo dhcp option82 { **insert** | **rebuild** } **enable**

In the VLAN view

dhcp option82 { **insert** | **rebuild** } **enable interface** *interface-type interface-number1* [**to** *interface-number2*]

undo dhcp option82 { **insert** | **rebuild** } **enable interface** *interface-type interface-number1* [**to** *interface-number2*]

Parameters

Parameter	Description	Value
insert	Enables a device to insert the Option 82 field to a DHCP message.	-
rebuild	Enables a device to forcibly insert the Option 82 field to a DHCP message.	-
interface *interface-type interface-number1* [**to** *interface-number2*]	Specifies the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	If this command is run in the VLAN view, the specified interface must have been added to the VLAN.

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

The device inserts the Option 82 field to a DHCP message in two modes:

- Insert mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device checks whether the Option 82 field contains the remote ID. If so, the device retains the Option 82 field; if not, the device inserts the remote ID.
- Rebuild mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device deletes the original Option 82 field and inserts the Option 82 field set by the administrator.

The device handles the reply packets from the DHCP server in the same way regardless of whether the Insert or Rebuild method is used.

- The DHCP reply packets contain Option 82:
  - If the DHCP request packets received by the device do not contain Option 82, the device deletes Option 82 from the DHCP reply packets, and forwards the packets to the DHCP client.
  - If the DHCP request packets contain Option 82, the device changes the Option 82 format in the DHCP reply packets into the Option 82 format in the DHCP request packets, and forwards the packets to the DHCP client.
- If the DHCP reply packets do not contain Option 82, the device directly forwards the packets.

NOTE

The physical interface can insert Option82 to the DHCP packets directly forwarded, but does not insert Option82 to the DHCP packets forwarded through a tunnel.

Prerequisites

DHCP snooping has been enabled on the device, or the device has been configured as a DHCP relay agent.

Precautions

- When receiving a DHCP Request message, the device checks whether the field GIADDR in the packet is 0. If so, the **dhcp option82 enable** command takes effect; if not, this command does not take effect.
- DHCP Option 82 must be configured on the user-side of a device; otherwise, the DHCP messages sent to the DHCP server will not carry Option 82.

Example

# Enable the device to insert the Option 82 field to DHCP messages on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 insert enable
```

Related Topics

6.3.28 dhcp select relay

14.8.20 dhcp snooping enable

14.8.41 display dhcp option82 configuration

14.8.5 dhcp option82 encapsulation

Function

The **dhcp option82 encapsulation** command configures suboptions inserted into the DHCP Option 82 field.

The **undo dhcp option82 encapsulation** command restores the default suboptions inserted into the DHCP Option 82 field.

By default, the circuit-id (CID), remote-id (RID), subscriber-id, and Sub9suboptions are inserted into the DHCP Option 82 field.

Format

dhcp option82 encapsulation { **circuit-id** | **remote-id** | **subscriber-id** | **vendor-specific-id** }*

undo dhcp option82 encapsulation

Parameters

Parameter	Description	Value
circuit-id	Inserts the circuit-id suboption.	-
remote-id	Inserts the remote-id suboption.	-
subscriber-id	Inserts the subscriber-id (SID) suboption.	-
vendor-specific-id	Inserts the vendor-specific suboption in the Sub9 field.	-

Views

System view, VLAN view, interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This function applies to a DHCP relay agent or a DHCP snooping-enabled device. The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security. The administrator can run this command to configure the device to insert one or more of the circuit-id suboption, remote-id suboption, subscriber-id suboption, and vendor-specific suboption in the Sub9 field into the DHCP Option 82 field. After the command is run, suboptions that are not configured to be inserted are not inserted into the DHCP Option 82 field by default.

Prerequisites

The DHCP function has been enabled in the system view using the **dhcp enable** command.

Example

# Insert the circuit-id suboption into the DHCP Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 encapsulation circuit-id
```

14.8.6 dhcp option82 format

Function

The **dhcp option82 format** command configures the format of the Option 82 field in a DHCP message.

The **undo dhcp option82 format** command restores the default format of the Option 82 field in a DHCP message.

By default, the Option 82 field in a DHCP message is in the format of **default**.

Format

dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }

undo dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format**

Parameters

Parameter	Description	Value
circuit-id	Indicates the circuit ID (CID) in the Option 82 field. If the CID is not specified, the format of the Option 82 field is **default**.	-
remote-id	Indicates the remote ID (RID) in the Option 82 field. If the RID is not specified, the format of the Option 82 field is **default**.	-
default	Indicates the default format of the Option 82 field. ● CID format: interface name:svlan.cvlan host name/0/0/0/0/0, in ASCII format ● RID format: device MAC address, in hexadecimal notation	-
common	Indicates the common format of the Option 82 field. ● CID format: {eth|trunk}slot ID/subcard ID/ port ID:svlan.cvlan host name0/0/0/0/0, in ASCII format ● RID format: device MAC address (6 bytes), in ASCII format	-
extend	Indicates the extended format of the Option 82 field. ● CID format: circuit-id type (0) + length (4) + S-VLAN ID (2 bytes) + slot ID (5 bits) + subslot ID (3 bits) + port (1 byte), in hexadecimal notation ● RID format: remote-id type (0) + length (6) + device MAC address (6 bytes), in hexadecimal notation In the CID and RID formats, the values without a unit are fixed values of the fields; the values with a unit indicate the field lengths.	-
user-defined *text*	Indicates the user-defined format of the Option 82 field.	The value is a string of 1 to 255 characters. For details, see the description in "Usage Guideline."

Parameter	Description	Value
vlan *vlan-id*	Indicates an outer VLAN ID. If a VLAN ID is specified, only the format of the Option 82 field in the DHCP messages sent from the specified VLAN is configured. If no VLAN is specified, the format of the Option 82 field in all the DHCP messages received by the interface is configured.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Indicates an inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of inserting the Option 82 field to DHCP messages is enabled, you can use the **dhcp option82 format** command to configure the format of the Option 82 field.

If you run the **dhcp option82 format** command in the system view, the command takes effect for all the DHCP messages on all the interfaces of the device.

You can use the following keywords to define the Option 82 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, GE0/0/1. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.

- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The keyword length can be configured only once.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 82 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in a character string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

- A hexadecimal notation string can contain numerals, spaces, and % + keywords.
- In a hexadecimal notation string, numbers are encapsulated in the Option 82 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
- All the spaces in a hexadecimal character string are ignored.
- By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
- If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
- A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
- If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Precautions

- All Option82 fields configured in the system view or in the same interface view share a length of 1-255 bytes. If their total length exceeds 255 bytes, some Option82 information will be lost.
- There is no limit on the number of Option 82 fields configured on the device. However, a large number of Option 82 fields will occupy a lot of memory and prolong the device processing time. To ensure device performance, you are advised to configure Option 82 fields based on the service requirements and device memory size.

Example

# Configure the default format for the CID in the Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 circuit-id format default
```

# Configure the extended format for the CID and RID in the Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 format extend
```

# Configure the user-defined string for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 circuit-id format user-defined "%portname:%svlan.%cvlan %sysname"
```

# Configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot %3subslot %8port
```

# Configure the user-defined string for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 remote-id format user-defined %mac
```

# On GE0/0/1, configure the default format for the CID in the Option 82 field.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 circuit-id format default
```

# On GE0/0/1, configure the extended format for the CID and RID in the Option 82 field of DHCP messages from VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 vlan 10 format extend
```

# On GE0/0/1, configure a user-defined format for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 circuit-id format user-defined "%portname:%svlan.
%cvlan %sysname"
```

# On GE0/0/1, configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot
%3subslot %8port
```

# On GE0/0/1, configure the user-defined format for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 remote-id format user-defined %mac
```

Related Topics

14.8.4 dhcp option82 enable

14.8.7 dhcp option82 subscriber-id format

Function

The **dhcp option82 subscriber-id format** command inserts the Sub6 suboption into the DHCP Option 82 field of DHCP messages and configures the format of the Sub6 suboption.

The **undo dhcp option82 subscriber-id format** command cancels the configuration of the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages.

By default, the Sub6 suboption is not inserted into the DHCP Option 82 field of DHCP messages.

Format

dhcp option82 subscriber-id format { **ascii** *ascii-text* | **hex** *hex-text* }

undo dhcp option82 subscriber-id format

Parameters

Parameter	Description	Value
ascii *ascii-text*	Specifies the ASCII character string in the Sub6 field.	The value is an ASCII character string and contains fewer than 129 characters.
hex *hex-text*	Specifies the HEX character string in the Sub6 field.	The value is in hexadecimal notation. The value can contain only digits 0 to 9, uppercase letters A to F, and lowercase letters a to f. If no space is included, the value length must be an even number smaller than 257.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an authentication system for wired Ethernet access based on DHCP, DHCP snooping, and Option82, a device can insert suboptions (suboption 1, suboption 2, suboption 6, and suboption 9) into the Option 82 field in DHCP Request messages. These suboptions in DHCP Request messages help locate user devices. Unauthorized users cannot access the network by using static IP addresses or stealing accounts of authorized users. You can run the **dhcp option82 subscriber-id format** command to configure the Sub6 suboption.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

# Configure the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages on GE0/0/1 and specify the ASCII character string in the Sub6 suboption.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp option82 subscriber-id format ascii hw
```

14.8.8 dhcp option82 vendor-specific format

Function

The **dhcp option82 vendor-specific format** command configures the Sub9 field in the Option 82 field.

The **undo dhcp option82 vendor-specific format** command deletes the configuration of the Sub9 field inserted into the DHCP Option 82 field.

By default, the Sub9 field inserted into the Option 82 field is not configured.

Format

dhcp option82 vendor-specific format vendor-sub-option *sub-option-num* { **ascii** *ascii-text* | **hex** *hex-text* | **ip-address** *ip-address* &<1-8> | **sysname** }

undo dhcp option82 vendor-specific format vendor-sub-option *sub-option-num*

Parameters

Parameter	Description	Value
vendor-sub-option *sub-option-num*	Specifies the vendor-specific suboption in the Sub9 field.	The value is an integer that ranges from 1 to 255.
ascii *ascii-text*	Specifies the ASCII character string in the vendor-specific suboption in the Sub9 field.	The value is an ASCII character string and must be smaller than 129 characters.

Parameter	Description	Value
hex *hex-text*	Specifies the HEX character string in the vendor-specific suboption in the Sub9 field.	The value is in hexadecimal notation. The value can contain only numerals 0 to 9, lowercase letters a to f, and uppercase letters A to F. If no space is included, the value length must be an even number smaller than 257.
ip-address *ip-address*	Specifies the IP address in the vendor-specific suboption in the Sub9 field.	-
sysname	Specifies the device name in the vendor-specific suboption in the Sub9 field.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In authentication for wired Ethernet access using DHCP, DHCP snooping, and Option 82, a device can insert suboptions (suboption 1, suboption 2, and suboption 9) to the Option 82 field in DHCP Request messages. These suboptions in DHCP Request messages carry information about user device locations. Unauthorized users cannot access the network by static IP addresses or embezzled accounts of authorized users. The **dhcp option82 vendor-specific format** command configures the suboptions in the Sub9 field.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

# Insert the device name to the vendor-specific suboption 1 in the Sub9 field.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp option82 vendor-specific format vendor-sub-option 1 sysname
```

Related Topics

6.3.17 dhcp enable

14.8.9 dhcp server detect

Function

The **dhcp server detect** command enables detection of DHCP servers.

The **undo dhcp server detect** command disables detection of DHCP servers.

By default, detection of DHCP servers is disabled.

Format

dhcp server detect

undo dhcp server detect

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If bogus DHCP servers exist on the network, they send incorrect information to DHCP clients, such as the incorrect gateway address, incorrect DNS server, and incorrect IP address. As a result, DHCP clients cannot access the network or access incorrect networks.

After detection of DHCP servers is enabled, a DHCP snooping device checks and stores all information about DHCP servers in the DHCP Reply messages, such as DHCP server address and DHCP client port number, in the log. Based on logs, the network administrator checks for bogus DHCP servers on the network to maintain the network.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

# Enable detection of DHCP servers.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp server detect
```

Related Topics

14.8.20 dhcp snooping enable

14.8.10 dhcp snooping alarm dhcp-rate enable

Function

The **dhcp snooping alarm dhcp-rate enable** command enables the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.

The **undo dhcp snooping alarm dhcp-rate enable** command disables the device from generating an alarm when the number of discarded DHCP messages reaches the threshold.

By default, the device is disabled from generating an alarm when the number of discarded DHCP messages reaches the threshold.

Format

dhcp snooping alarm dhcp-rate enable [**threshold** *threshold*]

undo dhcp snooping alarm dhcp-rate enable [**threshold**]

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the alarm threshold. If the number of discarded DHCP messages reaches the threshold, an alarm is generated. For details, see the **14.8.11 dhcp snooping alarm dhcp-rate threshold**.	The value is an integer that ranges from 1 to 1000. The default value is 100.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCP Request messages and Reply messages to the processing unit. If the rate of sending DHCP messages is high, processing efficiency of the processing unit is affected. After the **14.8.16 dhcp snooping check dhcp-rate enable** command is run, the device checks the rate of sending DHCP messages. DHCP messages that are sent in a specified rate are sent to the processing unit and those that exceed the rate are discarded.

If the number of discarded DHCP messages reaches the threshold, an alarm is generated. To set the alarm threshold, run the **14.8.11 dhcp snooping alarm dhcp-rate threshold** command.

If you run the **dhcp snooping alarm dhcp-rate enable** command in the system view, the command takes effect on all the interfaces of the device. If you run the **dhcp snooping alarm dhcp-rate enable** command in the interface view, the command only takes effect on the specified interface.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

To ensure that alarms can be properly reported, you need to run the **6.3.99 snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **6.3.69 display snmp-agent trap feature-name dhcp all** command.

Example

# In the system view, enable the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check dhcp-rate enable
[HUAWEI] dhcp snooping alarm dhcp-rate enable
```

# Enable the device to generate an alarm when the number of discarded DHCP messages reaches the threshold on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-rate enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-rate enable
```

Related Topics

14.8.11 dhcp snooping alarm dhcp-rate threshold

14.8.11 dhcp snooping alarm dhcp-rate threshold

Function

The **dhcp snooping alarm dhcp-rate threshold** command sets the alarm threshold for the number of discarded DHCP messages.

The **undo dhcp snooping alarm dhcp-rate threshold** command restores the default alarm threshold for the number of discarded DHCP messages.

By default, the global alarm threshold for the number of discarded DHCP messages is 100, and the alarm threshold for the number of discarded DHCP messages on an interface is the same as that configured in the system view.

Format

dhcp snooping alarm dhcp-rate threshold *threshold*

undo dhcp snooping alarm dhcp-rate threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold. If the number of discarded DHCP messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000. The default value is 100.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **14.8.10 dhcp snooping alarm dhcp-rate enable** command to enable a device to generate an alarm when the number of discarded DHCP messages reaches the threshold, you can set the alarm threshold using the **dhcp snooping alarm dhcp-rate threshold** command. An alarm is generated when the number of discarded DHCP messages reaches the threshold.

If the alarm threshold is set in the system view and interface view, the smaller value takes effect.

Prerequisites

DHCP snooping has been enabled on the device using the **14.8.20 dhcp snooping enable** command.

Example

# Set the alarm threshold for the number of discarded DHCP messages on GE0/0/1 to 50.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-rate threshold 50
```

Related Topics

14.8.10 dhcp snooping alarm dhcp-rate enable

14.8.13 dhcp snooping alarm threshold

14.8.12 dhcp snooping alarm enable

Function

The **dhcp snooping alarm enable** command enables alarm for discarded DHCP messages.

The **undo dhcp snooping alarm enable** command disables alarm for discarded DHCP messages.

By default, the alarm function for discarded DHCP messages is disabled.

Format

dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **enable** [**threshold** *threshold*]

undo dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **enable** [**threshold**]

Parameters

Parameter	Description	Value
dhcp-request	Generates an alarm when the number of DHCPv4 Request messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-
dhcp-chaddr	Generates an alarm when the number of DHCPv4 request messages discarded because the CHADDR field in the DHCP messages does not match the source MAC address in the data frame header reaches the threshold.	-
dhcp-reply	Generates an alarm when the number of DHCPv4 Response messages discarded by untrusted interfaces reaches the threshold.	-

Parameter	Description	Value
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCPv4 messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function is enabled, alarm messages are displayed if DHCP attacks occur and the number of discarded attack messages reaches the threshold. The minimum interval for sending alarm messages is 1 minute. You can run the **14.8.13 dhcp snooping alarm threshold** command to set the alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

By default, a device does not check messages received by the clients. Therefore, to make the command take effect, ensure the following is ready:

- The device has been enabled to check DHCP messages against the binding entries using the **14.8.18 dhcp snooping check dhcp-request enable** command before the **dhcp snooping alarm dhcp-request enable** command is run.
- The device has been enabled to check whether the CHADDR field is the same as the source MAC address in the header of a DHCPv4 Request message using the **14.8.17 dhcp snooping check dhcp-chaddr enable** command before the **dhcp snooping alarm dhcp-chaddr enable** command is run.

To ensure that alarms can be properly reported, you need to run the **6.3.99 snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP module is enabled to report the corresponding alarm using the **6.3.69 display snmp-agent trap feature-name dhcp all** command.

Example

# On GE0/0/1, enable DHCP snooping, enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address in the

Ethernet frame header, and enable alarm for the DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.13 dhcp snooping alarm threshold

14.8.13 dhcp snooping alarm threshold

Function

The **dhcp snooping alarm threshold** command sets the alarm threshold for the number of DHCP messages discarded by DHCP snooping.

The **undo dhcp snooping alarm threshold** command restores the default alarm threshold.

By default, an alarm is generated in the system when at least 100 DHCP snooping messages are discarded, and the alarm threshold on an interface is set using the **dhcp snooping alarm threshold** command in the system view.

Format

In the system view:

dhcp snooping alarm threshold *threshold*

undo dhcp snooping alarm threshold

In the interface view:

dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **threshold** *threshold*

undo dhcp snooping alarm { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **threshold**

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of DHCP snooping-discarded messages.	The value is an integer that ranges from 1 to 1000.

Parameter	Description	Value
dhcp-request	Specifies the alarm threshold for the number of DHCPv4 Request messages discarded because they do not match the DHCP snooping binding entries.	-
dhcp-chaddr	Specifies the alarm threshold for the number of DHCP messages discarded because the CHADDR field in the DHCPv4 request messages does not match the source MAC address in the data frame header.	-
dhcp-reply	Specifies the alarm threshold for the number of DHCPv4 Response messages discarded by untrusted interfaces.	-

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After trap for discarded DHCP messages is enabled, run the **dhcp snooping alarm threshold** command to specify the alarm threshold for the number of DHCP messages discarded by DHCP snooping. If the alarm threshold is not set on an interface, the interface uses the global alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

The DHCP snooping alarm function has been enabled using the **dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **enable** command.

Precautions

If you run the **dhcp snooping alarm threshold** command in the system view, the command takes effect on all the interfaces of the device.

If you specify an alarm threshold for the number of DHCP messages discarded by DHCP snooping in the system view, an alarm is generated when the number of all the discarded DHCP messages reaches the threshold.

Example

# Set the global alarm threshold for the number of discarded DHCP messages to 200.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping alarm threshold 200
```

# On GE0/0/1, enable DHCP snooping, enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address in the Ethernet frame header, and enable alarm for the DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address. Set the alarm threshold to 1000.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm dhcp-chaddr threshold 1000
```

14.8.14 dhcp snooping check dhcp-giaddr enable

Function

The **dhcp snooping check dhcp-giaddr enable** command enables the device to check whether the GIADDR field in DHCP messages is 0.

The **undo dhcp snooping check dhcp-giaddr enable** command disables the device from checking whether the GIADDR field in DHCP messages is 0.

By default, the device does not check whether the GIADDR field in DHCP messages is 0.

Format

In the system view:

dhcp snooping check dhcp-giaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping check dhcp-giaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

In the VLAN view and interface view:

dhcp snooping check dhcp-giaddr enable

undo dhcp snooping check dhcp-giaddr enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check whether the GIADDR field in DHCP messages sent from a specified VLAN is 0. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that the device obtains parameters such as MAC addresses for generating a binding table, DHCP snooping needs to be applied to Layer 2 access devices or the first DHCP relay agent from the device. Therefore, the GIADDR field in the DHCP messages received by the DHCP snooping-enabled device is 0. If the GIADDR field is not 0, the message is unauthorized and then discarded. This function is recommended if DHCP snooping is enabled on the DHCP relay agent.

In normal situations, the GIADDR field in DHCP messages sent by user PCs is 0. If the GIADDR field is not 0, the DHCP server cannot correctly allocate IP addresses. To prevent attackers from applying IP addresses with the DHCP messages containing a non-0 GIADDR field, you are advised to configure this function.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcp-giaddr enable** command in the VLAN view, the command takes effect on all the DHCP messages from the specified VLAN. If you run the **dhcp snooping check dhcp-giaddr enable** command in the interface view, the command takes effect on all the DHCP messages received by the specified interface.

Example

# Enable the device to check whether the GIADDR field in DHCP messages from VLAN1 10 is 0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping check dhcp-giaddr enable
```

# Enable the device to check whether the GIADDR field in DHCP messages received on GE0/0/1 is 0.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-giaddr enable
```

Related Topics

6.3.17 dhcp enable

14.8.20 dhcp snooping enable

14.8.15 dhcp snooping check dhcp-rate

Function

The **dhcp snooping check dhcp-rate** command sets the maximum rate of sending DHCP messages to the processing unit.

The **undo dhcp snooping check dhcp-rate** command restores the default maximum rate of sending DHCP messages to the processing unit.

By default, the maximum rate of sending global DHCP messages to the processing unit is 100 pps, which is the same as the maximum rate of sending DHCP messages on interfaces to the processing unit.

Format

In the system view:

dhcp snooping check dhcp-rate *rate* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping check dhcp-rate

In the VLAN view and interface view:

dhcp snooping check dhcp-rate *rate*

undo dhcp snooping check dhcp-rate

Parameters

Parameter	Description	Value
rate	Specifies the maximum rate of sending DHCP messages to the processing unit.	The value is an integer that ranges from 1 to 100, in pps.

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Specifies the maximum rate of sending DHCP messages from a specified VLAN to the processing unit. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. If this parameter is not specified, the command takes effect on all the DHCP messages.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCP Request messages and Reply messages to the processing unit. If the rate of sending DHCP messages is high, processing efficiency of the processing unit is affected. After the device is enabled to check the rate of sending DHCP messages to the processing unit, run the **dhcp snooping check dhcp-rate** command to set the maximum rate of sending DHCP messages to the processing unit. DHCP messages that exceed the rate are discarded.

Prerequisites

The device has been enabled to check the rate of sending DHCP messages to the processing unit using the **14.8.16 dhcp snooping check dhcp-rate enable** command.

Precautions

If the maximum rates of sending DHCP messages to the processing unit are set in the system view, VLAN view, and interface view, the smallest value takes effect.

Example

# In the system view, set the maximum rate of sending DHCP messages to the processing unit to 50 pps.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
```

```
[HUAWEI] dhcp snooping check dhcp-rate enable
[HUAWEI] dhcp snooping check dhcp-rate 50
```

Related Topics

14.8.16 dhcp snooping check dhcp-rate enable

14.8.16 dhcp snooping check dhcp-rate enable

Function

The **dhcp snooping check dhcp-rate enable** command enables the device to check the rate of sending DHCP messages to the processing unit.

The **undo dhcp snooping check dhcp-rate enable** command disables the device from checking the rate of sending DHCP messages to the processing unit.

By default, the device does not check the rate of sending DHCP messages to the processing unit.

Format

In the system view:

dhcp snooping check dhcp-rate enable [*rate*] [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping check dhcp-rate enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view and interface view:

dhcp snooping check dhcp-rate enable [*rate*]

undo dhcp snooping check dhcp-rate enable

Parameters

Parameter	Description	Value
rate	Specifies the maximum rate of sending DHCP messages to the processing unit. For the function of *rate*, see the command **14.8.15 dhcp snooping check dhcp-rate**.	The value ranges from 1 to 100, in pps. The default value is 100.

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check the rate of sending DHCP messages from a specified VLAN to the processing unit. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. If this parameter is not specified, the command takes effect on all the DHCP messages.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the device sends all the received DHCP Request messages and Reply messages to the processing unit. If the rate of sending DHCP messages is high, processing efficiency of the processing unit is affected. After the device is enabled to check the rate of sending DHCP messages to the processing unit, DHCP messages that exceed the specified rate are discarded.

The default maximum rate of sending DHCP messages is 100 pps. To set the maximum rate, run the **14.8.15 dhcp snooping check dhcp-rate** command.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

# In the system view, enable the device to check the rate of sending DHCP messages to the processing unit.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping check dhcp-rate enable
```

# In VLAN 10, enable the device to check the rate of sending DHCP messages to the processing unit.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
```

```
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping check dhcp-rate enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.15 dhcp snooping check dhcp-rate

14.8.11 dhcp snooping alarm dhcp-rate threshold

14.8.17 dhcp snooping check dhcp-chaddr enable

Function

The **dhcp snooping check dhcp-chaddr enable** command enables the device to check whether the CHADDR field matches the source MAC address in the header of a DHCP Request message.

The **undo dhcp snooping check dhcp-chaddr enable** command disables the device from checking whether the CHADDR field matches the source MAC address in the header of a DHCP Request message.

By default, the device does not check whether the CHADDR field is the same as the source MAC address in the header of a DHCP Request message.

Format

In the system view:

dhcp snooping check dhcp-chaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping check dhcp-chaddr enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

In the VLAN view and interface view:

dhcp snooping check dhcp-chaddr enable

undo dhcp snooping check dhcp-chaddr enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check whether the CHADDR field matches the source MAC address in the header of a DHCP Request message. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, the CHADDR field in a DHCP Request message matches the MAC address of the DHCP client that sends the message. The DHCP server identifies the client MAC address based on the CHADDR field in the DHCP Request message. If attackers continuously apply for IP addresses by changing the CHADDR field in the DHCP Request message, addresses in the address pool on the DHCP server may be exhausted. As a result, authorized users cannot obtain IP addresses.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcp-chaddr enable** command in the VLAN view, the command takes effect on all the DHCP messages in the specified VLAN received by all the interfaces on the device. If you run the **dhcp snooping check dhcp-chaddr enable** command in the interface view, the command takes effect for all the DHCP messages received on the interface.

Example

# Enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-chaddr enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.18 dhcp snooping check dhcp-request enable

14.8.18 dhcp snooping check dhcp-request enable

Function

The **dhcp snooping check dhcp-request enable** enables the device to check DHCP messages against the DHCP snooping binding table.

The **undo dhcp snooping check dhcp-request enable** disables the device from checking DHCP messages against the DHCP snooping binding table.

By default, the device does not check DHCP messages against the DHCP snooping binding table.

Format

In the system view:

dhcp snooping check dhcp-request enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping check dhcp-request enable vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

In the VLAN view and interface view:

dhcp snooping check dhcp-request enable

undo dhcp snooping check dhcp-request enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check DHCP messages from a specified VLAN against the DHCP snooping binding table.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP snooping binding table is generated, the device checks DHCP Request and Release messages against the binding table. The device forwards only DHCP messages that match binding entries. This prevents unauthorized users from sending bogus DHCP Request or Release messages to extend or release IP addresses.

The matching rules are as follows:

- When the device receives a DHCP Request message, it performs the following operations:
    a. Checks whether the destination MAC address is all Fs. If so, the device considers the user to have gone online for the first time and directly forwards the message. If not, the device considers the user to have sent the DHCP Request message to renew the IP address lease and checks the DHCP Request message against the DHCP snooping binding table.
    b. Checks whether the CHADDR field in the DHCP Request message matches a DHCP snooping binding entry. If not, the device considers the user to have gone online for the first time and directly forwards the message. If so, the device checks whether the VLAN ID, IP address, and interface number of the message match DHCP snooping binding entries. If all these fields match a DHCP snooping binding entry, the device forwards the message; otherwise, the device discards the message.
- When receiving a DHCP Release message, the device checks whether the VLAN ID, IP address, MAC address, and interface number of the message match a dynamic DHCP snooping binding entry. If so, the device forwards the message; otherwise, the device discards the message.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcp-request enable** command in the VLAN view, the command takes effect for all the DHCP messages received from the specified VLAN. If you run the **dhcp snooping check dhcp-request enable** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

Example

# Enable the device to check DHCP messages against the DHCP snooping binding table in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping check dhcp-request enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.17 dhcp snooping check dhcp-chaddr enable

14.8.19 dhcp snooping disable

Function

The **dhcp snooping disable** command disables DHCP snooping on an interface.

The **undo dhcp snooping disable** command cancels the configuration.

By default, if the **14.8.20 dhcp snooping enable** command is used on an interface or in a VLAN that an interface belongs to, DHCP snooping is enabled on this interface.

Format

dhcp snooping disable

undo dhcp snooping disable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you run the **dhcp snooping enable** command to enable DHCP snooping in a VLAN, DHCP snooping is enabled on all the interfaces in the VLAN. If you do not run the **dhcp snooping enable** command to enable DHCP snooping on an interface, you cannot run the **undo dhcp snooping enable** command to disable DHCP snooping on the interface. To address this problem, run the **dhcp snooping disable** command to disable DHCP snooping on the interface. Users can properly go online from this interface, but no dynamic binding entry is generated.

Precautions

- The **dhcp snooping disable** command does not only disable DHCP snooping on an interface, but also clears the DHCP snooping configuration and the dynamic binding table. The **undo dhcp snooping enable** command, however, only disables DHCP snooping on the interface and does not clear the configuration or the dynamic binding table.
- The **undo dhcp snooping disable** command enables DHCP snooping on an interface. To enable DHCP snooping, run the **dhcp snooping enable** command.

Example

# Disable DHCP snooping on GE0/0/1 in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping disable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.20 dhcp snooping enable

Function

The **dhcp snooping enable** command enables DHCP snooping.

The **undo dhcp snooping enable** command disables DHCP snooping.

By default, DHCP snooping is disabled on the device.

Format

In the system view:

dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view and interface view:

dhcp snooping enable

undo dhcp snooping enable

Parameters

Parameter	Description	Value
ipv4	Indicates that the device processes only DHCPv4 messages.	-
ipv6	Indicates that the device processes only DHCPv6 messages.	-

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables DHCP snooping in a specified VLAN. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The specified VLAN ID must exist.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCP snooping is a security function to protect DHCP. When you run the **dhcp snooping enable** command to enable DHCP snooping on a device, the device can process both DHCPv4 and DHCPv6 messages. In practice, however, if the DHCP snooping device needs to process only DHCPv4 or DHCPv6 messages, you can run the **dhcp snooping enable ipv4** or **dhcp snooping enable ipv6** command, which improves CPU efficiency.

You must enable DHCP snooping in the system view before enabling DHCP snooping on an interface or in a VLAN.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Follow-up Procedure

After DHCP snooping is enabled on the interface connected to users or in the VLAN, run the **dhcp snooping trusted** command to configure the interface connected to the DHCP server as a trusted interface. The binding entry can be generated only when DHCP snooping is enabled on the interface and the interface is configured as a trusted one.

Precautions

The **dhcp snooping enable** command in the system view is the prerequisite for DHCP snooping-related functions. After the **undo dhcp snooping enable** command is run, all DHCP snooping-related configurations of the device are deleted. After DHCP snooping is enabled again using the **dhcp snooping enable** command, all DHCP snooping-related configurations of the device are restored to the default configurations.

If you run the **dhcp snooping enable** command in the VLAN view, the command takes effect for all the DHCP messages from the specified VLAN. If you run the

dhcp snooping enable command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

If both DHCP relay and VRRP are configured on a device, DHCP snooping cannot be configured.

DHCP snooping cannot be enabled if the DHCP server is at the subordinate VLAN side and the DHCP client is at the principle VLAN side.

Example

# Enable DHCP snooping globally and configure the device to process only ipv4 messages.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable ipv4
```

# Enable DHCP snooping on GE 0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
```

# Enable DHCP snooping in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
```

# Enable DHCP snooping in VLANs ranging from VLAN 20 to VLAN 25 in a batch.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan batch 20 to 25
[HUAWEI] dhcp snooping enable vlan 20 to 25
```

14.8.21 dhcp snooping enable no-user-binding

Function

The **dhcp snooping enable no-user-binding** command disables the interfaces from generating DHCP snooping binding entries after DHCP snooping is enabled.

The **undo dhcp snooping enable no-user-binding** command restores the default setting.

By default, an interface generates DHCP snooping binding entries after DHCP snooping is enabled.

Format

System view:

dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

VLAN view, interface view:

dhcp snooping enable no-user-binding

undo dhcp snooping enable no-user-binding

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Disables the interfaces in the specified VLANs from generating DHCP snooping binding entries. - *vlan-id1* specifies the first VLAN ID. - **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

After DHCP snooping is enabled on a device, the device generates DHCP snooping binding entries for users by default. If the number of binding entries on the device reaches the upper limit, new users cannot go online. In certain scenarios, for example, on a trusted DHCP network, if you do not want to limit the number of online users but want to record user location information, run the **dhcp snooping enable no-user-binding** command to disable the device from generating DHCP snooping binding entries.

When the command is executed in an interface view, the command takes effect for all DHCP users connecting to the interface. When the command is executed in the VLAN view, the command takes effect for all the DHCP users belonging to this VLAN on all interfaces. When the command is executed in the system view, the command takes effect in the same way as it is executed in the VLAN view, except that multiple VLANs can be specified.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

After this command is executed, the device deletes the binding entries from the corresponding VLAN or interface.

If the DHCP snooping binding entry-dependent function such as IPSG or DAI is configured on the device, the corresponding function does not take effect after this command is run.

This command cannot be used together with **14.8.18 dhcp snooping check dhcp-request enable**; otherwise, online users cannot go offline.

Example

# In the system view, disable the interfaces in VLAN 10 and VLAN 20 from generating DHCP snooping binding entries.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable no-user-binding vlan 10 20
```

# In the VLAN view, disable the interfaces in VLAN 10 from generating DHCP snooping binding entries.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable no-user-binding
```

# In the interface view, disable GE0/0/1 from generating DHCP snooping binding entries.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable no-user-binding
```

Related Topics

14.8.20 dhcp snooping enable

14.8.40 dhcpv6 snooping relay-information enable

14.8.22 dhcp snooping max-user-number

Function

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface.

The **undo dhcp snooping max-user-number** command restores the default maximum number of DHCP snooping binding entries to be learned on an interface.

By default, the maximum number of DHCP snooping binding entries that can be learned on an interface is 256 for S1720GFR-TP and S2750EI, 512 for S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, and S2720EI, 1024 for S1720X and S1720X-E, 2048 for S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, and S6720S-SI, and 4096 for other models.

Format

In the system view:

dhcp snooping max-user-number *max-user-number* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping max-user-number [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view and interface view:

dhcp snooping max-user-number *max-user-number*

undo dhcp snooping max-user-number

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of DHCP snooping binding entries that can be learned on an interface.	The value is an integer that ranges from 1 to 256 for S1720GFR-TP and S2750EI, from 1 to 512 for S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, and S2720EI, from 1 to 1024 for S1720X and S1720X-E, from 1 to 2048 for S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI and S6720S-SI, and from 1 to 4096 for other models. **NOTE** If the maximum number of DHCP snooping binding entries to be learned by interfaces is N in the system or VLAN view, for a stack, the value in system view and VLAN view ranges from 1 to N * Number of stacked devices. That is, by default, a maximum of N * Number of stacked devices DHCP users are allowed to access the entire device or VLAN. A stack consisting of S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI, S6720S-SI, S5720EI, S5720HI, S6720EI, and S6720S-EI can learn a maximum of 9216 DHCP snooping binding entries. For example, when two S5720HI switches set up a stack, the stack can learn a maximum of DHCP snooping binding entries globally and in VLANs by default.

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the maximum number of DHCP snooping binding entries can be learned in a VLAN. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface. If the number of DHCP snooping binding entries reaches the maximum value, subsequent users cannot access.

When the command is executed in the system view, the value specified in this command is the total number of DHCP snooping binding entries to be learned by all interfaces on the device. If you run the **dhcp snooping max-user-number** command in the VLAN view, the command takes effect on all the interfaces in the VLAN. If you run the **dhcp snooping max-user-number** command in the system view, VLAN view, and the interface view, the smallest value takes effect.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

The maximum number of DHCP snooping binding entries to be learned in a stack environment will still be valid if the stack is split. For example, the maximum number of DHCP snooping binding entries to be learned by interfaces is set to N in the system or VLAN view. After the stack splits, run the **14.8.42 display dhcp snooping** command. You will find that the maximum number of entries learned by interfaces in the system or VLAN view is still N (even if N is greater than the maximum number (M) of entries supported by a stand-along device). Pay attention to the following points:

- For the users requiring to go online: The users are allowed to go online when the number of binding entries on the device is smaller than M, and not allowed to go online when the number of binding entries on the device is equivalent to or larger than M.
- For online users: The users are kept online no matter whether the number of binding entries on the device is larger than M. However, if the number of binding entries is larger than M, the users cannot go online again after they go offline.
- Binding entries that have been backed up: After the device restarts, all binding entries on the device can be restored no matter whether the number of binding entries is smaller than M, and the users matching these binding entries can go online.

Example

# Set the maximum number of DHCP users to 100 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping max-user-number 100
```

# Set the maximum number of DHCP users in VLAN 100 to 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping enable
[HUAWEI-vlan100] dhcp snooping max-user-number 100
```

Related Topics

14.8.20 dhcp snooping enable

14.8.42 display dhcp snooping

14.8.23 dhcp snooping over-vpls enable

Function

The **dhcp snooping over-vpls enable** command enables DHCP snooping on the device on a Virtual Private LAN Service (VPLS) network.

The **undo dhcp snooping over-vpls enable** command disables DHCP snooping on the device on a VPLS network.

By default, DHCP snooping is disabled on the device on a VPLS network.

NOTE

Only the S5720HI supports this command.

Format

dhcp snooping over-vpls enable

undo dhcp snooping over-vpls enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DHCP packets on a VPLS network are different from common DHCP packets. Therefore, DHCP snooping cannot take effect for the device on the VPLS network even if the function is enabled globally using the **dhcp snooping enable** command in the system view. To make DHCP snooping take effect for the device applied to the VPLS network, run the **dhcp snooping over-vpls enable** command to enable the function.

To enable DHCP snooping for the device on the VPLS network, enable it on the device closed to the user side so that the DHCP packets from the user side to the VPLS network can be controlled.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Precautions

The device management interfaces do not support DHCP snooping on a VPLS network.

After you run the **dhcp snooping over-vpls enable** command, the maximum number of concurrent users is 50 in the default CPCAR configuration.

When the device is applied to a VPLS network, you only need to run the **dhcp snooping over-vpls enable** command to enable DHCP snooping on the device and other DHCP snooping command have no changes.

Example

# Enable DHCP snooping on the device on a VPLS network.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping over-vpls enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.24 dhcp snooping trusted

Function

The **dhcp snooping trusted** command configures an interface as a trusted interface.

The **undo dhcp snooping trusted** command configures an interface as an untrusted interface.

By default, an interface is an untrusted interface.

Format

In the VLAN view:

dhcp snooping trusted interface *interface-type interface-number*

undo dhcp snooping trusted interface *interface-type interface-number*

In the interface view:

dhcp snooping trusted

undo dhcp snooping trusted

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface in a VLAN. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable DHCP clients to obtain IP addresses from authorized DHCP servers, DHCP snooping supports the trusted interface and untrusted interfaces. The trusted interface forwards DHCP messages while untrusted interfaces discard received DHCP ACK messages and DHCP Offer messages.

An interface directly or indirectly connected to the DHCP server trusted by the administrator needs to be configured as the trusted interface, and other interfaces are configured as untrusted interfaces. This ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

Prerequisites

In the system view, run the **dhcp snooping enable** command to enable DHCP snooping.

Precautions

If an interface has been configured as a DHCP trusted interface using the **dhcp snooping trusted** command, the device will not consider DHCP packets received by this interface as attack packets or perform attack defense operations on the DHCP packets received by this interface.

If you run the **dhcp snooping trusted** command in the VLAN view, the command takes effect for all the DHCP messages received from the specified VLAN. If you run the **dhcp snooping trusted** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

You are advised not to configured more than 15 trusted ports in a VLAN.

Example

# Configure GE0/0/1 in VLAN 100 as the trusted interface.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping trusted interface gigabitethernet 0/0/1
```

# Configure GE0/0/1 as the trusted interface.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping trusted
```

Related Topics

14.8.20 dhcp snooping enable

14.8.25 dhcp snooping user-alarm percentage

Function

The **dhcp snooping user-alarm percentage** command configures the alarm thresholds for the percentage of DHCP snooping binding entries.

The **undo dhcp snooping user-alarm percentage** command restores the default alarm thresholds for the percentage of DHCP snooping binding entries.

By default, the lower alarm threshold for the percentage of DHCP snooping binding entries is 50, and the upper alarm threshold for the percentage of DHCP snooping binding entries is 100.

Format

dhcp snooping user-alarm percentage *percent-lower-value percent-upper-value*

undo dhcp snooping user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of DHCP snooping binding entries.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of DHCP snooping binding entries.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **14.8.22 dhcp snooping max-user-number** command to set the maximum number of DHCP snooping binding entries on an interface, you can run the **dhcp snooping user-alarm percentage** command to set the alarm thresholds for the percentage of DHCP snooping binding entries.

When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or exceeds the upper alarm threshold, the device generates an alarm. When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

Example

# Set the lower alarm threshold for the DHCP user count percentage to 30 and the upper alarm threshold to 80.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping user-alarm percentage 30 80
```

Related Topics

14.8.22 dhcp snooping max-user-number

14.8.26 dhcp snooping user-bind autosave

Function

The **dhcp snooping user-bind autosave** command enables local automatic backup of the DHCP snooping binding table.

The **undo dhcp snooping user-bind autosave** command disables local automatic backup of the DHCP snooping binding table.

By default, local automatic backup of the DHCP snooping binding table is disabled.

Format

dhcp snooping user-bind autosave *file-name* [**write-delay** *delay-time*]

undo dhcp snooping user-bind autosave

Parameters

Parameter	Description	Value
file-name	Specifies the path for storing the file that backs up the binding table and the file name. The file path and name supported by the device must be both entered.	The value is a string of 1 to 51 case-insensitive characters without spaces.
write-delay *delay-time*	Specifies the interval for local automatic backup of the DHCP snooping binding table. If this parameter is not specified, the backup interval is the default value.	The value is an integer that ranges from 60 to 4294967295, in seconds. By default, the interval for local automatic backup of the DHCP snooping binding table is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping user-bind autosave** command can retain the configured DHCP snooping binding entries after the device restarts. After a DHCP snooping binding table is generated, you can run the **dhcp snooping user-bind autosave** command to enable local automatic backup of the DHCP snooping binding table.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

This prevents data loss in the DHCP snooping binding table. The suffix of the file must be .tbl.

If the system restarts within one day after the system time is changed, immediately run the **dhcp snooping user-bind autosave** command again to back up the latest dynamic binding entries because it is not the time to update the binding table. If you do not run this command, the lease will be inconsistent with the current system time after the dynamic binding table is restored.

If a device where the DHCP snooping binding table is backed up is powered off and then restarted after the lease of DHCP snooping binding table expires, the DHCP snooping entries cannot be restored.

Example

# Configure the device to back up the DHCP snooping binding table to the file **backup.tbl** in the flash every 5000 seconds.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind autosave flash:/backup.tbl write-delay 5000
```

Related Topics

14.8.20 dhcp snooping enable

14.8.27 dhcp snooping user-bind ftp

Function

The **dhcp snooping user-bind ftp** command enables the device to automatically back up DHCP snooping binding entries on the remote FTP server.

The **undo dhcp snooping user-bind ftp** command disables the device from automatically backing up DHCP snooping binding entries on the remote FTP server.

By default, the device is not enabled to automatically back up DHCP snooping binding entries on the remote FTP server.

Format

dhcp snooping user-bind ftp remotefilename *filename* **host-ip** *ip-address* **username** *username* **password** *password* [**write-delay** *delay-time*]

undo dhcp snooping user-bind ftp

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file where DHCP snooping binding entries will be backed up on the remote FTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the remote FTP server.	The value is in dotted decimal notation.
username *username*	Specifies the user name to connect to the FTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces.
password *password*	Specifies the password to connect to the FTP server.	The value is a string of case-sensitive characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.
write-delay *delay-time*	Specifies the interval for automatically backing up DHCP snooping binding entries. If this parameter is not used, the default interval is used.	The value is an integer that ranges from 300 to 4294967295, in seconds. By default, the system backs up DHCP snooping binding entries every two days.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device restarts, to prevent loss of generated DHCP snooping binding entries on the device, run the **dhcp snooping user-bind ftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote FTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The FTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp** command is recommended.

Example

# Enable the device to automatically back up DHCP snooping binding entries to the **backup** file on the FTP server at 10.137.12.10 with the FTP user name **huawei** and password **Huawei@123**.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind ftp remotefilename backup host-ip 10.137.12.10 username huawei
password Huawei@123
```

Related Topics

14.8.20 dhcp snooping enable

14.8.28 dhcp snooping user-bind ftp load

14.8.28 dhcp snooping user-bind ftp load

Function

The **dhcp snooping user-bind ftp load** command configures the device to obtain and restore backup DHCP snooping binding entries on the remote FTP server.

Format

dhcp snooping user-bind ftp load remotefilename *filename* **host-ip** *ip-address* **username** *username* **password** *password*

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file from which the device obtains DHCP snooping binding entries.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.

Parameter	Description	Value
host-ip *ip-address*	Specifies the IP address of the remote FTP server.	The value is in dotted decimal notation.
username *username*	Specifies the user name to connect to the FTP server.	The value is a string of 1 to 64 characters without spaces.
password *password*	Specifies the password to connect to the FTP server.	The value is a string of characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **14.8.27 dhcp snooping user-bind ftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote FTP server, you can run the **dhcp snooping user-bind ftp load** command to configure the device to obtain and restore backup DHCP snooping binding entries on the remote FTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The FTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp load** command is recommended.

Example

# Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote FTP server at 10.137.12.10 with the FTP user name **huawei** and password **Huawei@123**.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind ftp load remotefilename backup host-ip 10.137.12.10 username
huawei password Huawei@123
Warning: FTP is not a secure protocol, and it is recommended to use SFTP.
Info: Downloading the file from the remote FTP server. Please wait...done.
 Total number of dynamic binding table in remote file: 30
 Recovering dynamic binding table, please wait for a moment....
 10 successful, 20 failed.
 Binding Collisions         :    20     Exceeds max limits     :     0
 Invalid interfaces         :     0     Invalid vlans          :     0
 Invalid snp configurations :     0     Expired leases         :     0
 Parse failures             :     0
```

Table 14-52 Description of the **dhcp snooping user-bind ftp load** command output

Item	Description
Total number of dynamic binding table in remote file	Number of DHCP snooping binding entries stored on the remote server.
m successful, *n* failed	*m* DHCP snooping binding entries are recovered successfully, and *n* DHCP snooping binding entries fail to be recovered.
Binding Collisions	Number of DHCP snooping binding entries that cannot be restored because of collision between local entries and remote entries.
Exceeds max limits	Number of DHCP snooping binding entries that cannot be restored because the number of local entries reaches the upper limit.
Invalid interfaces	Number of DHCP snooping binding entries that cannot be restored because the local interface becomes invalid, for example, Down.
Invalid vlans	Number of DHCP snooping binding entries that cannot be restored because the VLAN on local device becomes invalid, for example, unavailable VLAN.
Invalid snp configurations	Number of DHCP snooping binding entries that cannot be restored because the DHCP snooping function is not enabled.

Item	Description
Expired leases	Number of DHCP snooping binding entries that cannot be restored because the lease of DHCP snooping binding table expires.
Parse failures	Number of DHCP snooping binding entries that cannot be restored because the device fails to parse the binding table file.

Related Topics

14.8.20 dhcp snooping enable

14.8.27 dhcp snooping user-bind ftp

14.8.29 dhcp snooping user-bind sftp

Function

The **dhcp snooping user-bind sftp** command enables the device to automatically back up DHCP snooping binding entries on the remote SFTP server.

The **undo dhcp snooping user-bind sftp** command disables the device from automatically backing up DHCP snooping binding entries on the remote SFTP server.

By default, the device is not enabled to automatically back up DHCP snooping binding entries on the remote SFTP server.

Format

dhcp snooping user-bind sftp remotefilename *filename* **host-ip** *ip-address* **username** *username* **password** *password* [**write-delay** *delay-time*]

undo dhcp snooping user-bind sftp

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file where DHCP snooping binding entries will be backed up on the remote SFTP server.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.

Parameter	Description	Value
host-ip *ip-address*	Specifies the IP address of the remote SFTP server.	The value is in dotted decimal notation.
username *username*	Specifies the user name to connect to the SFTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces.
password *password*	Specifies the password to connect to the SFTP server.	The value is a string of case-sensitive characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.
write-delay *delay-time*	Specifies the interval for automatically backing up DHCP snooping binding entries. If this parameter is not used, the default interval is used.	The value is an integer that ranges from 300 to 4294967295, in seconds. By default, the system backs up DHCP snooping binding entries every two days.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device restarts, to prevent loss of generated DHCP snooping binding entries on the device, run the **dhcp snooping user-bind sftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote SFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The suffix of the file must be .tbl.

Example

# Enable the device to automatically back up DHCP snooping binding entries to the **backup** file on the SFTP server at 10.137.12.10 with the SFTP user name **huawei** and password **Huawei@123**.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind sftp remotefilename backup host-ip 10.137.12.10 username
huawei password Huawei@123
```

Related Topics

14.8.20 dhcp snooping enable

14.8.30 dhcp snooping user-bind sftp load

14.8.30 dhcp snooping user-bind sftp load

Function

The **dhcp snooping user-bind sftp load** command configures the device to obtain and restore backup DHCP snooping binding entries on the remote SFTP server.

Format

dhcp snooping user-bind sftp load remotefilename *filename* **host-ip** *ip-address* **username** *username* **password** *password*

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file from which the device obtains DHCP snooping binding entries.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the remote SFTP server.	The value is in dotted decimal notation.
username *username*	Specifies the user name to connect to the SFTP server.	The value is a string of 1 to 64 characters without spaces.

Parameter	Description	Value
password *password*	Specifies the password to connect to the SFTP server.	The value is a string of characters without spaces. It can be a cipher-text password of 48 characters or a plain-text password of 1 to 16 characters. **NOTE** To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **14.8.29 dhcp snooping user-bind sftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote SFTP server, you can run the **dhcp snooping user-bind sftp load** command to configure the device to obtain and restore backup DHCP snooping binding entries on the remote SFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Example

# Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote SFTP server at 10.137.12.10 with the SFTP user name **huawei** and password **Huawei@123**.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind sftp load remotefilename backup host-ip 10.137.12.10 username
huawei password Huawei@123
Info: Downloading the file from the remote SFTP server. Please wait...done.
 Total number of dynamic binding table in remote file: 30
 Recovering dynamic binding table, please wait for a moment....
 10 successful, 20 failed.
 Binding Collisions        :    20     Exceeds max limits     :     0
 Invalid interfaces        :     0    Invalid vlans          :     0
 Invalid snp configurations :     0    Expired leases         :     0
 Parse failures            :     0
```

Table 14-53 Description of the **dhcp snooping user-bind sftp load** command output

Item	Description
Total number of dynamic binding table in remote file	Number of DHCP snooping binding entries stored on the remote server.
m successful, *n* failed	*m* DHCP snooping binding entries are recovered successfully, and *n* DHCP snooping binding entries fail to be recovered.
Binding Collisions	Number of DHCP snooping binding entries that cannot be restored because of collision between local entries and remote entries.
Exceeds max limits	Number of DHCP snooping binding entries that cannot be restored because the number of local entries reaches the upper limit.
Invalid interfaces	Number of DHCP snooping binding entries that cannot be restored because the local interface becomes invalid, for example, Down.
Invalid vlans	Number of DHCP snooping binding entries that cannot be restored because the VLAN on local device becomes invalid, for example, unavailable VLAN.
Invalid snp configurations	Number of DHCP snooping binding entries that cannot be restored because the DHCP snooping function is not enabled.
Expired leases	Number of DHCP snooping binding entries that cannot be restored because the lease of DHCP snooping binding table expires.
Parse failures	Number of DHCP snooping binding entries that cannot be restored because the device fails to parse the binding table file.

Related Topics

14.8.20 dhcp snooping enable

14.8.29 dhcp snooping user-bind sftp

14.8.31 dhcp snooping user-bind tftp

Function

The **dhcp snooping user-bind tftp** command enables the device to automatically back up DHCP snooping binding entries on the remote TFTP server.

The **undo dhcp snooping user-bind tftp** command disables the device from automatically backing up DHCP snooping binding entries on the remote TFTP server.

By default, the device is not enabled to automatically back up DHCP snooping binding entries on the remote TFTP server.

Format

dhcp snooping user-bind tftp remotefilename *filename* **host-ip** *ip-address* [**write-delay** *delay-time*]

undo dhcp snooping user-bind tftp

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file where DHCP snooping binding entries will be backed up on the remote TFTP server.	The value is a string of 1 to 64 case-sensitive characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.
host-ip *ip-address*	Specifies the IP address of the TFTP server.	The value is in dotted decimal notation.
write-delay *delay-time*	Specifies the interval for automatically backing up DHCP snooping binding entries. If this parameter is not used, the default interval is used.	The value is an integer that ranges from 300 to 4294967295, in seconds. By default, the interval for local automatic backup of the DHCP snooping binding table is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device restarts, to prevent loss of generated DHCP snooping binding entries on the device, run the **dhcp snooping user-bind tftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote TFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The TFTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp** command is recommended.

Example

# Enable the device to automatically back up DHCP snooping binding entries to the **backup** file on the TFTP server at 10.137.12.10 at intervals of 5000s.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind tftp remotefilename backup host-ip 10.137.12.10 write-delay 5000
```

Related Topics

14.8.20 dhcp snooping enable

14.8.32 dhcp snooping user-bind tftp load

14.8.32 dhcp snooping user-bind tftp load

Function

The **dhcp snooping user-bind tftp load** command configures the device to obtain and restore backup DHCP snooping binding entries on the remote TFTP server.

Format

dhcp snooping user-bind tftp load remotefilename *filename* **host-ip** *ip-address*

Parameters

Parameter	Description	Value
remotefilename *filename*	Specifies the name of the file from which the device obtains DHCP snooping binding entries.	The value is a string of 1 to 64 characters without spaces. The string cannot contain the following characters: ~ * \ | : " ? < >.

Parameter	Description	Value
host-ip *ip-address*	Specifies the IP address of the remote TFTP server.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After running the **14.8.31 dhcp snooping user-bind tftp** command to enable the device to automatically back up DHCP snooping binding entries on the remote TFTP server, you can run the **dhcp snooping user-bind tftp load** command to configure the device to obtain and restore backup DHCP snooping binding entries on the remote TFTP server.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The TFTP protocol will bring risk to device security. The SFTP protocol configured using the **dhcp snooping user-bind sftp load** command is recommended.

Example

# Configure the device to obtain and restore backup DHCP snooping binding entries from the **backup** file on the remote TFTP server at 10.137.12.10.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-bind tftp load remotefilename backup host-ip 10.137.12.10
Info: Transfer file in binary mode.
Downloading the file from the remote TFTP server. Please wait...
100%
TFTP: Downloading the file successfully.
656 byte(s) received in 1 second(s).
 Total number of dynamic binding table in remote file: 20
 Recovering dynamic binding table, please wait for a moment....
 10 successful, 10 failed.
 Binding Collisions        :    10     Exceeds max limit    :     0
 Invalid interfaces        :     0    Invalid vlan         :     0
 Invalid snp configurations :     0    Expired leases       :     0
 Parse failures            :     0
```

Table 14-54 Description of the dhcp snooping user-bind tftp load command output

Item	Description
Total number of dynamic binding table in remote file	Number of DHCP snooping binding entries stored on the remote server.
Binding Collisions	Number of DHCP snooping binding entries that cannot be restored because of collision between local entries and remote entries.
Exceeds max limit	Number of DHCP snooping binding entries that cannot be restored because the number of local entries reaches the upper limit.
Invalid interfaces	Number of DHCP snooping binding entries that cannot be restored because the local interface becomes invalid, for example, Down.
Invalid vlan	Number of DHCP snooping binding entries that cannot be restored because the VLAN on local device becomes invalid, for example, unavailable VLAN.
Invalid snp configurations	Number of DHCP snooping binding entries that cannot be restored because the DHCP snooping function is not enabled.
Expired leases	Number of DHCP snooping binding entries that cannot be restored because the lease of DHCP snooping binding table expires.
Parse failures	Number of DHCP snooping binding entries that cannot be restored because the device fails to parse the binding table file.

Related Topics

14.8.20 dhcp snooping enable

14.8.31 dhcp snooping user-bind tftp

14.8.33 dhcp snooping user-offline remove mac-address

Function

The **dhcp snooping user-offline remove mac-address** command enables the device to delete the MAC address entry of a user whose DHCP snooping binding entry is deleted.

The **undo dhcp snooping user-offline remove mac-address** command disables the device from deleting the MAC address entry of a user whose binding entry is deleted.

By default, the device does not delete the MAC address entry of a user whose DHCP snooping binding entry is deleted.

Format

dhcp snooping user-offline remove mac-address

undo dhcp snooping user-offline remove mac-address

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a user goes offline but its MAC address entry is not aged, the device forwards the packet whose destination address is the IP address of the user based on the dynamic MAC address entry. After the **dhcp snooping user-offline remove mac-address** command is executed, the user MAC address entry is deleted when the DHCP snooping binding entry is deleted. With the function of discarding unknown unicast packets on the network-side interface, the device discards packets destined to offline users.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

# Enable the device to delete the MAC address entry of a user whose DHCP snooping binding entry is deleted.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping user-offline remove mac-address
```

Related Topics

14.8.20 dhcp snooping enable

14.8.34 dhcp snooping user-transfer enable

Function

The **dhcp snooping user-transfer enable** command enables location transition for DHCP snooping users.

The **undo dhcp snooping user-transfer enable** command disables location transition for DHCP snooping users.

By default, location transition is enabled for DHCP snooping users.

Format

dhcp snooping user-transfer enable

undo dhcp snooping user-transfer enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a mobile user goes online through interface A, goes offline, and then goes online through interface B, the user sends a DHCP Discover message to apply an IP address. By default, if DHCP snooping is enabled on the device, the device allows the user to go online and updates the DHCP snooping binding entries. However, this may bring security risks. For example, if an attacker pretends an authorized user to send a DHCP Discover message, the authorized user cannot access the network after the DHCP snooping binding table is updated. To prevent such attacks, you can disable the DHCP snooping location transition function. After this function is disabled, the device discards the DHCP Discover messages sent by a user who has an entry in the DHCP snooping binding table (user's MAC address exists in the DHCP snooping binding table) through another interface.

Prerequisites

DHCP snooping has been enabled on the device using the **14.8.20 dhcp snooping enable** command.

Example

# Disable location transition for DHCP snooping users.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] undo dhcp snooping user-transfer enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.35 dhcpv6 interface-id format

Function

The **dhcpv6 interface-id format** command configures the Interface-ID format in DHCPv6 packets.

The **undo dhcpv6 interface-id format** command restores the default Interface-ID format in DHCPv6 packets.

By default, the Interface-ID format in DHCPv6 packets is **default**.

Format

dhcpv6 interface-id format { **default** | **user-defined** *text* }

undo dhcpv6 interface-id format

Parameters

Parameter	Description	Value
default	Specifies the default Interface-ID format. The default Interface-ID format is %04svlan.%04cvlan.%mac:%portname. The values of the S-VLAN and C-VLAN are integers containing four characters. If the length is fewer than four characters, the value is prefixed with 0s. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the device MAC address is 6afe-870b-0000, the Interface-ID generated during the system parsing process is 0011.0022.6afe870b0000:vlanif100.	-

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Interface-ID format. A user-defined format can be: ● Format defined by keywords: The Interface-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Interface-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 14-55**. ● Format defined by common character strings: The Interface-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Interface-ID can be directly defined as N8. ● Mixed format: The Interface-ID is defined by both the keywords and common character strings. For example, the Interface-ID can be defined as %sysname N8.	The value is a string of case-sensitive characters without spaces. The character string contains 1 to 251 characters, excluding the quotation marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID records user access information such as the inbound interfaces of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Interface-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 interface-id format** command to configure the format of the Interface-ID inserted into DHCPv6 packets.

Table 14-55 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.

- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

# Configure a user-defined format as the format of the Interface-ID in DHCPv6 packets and the device MAC address as the encapsulated content.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcpv6 interface-id format user-defined "%mac"
```

14.8.36 dhcpv6 option18 format

Function

The **dhcpv6 option18 format** command configures the format of the Option 18 field in a DHCPv6 message.

The **undo dhcpv6 option18 format** command restores the default format of the Option 18 field in a DHCPv6 message.

By default, the format of the Option 18 field is not configured in a DHCPv6 message.

Format

dhcpv6 option18 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option18 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 18 field.	The value is a string of 1 to 251 characters. The details about the user-defined format string are provided in the Usage Guidelines.
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** ● If a VLAN is specified, only the format of the Option 18 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 18 field in all DHCPv6 messages received by the interface is configured. ● If the format of the Option 18 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. ● This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
all	Deletes all formats of the Option 18 field.	-

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dhcpv6 option18** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 18 field to a DHCPv6 message, you can run the **dhcpv6 option18 format** command to configure the format of the Option 18 field in a DHCPv6 message.

You can use the following keywords to define the Option 18 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, GE0/0/1. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is

added to the Option 18 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].

- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in an ASCII string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, spaces, and % + keywords.
  - In a hexadecimal notation string, numbers are encapsulated in the Option 18 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
  - All the spaces in a hexadecimal character string are ignored.
  - By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
  - A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

# Configure the format of the Option 18 field in a DHCPv6 message in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
```

```
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcpv6 option18 format user-defined "%length %svlan %5slot %3subslot %8port"
```

# Configure the format of the Option 18 field in a DHCPv6 message on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 option18 format user-defined "%length %svlan %5slot
%3subslot %8port"
```

Related Topics

14.8.38 dhcpv6 { option18 | option37 } enable

14.8.37 dhcpv6 option37 format

Function

The **dhcpv6 option37 format** command configures the format of the Option 37 field in a DHCPv6 message.

The **undo dhcpv6 option37 format** command restores the default format of the Option 37 field in a DHCPv6 message.

By default, the format of the Option 37 field is not configured in a DHCPv6 message.

Format

dhcpv6 option37 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option37 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 37 field.	The value is a string of 1 to 247 characters. The details about the user-defined format string are provided in the Usage Guidelines.

Parameter	Description	Value
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** ● If a VLAN is specified, only the format of the Option 37 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 37 field in all DHCPv6 messages received by the interface is configured. ● If the format of the Option 37 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. ● This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
all	Deletes all formats of the Option 37 field.	-

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dhcpv6 option37** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 37 field to a DHCPv6 message, you can run the **dhcpv6 option37 format** command to configure the format of the Option 37 field in a DHCPv6 message.

You can use the following keywords to define the Option 37 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, GE0/0/1. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.

- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 37 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in an ASCII string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:

- An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
- A hexadecimal notation string can contain numerals, spaces, and % + keywords.
- In a hexadecimal notation string, numbers are encapsulated in the Option 37 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
- All the spaces in a hexadecimal character string are ignored.
- By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
- If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
- A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
- If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

# Configure the format of the Option 37 field in a DHCPv6 message in VLAN 10.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcpv6 option37 format user-defined "%length %svlan %5slot %3subslot %8port"
```

# Configure the format of the Option 37 field in a DHCPv6 message on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 option37 format user-defined "%length %svlan %5slot
%3subslot %8port"
```

Related Topics

14.8.38 dhcpv6 { option18 | option37 } enable

14.8.38 dhcpv6 { option18 | option37 } enable

Function

The **dhcpv6 { option18 | option37 } enable** command enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.

The **undo dhcpv6 { option18 | option37 } enable** command disables the device from inserting the Option 18 or Option 37 field to a DHCPv6 message.

By default, the device does not insert the Option 18 or Option 37 field to a DHCPv6 message.

Format

dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

undo dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

Parameters

Parameter	Description	Value
insert	Enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.	-
rebuild	Enables the device to forcibly insert the Option 18 or Option 37 field to a DHCPv6 message.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The function of the Option 18 and Option 37 field is similar to the function of the Option 82 field (see the **dhcp option82 enable** command). The Option 18 field contains the port number of a client and the Option 37 field contains the MAC address of the client. A device inserts the Option 18 or Option 37 field to a

DHCPv6 Request message to notify the DHCP server of the DHCPv6 client location. The DHCP server can properly assign an IP address and other configurations to the DHCPv6 client, ensuring DHCP client security.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcpv6 { option18 | option37 } enable** command in the VLAN view, the command takes effect for all the DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 { option18 | option37 } enable** command in the interface view, the command takes effect for all the DHCPv6 messages received on the specified interface.

Example

# Insert the Option 37 field to DHCPv6 Request messages sent by GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcpv6 option37 insert enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.39 dhcpv6 remote-id format

Function

The **dhcpv6 remote-id format** command sets the format of the Remote-ID in DHCPv6 messages.

The **undo dhcpv6 remote-id format** command restores the default format of the Remote-ID in DHCPv6 messages.

By default, the default format of the Remote-ID in DHCPv6 messages is used.

Format

dhcpv6 remote-id format { **default** | **user-defined** *text* }

undo dhcpv6 remote-id format

Parameters

Parameter	Description	Value
default	Indicates to adopt the default format of the remote ID. The default format of the remote ID is %duid %portname:%04svlan.%04cvlan, where the values of the outer VLAN ID and inner VLAN ID are integers and composed of four characters. If the length is shorter than four characters, 0s are prefixed to the value. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is GE0/0/1, and the client DUID is 0003000180FB063545B3, the Remote-ID option generated during the system parsing process is 0003000180FB063545B3 GigabitEthernet 0/0/1:0011.0022.	-

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Remote-ID format. A user-defined format can be: ● Format defined by keywords: The Remote-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Remote-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 14-56**. ● Format defined by common character strings: The Remote-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Remote-ID can be directly defined as N8. ● Mixed format: The Remote-ID is defined by both the keywords and common character strings. For	The value is a string of 3 to 247 case-sensitive characters with spaces.

Parameter	Description	Value
	example, the Remote-ID can be defined as %sysname N8.	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The Remote-ID records user access information such as the DUID of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPfv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Remote-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 remote-id format** command to configure the format of the Remote-ID inserted into DHCPv6 packets.

Table 14-56 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.

Keyword	Description
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Follow-up Procedure

When the device functions as a DHCPv6 relay, you must run the **6.11.21 dhcpv6 remote-id insert enable** or **6.11.22 dhcpv6 remote-id rebuild enable** command to enable the function of inserting the Remote-ID into DHCPv6 relay packets after running the **dhcpv6 remote-id format** command to configure the Remote-ID format in DHCPv6 packets.

NOTE

When the device functions as an LDRA, the Remote-ID is inserted into DHCPv6 relay packets by default and the function does not need to be enabled.

Precautions

- The user-defined format content must be specified between the double quotation marks (""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.

- An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

# Set the customized format for the remote ID carried in DHCPv6 messages and encapsulate the MAC address of the device into the remote ID.

```
<HUAWEI> system-view
[HUAWEI] dhcpv6 remote-id format user-defined "%mac"
```

Related Topics

6.11.21 dhcpv6 remote-id insert enable

14.8.40 dhcpv6 snooping relay-information enable

Function

The **dhcpv6 snooping relay-information enable** command enables Lightweight DHCPv6 Relay Agent (LDRA) for DHCPv6 snooping.

The **undo dhcpv6 snooping relay-information enable** command disables LDRA.

By default, LDRA is disabled for DHCPv6 snooping.

Format

dhcpv6 snooping relay-information enable [**trust**]

undo dhcpv6 snooping relay-information enable [**trust**]

Parameters

Parameter	Description	Value
trust	Configures the device to trust the received Relay-Forward messages. If this parameter is not specified, the device does not trust the received Relay-Forward messages.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

In some scenarios, for example, interfaces in the same VLAN have different network access rights and QoS requirements, the DHCPv6 server must be able to detect user access locations, and assign corresponding access control and QoS policies. The DHCPv6 relay agent is usually configured on the gateway. The relay agent can record user access locations; however, if access devices are located between the relay agent and users, the relay agent cannot detect the access locations of users.

LDRA can meet the requirements of these scenarios. LDRA is configured on the user-side access device. The LDRA-enabled device can forward user access locations (such as the network-side interfaces on clients) to the DHCPv6 server. The DHCPv6 server delivers policies to users accordingly.

This command enables LDRA for DHCPv6 snooping and configures the handling methods for received Relay-Forward messages:

- Trust: The device forwards the received Relay-Forward messages to the DHCPv6 server. This method is usually used when multiple LDRA-enabled devices are directly connected. If the downstream LDRA-enabled device trusts the Relay-Forward messages from the upstream LDRA-enabled device, this method can be used.
- Untrust: The device discards the received Relay-Forward messages. This method is usually used when an LDRA-enabled device directly connects to users, and the users may send invalid Relay-Forward messages.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The LDRA function only records the client location information and forwards the information to the DHCPv6 server. The differentiated policies for IP address allocation, accounting, access control, and QoS are configured on the DHCPv6 server.

Example

# Enable LDRA for DHCPv6 snooping in VLAN10.

```
<HUAWEI> system-view
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcpv6 snooping relay-information enable
```

Related Topics

14.8.20 dhcp snooping enable

14.8.21 dhcp snooping enable no-user-binding

6.11.9 dhcpv6 interface-id format

14.8.41 display dhcp option82 configuration

Function

The **display dhcp option82 configuration** command displays the DHCP Option 82 configuration.

Format

display dhcp option82 configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP Option 82 configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP Option 82 configuration on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can properly assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

After the Option 82 field is inserted to a DHCP message, run the **display dhcp option82 configuration** command to display the DHCP Option 82 configuration.

Example

# Display all the DHCP Option82 configurations.

```
<HUAWEI> display dhcp option82 configuration
#
dhcp option82 vendor-specific format vendor-sub-option 1 ascii 22
#
interface GigabitEthernet0/0/1
 dhcp option82 subscriber-id format ascii 222
 dhcp option82 insert enable
 dhcp option82 encapsulation circuit-id
 dhcp option82 append vendor-specific
 dhcp option82 circuit-id format common
#
```

Table 14-57 Description of the **display dhcp option82 configuration** command output

Item	Description
interface *ifn*	Option 82 configuration on interface *ifn*.
dhcp option82 vendor-specific format vendor-sub-option *i* ascii *text1*	The Sub9 of the old format is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **14.8.8 dhcp option82 vendor-specific format** command.
dhcp option82 subscriber-id format ascii *text2*	The Sub6 suboption is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **14.8.7 dhcp option82 subscriber-id format** command.
dhcp option82 insert enable	The function of inserting Option 82 to DHCP messages is enabled and the insertion method is configured: ● dhcp option82 rebuild enable: Rebuild mode ● dhcp option82 insert enable: Insert mode To specify the parameter, run the **14.8.4 dhcp option82 enable** command.
dhcp option82 encapsulation circuit-id	The suboption inserted into the Option 82 field of DHCP messages is configured. To specify the parameter, run the **14.8.5 dhcp option82 encapsulation** command.
dhcp option82 append vendor-specific	The Sub9 of the new format is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **14.8.3 dhcp option82 append vendor-specific** command.

Item	Description
dhcp option82 circuit-id format common	Format of the circuit-id suboption. To specify the parameter, run the **14.8.6 dhcp option82 format** command.

14.8.42 display dhcp snooping

Function

The **display dhcp snooping** command displays DHCP snooping running information.

Format

display dhcp snooping [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCP snooping running information on a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-
vlan *vlan-id*	Displays DHCP snooping running information in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcp snooping** command displays DHCP snooping running information. If no interface or VLAN is specified, global DHCP snooping running information is displayed. If an interface or a VLAN ID is specified, DHCP snooping running information about the interface or VLAN is displayed.

Example

# Display global DHCP snooping running information.

```
<HUAWEI> display dhcp snooping
 DHCP snooping global running information   :
 DHCPv4 snooping                            : Enable
 DHCPv6 snooping                            : Enable
 Static user max number                     : 1024
 Current static user number                 : 1
 Dhcp user max number                       : 100
 Current dhcp user number                   : 0
 Arp dhcp-snooping detect                   : Disable  (default)
 Alarm threshold                            : 100      (default)
 Check dhcp-rate                            : Disable  (default)
 Dhcp-rate limit(pps)                       : 100      (default)
 Alarm dhcp-rate                            : Disable  (default)
 Alarm dhcp-rate threshold                  : 100      (default)
 Discarded dhcp packets for rate limit      : 0
 Bind-table autosave                        : Disable  (default)
 Offline remove mac-address                 : Disable  (default)
 Client position transfer allowed           : Enable   (default)

 DHCP snooping running information for interface GigabitEthernet0/0/1   :
 DHCP snooping                              : Enable
 Trusted interface                          : No
 Dhcp user max number                       : 100
 Current dhcp user number                   : 0
 Check dhcp-giaddr                          : Enable
 Check dhcp-chaddr                          : Disable  (default)
 Alarm dhcp-chaddr                          : Disable  (default)
 Check dhcp-request                         : Disable  (default)
 Alarm dhcp-request                         : Disable  (default)
 Check dhcp-rate                            : Enable
 Dhcp-rate limit(pps)                       : 100
 Alarm dhcp-rate                            : Enable
 Alarm dhcp-rate threshold                  : 100
 Discarded dhcp packets for rate limit      : 0
 Alarm dhcp-reply                           : Disable  (default)
```

Table 14-58 Description of the **display dhcp snooping** command output

Item	Description
DHCPv4 snooping	Whether DHCPv4 snooping is enabled globally. To enable DHCP snooping, run the **14.8.20 dhcp snooping enable** command.
DHCPv6 snooping	Whether DHCPv6 snooping is enabled globally. To enable DHCP snooping, run the **14.8.20 dhcp snooping enable** command.
DHCP snooping	Whether DHCP snooping is enabled on the interface or in the VLAN. To enable DHCP snooping, run the **14.8.20 dhcp snooping enable** command.

Item	Description
Static user max number	Maximum number of static users.
Current static user number	Number of current static users.
Dhcp user max number	Maximum number of DHCP snooping users. To set the maximum number of DHCP snooping users, run the **14.8.22 dhcp snooping max-user-number** command.
Current dhcp user number	Number of current DHCP snooping users.
Arp dhcp-snooping detect	Whether association between ARP and DHCP snooping is enabled. To enable association between ARP and DHCP snooping, run the **14.8.2 arp dhcp-snooping-detect enable** command.
Alarm threshold	Global alarm threshold for the number of discarded DHCP snooping messages. To set the global alarm threshold for the number of discarded DHCP snooping messages, run the **14.8.13 dhcp snooping alarm threshold** command.
Check dhcp-rate	Whether a device is enabled to check the rate of sending DHCP messages. To enable the device to check the rate of sending DHCP messages, run the **14.8.16 dhcp snooping check dhcp-rate enable** command.
Dhcp-rate limit(pps)	Rate limit of DHCP messages, in pps. To set the rate limit of DHCP messages, run the **14.8.15 dhcp snooping check dhcp-rate** command.
Alarm dhcp-rate	Whether trap for checking the rate of sending DHCP messages to the processing unit is enabled. To enable trap for checking the rate of sending DHCP messages to the processing unit, run the **14.8.10 dhcp snooping alarm dhcp-rate enable** command.

Item	Description
Alarm dhcp-rate threshold	Alarm threshold for the number of discarded DHCP messages. An alarm is generated if the number of discarded DHCP messages reaches the alarm threshold. To set the alarm threshold for the number of discarded DHCP messages, run the **14.8.11 dhcp snooping alarm dhcp-rate threshold** command.
Discarded dhcp messages for rate limit	Number of discarded DHCP messages whose rate exceeds the rate limit.
Bind-table autosave	Whether a device is enabled to save the DHCP Snooping binding table. To enable the device to save the binding table, run the **14.8.26 dhcp snooping user-bind autosave** command.
Offline remove mac-address	Whether a device is enabled to delete MAC addresses of offline users. To enable the device to delete MAC addresses of offline users, run the **14.8.33 dhcp snooping user-offline remove mac-address** command.
Client position transfer allowed	Whether location transition is enabled for DHCP snooping users. To enable location transition for DHCP snooping users, run the **14.8.34 dhcp snooping user-transfer enable** command.
Trusted interface	Whether an interface is a trusted interface. To configure an interface as a trusted interface, run the **14.8.24 dhcp snooping trusted** command.
Check dhcp-giaddr	Whether a device is enabled to check the GIADDR field in a DHCP Request message. To enable the device to check the GIADDR field in a DHCP Request message, run the **14.8.14 dhcp snooping check dhcp-giaddr enable** command.

Item	Description
Check dhcp-chaddr	Whether a device is enabled to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header. To enable the device to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header, run the **14.8.17 dhcp snooping check dhcp-chaddr enable** command.
Alarm dhcp-chaddr	Whether a device is enabled to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold. To enable the device to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold, run the **14.8.12 dhcp snooping alarm enable** command.
Check dhcp-request	Whether an interface is enabled to check DHCP Request messages. To enable the interface to check DHCP Request messages, run the **14.8.18 dhcp snooping check dhcp-request enable** command.
Alarm dhcp-request	Whether a device is enabled to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold. To enable the device to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold, run the **14.8.12 dhcp snooping alarm enable** command.

Item	Description
Alarm dhcp-reply	Whether a device is enabled to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface. To enable the device to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface, run the **14.8.12 dhcp snooping alarm enable** command.

14.8.43 display dhcp snooping configuration

Function

The **display dhcp snooping configuration** command displays the DHCP snooping configuration.

Format

display dhcp snooping configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP snooping configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP snooping configuration on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping configuration is complete, run the **display dhcp snooping configuration** command to view the DHCP snooping configuration. If no VLAN or interface is specified, all the DHCP snooping configurations are displayed. If a VLAN or an interface is specified, only the DHCP snooping configuration in the VLAN or on the interface is displayed.

Example

# Display all the DHCP snooping configurations.

```
<HUAWEI> display dhcp snooping configuration
#
dhcp snooping enable
#
vlan 3
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
#
interface GigabitEthernet0/0/1
 dhcp snooping enable
#
```

Related Topics

14.8.20 dhcp snooping enable

14.8.18 dhcp snooping check dhcp-request enable

14.8.44 display dhcp snooping statistics

Function

The **display dhcp snooping statistics** command displays statistics on the received DHCP messages.

Format

display dhcp snooping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display dhcp snooping statistics** command to view statistics on the received DHCP messages of all types.

Example

# Display statistics on the received DHCP messages.

```
<HUAWEI> display dhcp snooping statistics
 DHCP Snooping Statistics:

 Client Request:
  Dhcp Discover:                0
  Dhcp Request:                 0
  Dhcp Decline:                 0
  Dhcp Release:                 0
  Dhcp Inform:                  0
 Server Reply:
  Dhcp Offer:                   0
  Dhcp Ack:                     0
  Dhcp Nak:                     0
 Drop Packet:
  Dropped by mac-address check:   0
  Dropped by untrust reply:       0
  Dropped by request conflict:    0
  Dropped by untrust relay-forw:  0
 Delete DHCP snooping table:
  Receive release packet:         0
  Receive decline packet:         0
  Lease expired:                  0
  User command:                   0
  Client transferes:              0
  Interface down:                 0
  Arp detect:                     0
  Ucm notify:                     0
```

Table 14-59 Description of the display dhcp snooping statistics command output

Item	Description
Client Request	Number of packets sent by DHCP clients, including: ● Number of DHCP Discover packets ● Number of DHCP Request packets ● Number of DHCP Decline packets ● Number of DHCP Release packets ● Number of DHCP Inform packets
Server Reply	Number of packets sent by the DHCP server, including: ● Number of DHCP Offer packets ● Number of DHCP ACK packets ● Number of DHCP NAK packets
Drop Packet	Number of discarded packets.

Item	Description
Dropped by mac-address check	Number of discarded DHCP messages whose MAC address is different from the CHADDR value.
Dropped by untrust reply	Number of untrusted reply packets that are discarded.
Dropped by request conflict	Number of packets that are discarded because the client and server MAC addresses conflict.
Dropped by untrust relay-forw	Number of untrusted Relay-Forward packets that are discarded.
Delete DHCP snooping table	Number of DHCP snooping binding entries deleted by the device.
Receive release packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP release packets.
Receive decline packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP decline packets.
Lease expired	Number of DHCP snooping entries deleted by the device because of lease expiry.
User command	Number of DHCP snooping binding entries deleted by using commands.
Client transferes	Number of DHCP snooping binding entries deleted because the client connects to another interface on the device.
Interface down	Number of DHCP snooping binding entries deleted because the port is shut down.
Arp detect	Number of DHCP snooping binding entries deleted due to ARP detection.
Ucm notify	Number of times the Ucm module requests DHCP snooping to delete user binding entries.

Related Topics

14.8.20 dhcp snooping enable

14.8.45 display dhcp snooping user-bind

Function

The **display dhcp snooping user-bind** command displays the DHCP snooping binding table.

Format

display dhcp snooping user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays the binding entry mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 4 digits.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table. A binding entry contains the MAC address, IP address, number of the interface connected to the DHCP client, and VLAN ID on the interface. You can run the **display dhcp snooping user-bind** command to view the DHCP snooping binding table.

Example

# Display information about the DHCP snooping binding table.

- Display all binding entries.

```
<HUAWEI> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.28.141      78ac-d4b5-b858  10  /--  /--    GE0/0/1       2008.10.17-07:31
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

- Display detailed information about binding entries.

```
<HUAWEI> display dhcp snooping user-bind all verbose
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : 10.10.21.254
 MAC Address : 0200-0000-00e8
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : GE0/0/1
 Renew time  : 2017.03.07-11:32
 Expire time : 2017.03.08-11:32
 Gateway     : 10.10.21.1
 Server-ip   : 10.10.21.1
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Table 14-60 Description of the **display dhcp snooping user-bind** command output

Item	Description
DHCP Dynamic Bind-table	DHCP snooping binding entries.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: Vlan-mapping
IP Address	User IP address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.

Item	Description
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.
Renew time	Address renew time.
Expire time	Aging time of entries.
Gateway	Gateway address.
Server-ip	IP addresses of the DHCP server.

Related Topics

14.8.48 reset dhcp snooping user-bind

14.8.46 display dhcpv6 snooping user-bind

Function

The **display dhcpv6 snooping user-bind** command displays the DHCPv6 snooping binding table.

Format

display dhcpv6 snooping user-bind { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

display dhcpv6 snooping user-bind ipv6-prefix { *prefix/prefix-length* | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. - *interface-type* specifies the interface type. - *interface-number* specifies the interface number.	-

Parameter	Description	Value
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
ipv6-prefix	Displays an IPv6 suffix binding entry.	-
prefix/*prefix-length*	Displays the binding entry mapping a specified IPv6 prefix.	*prefix* is a 32-digit hexadecimal number, in the format of X:X::X:X. *prefix-length* is an integer that ranges from 1 to 128.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table. If the parameter is not specified, brief information about the binding table is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table by listening to DHCP Request messages and Reply messages. A binding entry contains the MAC address, IP address, number of the interface connected to the DHCP client, and VLAN ID. You can run the **display dhcpv6 snooping user-bind** command to view the DHCPv6 snooping binding table.

If prefix delegation (PD) users exist on the network, the device generates an IPv6 prefix binding entry. The **display dhcpv6 snooping user-bind ipv6-prefix** command displays IPv6 prefix binding entries.

Example

# Display the DHCPv6 binding table.

- Display all the dynamic binding entries.

```
<HUAWEI> display dhcpv6 snooping user-bind all
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                    MAC Address     VSI/VLAN(O/I/P) Lease
--------------------------------------------------------------------------------
FC00:1::1                     00d5-0191-02de  500 /--  /--    2008.10.01-00:26
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

- Display detailed information about the DHCPv6 binding table.

```
<HUAWEI> display dhcpv6 snooping user-bind all verbose
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : FC00:1::1
 MAC Address : 00d5-0191-02de
 VSI         : --
 VLAN(O/I/P) : 500 /--  /--
 Interface   : GE0/0/1
 Lease       : 2008.10.01-00:27
 IPSG Status : ineffective
 User State  : BOUND
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

# Display the IPv6 prefix binding table.

- Display all binding entries.

```
<HUAWEI> display dhcpv6 snooping user-bind ipv6-prefix all
PD Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IPv6 Prefix                   MAC Address     VSI/VLAN(O/I/P) Lease
--------------------------------------------------------------------------------
FC00:2::/36                   00d5-0191-02de  500 /--  /--    2008.10.03-00:30
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

- Display detailed information about IPv6 suffix binding entries.

```
<HUAWEI> display dhcpv6 snooping user-bind ipv6-prefix all verbose
PD Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : FC00:2::/36
 MAC Address : 00d5-0191-02de
 VSI         : --
 VLAN(O/I/P) : 500 /--  /--
 Interface   : GE0/0/1
 Lease       : 2008.10.03-00:30
 User State  : BOUND
--------------------------------------------------------------------------------
print count:           1          total count:           1
```

Table 14-61 Description of the display dhcpv6 snooping user-bind command output

Item	Description
DHCPV6 Dynamic Bind-table	DHCPv6 Snooping dynamic binding table.
PD Dynamic Bind-table	IPv6 prefix binding table.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: VLAN mapping
IP Address	User IPv6 address.
IPv6 Prefix	User IPv6 prefix.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.
Lease	Time when the lease of the IP address used by the user expires.
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: ● effective ● ineffective This field is invalid if IP packet checking is not enabled.
User State	Status of a DHCPv6 snooping binding entry is as follows: ● START ● DETECTION ● BOUND ● LIVE

14.8.47 reset dhcp snooping statistics

Function

The **reset dhcp snooping statistics** command clears DHCP snooping statistic.

Format

reset dhcp snooping statistics { **global** | **interface** *interface-type interface-number* [**vlan** *vlan-id*] | **vlan** *vlan-id* [**interface** *interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Clears DHCP Snooping statistics on the globally.	-
interface *interface-type interface-number*	Clears DHCP Snooping statistics on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Clears DHCP Snooping statistics in a specified VLAN. *vlan-id* specifies the ID of the VLAN.	*vlan-id* is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, if statistics are collected, you can run the **reset dhcp snooping statistics** command to clear the statistics.

Precautions

If both **interface** and **vlan** are specified, the specified interface must belong to the specified VLAN. The **reset dhcp snooping statistics** command clears DHCP Snooping statistics in the specified VLAN that the interface belongs to.

Example

# Clear DHCP Snooping statistics on GE0/0/1.

```
<HUAWEI> reset dhcp snooping statistics interface gigabitethernet 0/0/1
```

Related Topics

14.8.42 display dhcp snooping

14.8.20 dhcp snooping enable

14.8.48 reset dhcp snooping user-bind

Function

The **reset dhcp snooping user-bind** command clears DHCP snooping binding entries.

Format

reset dhcp snooping user-bind [**vlan** *vlan-id* | **interface** *interface-type interface-number*] * [**ipv4** | **ipv6**]

reset dhcp snooping user-bind [**ip-address** [*ip-address*] | **ipv6-address** [*ipv6-address*] | **vpls** *vpls-name*]

reset dhcp snooping user-bind [**ipv6-prefix** [*prefix*/*prefix-length*]]

NOTE

The parameter **vpls** *vpls-name* is only supported by the S5720HI.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears DHCP snooping binding entries mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Clears DHCP snooping binding entries mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ipv4 or **ip-address**	Clears DHCP snooping binding entries mapping IPv4 addresses.	-

Parameter	Description	Value
ipv6-address, **ipv6** or **ipv6-prefix**	Clears DHCP snooping binding entries mapping IPv6 addresses or IPv6 prefixes. ● **ipv6** indicates that DHCP snooping binding entries mapping IPv6 addresses or IPv6 prefixes are cleared. ● **ipv6-address** indicates that DHCP snooping binding entries mapping IPv6 addresses are cleared. ● **ipv6-prefix** indicates that DHCP snooping binding entries mapping IPv6 prefixes are cleared.	-
ip-address	Clears DHCP snooping binding entries mapping a specified IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Clears DHCP snooping binding entries mapping a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix/*prefix-length*	Clears DHCP snooping binding entries mapping a specified IPv6 prefix. ● *prefix* specifies the IPv6 prefix. ● *prefix-length* specifies the IPv6 prefix length.	*prefix* is a 32-digit hexadecimal characters in the format of X:X::X:X. *prefix-length* is an integer that ranges from 1 to 128.
vpls *vpls-name*	Clears DHCP snooping binding entries mapping a specified VPLS name.	The value must be an existing VPLS name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the mapping DHCP snooping binding entries are generated after DHCP users log in. The **reset dhcp snooping user-bind** command clears binding entries mapping a specified parameter. If no parameter is specified, all the binding entries are cleared.

Precautions

If both **interface** *interface-type interface-number* and **vlan** *vlan-id* are configured, the interface specified by **interface** *interface-type interface-number* must have been added to the VLAN specified by **vlan** *vlan-id*. In this case, the command clears the DHCP snooping binding entries on a specified interface belonging to a certain VLAN.

Example

# Clear DHCP snooping binding entries in VLAN 100.

```
<HUAWEI> reset dhcp snooping user-bind vlan 100
```

Related Topics

14.8.20 dhcp snooping enable

14.8.45 display dhcp snooping user-bind

14.9 ND Snooping Configuration Commands

14.9.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.9.2 display nd snooping configuration

Function

The **display nd snooping configuration** command displays the ND snooping configuration.

Format

display nd snooping configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

ND snooping configuration includes whether ND snooping is enabled or disabled and information about ND snooping trusted interfaces.

To view ND snooping configuration, run the **display nd snooping configuration** command.

Example

# Display ND snooping configuration.

```
<HUAWEI> display nd snooping configuration
#
nd snooping enable
#
interface GigabitEthernet0/0/0
 nd snooping trusted
#
interface Wlan-Bss0
```

```
 nd snooping enable
#
interface Wlan-Capwap0
 nd snooping trusted
#
```

14.9.3 display nd snooping prefix

Function

The **display nd snooping prefix** command displays prefix management entries of users.

Format

display nd snooping prefix [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays details about prefix management entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The IPv6 address of a user is automatically generated based on prefix information in an RA packet. After the IPv6 address is generated, the user sends a neighbor solicitation (NS) packet to check whether the IPv6 address is used by another user. To facilitate management of users' IP addresses, a device can establish a prefix management table. After ND snooping is enabled, the device obtains a router advertisement (RA) packet from an ND snooping trusted interface and generates a prefix management entry based on the RA packet. You can run the **display nd snooping prefix** command to check prefix management entries.

Example

# Display prefix management entries of users.

```
<HUAWEI> display nd snooping prefix
prefix-table:
Prefix                          Length   Valid-Time  Preferred-Time
-------------------------------------------------------------------------------
FC00:1::                         64       100000      100000
```

```
--------------------------------------------------------------------------------
Prefix table total count:      1
```

Table 14-62 Description of the **display nd snooping prefix** command output

Item	Description
prefix-table	Prefix management table of users.
Prefix	Prefix. The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.
Length	Prefix length. The value is an integer that ranges from 1 to 128.
Valid-Time	Valid lifetime of a prefix. The value ranges from 0 to 4294967295, in seconds.
Preferred-Time	Preferred lifetime of a prefix. The value ranges from 0 to 4294967295, in seconds.
Prefix table total count	Total number of entries in the prefix management table.

# Display prefix management entries of users.

```
<HUAWEI> display nd snooping prefix verbose
prefix-table:
--------------------------------------------------------------------------------
 Prefix                  : FC00:1::
 Prefix Length           : 64
 Valid Lifetime(sec)     : 2592000
 Preferred Lifetime(sec) : 604800
 Interface               : Wlan-Capwap0
 VLAN ID(Outer/Inner)    : 101/-
--------------------------------------------------------------------------------
 Prefix                  : FC00:2::
 Prefix Length           : 64
 Valid Lifetime(sec)     : 2592000
 Preferred Lifetime(sec) : 604800
 Interface               : Wlan-Capwap0
 VLAN ID(Outer/Inner)    : 102/-
--------------------------------------------------------------------------------
Prefix table total count:      2
```

Table 14-63 Description of the **display nd snooping prefix verbose** command output

Item	Description
prefix-table	Prefix management table of users.
Prefix	Prefix. The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.
Prefix Length	Prefix length. The value is an integer that ranges from 1 to 128.

Item	Description
Valid Lifetime(sec)	Valid lifetime of a prefix. The value ranges from 0 to 4294967295, in seconds.
Preferred Lifetime(sec)	Preferred lifetime of a prefix. The value ranges from 0 to 4294967295, in seconds.
Interface	Interface information in a prefix management entry.
VLAN ID(Outer/Inner)	VLAN information in a prefix management entry.
Prefix table total count	Total number of entries in the prefix management table.

14.9.4 display nd snooping statistics

Function

The **display nd snooping statistics** command displays statistics about the ND snooping packets received and discarded by the device.

Format

display nd snooping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ND snooping is enabled, the device records statistics on the received and discarded ND snooping packets to facilitate maintenance.

Example

# Display statistics on the ND snooping packets received and discarded on the device.

```
<HUAWEI> display nd snooping statistics
Input: total 203 packets, discarded 14 packets
```

```
 ns                                           :       178
 na                                           :        21
 rs                                          :        4
 ra                                          :        0
 other                                         :        0
Drop Packet:
 The local link address is incorrect            :         7
 It does not match the binding table             :         1
 The destination IP address is incorrect        :         6
```

Table 14-64 Description of the **display nd snooping statistics** command output

Item	Description
Input: total *n* packets, discarded *m* packets	Number (*n*) of ND packets received by the device and number (*m*) of discarded ND packets.
ns	Number of received NS packets on a device.
na	Number of received NA packets.
rs	Number of received RS packets.
ra	Number of received RA packets.
other	Number of received other packets.
Drop Packet	Number of dropped packets. The displayed information varies according to the packet drop reasons.
The local link address is incorrect	Number of packets dropped due to incorrect link-local address.
It does not match the binding table	Number of packets dropped because the packets do not match the binding entries.
The destination IP address is incorrect	Number of packets dropped due to incorrect destination IP addresses.

Related Topics

14.9.16 reset nd snooping statistics

14.9.5 display nd snooping user-bind

Function

The **display nd snooping user-bind** command displays the ND snooping dynamic binding table.

Format

display nd snooping user-bind all [**verbose**]

display nd snooping user-bind { **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* } * [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all ND snooping dynamic binding entries.	-
verbose	Displays detailed information about ND snooping dynamic binding entries.	-
ipv6-address *ipv6-address*	Displays information about the IPv6 address in the ND snooping dynamic binding table.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
mac-address *mac-address*	Displays information about the MAC address in the ND snooping dynamic binding table.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits.
vlan *vlan-id*	Displays information about the VLAN in the ND snooping dynamic binding table.	The value is an integer ranging from 1 to 4094.
interface *interface-type interface-number*	Displays interface information in the ND snooping dynamic binding table. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ND snooping dynamic binding entry includes the source IPv6 address and source MAC address of a user, and the VLAN that a user belongs to. You can run the **display nd snooping user-bind** command to view details in the ND snooping dynamic binding table.

Example

# Display all ND snooping dynamic binding entries.

```
<HUAWEI> display nd snooping user-bind all
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                     MAC Address     VSI/VLAN(O/I/P) Lease
--------------------------------------------------------------------------------
FC00:1::2                      00e0-4c7c-af8f  10  /--  /--    2011.05.06-20:09
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

# Display detailed information about ND snooping dynamic binding entries.

```
<HUAWEI> display nd snooping user-bind all verbose
ND Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : FC00:1::2
 MAC Address : 00e0-4c7c-af8f
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : GE0/0/1
 Lease       : 2011.05.06-20:09
 IPSG Status : ineffective
 User State  : DETECTION
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Table 14-65 Description of the **display nd snooping user-bind** command output

Item	Description
ND Dynamic Bind-table	ND snooping dynamic binding table.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	O indicates the outer VLAN ID; I indicates the inner VLAN ID; P indicates the mapped VLAN ID.
IP Address	IPv6 address of a user.
MAC Address	MAC address of a user.
VSI	VPN instance that a user belongs to.
VLAN(O/I/P)	Inner VLAN ID, outer VLAN ID, or VLAN mapping information of the online user. **NOTE** The ND snooping binding table does not contain VLAN mapping information. Therefore, no value is displayed in the P field.
Interface	User access interface.
Lease	ND user lease.

Item	Description
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: ● effective ● ineffective This field is invalid if IP packet checking is not enabled.
User State	Status of an ND snooping dynamic binding entry is as follows: ● START: The binding entry is being created and is in the initialization state. ● DETECTION: The system is performing detection for the binding entry to check whether the user is online. ● BOUND: The binding entry has been successfully created.

14.9.6 nd snooping check enable

Function

The **nd snooping check enable** command enables ND protocol packet validity check.

The **undo nd snooping check enable** command disables ND protocol packet validity check.

By default, ND protocol packet validity check is disabled.

Format

nd snooping check { **na** | **ns** | **rs** } **enable**

undo nd snooping check { **na** | **ns** | **rs** } **enable**

Parameters

Parameter	Description	Value
na	Enables validity check for Neighbor Advertisement (NA) packets.	-
ns	Enables validity check for Neighbor Solicitation (NS) packets.	-

Parameter	Description	Value
rs	Enables validity check for Router Solicitation (RS) packets.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ND packet validity check prevents forged NA/NS/RS packets.

After ND packet validity check is enabled, the device verifies the NA/NS/RS packets received by untrusted interfaces against the ND snooping binding table, to determine whether the NA/NS/RS packets are sent from valid users in the VLAN on the interface. The device forwards the ND packets from valid users and drops invalid ND packets.

Prerequisites

ND snooping has been enabled globally using the **nd snooping enable** command.

Example

# Enable NA packet validity check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping check na enable
```

Related Topics

14.9.7 nd snooping enable

14.9.7 nd snooping enable

Function

The **nd snooping enable** command enables ND snooping.

The **undo nd snooping enable** command disables ND snooping.

By default, ND snooping is disabled.

Format

nd snooping enable

undo nd snooping enable

Parameters

None

Views

System view, VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

ND provides powerful functions but has no security mechanism. Attackers often use ND to attack network devices. Common ND attacks are as follows:

- An attacker uses the IP address of host A to send NS, NA, or RS packets to host B or the gateway. Host B or the gateway then modifies their ND entries. As a result, all packets sent from host B or the gateway to host A are sent to the attacker.
- An attacker uses the gateway IP address to send RA packets to hosts. Then the hosts incorrectly set IPv6 parameters and modify their ND entries.

To prevent ND attacks, enable ND snooping on the device. The device detects NS packets in the DAD process to establish an ND snooping dynamic binding table that includes source IPv6 addresses, source MAC addresses, VLANs, and inbound ports. When receiving ND packets, the device checks the validity of ND packets based on the ND snooping binding table and checks whether the user is an authorized user in the VLAN that the port receiving ND packets belongs to. The device forwards valid ND packets and discards invalid ND packets to defend against ND attacks from bogus hosts or gateways.

NOTE

By default, the system reports a port-Up event 2 seconds after a user-side interface transits from Down to Up state. If ND snooping is enabled before the port-Up event is reported, the system cannot generate the ND snooping entry of the user connected to this interface. To avoid this problem, run the **carrier up-hold-time** *interval* command to change the delay in reporting the port-Up event to 0.

Example

# Enable ND snooping globally and on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping enable
```

14.9.8 nd snooping enable dhcpv6 only

Function

The **nd snooping enable dhcpv6 only** command enables ND snooping in the DHCPv6 Only scenario.

The **undo nd snooping enable** command disables ND snooping in the DHCPv6 Only scenario.

By default, ND snooping is disabled in the DHCPv6 Only scenario.

Format

nd snooping enable dhcpv6 only

undo nd snooping enable

Parameters

None

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device checks the validity of ND protocol packets against the IPv6 static binding table, DHCPv6 dynamic binding table, and ND snooping binding table. The IPv6 static binding table is manually configured by the administrator, the DHCPv6 dynamic binding table is automatically generated by extracting information from DHCPv6 Reply packets, and the ND snooping binding table is automatically generated by extracting information from DAD NS packets. At the same time, the ND protocol packet validity check function depends on the ND snooping function (including enabling ND snooping and configuring ND snooping trusted interfaces). In the DHCPv6 Only scenario, users are only allowed to obtain IPv6 addresses using DHCPv6 and IPv6 addresses that are privately configured by users and automatically generated using the PD address prefix are considered as invalid addresses. In this scenario, ND snooping is disabled to prevent ND snooping binding entries from being generated for such invalid addresses. In this case, the ND protocol packet validity check function cannot be performed, so that address spoofing attacks may exist on the network.

To resolve this problem, you can run the **nd snooping enable dhcpv6 only** and **nd snooping trusted dhcpv6 only** commands to enable the ND snooping function in the DHCPv6 Only scenario. After the **nd snooping enable dhcpv6 only** command is configured, no ND snooping binding entry is generated for the IPv6 global unicast addresses that are manually configured by users and automatically generated using the PD address prefixes. The device checks the validity of ND protocol packets against the IPv6 static binding table and DHCPv6 dynamic binding table.

Prerequisites

ND snooping has been enabled globally using the **nd snooping enable** command.

Precautions

- In the DHCPv6 Only scenario, ND snooping binding entries are generated for the IPv6 link-local addresses that are manually configured by users and automatically generated. To be specific, only records corresponding to the IPv6 link-local addresses exist in the ND snooping binding table in the DHCPv6 Only scenario.
- IPv6 addresses obtained using DHCPv6 PD also apply to the DHCPv6 Only scenario.

Example

# Enable ND snooping globally and on interface GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping enable dhcpv6 only
```

14.9.9 nd snooping max-user-number

Function

The **nd snooping max-user-number** command sets the maximum number of ND snooping dynamic binding entries to be learned by an interface.

The **undo nd snooping max-user-number** command restores the default maximum number of ND snooping dynamic binding entries to be learned by an interface.

By default, the maximum number of DHCP snooping binding entries that can be learned on an interface is 256 for S1720GFR-TP and S2750EI, 512 for S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, and S2720EI, 1024 for S1720X and S1720X-E, 2048 for S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI and S6720S-SI, and 4096 for other models.

Format

nd snooping max-user-number *max-user-number*

undo nd snooping max-user-number

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of ND snooping dynamic binding entries to be learned by an interface.	The value is an integer that ranges from 1 to 256 for S1720GFR-TP and S2750EI, from 1 to 512 for S1720GW, S1720GWR, S1720GW-E, S1720GWR-E, and S2720EI, from 1 to 1024 for S1720X and S1720X-E, from 1 to 2048 for S5700LI, S5700S-LI, S5710-X-LI, S5720LI, S5720S-LI, S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720LI, S6720S-LI, S6720SI and S6720S-SI, and from 1 to 4096 for other models.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a lot of users go online through an interface, the device consumes many ND snooping dynamic binding entries to process the NS packets. To prevent this problem, you can set the maximum number of ND snooping dynamic binding entries to be learned by an interface. If the number of the ND snooping dynamic binding entries learned by an interface reaches the maximum number, no entry can be added.

You can set the maximum number ND snooping entries in the system view or interface view. The configuration in the system view is valid for all interfaces. The settings in the interface view only take effect on the specified interface. If the settings are performed in both the interface view and system view, the smaller value is adopted.

Prerequisites

Before setting the maximum number of ND snooping dynamic binding entries to be learned by an interface, ensure that ND snooping has been enabled in the system view using the **nd snooping enable** command.

Example

# Set the maximum number of ND snooping binding entries to 200 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping max-user-number 200
```

Related Topics

14.9.7 nd snooping enable

14.9.10 nd snooping trusted

Function

The **nd snooping trusted** command configures the trusted interface.

The **undo nd snooping trusted** command restores the trusted interface to an untrusted interface.

By default, all interfaces are untrusted interfaces.

Format

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

nd snooping trusted

undo nd snooping trusted

VLAN view

nd snooping trusted interface *interface-type interface-number*

undo nd snooping trusted interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the trusted interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ND snooping classifies interfaces connected to IPv6 nodes into trusted and untrusted interfaces. The trusted interfaces connect to trusted IPv6 nodes and untrusted interfaces connect to untrusted IPv6 nodes. By default, all interfaces are untrusted.

- You must configure the interface connected to a trusted IPv6 node as a trusted interface so that the device can forward the ND packets received by this interface. In addition, the device creates a prefix management table according to the received RA packet to help network administrators manage IPv6 addresses.
- The interface connected to an untrusted IPv6 node must be configured as an untrusted interface. The device discards the RA packets received by the untrusted interface to prevent RA attacks.

NOTE

Generally, the interface connecting to the gateway is configured as the trusted interface, and other interfaces are all untrusted interfaces.

Prerequisites

ND snooping has been enabled using the **nd snooping enable** command in the system view.

Precautions

After the **nd snooping trusted** command is executed, ND snooping is enabled on the interface.

When you run the **nd snooping trusted** command in the VLAN view, the specified interface must belong to the VLAN.

Example

# Configure GE0/0/1 as a trusted interface.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping trusted
```

# Configure GE0/0/1 in VLAN 10 as a trusted interface.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] nd snooping trusted interface gigabitethernet 0/0/1
```

Related Topics

14.9.7 nd snooping enable

14.9.11 nd snooping trusted dhcpv6 only

Function

The **nd snooping trusted dhcpv6 only** command configures the interfaces in the DHCPv6 Only scenario as ND snooping trusted interfaces.

The **undo nd snooping trusted** command restores the interfaces to untrusted.

By default, all interfaces are untrusted.

Format

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

nd snooping trusted dhcpv6 only

undo nd snooping trusted

VLAN view

nd snooping trusted interface *interface-type interface-number* **dhcpv6 only**

undo nd snooping trusted interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface that will be configured as an ND snooping trusted interface in the DHCPv6 Only scenario. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

The device checks the validity of ND protocol packets against the IPv6 static binding table, DHCPv6 dynamic binding table, and ND snooping binding table. The IPv6 static binding table is manually configured by the administrator, the DHCPv6 dynamic binding table is automatically generated by extracting information from DHCPv6 Reply packets, and the ND snooping binding table is automatically generated by extracting information from DAD NS packets. At the same time, the ND protocol packet validity check function depends on the ND snooping function (including enabling ND snooping and configuring ND snooping trusted interfaces). In the DHCPv6 Only scenario, users are only allowed to obtain IPv6 addresses using DHCPv6 and IPv6 addresses that are privately configured by users and automatically generated using the PD address prefix are considered as invalid addresses. In this scenario, ND snooping is disabled to prevent ND snooping binding entries from being generated for such invalid addresses. In this case, the ND protocol packet validity check function cannot be performed, so that address spoofing attacks may exist on the network.

To resolve this problem, you can run the **nd snooping enable dhcpv6 only** and **nd snooping trusted dhcpv6 only** commands to enable the ND snooping function in the DHCPv6 Only scenario. After the **nd snooping trusted dhcpv6 only** command is configured, no prefix management entry is generated when the trusted interface receives an RA packet, which is different from the **nd snooping trusted** command. This is because the prefix management entries need to be matched before the corresponding ND snooping binding entries are generated for the IPv6 addresses excluding the IPv6 link-local addresses. However, only records corresponding to the IPv6 link-local addresses exist in the ND snooping binding table in the DHCPv6 Only scenario. Therefore, the prefix management entries do not need to be generated.

Example

# Configure GE0/0/1 as an ND snooping trusted interface.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] nd snooping trusted dhcpv6 only
```

# Configure GE0/0/1 as an ND snooping trusted interface in VLAN 2.

```
<HUAWEI> system-view
[HUAWEI] nd snooping enable
[HUAWEI] vlan 2
[HUAWEI-vlan2] nd snooping trusted interface gigabitethernet 0/0/1 dhcpv6 only
```

Related Topics

14.9.7 nd snooping enable

14.9.12 nd snooping user-alarm percentage

Function

The **nd snooping user-alarm percentage** command configures the alarm thresholds for the percentage of ND snooping dynamic binding entries.

The **undo nd snooping user-alarm percentage** command restores the default alarm thresholds for the percentage of ND snooping dynamic binding entries.

By default, the lower alarm threshold for the percentage of ND snooping dynamic binding entries is 50, and the upper alarm threshold for the percentage of ND snooping dynamic binding entries is 100.

Format

nd snooping user-alarm percentage *percent-lower-value percent-upper-value*

undo nd snooping user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of ND snooping dynamic binding entries.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of ND snooping dynamic binding entries.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **14.9.9 nd snooping max-user-number** command to set the maximum number of ND snooping dynamic binding entries on an interface, you can run the **nd snooping user-alarm percentage** command to set the alarm thresholds for the percentage of ND snooping dynamic binding entries.

When the percentage of learned ND snooping dynamic binding entries against the maximum number of ND snooping dynamic entries allowed by the device reaches or exceeds the upper alarm threshold, the device generates an alarm. When the percentage of learned ND snooping dynamic binding entries against the maximum number of ND snooping dynamic entries allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm. The alarm information helps network administrators monitor the status of ND snooping binding table in real time.

Example

# Set the lower alarm threshold for the percentage of ND snooping dynamic binding entries to 30 and the upper alarm threshold to 80.

```
<HUAWEI> system-view
[HUAWEI] nd snooping user-alarm percentage 30 80
```

Related Topics

14.9.9 nd snooping max-user-number

14.9.13 nd user-bind detect

Function

The **nd user-bind detect** command configures the number of times and interval for sending NS packets to detect the user status.

The **undo nd user-bind detect** command restores the default setting.

After automatic user status detection is enabled for users mapping ND snooping dynamic binding entries, the default number of detection times is 2, and the default detection interval is 1000 milliseconds.

Format

nd user-bind detect retransmit *retransmit-times* **interval** *retransmit-interval*

undo nd user-bind detect retransmit interval

Parameters

Parameter	Description	Value
retransmit *retransmit-times*	Specifies the number of times for sending NS packets to detect the user status.	The value is an integer ranging from 1 to 10. The default value is 2.
interval *retransmit-interval*	Specifies the interval for sending NS packets to detect the user status.	The value is an integer ranging from 1 to 10000, in milliseconds. The default value is 1000 milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After automatic user status detection for users mapping ND snooping dynamic binding entries is enabled, the device sends NS packets to users based on the configured detection times and interval. If no NA packet is returned from a user after NS packets are sent for configured times, the device considers the user to be offline and deletes the mapping ND snooping dynamic binding entry.

You can run the **nd user-bind detect** command to change the number of times and interval for sending NS packets to detect the user status. On a small network with good network quality, the user returns an NA packet quickly. In this scenario, you can set the interval for sending NS packets to a small value. On a large network with poor network quality, the user returns an NA packet slowly. You can set the interval to a large value to prevent the device from sending the next NS packet before receiving the NA packet. You can change the interval based on the actual network environment.

Prerequisites

Automatic user status detection for users mapping ND snooping dynamic binding entries has been enabled using the **nd user-bind detect enable** command.

Precautions

After you run the **nd user-bind detect enable** command, the device sends an NS packet after a period of time. The maximum value of this period is 20 seconds.

Example

# Set the number of times for sending NS packets to 10, and the interval for sending NS packets to 1000 milliseconds.

```
<HUAWEI> system-view
[HUAWEI] nd user-bind detect enable
[HUAWEI] nd user-bind detect retransmit 10 interval 1000
```

Related Topics

14.9.14 nd user-bind detect enable

14.9.14 nd user-bind detect enable

Function

The **nd user-bind detect enable** command enables the function for automatically detecting status of users mapping ND snooping dynamic binding entries.

The **undo nd user-bind detect enable** command disables the function for automatically detecting status of users mapping ND snooping dynamic binding entries.

By default, the function for automatically detecting status of users mapping ND snooping dynamic binding entries is disabled.

Format

nd user-bind detect enable

undo nd user-bind detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After ND snooping is enabled, the device snoops NS packets in the DAD process to establish ND dynamic binding entries. The aging time of an ND snooping dynamic binding table depends on the IPv6 address lease. If the address lease does not expire but the user is offline, the ND snooping dynamic entry mapping the user cannot be deleted, which occupies binding entry resources on the device.

To prevent this problem, you can enable the automatic user status detection for users mapping ND snooping dynamic binding entries on the device. After this function is enabled, the device sends NS packets to the user according to the detection times (n) specified in **nd user-bind detect** and detection interval. If the device receives no NA packet from the user after sending the NS packets n times, the device considers the user to be offline and deletes the dynamic ND snooping binding entry matching the user.

Precautions

After you run the **nd user-bind detect enable** command, the device sends an NS packet after a period of time. The maximum value of this period is 20 seconds.

Example

# Enable the function for automatically detecting status of users mapping ND snooping dynamic binding entries.

```
<HUAWEI> system-view
[HUAWEI] nd user-bind detect enable
```

Related Topics

14.9.13 nd user-bind detect

14.9.15 reset nd snooping prefix

Function

The **reset nd snooping prefix** command clears prefix management entries of users.

Format

reset nd snooping prefix [*ipv6-address*/*prefix-length*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
prefix-length	Specifies the prefix length.	The value is an integer ranging from 1 to 128. If the global unicast address needs to be set in EUI-64 format, the value of *prefix-length* ranges from 1 to 64.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The ND server that functions as the gateway router sends RA packets periodically to instruct users to update prefixes. The switch that functions as the access device establishes prefix management entries based on RA packets to maintain and manage user prefixes.

Generally, do not delete prefix management entries of users manually. Run the **reset nd snooping prefix** command to delete prefix management entries of users if the following requirements are met:

- The user lease does not expire and the prefix management table cannot age automatically.
- The user is no longer connected to the network.

Precautions

After a prefix management entry is deleted, the switch cannot establish the ND snooping dynamic binding table for new users with the prefix management entry.

Example

# Delete the prefix management entry with the prefix address being fc00:1::1 and the prefix length being 64.

```
<HUAWEI> reset nd snooping prefix fc00:1::1/64
```

Related Topics

14.9.3 display nd snooping prefix

14.9.16 reset nd snooping statistics

Function

The **reset nd snooping statistics** command deletes statistics on ND snooping packets.

Format

reset nd snooping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Use Scenario

After ND snooping is enabled, the device records statistics on the sent and received ND packets. This command deletes the statistics on ND packets.

Precautions

Deleted statistics cannot be restored. Exercise caution.

Example

# Delete statistics on ND snooping packets.

```
<HUAWEI> reset nd snooping statistics
```

Related Topics

14.9.4 display nd snooping statistics

14.9.17 reset nd snooping user-bind

Function

The **reset nd snooping user-bind** command clears ND snooping dynamic binding entries on the device.

Format

reset nd snooping user-bind [**interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface in the ND snooping dynamic binding entry to be cleared. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Specifies the IPv6 address in the ND snooping dynamic binding entry to be cleared.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
mac-address *mac-address*	Specifies the MAC address in the ND snooping dynamic binding entry to be cleared.	The value is in the format of H-H-H. An H is a hexadecimal number of 1 to 4 digits.
vlan *vlan-id*	Specifies the VLAN ID in the ND snooping dynamic binding entry to be cleared.	The value is an integer ranging from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

You need to manually delete ND snooping dynamic binding entries if the following requirements are met:

- The ND snooping dynamic binding entry does not reach the aging time, so the entry cannot age automatically.
- The user is no longer connected to the network.
- The user VLAN or interface information changes.

The networking environment change may lead to the change in the VLAN or interface information, while the ND snooping dynamic binding entry mapping a user does not age out and cannot update in real time. As a result, the device discards valid ND packets that do not match the old ND snooping dynamic binding entries. Before changing the networking environment, clear all ND snooping dynamic binding entries manually so that a device generates a new ND snooping dynamic binding table based on the new networking environment.

Example

# Delete the ND snooping dynamic binding entry that contains the IPv6 address being fc00:1::1.

```
<HUAWEI> reset nd snooping user-bind ipv6-address fc00:1::1
```

# Delete the ND snooping dynamic binding entry that contains the MAC address being 00e0-1111-2222.

```
<HUAWEI> reset nd snooping user-bind mac-address 00e0-1111-2222
```

Related Topics

14.9.5 display nd snooping user-bind

14.10 PPPoE+ Configuration Commands

14.10.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.10.2 display pppoe intermediate-agent information encapsulation

Function

The **display pppoe intermediate-agent information encapsulation** command displays the fields and vendor ID added to PPPoE packets.

Format

display pppoe intermediate-agent information encapsulation

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the fields and vendor ID added to PPPoE packets, you can run **display pppoe intermediate-agent information encapsulation** command to view the information.

Example

# Display the fields and vendor ID added to PPPoE packets.

```
<HUAWEI> display pppoe intermediate-agent information encapsulation
 The vendor id is: 2011
 Encapsulation content contains: Circuit-id and Remote-id
```

Table 14-66 Description of the display pppoe intermediate-agent information encapsulation command output

Item	Description
The vendor id is	Vendor ID added to PPPoE packets. You can run the **pppoe intermediate-agent information vendor-id** *vendor-id* command to set this parameter.
Encapsulation content contains	Fields added to PPPoE packets. You can run the **pppoe intermediate-agent information encapsulation** { **circuit-id** | **remote-id** } * command to set this parameter.

Related Topics

14.10.11 pppoe intermediate-agent information vendor-id

14.10.6 pppoe intermediate-agent information encapsulation

14.10.3 display pppoe intermediate-agent information format

Function

The **display pppoe intermediate-agent information format** command displays formats of circuit ID and remote ID that are configured globally.

Format

display pppoe intermediate-agent information format

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After PPPoE+ is enabled globally, you can run the **display pppoe intermediate-agent information format** command to check whether the configuration of the circuit ID or remote ID added to PPPoE packets is correct.

Example

# Display formats of circuit ID and remote ID that are configured globally.

```
<HUAWEI> display pppoe intermediate-agent information format
 The current information format :
  Circuit ID : EXTEND
  Remote  ID : COMMON
 For example:
  interface GigabitEthernet0/0/1 SVLAN:200 CVLAN:100
  The PPPOE Intermediate Agent information follow:
  Circuit ID:00 04 00 c8 00 00
  Remote  ID:0022-0033-0044
```

Table 14-67 Description of the **display pppoe intermediate-agent information format** command output

Item	Description
Circuit ID	Format of the circuit ID ● COMMON: indicates the standard fill format. ● EXTEND: indicates the extended fill format. ● USER DEFINE: indicates user-defined fill format. You can run the **pppoe intermediate-agent information format** command to set this parameter. If the **portdescription** keyword is specified in the user-defined circuit-id and no interface description is configured, the **Circuit ID** in **For example** displays **portdescription**.
Remote ID	Format of the remote ID ● COMMON: indicates the standard fill format. ● EXTEND: indicates the extended fill format. ● USER DEFINE: indicates user-defined fill format. You can run the **pppoe intermediate-agent information format** command to set this parameter. Remote IDs vary according to devices. If the **portdescription** keyword is specified in the user-defined **remote-id** and no interface description is configured, the **Remote ID** in **For example** displays **portdescription**.

Related Topics

14.10.7 pppoe intermediate-agent information format

14.10.4 display pppoe intermediate-agent information policy

Function

The **display pppoe intermediate-agent information policy** command displays the global policy for processing original fields in PPPoE packets at the user side and PPPoE server side.

Format

display pppoe intermediate-agent information policy

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pppoe intermediate-agent information policy** command displays the global policy for processing original fields in PPPoE packets at the user side and PPPoE server side.

Example

# Display the global policy for processing original information fields in PPPoE packets at the user side and PPPoE server side.

```
<HUAWEI> display pppoe intermediate-agent information policy
The current information Policy :REPLACE
The current ignore-reply Policy:ENABLE
```

Table 14-68 Description of the display pppoe intermediate-agent information policy command output

Item	Description
The current information Policy	Global policy for processing original information fields in PPPoE packets at the user side: ● DROP: removes original information fields from PPPoE packets. ● REPLACE: replaces original fields in PPPoE packets according to the field format. ● KEEP: reserves the content and format of original fields in PPPoE packets. You can run the **pppoe intermediate-agent information policy (system view)** command to set this parameter.
The current ignore-reply Policy	Global policy for processing PPPoE reply packets sent by the PPPoE server: ● ENABLE: indicates that the device does not process PPPoE reply packets sent by the PPPoE server. ● DISABLE: indicates that the device processes PPPoE reply packets sent by the PPPoE server. You can run the **pppoe intermediate-agent information ignore-reply** command to set this parameter.

Related Topics

14.10.10 pppoe intermediate-agent information policy (system view)

14.10.8 pppoe intermediate-agent information ignore-reply

14.10.5 pppoe intermediate-agent information enable

Function

The **pppoe intermediate-agent information enable** command enables PPPoE+ globally.

The **undo pppoe intermediate-agent information enable** command disables PPPoE+.

By default, PPPoE+ is disabled.

Format

pppoe intermediate-agent information enable

undo pppoe intermediate-agent information enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After PPPoE+ is enabled globally, the device can add information about the interface connected to the PPPoE client such as the slot ID/subcard ID/interface number to PPPoE packets. The user account and access interface information are both authenticated, preventing user account embezzling.

After the **pppoe intermediate-agent information enable** command is executed in the system view, PPPoE+ is enabled on all interfaces.

NOTE

If PPPoE+ is enabled on the device that has no ACL resources, the system displays the following message "Warning: Allocate acl resources failed." In this case, PPPoE+ does not work.

Example

# Enable PPPoE+ globally.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
```

Related Topics

14.10.7 pppoe intermediate-agent information format

14.10.10 pppoe intermediate-agent information policy (system view)

14.10.9 pppoe intermediate-agent information policy (interface view)

14.10.6 pppoe intermediate-agent information encapsulation

Function

The **pppoe intermediate-agent information encapsulation** command configures fields added to PPPoE packets.

The **undo pppoe intermediate-agent information encapsulation** command restores the default fields added to PPPoE packets.

By default, the device adds the **circuit-id** and **remote-id** fields to PPPoE packets.

Format

pppoe intermediate-agent information encapsulation { **circuit-id** | **remote-id** } *

undo pppoe intermediate-agent information encapsulation

Parameters

Parameter	Description	Value
circuit-id	Indicates the circuit ID (CID).	-
remote-id	Indicates the remote ID (RID).	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PPPoE+ is enabled, the device adds the **circuit-id** and **remote-id** fields to PPPoE packets by default. If the remote non-Huawei PPPoE server can identify only the **circuit-id** or **remote-id** field, run the **pppoe intermediate-agent information encapsulation** command to configure the device only to add the **circuit-id** or **remote-id** fields to PPPoE packets.

Prerequisites

The PPPoE+ function has been enabled by running the **pppoe intermediate-agent information enable** command in the system view.

Example

# Configure the device only to add the **circuit-id** field to PPPoE packets.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information encapsulation circuit-id
```

Related Topics

14.10.5 pppoe intermediate-agent information enable

14.10.7 pppoe intermediate-agent information format

Function

The **pppoe intermediate-agent information format** command configures the format of fields added to PPPoE packets.

The **undo pppoe intermediate-agent information format** command restores the format of fields added to PPPoE packets to default values.

By default, the format of fields **circuit-id** and **remote-id** added to PPPoE packets is **common**.

Format

pppoe intermediate-agent information [**vlan** *vlan-id*] [**ce-vlan** *cevlan-id*] **format** { **circuit-id** | **remote-id** } { **common** | **extend** | **user-defined** *text* }

undo pppoe intermediate-agent information format all

undo pppoe intermediate-agent information [**vlan** *vlan-id*] [**ce-vlan** *cevlan-id*] **format** { **circuit-id** | **remote-id** }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Indicates the outer VLAN ID. **NOTE** This parameter is not supported in the system view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *cevlan-id*	Indicates the end inner VLAN ID. **NOTE** This parameter is not supported in the system view.	The value is an integer that ranges from 1 to 4094.
circuit-id	Indicates the circuit ID (CID).	-
remote-id	Indicates the remote ID (RID).	-

Parameter	Description	Value
common	Indicates the standard fill format. ● CID format: {eth|trunk}slot ID/subcard ID/port ID:svlan.cvlan host name0/0/0/0/0, in ASCII format ● RID format: device MAC address (6 bytes), in ASCII format	-
extend	Indicates the extended format. ● CID format: circuit-id type (0) + length (4) + S-VLAN ID (2 bytes) + slot ID (5 bits) + subslot ID (3 bits) + port (1 byte), in hexadecimal notation ● RID format: remote-id type (0) + length (6) + MAC address (6 bytes), in hexadecimal notation In the format of the CID or RID, the values in parentheses without a unit are fixed values of the fields, and the values in parentheses with a unit indicate the length of the corresponding fields.	-
user-defined *text*	Indicates the user-defined format.	The *text* parameter specifies a user-defined format, and the value is a string of 1 to 127 characters. The details about the customized format string are provided in Precautions.

Parameter	Description	Value
all	Indicates the all format of fields. **NOTE** This parameter is not supported in the system view.	-

Views

System view and interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PPPoE+ is enabled globally, the default policy for processing user-side PPPoE packets is **replace**. The device replaces original information fields in the PPPoE packets received at the user side with those in common format. You can run the **pppoe intermediate-agent information format** command to change the format of information fields.

When the policy for processing user-side PPPoE packets is **replace** and the **pppoe intermediate-agent information format** command is executed, all interfaces add fields in a specified format to received PPPoE packets in the system view.

When the **pppoe intermediate-agent information format** command is configured, the device uses the following matching rules to encapsulate the information fields in PPPoE packets:

- For a double-tagged packet, the device matches the VLAN IDs in both the outer and inner VLAN tags. If the match fails, the device matches the VLAN ID in the inner VLAN tag, followed by that in the outer VLAN tag. If the match still fails, the device considers the packet does not carry a VLAN ID, and does not encapsulate the packet.
- For a single-tagged packet, the device matches the VLAN ID in the outer VLAN tag. If the match fails, the device considers the packet does not carry a VLAN ID, and does not encapsulate the packet.

If the **pppoe intermediate-agent information format** command is configured in both the interface and system views, the configuration in the interface view takes effect.

NOTE

Fields in PPPoE Intermediate-Agent Information packets support the following formats: **common**, **extend**, and **user-defined**. The formats are the same as those of DHCP Option 82. For description of the three parameters, see **dhcp option82 format**.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Precautions

You can use the following keywords to define the format. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port. For example, GigabitEthernet0/0/1. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is valid in ASCII or hexadecimal notation.
- iftype: indicates the type of an interface. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of an interface. In ASCII format, the value is expressed as H-H-H in hexadecimal notation, and the value is a number of six bytes.
- Slot: specifies the slot ID. This keyword is valid in ASCII or hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII or hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII or hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 0 to 4095. This keyword is valid in ASCII or hexadecimal notation.
- cvlan: indicates the inner VLAN ID. The value ranges from 0 to 4095. This keyword is valid in ASCII or hexadecimal notation.
- n: specifies the value of the svlan or cvlan keyword if the outer VLAN tag or inner VLAN tag does not exist. The n keyword is on the left of the svlan or cvlan keyword. If the corresponding VLAN does not exist, the default value of the svlan or cvlan keyword is 4096 in ASCII format and is all Fs in hexadecimal notation. If the keyword n is added to the left of the svlan or cvlan keyword, the svlan or cvlan keyword is set to 0. This keyword is valid in ASCII or hexadecimal notation.
- length: indicates the total length of the keywords following the length keyword.
- portdescription: indicates the interface description. It is available only in ASCII format.

NOTE

Separators must be added between keywords; otherwise, they cannot be parsed. The separators cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number between the % symbol and a keyword indicates the length of the keyword. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the length of the corresponding keyword in bits.

- The [] symbol indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the [] symbol is added to information fields only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nested [] symbols.
- The \ symbol is an escape character. The %, \, and [] symbols following the escape character indicate themselves. For example, \\ represents \.
- The content in quotation marks (" ") is expressed in a character string, and the content outside the quotation marks are expressed in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain letters, numerals, and symbols ! @ # $ % ^ & * () _ + | - = \ [] {} ; : '" / ? . , <> `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, space characters, %, and the keywords.
  - In a hexadecimal notation string, numbers are encapsulated in information fields. A number in the range of 0-255 occupies one byte; a number in the range of 256-65535 occupies two bytes; a number in the range of 65536-4294967295 occupies four bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by space characters; otherwise, they are considered as a number.
  - All the space characters in a hexadecimal character string are ignored.
  - By default, each slot ID, subslot ID, port number, and VLAN ID in a hexadecimal notation string occupy two bytes. The length field occupies one byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the specified length of a keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal character string can contain only the keywords whose values are numbers. Other keywords, such as the port name, cannot be added to the hexadecimal character string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate to the string in the ASCII format, add the string into a pair of quotation marks. For example, the slot ID is 3, and the port ID is 4. If the format string is %slot %port, the value of the string after encapsulation is a hexadecimal number 00030004. If the format string is "%slot %port", the value of the string after encapsulation is 3 4.
  - A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

# Configure the extended format for the **remote-id** field added to PPPoE packets.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information format remote-id extend
```

# Configure the user-defined format for the **circuit-id** field added to PPPoE packets and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information format circuit-id user-defined "%portname:%svlan.
%cvlan %sysname"
```

# Configure the extended format for the **remote-id** field added to PPPoE packets on GE1/0/1.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] pppoe intermediate-agent information format remote-id extend
```

Related Topics

14.10.5 pppoe intermediate-agent information enable

14.10.10 pppoe intermediate-agent information policy (system view)

14.10.9 pppoe intermediate-agent information policy (interface view)

14.8.6 dhcp option82 format

14.10.8 pppoe intermediate-agent information ignore-reply

Function

The **pppoe intermediate-agent information ignore-reply** command configures the device whether to directly forward PPPoE reply packets sent by the PPPoE server.

The **undo pppoe intermediate-agent information ignore-reply** command restores the default policy for processing PPPoE packets sent by the PPPoE server.

By default, the device does not process PPPoE reply packets sent by the PPPoE server.

Format

pppoe intermediate-agent information ignore-reply { **disable** | **enable** }

undo pppoe intermediate-agent information ignore-reply

Parameters

Parameter	Description	Value
disable	Indicates that the device processes PPPoE reply packets sent by the PPPoE server.	-
enable	Indicates that the device does not process PPPoE reply packets sent by the PPPoE server.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the device does not process PPPoE reply packets and directly forwards them to the PPPoE client. Only when the PPPoE client cannot identify PPPoE packets that the device directly forwards, the device needs to process the PPPoE reply packets sent by the PPPoE server to ensure communication between the PPPoE server and PPPoE client. The PPPoE reply packets are processed as follows:

- When the policy for processing original fields in PPPoE packets is **replace** or **keep**:
  - If fields are not contained in PPPoE reply packets sent by the PPPoE server, the device directly forwards PPPoE reply packets.
  - If fields are contained in PPPoE reply packets sent by the PPPoE server and the format and content are consistent with those of the fields added to the user-side PPPoE packets, the device removes the original fields from PPPoE packets and forwards the packets. If the format and content are different from those of the fields added to the user-side PPPoE packets, the device directly forwards PPPoE reply packets.
- When the policy for processing original fields in PPPoE packets is **drop**, the device directly forwards the PPPoE packets:

Precautions

The **pppoe intermediate-agent information ignore-reply** command takes effect only after PPPoE+ is enabled globally. To modify the configuration, disable PPPoE+ globally first.

If the device is configured to process the PPPoE reply packets sent by the PPPoE server, the user access rate is reduced when the PPPoE server sends a large number of PPPoE+ packets.

Example

# Configure the device to process PPPoE reply packets sent by the PPPoE server.

```
<HUAWEI> system-view
[HUAWEI] undo pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information ignore-reply disable
[HUAWEI] pppoe intermediate-agent information enable
```

Related Topics

14.10.5 pppoe intermediate-agent information enable

14.10.4 display pppoe intermediate-agent information policy

14.10.9 pppoe intermediate-agent information policy (interface view)

Function

The **pppoe intermediate-agent information policy** command configures the policy for a specified interface to process original fields in user-side PPPoE packets.

The **undo pppoe intermediate-agent information policy** command restores the default policy for a specified interface to process original fields in user-side PPPoE packets.

By default, the policy configured on an interface to process original fields in user-side PPPoE packets is **replace**.

Format

pppoe intermediate-agent information policy { **drop** | **replace** | **keep** }

undo pppoe intermediate-agent information policy

Parameters

Parameter	Description	Value
drop	Removes the original fields from PPPoE packets.	-
replace	Replaces original fields in PPPoE packets according to the field format.	-
keep	Reserves the content and format of original fields in PPPoE packets.	-

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the policy for processing original fields in user-side PPPoE packets is configured, the device can add information about the interface connected to the

PPPoE client such as the slot ID/subcard ID/interface number, VLAN ID, and MAC address to PPPoE packets. The user account and access interface information are both authenticated, preventing user account embezzling. If received PPPoE packets contain fields related to the interface that connected to the PPPoE client, the device removes or reserves original fields as required.

You can run the **pppoe intermediate-agent information policy (system view)** command to configure the PPPoE packet processing policy for all interfaces in the system view. To use a different policy on a specified interface, run the **pppoe intermediate-agent information policy** command. In this case, the policy for processing PPPoE packets on the interface depends on the interface configuration.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Example

# Configure GE0/0/1 to replace original fields in the received PPPoE packets with the circuit ID and remote ID of the local device.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] pppoe intermediate-agent information policy replace
```

Related Topics

14.10.5 pppoe intermediate-agent information enable

14.10.10 pppoe intermediate-agent information policy (system view)

14.10.10 pppoe intermediate-agent information policy (system view)

Function

The **pppoe intermediate-agent information policy** command configures the policy for all interfaces to process original fields in user-side PPPoE packets.

The **undo pppoe intermediate-agent information policy** command restores the policy for all interfaces to process original fields in user-side PPPoE packets.

By default, the policy configured on all interfaces to process original fields in user-side PPPoE packets is **replace**.

Format

pppoe intermediate-agent information policy { **drop** | **replace** | **keep** }

undo pppoe intermediate-agent information policy

Parameters

Parameter	Description	Value
drop	Removes the original fields from PPPoE packets.	-
replace	Replaces original information fields in PPPoE packets according to the field format.	-
keep	Reserves the content and format of original fields in PPPoE packets. If a PPPoE packet does not contain the fields, the device adds the fields to the packet according to the configuration.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the policy for processing original fields in user-side PPPoE packets is configured, the device can add information about the interface connected to the PPPoE client such as the slot ID/subcard ID/interface number, VLAN ID, and MAC address to PPPoE packets. The user account and access interface information are both authenticated, preventing user account embezzling. If received PPPoE packets contain fields related to the interface that connected to the PPPoE client, the device removes or reserves original fields as required.

After the command is executed, the policy for processing PPPoE packets takes effect on all interfaces. To configure a policy on a specified interface, run the **pppoe intermediate-agent information policy (interface view)** command. In this case, the policy for processing PPPoE packets on the interface depends on the interface configuration.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Example

# Configure all interfaces to replace original fields in the received PPPoE packets with the circuit ID and remote ID of the local device.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information policy replace
```

Related Topics

14.10.4 display pppoe intermediate-agent information policy

14.10.5 pppoe intermediate-agent information enable

14.10.9 pppoe intermediate-agent information policy (interface view)

14.10.11 pppoe intermediate-agent information vendor-id

Function

The **pppoe intermediate-agent information vendor-id** command sets the vendor ID that the device adds to PPPoE packets.

The **undo pppoe intermediate-agent information vendor-id** command restores the default vendor ID that the device adds to PPPoE packets.

The default vendor ID that the device adds to PPPoE packets is 2011.

Format

pppoe intermediate-agent information vendor-id *vendor-id*

undo pppoe intermediate-agent information vendor-id

Parameters

Parameter	Description	Value
vendor-id *vendor-id*	Specifies a vendor ID added to PPPoE packets.	The value is an integer ranging from 0 to 4294967295. The default value is 2011.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PPPoE+ is enabled, the device must negotiate with the PPPoE server using PPPoE packets containing the vendor ID. By default, the device adds vendor ID

2011 to PPPoE packets. If the device is connected to a non-Huawei PPPoE server, the vendor ID may not be 2011; for example, the vendor ID is 3561. In this case, run the **pppoe intermediate-agent information vendor-id** *vendor-id* command to set the vendor ID to be the same as that in PPPoE packets sent from the non-Huawei PPPoE server.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Example

# Set the vendor ID added to PPPoE packets to 3561.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] pppoe intermediate-agent information vendor-id 3561
```

Related Topics

14.10.5 pppoe intermediate-agent information enable

14.10.12 pppoe uplink-port trusted

Function

The **pppoe uplink-port trusted** command configures an interface as a trusted interface.

The **undo pppoe uplink-port trusted** command restores an interface to be untrusted.

By default, all interfaces are untrusted interfaces.

Format

pppoe uplink-port trusted

undo pppoe uplink-port trusted

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent bogus PPPoE servers and the security risk caused by PPPoE packets forwarded to non-PPPoE service interfaces, the interface connecting the device and the PPPoE server must be configured as the trusted interface. Then PPPoE protocol packets are forwarded to the PPPoE server through the trusted interface only. In addition, only the PPPoE protocol packets received on the trusted interface can be forwarded to the PPPoE client.

Prerequisites

PPPoE+ has been enabled globally by running the **pppoe intermediate-agent information enable** command.

Precautions

The trusted interface controls PPPoE protocol packets at the PPPoE discovery stage only. PPPoE service packets at the PPPoE session stage are not controlled.

If the trusted interface is configured on the device that has no ACL resources, the system displays the following message "Warning: Allocate acl resources failed." In this case, the trusted interface fails to be configured.

Example

# Configure GE0/0/1 as the PPPoE trusted interface.

```
<HUAWEI> system-view
[HUAWEI] pppoe intermediate-agent information enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] pppoe uplink-port trusted
```

Related Topics

14.10.5 pppoe intermediate-agent information enable

14.11 IP Source Guard Configuration Commands

14.11.1 Command Support

After hardware-based Layer 3 forwarding for IPv4 packets is enabled on an S2750EI, S5700-10P-LI-AC, or S5700-10P-PWR-LI-AC, an IPSG binding table can be configured, but the IPSG function is not supported.

14.11.2 display dhcp static user-bind

Function

The **display dhcp static user-bind** command displays information about a static binding table.

Format

display dhcp static user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays binding entries mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays binding entries mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays binding entries mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-

Parameter	Description	Value
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to view information about a configured static binding table. The information includes the IP address, MAC address, VLAN information, and interface information.

Example

# Display information about the static binding table.

```
<HUAWEI> display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address          MAC Address   VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.1.1.1            0001-0002-0003 10 /-- /--      GE0/0/1
--------------------------------------------------------------------------------
Print count:      1      Total count:      1
```

# Display detailed information about the static binding table.

```
<HUAWEI> display dhcp static user-bind all verbose
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : 10.21.21.254
 MAC Address : --
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : GE0/0/1
 IPSG Status : effective
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Table 14-69 Description of the display dhcp static user-bind command output

Item	Description
DHCP static Bind-table	Static DHCP binding entries. To configure a static DHCP binding table, run the **14.11.12 user-bind static** command.

Item	Description
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. - O: Outer VLAN - I: Inner VLAN - P: Vlan-mapping
IP Address	User IP address.
MAC Address	User MAC address.
VSI	Name of the VSI that the online user belongs to.
VLAN(O/I/P)	Inner VLAN ID, outer VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: - Effective - Ineffective This field is invalid if IP packet checking is not enabled.

14.11.3 display dhcpv6 static user-bind

Function

The **display dhcpv6 static user-bind** command displays the IPv6 binding table.

Format

display dhcpv6 static user-bind { { **interface** *interface-type interface-number* | **ipv6-address** { *ipv6-address* | **all** } | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

display dhcpv6 static user-bind ipv6-prefix { *prefix/prefix-length* | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 32-digit hexadecimal number, in the format of X:X::X:X.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
ipv6-prefix	Displays an IPv6 suffix binding entry.	-
prefix/prefix-length	Displays the binding entry mapping a specified IPv6 prefix.	*prefix* is a 32-digit hexadecimal number, in the format of X:X::X:X. *prefix-length* is an integer that ranges from 1 to 128.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to view information about a configured DHCPv6 static binding table. The information includes the IPv6 address, MAC address, VLAN information, and interface information.If prefix delegation (PD) users exist on the network, the device generates an IPv6 prefix binding entry. The **display dhcpv6 static user-bind ipv6-prefix** command displays the static IPv6 prefix binding entries.

Example

# Display the DHCPv6 static binding table.

```
<HUAWEI> display dhcpv6 static user-bind all
DHCPV6 static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address                        MAC Address      VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
fc00:1::1                       0001-0002-0003  10  /--  /--     --
--------------------------------------------------------------------------------
Print count:            1           Total count:            1
```

# Display detailed information about the DHCPv6 static binding table.

```
<HUAWEI> display dhcpv6 static user-bind all verbose
DHCPV6 static Bind-table:
--------------------------------------------------------------------------------
 IP Address  : fc00:1::1
 MAC Address : 0001-0002-0003
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : --
 IPSG Status : effective
--------------------------------------------------------------------------------
Print count:            1           Total count:            1
```

# Display the IPv6 prefix static binding table.

```
<HUAWEI> display dhcpv6 static user-bind ipv6-prefix all
PD static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IPv6 Prefix                       MAC Address      VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
fc00:1000::12/32                0001-0002-0003  10  /--  /--     --
--------------------------------------------------------------------------------
Print count:            1           Total count:            1
```

Table 14-70 Description of the display dhcpv6 static user-bind command output

Item	Description
DHCPV6 static Bind-table	Static DHCPv6 binding entries. To configure a static DHCPv6 binding table, run the **14.11.12 user-bind static** command.
Flags:O - outer vlan ,I - inner vlan ,P - map vlan	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: Map VLAN
IPv6 Prefix	User IPv6 prefix.

Item	Description
IP Address	User IPv6 address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: ● effective ● ineffective This field is invalid if IP packet checking is not enabled.

Related Topics

14.11.11 ip source check user-bind enable

14.11.12 user-bind static

14.11.4 display ip source check user-bind

Function

The **display ip source check user-bind** command displays the IPSG configurations.

Format

display ip source check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the IP packet check configuration on a specified interface. The interface is specified by the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ip source check user-bind** command displays the IP packet check configuration on an interface, including IP packet check items and the alarm function of IP packet check.

Example

# Display the IP packet check configuration on GE0/0/1.

```
<HUAWEI> display ip source check user-bind interface gigabitethernet 0/0/1
 ip source check user-bind enable
 ip source check user-bind check-item ip-address
 ip source check user-bind alarm enable
 ip source check user-bind alarm threshold 200
```

Table 14-71 Description of the display ip source check user-bind command output

Item	Description
ip source check user-bind enable	IP packet check is enabled.
ip source check user-bind check-item ip-address	IP packet check items. An IP packet check item can contain the IP address, MAC address, VLAN ID, and interface number. To specify check items, run the **ip source check user-bind check-item (interface view)** or **ip source check user-bind check-item (VLAN view)** commands.
ip source check user-bind alarm enable	Alarm function of IP packet check is enabled. To enable the alarm function of IP packet check, run the **ip source check user-bind alarm enable** command.
ip source check user-bind alarm threshold 200	Alarm threshold for IP packet check. To set the alarm threshold for IP packet check, run the **ip source check user-bind alarm threshold** command.

Related Topics

14.11.7 ip source check user-bind alarm enable

14.11.8 ip source check user-bind alarm threshold

14.11.9 ip source check user-bind check-item (interface view)

14.11.10 ip source check user-bind check-item (VLAN view)

14.11.11 ip source check user-bind enable

14.11.5 display mac-address snooping

Function

The **display mac-address snooping** command displays snooping MAC address entries generated based on the snooping binding table.

Format

display mac-address snooping [*interface-type interface-number* | **vlan** *vlan-id*] * [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the static MAC address entry on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Displays all the static MAC address entries on all the interfaces in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
verbose	Displays detailed information about static MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **14.11.13 user-bind ip sticky-mac** command in the interface view, the device generates snooping MAC address entries based on the snooping binding table. A snooping MAC address entry includes the user MAC address and VLAN ID. The **display mac-address snooping** command displays snooping MAC address entries generated based on the snooping binding table. If no interface or

VLAN is specified, all the snooping MAC address entries generated based on the snooping binding table are displayed.

Example

# Display the snooping MAC address entries generated based on the snooping binding table on the device.

```
<HUAWEI> display mac-address snooping
-------------------------------------------------------------------------------
MAC Address    VLAN/VSI/BD                     Learned-From        Type
-------------------------------------------------------------------------------
0000-c102-0602 10/-/-                          GE0/0/1             snooping
-------------------------------------------------------------------------------
Total items displayed = 1
```

Table 14-72 Description of the display mac-address snooping command output

Item	Description
MAC Address	User MAC address.
VLAN/VSI/BD	ID of the VLAN, name of the VSI, or ID of the BD that the user belongs to.
Learned-From	Port number.
Type	Type of a MAC address entry, including: ● static: indicates a static MAC address entry. ● blackhole: indicates a blackhole MAC address entry. ● dynamic: indicates a dynamic MAC address entry. ● security: indicates a security MAC address entry. ● sticky: indicates a sticky MAC address entry. ● snooping: indicates a MAC address entry generated based on the snooping binding table.

Related Topics

14.11.13 user-bind ip sticky-mac

14.11.6 ip anti-attack source-ip equals destination-ip drop

Function

The **ip anti-attack source-ip equals destination-ip drop** command enables the device to discard IP packets with the same source and destination IP addresses.

The **undo ip anti-attack source-ip equals destination-ip drop** command disables the device from discarding IP packets with the same source and destination IP addresses.

By default, the device does not discard IP packets with the same source and destination IP addresses.

NOTE

Only the S5720EI, S5720HI and S6720EI/S6720S-EI support this command.

Format

ip anti-attack source-ip equals destination-ip drop

undo ip anti-attack source-ip equals destination-ip drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Generally, IP packets with the same source and destination IP addresses can be forwarded. When you determine that the IP packets are attack packets, you can use the **ip anti-attack source-ip equals destination-ip drop** command to enable the device to discard the IP packets.

Example

# Enable the device to discard IP packets with the same source and destination IP addresses.

```
<HUAWEI> system-view
[HUAWEI] ip anti-attack source-ip equals destination-ip drop
```

14.11.7 ip source check user-bind alarm enable

Function

The **ip source check user-bind alarm enable** command enables the alarm function of IP packet check.

The **undo ip source check user-bind alarm enable** command disables the alarm function of IP packet check.

By default, the alarm function of IP packet check is disabled.

Format

ip source check user-bind alarm enable

undo ip source check user-bind alarm enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is run, the switch records logs when discarding IP packets. The log information includes the inbound interface, number of discarded packets, and discarding time. If the number of discarded packets exceeds the alarm threshold, the device sends an alarm to the NMS.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command on the interface.

Follow-up Procedure

Run the **ip source check user-bind alarm threshold** command to set the alarm threshold.

Example

# Enable the alarm function for IP packet check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind alarm enable
```

Related Topics

14.11.11 ip source check user-bind enable

14.11.8 ip source check user-bind alarm threshold

14.11.8 ip source check user-bind alarm threshold

Function

The **ip source check user-bind alarm threshold** command sets the alarm threshold for IP packet check.

The **undo ip source check user-bind alarm threshold** command restores the default alarm threshold for IP packet check.

By default, the alarm threshold is 100.

Format

ip source check user-bind alarm threshold *threshold*

undo ip source check user-bind alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies an alarm threshold for IP packet check.	The value is an integer that ranges from 1 to 1000.

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of IP packet check is enabled, run the **ip source check user-bind alarm threshold** command to set the alarm threshold for IP packet check.

Prerequisites

The alarm function of IP packet check has been enabled using the **ip source check user-bind alarm enable** command.

Example

# Set the alarm threshold for IP packet check to 200 on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind alarm enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind alarm threshold 200
```

Related Topics

14.11.11 ip source check user-bind enable

14.11.7 ip source check user-bind alarm enable

14.11.9 ip source check user-bind check-item (interface view)

Function

The **ip source check user-bind check-item** command configures IP packet check items on an interface.

The **undo ip source check user-bind check-item** command restores the default IP packet check items.

By default, the check items contain the IP address, MAC address, VLAN and interface information.

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo ip source check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
vlan	Checks whether VLAN information of an IP packet matches a binding entry.	-

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (interface view)** command to specify items in the IP packet to be checked on a specified interface. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP packet contain the source IP address, source MAC address, and VLAN information. Interface information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the interface view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

Example

# Enable IP packet check on GE0/0/1 to check whether the IP address in the IP packet matches the binding entry.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind check-item ip-address
```

Related Topics

14.11.11 ip source check user-bind enable

14.11.10 ip source check user-bind check-item (VLAN view)

Function

The **ip source check user-bind check-item** command configures IP packet check items in a VLAN.

The **undo ip source check user-bind check-item** command restores the default IP packet check items in a VLAN.

By default, the check items contain the IP address, MAC address, VLAN and interface information.

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo ip source check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
interface	Checks whether interface information of an IP packet matches a binding entry.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (VLAN view)** command to configure IP packet check items in a specified VLAN. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP packet contain the source IP address, source MAC address, and interface information. VLAN information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the VLAN view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

Example

# Enable IP packet check in VLAN 100 and check whether the IP address in the IP packet matches the binding entry.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] ip source check user-bind enable
[HUAWEI-vlan100] ip source check user-bind check-item ip-address
```

Related Topics

14.11.11 ip source check user-bind enable

14.11.11 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP packet check.

The **undo ip source check user-bind enable** command disables IP packet check.

By default, IP packet check is disabled.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

VLAN view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unauthorized users often send bogus packets with the source IP address and MAC address of authorized users to access or attack the network. Then authorized users cannot access stable and secure networks. To address this problem, you can configure IP packet check.

When IP packet check is enabled, the device checks the IP address, MAC address, VLAN information, and interface information against the binding table. You can run the **14.11.9 ip source check user-bind check-item (interface view)** or **14.11.10 ip source check user-bind check-item (VLAN view)** command to specify IP packet check items. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded.

Prerequisites

The IP packet check is based by binding table. So,

- The dynamic DHCP snooping binding table has been generated for DHCP users.
- The static binding table has been configured manually for users using static IP addresses.
- The dynamic ND snooping binding table has been generated for users dynamically obtaining IPv6 addresses through Stateless Address Autoconfiguration.

Precautions

After IP packet check is enabled, the device checks both the source IPv4 addresses and source IPv6 addresses of IP packets from users.

Example

# Enable IP packet check on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] ip source check user-bind enable
```

14.11.12 user-bind static

Function

The **user-bind static** command configures a static binding table.

The **undo user-bind static** command deletes a static binding table.

By default, no static binding table is configured.

Format

user-bind static { { { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-prefix** *prefix/prefix-length* } | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]

undo user-bind static [{ **ip-address** { *start-ip* [**to** *end-ip*] } &<1-10> | **ipv6-address** [*start-ip* [**to** *end-ip*]] &<1-10> | **ipv6-prefix** [*prefix/prefix-length*] } | **mac-address** *mac-address* | **interface** *interface-type interface-number* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface connected to a user in a static binding entry. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address	Indicates the static IPv4 address.	-
ipv6-address	Indicates the static IPv6 address.	-
start-ip [**to** *end-ip*]	Specifies the user IP address in a static binding entry. ● *start-ip* specifies the first IP address. ● **to** *end-ip* specifies the last IP address. The value of *end-ip* must be larger than the value of *start-ip*. *start-ip* and *end-ip* identify a VLAN range. If **to** *end-ip* is not specified, only the start IP address is added to the static binding entry. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	The IPv4 address is in dotted decimal notation in the format of X.X.X.X. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
ipv6-prefix *prefix/prefix-length*	Specifies the prefix of an IPv6 address	The prefix consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X. *prefix-length* is an integer that ranges from 1 to 128.
mac-address *mac-address*	Specifies the user MAC address in a static binding entry.	The value is in hexadecimal notation. The value is in the format of H-H-H.
vlan *vlan-id*	Specifies the user VLAN ID in a static binding entry.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN tag of a QinQ packet in a static binding entry.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When DHCP snooping is enabled, a dynamic binding table is automatically generated for dynamic users. However, a static binding table cannot be generated for static users. If IP source guard is enabled but no static binding table is available, the device discards all static users' forwarding packets. To enable the device to forward static users' packets, run the **user-bind static** command to configure a static binding table.

Precautions

After a static binding table is configured and IP source guard is enabled, the device performs a match check on IP packets based on the configured binding entries. If the match check fails, the device discards the IP packets.

Example

# Configure a static binding entry for a user in VLAN 2 with the IP address 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] user-bind static ip-address 10.1.1.1 vlan 2
```

Related Topics

14.11.2 display dhcp static user-bind

14.11.13 user-bind ip sticky-mac

Function

The **user-bind ip sticky-mac** command enables the device to generate snooping MAC entries.

The **undo user-bind ip sticky-mac** command disables the device from generating snooping MAC entries.

By default, the device does not generate snooping MAC entries.

Format

user-bind ip sticky-mac

undo user-bind ip sticky-mac

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, MultiGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the users with unauthorized MAC addresses from attacking the network, run the **user-bind ip sticky-mac** command to configure the device to generate snooping MAC entries on the interface that is prone to attack. After the device is configured to generate snooping MAC entries, it translates the dynamic MAC entries learned by the interface into snooping MAC entries (snooping MAC entries are a type of static MAC entries) based on the DHCP snooping binding table and ND snooping binding table, or generates snooping MAC entries based on the static binding entries.

After the configuration is complete, the interface forwards only the IP packets of which the source MAC addresses are included in the static MAC entries (static and snooping), and discards other IP packets.

NOTE

- To view MAC entry information on the device, see **5.1.3 display mac-address**.
- If a binding entry is modified, the matching snooping MAC entry is also modified.

Prerequisites

Before using the **user-bind ip sticky-mac** command, ensure that the DHCP snooping function has been enabled by the **dhcp snooping enable** command.

Precautions

To ensure correct packet forwarding for authorized static users on an interface, you can run the **14.11.12 user-bind static** command to configure static binding entries, which generate static MAC entries, or run the **mac-address static** command to configure static MAC entries.

When configuring a static binding entry, specify the MAC address, VLAN ID, and interface number. The VLAN ID must already exist on the device. If you do not specify the three parameters, a snooping MAC entry cannot be generated based on this static binding entry.

To allow DHCPv6 users to go online, enable both DHCP snooping and ND snooping.

The **user-bind ip sticky-mac** command cannot be used together with the following commands.

Command	Description
dot1x enable	Enables 802.1X authentication on an interface.
mac-authen	Enables MAC address-based authentication on an interface.
authentication-profile (Interface view or VAP profile view)	Applies an authentication profile to the interface or VAP profile.
mac-address learning disable (Interface view and VLAN view)	Enables MAC address learning.
mac-limit	Sets the maximum number of MAC addresses to be learned.
port vlan-mapping vlan map-vlan **port vlan-mapping vlan inner-vlan**	Enables VLAN mapping.
port-security enable	Enables port security.

Example

# Configure the GE0/0/1 interface to generate snooping MAC entries based on the snooping binding table.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
```

```
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] user-bind ip sticky-mac
```

Related Topics

14.8.20 dhcp snooping enable

14.9.7 nd snooping enable

14.12 SAVI Configuration Commands

14.12.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.12.2 savi max dad-delay

Function

The **savi max dad-delay** command sets the time for listening to an NA packet responding to address conflicts.

The **undo savi max dad-delay** command restores the default setting.

By default, the time for listening to an NA packet responding to address conflicts is 2 seconds.

Format

savi max dad-delay *value*

undo savi max dad-delay

Parameters

Parameter	Description	Value
value	Specifies the time for listening to an NA packet responding to address conflicts.	The value is an integer that ranges from 1 to 100, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **savi max dad-delay** command is applicable only for SLAAC-Only scenarios and DHCPv6+SLAAC scenarios.

- In SLAAC-Only scenarios:

  When obtaining an IP address in SLAAC mode, an ND client generates the IPv6 address based on the prefix in the RA packet. After the IPv6 address is generated, the ND client sends an NS packet to check whether duplicate addresses exist on the network. When detecting the NS packet in the DAD process from the ND client, the device generates an ND snooping entry, sets the entry to the detect state, and listens to the mapping NA packet.

  - If a mapping NA packet is detected in the configured listening period, IPv6 address conflict occurs and the device deletes this ND snooping entry.
  - If no mapping NA packet is detected in the configured listening period, the IPv6 address is available and the device sets the ND snooping entry to the bound state. The device deletes the ND snooping entry only when the entry ages out. If automatic user status detection for users mapping ND snooping dynamic binding entries is enabled using the **nd user-bind detect enable** command on the device, and no NA packet is returned from the user after NS packets are sent for times configured using the **nd user-bind detect retransmit** *retransmit-times* **interval** *retransmit-interval* command, the device considers the user to be offline and deletes the mapping ND snooping entry.
- In DHCPv6+SLAAC scenarios:
  - The procedure for processing packets by SAVI in SLAAC mode is the same as that in SLAAC-Only scenarios.
  - When obtaining an IP address in DHCPv6 mode, a DHCPv6 client may send an NS packet to check whether duplicate addresses exist on the network. When detecting the NS packet in the DAD process from the DHCPv6 client, the device sets the mapping DHCPv6 snooping entry to the detect state, and listens to the mapping NA packet.

    - If a mapping NA packet is detected in the configured listening period, IPv6 address conflict occurs and the device deletes this DHCPv6 snooping entry.

    - If no mapping NA packet is detected in the configured listening period, the IPv6 address is available and the device sets the DHCPv6 snooping entry to the bound state.

    When the DHCPv6 Snooping entry is in detection state, the device deletes this entry after detecting the NA packets within the time of listening on

NA packets with response address conflicts. When the DHCPv6 Snooping entry is in bound state, the device deletes this entry after detecting the DHCPv6 Decline or DHCPv6 Release packets sent from the DHCPv6 clients.

Prerequisites

The SAVI function has been enabled using the **savi enable** command.

Precautions

This command is used together with ND snooping and DHCPv6 snooping.

Example

# Set the time for listening to an NA packet responding to address conflicts to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] savi enable
[HUAWEI] savi max dad-delay 5
```

Related Topics

14.12.5 savi enable

14.12.3 savi max dad-prepare-delay

Function

The **savi max dad-prepare-delay** command sets the time for listening to the duplicate address detection performed by the DHCPv6 client.

The **undo savi max dad-prepare-delay** command restores the default setting.

By default, the time for listening to the duplicate address detection performed by the DHCPv6 client is 2 seconds.

Format

savi max dad-prepare-delay *value*

undo savi max dad-prepare-delay

Parameters

Parameter	Description	Value
value	Specifies the time for listening to the duplicate address detection performed by the DHCPv6 client.	The value is an integer that ranges from 1 to 100, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **savi max dad-prepare-delay** command is applicable only for DHCPv6-Only scenarios and DHCPv6+SLAAC scenarios.

After detecting that the DHCPv6 client obtains the IPv6 address, the device detects whether the DHCPv6 client sends an NS packet for duplicate address detection.

- In DHCPv6-Only scenarios:
  - If no NS packet in the DAD process is detected in the configured listening period, the device sets the DHCPv6 snooping entry to the bound state. It indicates that the DHCPv6 does not perform the duplicate address detection on the obtained IPv6 address or no duplicate IPv6 address exists.
  - If an NS packet in the DAD process is detected in the configured listening period, the device does not change the status of the mapping DHCPv6 snooping entry. The device sets the DHCPv6 snooping entry to the bound state only when the listening period expires.

  In DHCPv6-Only scenarios, when detecting the DHCPv6 Decline packet or DHCPv6 Release packet from the DHCPv6 client, the device deletes the corresponding DHCPv6 snooping entry.
- In DHCPv6+SLAAC scenarios:
  - If no NS packet in the DAD process is detected in the configured listening period, the device sets the DHCPv6 snooping or ND snooping entry to the bound state. It indicates that the client does not perform the duplicate address detection on the obtained IPv6 address or no duplicate IPv6 address exists, and the client can use this IPv6 address.
  - If an NS packet in the DAD process is detected in the configured listening period, the device sets the mapping DHCPv6 snooping or ND snooping entry to the detection state, and listens to the mapping NA packet. For the listening method, see **14.12.2 savi max dad-delay**.

Prerequisites

The SAVI function has been enabled using the **savi enable** command.

Precautions

This command is used together with ND snooping and DHCPv6 snooping.

Example

# Set the time for listening to the duplicate address detection performed by the DHCPv6 client to 5 seconds.

```
<HUAWEI> system-view
[HUAWEI] savi enable
[HUAWEI] savi max dad-prepare-delay 5
```

Related Topics

14.12.5 savi enable

14.12.4 savi max-binding-table

Function

The **savi max-binding-table** command sets the maximum number of SAVI binding entries on an interface.

The **undo savi max-binding-table** command restores the default maximum number of SAVI binding entries on an interface.

By default, the maximum number of SAVI binding entries is the same as the number of binding entries supported by the device.

Format

savi max-binding-table *max-number*

undo savi max-binding-table

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of SAVI binding entries on an interface.	The value is an integer that varies depending on product models.

Views

Ethernet interface view, GE interface view, XGE interface view, MultiGE interface view, 40GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SAVI binding table is a set of the ND snooping binding table and DHCPv6 snooping binding table. When the sum of ND snooping binding entries and DHCPv6 snooping binding entries on an interface reaches the configured maximum number of SAVI binding entries, subsequent users cannot connect to the network. After the maximum number of SAVI binding entries is set, the device does not process many ND packets and DHCPv6 packets with invalid source addresses to defend against attacks.

Prerequisites

Ensure that SAVI has been enabled globally using the **savi enable** command.

Example

# Set the maximum number of SAVI binding entries on the GE0/0/1 to 8.

```
<HUAWEI> system-view
[HUAWEI] savi enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] savi max-binding-table 8
```

Related Topics

14.12.5 savi enable

14.12.5 savi enable

Function

The **savi enable** command enables the SAVI function.

The **undo savi enable** command disables the SAVI function.

By default, the SAVI function is disabled.

Format

savi enable

undo savi enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the SAVI function is enabled, the device checks the validity of the source addresses in the ND, DHCPv6, and IPv6 data packets based on the bindings between IP addresses and ports and filters out invalid packets. The bindings between IP addresses and ports are generated based on ND snooping and DHCPv6 snooping.

Precautions

The SAVI function must be used together with ND snooping, DHCPv6 snooping, or IP source guard.

After the SAVI function is enabled, only when both ND snooping and IP source guard are enabled or both DHCPv6 snooping and IP source guard are enabled on an interface, the device checks the validity of the source addresses in IPv6 data packets received on this interface.

Example

# Enable the SAVI function.

```
<HUAWEI> system-view
[HUAWEI] savi enable
```

14.13 URPF Configuration Commands

14.13.1 Command Support

This command is only supported by S5720SI, S5720S-SI, S5720EI, S5720HI, S5730SI, S5730S-EI, S6720SI, S6720S-SI, S6720EI, and S6720S-EI.

14.13.2 urpf (interface view)

Function

The **urpf** command enables URPF on an interface and configures the URPF mode.

The **undo urpf** command disables URPF on an interface.

By default, URPF is disabled on an interface.

NOTE

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support this command.

For the S5720EI, S6720EI, and S6720S-EI, only Layer 2 Ethernet interfaces support URPF strict check.

Format

urpf { **loose** | **strict** } [**allow-default-route**]

undo urpf

Parameters

Parameter	Description	Value
loose	Indicates URPF check in loose mode. A packet passes the check as long as the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet is not required to be the same as the outbound interface of the route.	-
strict	Indicates URPF check in strict mode. A packet passes the check only when the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet should be the same as the outbound interface of the route.	-
allow-default-route	Allows the route to the source IP address of the packet to be configured as the default route. If this parameter is not configured, the device does not allow the route to the source IP address of the packet to be configured as the default route during the URPF check.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Denial of Service (DoS) attack disables users from connecting to a server. DoS attacks aim to occupy many resources by sending a large number of connection requests to a specified server. The attacked server cannot respond to authorized users.

URPF searches for the route to the source IP address in the routing table based on the source IP address of the packet, and checks whether the inbound interface of the packet is the same as the outbound interface of the route. If no route to the source IP address of the packet exists in the routing table, or the inbound interface of the packet is different from the outbound interface of the route, the packet is discarded. This prevents IP spoofing attacks, especially DoS attacks with bogus source IP address.

In a complicated networking environment, asymmetric routes may exist. That is, the routes recorded on the local end and remote end are different. A URPF-enabled device on this network may discard the packets transmitted along the correct path, but forward the packets transmitted along incorrect paths. The device provides the following two URPF modes to solve this problem:

- **Strict mode**

In strict mode, a packet passes the check only when the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet should be the same as the outbound interface of the route.

If route symmetry is ensured, you are advised to use the URPF strict mode. For example, if there is only one path between two network edge devices, URPF strict mode can be used to ensure network security.

- **Loose mode**

  In loose mode, a packet passes the check as long as the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet is not required to be the same as the outbound interface of the route.

  If route symmetry is not ensured, you are advised to use the URPF loose mode. For example, if there are multiple paths between two network edge devices, URPF loose mode can be used to ensure network security and prevent the packets transmitted along the correct path from being discarded.

Prerequisites

For the S5720EI, S6720EI, and S6720S-EI, configurations on the interface take effect only after global URPF is enabled using the **14.13.3 urpf (system view)** command.

Precautions

In the Eth-Trunk interface view, this command conflicts with the **6.10.72 service type tunnel** command; therefore, the two commands cannot be run in the same Eth-Trunk interface view.

For the S6720EI and S6720S-EI, the **allow-default-route** parameter does not take effect when the resource allocation mode is set to **enhanced-ipv4** or **ipv4-ipv6 6:1** using the **3.2.2 assign resource-mode** command.

Example

# Enable URPF strict check on a Layer 2 interface GE0/0/1 and allow the route to the source IP address of the packet to be configured as the default route.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] urpf strict allow-default-route
```

# Enable URPF loose check on a Layer 3 interface GE0/0/2 and allow the route to the source IP address of the packet to be configured as the default route.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] undo portswitch
[HUAWEI-GigabitEthernet0/0/2] urpf loose allow-default-route
```

14.13.3 urpf (system view)

Function

The **urpf** command enables global URPF.

The **undo urpf** command disables global URPF.

By default, the switch does not enable global URPF.

NOTE

S5720HI does not support this command.

Format

For S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI:

urpf [**slot** *slot-id*]

undo urpf [**slot** *slot-id*]

For S5720EI, S6720EI, and S6720S-EI:

urpf slot *slot-id* [**based-logic-port**]

undo urpf slot *slot-id* [**based-logic-port**]

Parameters

Parameter	Description	Value
slot *slot-id*	- Specifies the slot ID if stacking is not configured. - Specifies the stack ID if stacking is configured.	Set the value according to the device configuration.
based-logic-port	- If this parameter is specified, URPF check configured on logical interfaces takes effect, including VLANIF interfaces and subinterfaces, and URPF check configured on Ethernet interfaces does not take effect, including Layer 2 and Layer 3 Ethernet interfaces. - If this parameter is not specified, URPF check configured on Ethernet interfaces takes effect, and URPF check configured on logical interfaces does not take effect.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Denial of Service (DoS) attack disables users from connecting to a server. DoS attacks aim to occupy many resources by sending a large number of connection requests to a specified server. The attacked server cannot respond to authorized users.

URPF searches for the route to the source IP address in the routing table based on the source IP address of the packet, and checks whether the inbound interface of the packet is the same as the outbound interface of the route. If no route to the source IP address of the packet exists in the routing table, or the inbound interface of the packet is different from the outbound interface of the route, the packet is discarded. This prevents IP spoofing attacks, especially DoS attacks with bogus source IP address.

In a complicated networking environment, asymmetric routes may exist. That is, the routes recorded on the local end and remote end are different. A URPF-enabled device on this network may discard the packets transmitted along the correct path, but forward the packets transmitted along incorrect paths. The device provides the following two URPF modes to solve this problem:

- **Strict mode**

  In strict mode, a packet passes the check only when the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet should be the same as the outbound interface of the route.

  If route symmetry is ensured, you are advised to use the URPF strict mode. For example, if there is only one path between two network edge devices, URPF strict mode can be used to ensure network security.

- **Loose mode**

  In loose mode, a packet passes the check as long as the device has a route to the source IP address of the packet in the routing table, and the inbound interface of the packet is not required to be the same as the outbound interface of the route.

  If route symmetry is not ensured, you are advised to use the URPF loose mode. For example, if there are multiple paths between two network edge devices, URPF loose mode can be used to ensure network security and prevent the packets transmitted along the correct path from being discarded.

Precautions

- Enabling or disabling global URPF will affect packet forwarding in a short period of time.
- The URPF check enabled by running the **urpf (system view)** command takes effect only on the master switch in a stack.
- The S5720SI, S5720S-SI, S5730SI, S5730S-EI, S6720SI, and S6720S-SI only support URPF strict check.
- For S5720EI, S6720EI, and S6720S-EI, you are advised to enable URPF before services are deployed. If you need to enable URPF after services are deployed, you can configure when less traffic is transmitted and ensure that the FIB table reduced by a half can meet network requirements.
- If both the **urpf slot** *slot-id* and **urpf slot** *slot-id* **based-logic-port** commands are executed, the last configured one takes effect.

Follow-up Procedure

For S5720EI, S6720EI, and S6720S-EI, run the **14.13.2 urpf (interface view)** command to configure the URPF check function on interfaces.

Example

# Enable global URPF on the device.

```
<HUAWEI> system-view
[HUAWEI] urpf slot 0
Warning: Changing the global URPF status may interrupt some services for several seconds and FIB entries
supported may be reduced. Continue? [Y/N]:y
```

# Change URPF from Ethernet interface-based to logical interface-based.

```
<HUAWEI> system-view
[HUAWEI] urpf slot 0 based-logic-port
Warning: Changing the global URPF status may interrupt some services for several seconds and FIB entries
supported may be reduced. Continue? [Y/N]: y
Warning: The global URPF mode will be changed from physical interface-based to logical interface-based.
The URPF configuration on all Layer 2 or Layer 3 physical interfaces of the card will become invalid. Are
you sure to continue? [Y/N]: y
```

# Change URPF from logical interface-based to Ethernet interface-based.

```
<HUAWEI> system-view
[HUAWEI] urpf slot 0
Warning: Changing the global URPF status may interrupt some services for several seconds and FIB entries
supported may be reduced. Continue? [Y/N]: y
Warning: The global URPF mode will be changed from logical interface-based to physical interface-based.
The URPF configuration on all sub-interfaces or VLANIF interfaces of the card will become invalid. Are you
sure to continue? [Y/N]: y
```

Related Topics

14.13.2 urpf (interface view)

14.14 Keychain Configuration Commands

14.14.1 Command Support

Only the S5720HI, S5720EI, S6720S-EI, and S6720EI support Keychain.

14.14.2 algorithm

Function

The **algorithm** command configures a key authentication algorithm.

The **undo algorithm** command deletes a key authentication algorithm.

By default, no algorithm is configured.

Format

algorithm { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }

undo algorithm

Parameters

Parameter	Description	Value
hmac-md5	Indicates that Keyed-Hashing for Message Authentication-Message Digest 5 (HMAC-MD5) is used for packet encryption and authentication. **NOTE** HMAC-MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
hmac-sha-256	Indicates that HMAC-Secure Hash Algorithm 256 (SHA-256) is used for packet encryption and authentication.	-
hmac-sha1-12	Indicates that HMAC-Secure Hash Algorithm 1-12 (SHA1-12) is used for packet encryption and authentication.	-
hmac-sha1-20	Indicates that HMAC-SHA1-20 is used for packet encryption and authentication.	-

Parameter	Description	Value
md5	Indicates that MD5 is used for packet encryption and authentication. **NOTE** MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
sha-1	Indicates that SHA-1 is used for packet encryption and authentication. **NOTE** To ensure high security, do not use the SHA-1 algorithm.	-
sha-256	Indicates that SHA-256 is used for packet encryption and authentication.	-
simple	Indicates that the configured key is used for packet authentication. **NOTE** The authentication algorithm specified by **simple** is not secure. HMAC-SHA-256 or SHA-256 is recommended.	-

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. A keychain consists of multiple keys, each of which needs to be configured with an authentication algorithm. Different keys are valid within different time periods, ensuring dynamic change of keychain authentication algorithms.

Packets are authenticated and encrypted based on the authentication algorithm and key string associated with a specified key. This improves the packet transmission security.

The characteristics of each authentication algorithm are as follows:

- MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length.
- SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.
- SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code.

The calculation speed of the MD5 algorithm is faster than that of the SHA algorithm; the SHA algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA, HMAC is more secure, but slower in calculation speed. MD5 or SHA-1 algorithm has a low security level, so they are not recommended.

Simple authentication is insecure. Therefore, changing it to another algorithm is recommended.

Prerequisites

key-id has been configured.

Precautions

Keys configured on the sender and receiver of packets must correspond to the same authentication and encryption algorithms. Otherwise, packet transmission fails for not passing the authentication.

If algorithm is not configured, key will never be active.

Different protocols support different algorithms.

- RIP supports MD5 and simple.

- BGP and BGP4+ support MD5.
- IS-IS supports HMAC-MD5 and simple.
- OSPF supports MD5, simple and HMAC-MD5.
- MSDP supports MD5.
- MPLS LDP supports MD5. MPLS TE supports HMAC-MD5.

Example

# Configure algorithm sha-256 on key-id 1.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
[HUAWEI-keychain-huawei] key-id 1
[HUAWEI-keychain-huawei-keyid-1] algorithm sha-256
```

Related Topics

14.14.6 key-id

14.14.7 key-string

14.14.3 default send-key-id

Function

The **default send-key-id** command configures a particular key as the default send key for that keychain.

The **undo default send-key-id** command deletes default send key.

By default, no key is configured as default send key.

Format

default send-key-id

undo default send-key-id

Parameters

None

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key-sting dynamically. This can reduce the workload of changing the algorithm and key manually. A keychain consists of multiple authentication keys, each of which is valid within different time periods. When a key becomes valid, the authentication algorithm corresponding to the key is used, and packets passing the authentication will be sent or received.

If a key for packet sending is not configured in a keychain or no key for packet sending is valid within a certain period, protocol packets cannot be authenticated and encrypted. As a result, protocol packet transmission fails. To address such a problem, configure a default key for packet sending. If no key is valid, the default key for packet sending is used.

Precautions

Each keychain can have only one default key for packet sending.

- If the default key for packet sending is an existing key, the authentication and encryption algorithms, and key corresponding to the key are used.
- If the default key for packet sending is a newly created key, configure the authentication and encryption algorithms.

Example

# Configure the key-1 as default send key in keychain huawei.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
[HUAWEI-keychain-huawei] key-id 1
[HUAWEI-keychain-huawei-keyid-1] default send-key-id
```

Related Topics

14.14.6 key-id

14.14.4 display keychain

Function

The **display keychain** command displays the configuration of a specified keychain.

Format

display keychain *keychain-name* [**key-id** *key-id*]

Parameters

Parameter	Description	Value
keychain-name	Displays the configuration of a keychain with a specified name.	The keychain must already exist.
key-id *key-id*	Displays the configuration of a specified key in the keychain.	The key must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To troubleshoot a keychain authentication failure or collect required information before configuration, run the **display keychain** command to view configurations of a specified keychain.

Example

# Display the configuration of keychain **huawei** when no key ID is configured for the keychain.

```
<HUAWEI> display keychain huawei
 Keychain Information:
 ---------------------
 Keychain Name             : huawei
   Timer Mode              : Absolute
   Time Type               : Lmt
   Receive Tolerance(min)  : 0
   TCP Kind                : 254
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     HMAC-SHA-256          : 7
     SHA-256               : 8
     MD5                   : 3
     SHA1                  : 4
 Number of Key IDs         : 0
 Active Send Key ID        : None
 Active Receive Key IDs    : None
 Default send Key ID       : Not configured
```

# Display the configuration of keychain **huawei** when a key ID is configured for the keychain.

```
<HUAWEI> display keychain huawei
 Keychain Information:
 ---------------------
 Keychain Name             : huawei
   Timer Mode              : Absolute
   Time Type               : Lmt
   Receive Tolerance(min)  : 100
   TCP Kind                : 182
   TCP Algorithm IDs       :
     HMAC-MD5              : 5
     HMAC-SHA1-12          : 2
     HMAC-SHA1-20          : 6
     HMAC-SHA-256          : 7
     SHA-256               : 8
     MD5                   : 3
     SHA1                  : 4
 Number of Key IDs         : 1
 Active Send Key ID        : 1
 Active Receive Key IDs    : 01
 Default send Key ID       : 1
```

```
Key ID Information:
-------------------
Key ID                 : 1
  Key string             : ******
  Algorithm              : MD5
  SEND TIMER             :
    Start time           : 2012-03-14 00:00
    End time             : 2012-08-08 23:59
    Status             : Active
  RECEIVE TIMER          :
    Start time           : 2012-03-14 00:00
    End time             : 2012-08-08 23:59
    Status             : Active

Key ID                 : 2
  Key string             : -
  Algorithm              : -
  SEND TIMER             :
    Status             : Inactive
  RECEIVE TIMER          :
    Status             : Inactive
```

# Display the configuration of key-id 1 in the keychain **huawei**.

```
<HUAWEI> display keychain huawei key-id 1
 Keychain Information:
 ---------------------
 Keychain Name            : huawei
   Timer Mode             : Absolute
   Time Type              : Lmt
   Receive Tolerance(min)  : 100
   TCP Kind               : 182
   TCP Algorithm IDs      :
     HMAC-MD5             : 5
     HMAC-SHA1-12         : 2
     HMAC-SHA1-20         : 6
     HMAC-SHA-256         : 7
     SHA-256              : 8
     MD5                  : 3
     SHA1                 : 4

 Key ID Information:
 -------------------
 Key ID                 : 1
   Key string             : ******
   Algorithm              : MD5
   SEND TIMER             :
     Start time           : 2012-03-14 00:00
     End time             : 2012-08-08 23:59
     Status             : Active
   RECEIVE TIMER          :
     Start time           : 2012-03-14 00:00
     End time             : 2012-08-08 23:59
     Status             : Active
   DEFAULT SEND KEY ID INFORMATION
     Default              : Configured
     Status             : Inactive
```

Table 14-73 Description of the display keychain command output

Item	Description
Keychain Name	Name of a keychain. To set the keychain name, run the **keychain** command.

Item	Description
Timer Mode	Time mode of a keychain. - Absolute: The keychain takes effect in an absolute time range. - Daily periodic: The keychain is valid on a daily basis. - Weekly periodic: The keychain is valid on a weekly basis. - Monthly periodic: The keychain is valid on a monthly basis. - Yearly periodic: The keychain is valid on a yearly basis. To set the time mode, run the **keychain** command.
Time Type	Specifies the timing type of the keychain.
Receive Tolerance(min)	Receive tolerance time configured for a keychain. To set the receive tolerance time, run the **receive-tolerance** command.
TCP Kind	TCP kind value configured for a keychain. To set the TCP kind value, run the **tcp-kind** command.

Item	Description
TCP Algorithm IDs	TCP algorithm ID configured for a keychain. The characteristics of each authentication algorithm are as follows: ● MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length. ● SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message. ● HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. ● HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. ● SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code. The calculation speed of the MD5 algorithm is faster than that of the SHA algorithm; the SHA algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA, HMAC is more secure, but slower in calculation speed. MD5 or SHA-1 algorithm has a low security level, so they are not recommended. To set the TCP algorithm ID, run the **tcp-algorithm-id** command.

Item	Description
Number of Key IDs	Number of key IDs.
Active Send Key ID	ID of the active send key.
Active Receive Key IDs	ID of the active receive key.
Default send Key ID	ID of the default send key.
Key ID	Key configured in a keychain. To set the key ID, run the **key-id** command.
Key string	Key string configured for the key. To set the key string, run the **key-string** command.

Item	Description
Algorithm	Algorithm configured for the key. To set the algorithm for a key, run the **algorithm** command. The characteristics of each authentication algorithm are as follows: ● MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length. ● SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message. ● HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. ● HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. ● SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code. The calculation speed of the MD5 algorithm is faster than that of the SHA algorithm; the SHA algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA, HMAC is more secure, but slower in calculation speed. MD5 or SHA-1 algorithm has a low security level, so they are not recommended.

Item	Description
SEND TIMER	Send time of a key. To set the send time of a key, run the **send-time** command.
Start time	Time when a key becomes valid.
End time	Time when a key becomes invalid.
Status	Status of send/receive keys: ● Active ● Inactive
RECEIVE TIMER	Receive time of a key. To set the receive time of a key, run the **receive-time** command.
DEFAULT SEND KEY ID INFORMATION	Information about the default send key.
Default	Configuration of the default send key: ● Not configured ● Configured
Status	Status of the default send key: ● Active ● Inactive

14.14.5 keychain

Function

The **keychain** command creates a new set of keychain rules or displays the keychain view.

The **undo keychain** command deletes the keychain configuration.

By default, no keychain is configured.

Format

keychain *keychain-name* [**mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } }]

undo keychain *keychain-name*

Parameters

Parameter	Description	Value
keychain-name	Specifies the keychain name. All the applications identify the set of keychain rules by keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
mode	Indicates the time mode of a keychain. **NOTE** ● The time mode of a keychain must be specified when a keychain is created. ● You do not need to specify the time mode for a created keychain.	-
absolute	Indicates that the given keychain is non-periodic.	-
periodic	Indicates that the given keychain is periodic.	-
daily	Indicates that the given keychain is day-periodic.	-
weekly	Indicates that the given keychain is week-periodic.	-
monthly	Indicates that the given keychain is month-periodic.	-
yearly	Indicates that the given keychain is year-periodic.	-

Views

System view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

There are two keychain time modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

Follow-up Procedure

Run the **key-id** command to configure a key. If the key is not configured, the keychain cannot authenticate and encrypt protocol packets.

The time mode of a key must be the same as the time mode of the keychain.

Precautions

A keychain supports a maximum of 64 keys.

The **keychain** *keychain-name* command displays a specific keychain view. If the keychain specified by *keychain-name* does not exist, the **keychain** *keychain-name* command cannot be executed. To create a keychain, run the **keychain** *keychain-name* **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } } command.

Example

# Configure the keychain **huawei** and enter keychain view.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
[HUAWEI-keychain-huawei]
```

Related Topics

14.14.6 key-id

14.14.6 key-id

Function

The **key-id** command creates a new set of key-ids or displays the key-id view.

The **undo key-id** command deletes the key-id configuration.

By default, no key-id is configured.

Format

key-id *key-id*

undo key-id *key-id*

Parameters

Parameter	Description	Value
key-id	Specifies the key identification number of a keychain.	The integer value ranges from 0 to 63.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key dynamically. This can reduce the workload of manually changing the algorithm and key.

The dynamic change of the keychain authentication algorithm is implemented based on the keys. Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Follow-up Procedure

After key-id is specified, perform the following operations:

- Run the **algorithm** command to configure an algorithm used by the key.
- Run the **key-string** command to specify a key string.
- Run the **send-time** command to specify the send time of the key.
- Run the **receive-time** command to specify the receive time of the key.

Precautions

A **key-id** represents a key on the device.

A keychain supports 64 keys, but only one key takes effect during one period.

No active key can be used to authenticate and encrypt protocol packets at the intervals of keys. Therefore, run the **default send-key-id** command to specify a default key.

The time mode of the key must be the same as the time mode of Keychain.

Example

# Configure key-id 1.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
```

```
[HUAWEI-keychain-huawei] key-id 1
[HUAWEI-keychain-huawei-keyid-1]
```

Related Topics

14.14.7 key-string

14.14.2 algorithm

14.14.10 send-time

14.14.8 receive-time

14.14.7 key-string

Function

The **key-string** command specifies a key used for keychain authentication.

The **undo key-string** command deletes a key used for keychain authentication.

By default, no key is configured for keychain authentication.

Format

key-string { **plain** *plain-text* | [**cipher**] *cipher-text* }

undo key-string

Parameters

Parameter	Description	Value
plain *plain-text*	Indicates the plain text used for authentication. The configured text will be stored as unencrypted text and displayed as unencrypted text. **NOTE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is case-sensitive and ranges from 1 to 255 characters. Spaces are not supported. If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.
cipher	Specifies the cipher key string used for encryption and decryption.	-

Parameter	Description	Value
cipher-text	Indicates the cipher text used for authentication.	The value is a string of case-sensitive characters that can be letters or digits. The authentication password can be a string of 1 to 255 characters in plaintext or a string of 20 to 392 characters in ciphertext. If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Precautions

An authentication key configured in cipher text mode will be also displayed in cipher text mode. Therefore, remember the plaintext key string when configuring the key in cipher text mode.

If the authentication key is not configured, the corresponding key remains in inactive state.

Example

# Configure the key string **Huawei@1234**.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
[HUAWEI-keychain-huawei] key-id 1
[HUAWEI-keychain-huawei-keyid-1] key-string cipher Huawei@1234
```

Related Topics

14.14.6 key-id

14.14.2 algorithm

14.14.8 receive-time

Function

The **receive-time** command configures a key as a receive key for the specified interval of time.

The **undo receive-time** command deletes the receive time configuration.

By default, no receive time is configured.

Format

receive-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

receive-time daily *start-time* **to** *end-time*

receive-time day { *start-day-name* **to** *end-day-name* | *day-name* &<1-7> }

receive-time date { *start-date-value* **to** *end-date-value* | *date-value* &<1-31> }

receive-time month { *start-month-name* **to** *end-month-name* | *month-name* &<1-12> }

undo receive-time

Parameters

Parameter	Description	Value
start-time	Specifies the start receive time.	In HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specifies the start date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the receive time in minutes.	The value ranges from 1 to 26280000.
infinite	Indicates that the key will be acting as an active receive key forever from the configured start time.	-
to	Indicates a separator.	-

Parameter	Description	Value
end-time	Specifies the end receive time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start start.
end-date	Specifies the end date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily receive time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end receive day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end receive date of the month.	The value ranges from 2 to 31. The end date must be later than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-

Parameter	Description	Value
start-month-name	Specifies the month of the year to be configured as the start receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
end-month-name	Specifies the end receive month. The end month must be greater than the start month.	The end month must be later than the start month. It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
month-name &<1-12>	Specifies the month of the year to be configured as the receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different keys for packet sending and receiving to be valid within different time periods.

When the system time is within the specified interval, the receive key is in active state.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which receive keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys can be active at the same time. The device will select a key for decryption based on the received packet.

Example

# Configure the time for packet receiving with the timing mode as absolute and range as infinite.

```
<HUAWEI> system-view
[HUAWEI] keychain one mode absolute
[HUAWEI-keychain-one] key-id 5
[HUAWEI-keychain-one-keyid-5] receive-time 14:52 2014-11-1 duration infinite
```

# Configure the time for packet receiving with the timing mode as absolute.

```
<HUAWEI> system-view
[HUAWEI] keychain two mode absolute
[HUAWEI-keychain-two] key-id 5
[HUAWEI-keychain-two-keyid-5] receive-time 14:52 2014-11-1 to 14:52 2040-10-1
```

# Configure the time for packet receiving with the timing mode as daily periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain three mode periodic daily
[HUAWEI-keychain-three] key-id 5
[HUAWEI-keychain-three-keyid-5] receive-time daily 14:52 to 18:10
```

# Configure the time for packet receiving with the timing mode as weekly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain four mode periodic weekly
[HUAWEI-keychain-four] key-id 5
[HUAWEI-keychain-four-keyid-5] receive-time day mon
```

# Configure the time for packet receiving with the timing mode as monthly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain five mode periodic monthly
[HUAWEI-keychain-five] key-id 5
[HUAWEI-keychain-five-keyid-5] receive-time date 12 to 25
```

# Configure the time for packet receiving with the timing mode as yearly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain six mode periodic yearly
[HUAWEI-keychain-six] key-id 5
[HUAWEI-keychain-six-keyid-5] receive-time month oct to dec
```

Related Topics

14.14.10 send-time

14.14.9 receive-tolerance

Function

The **receive-tolerance** command sets receive tolerance for all the receive keys in the keychain.

The **undo receive-tolerance** command deletes the receive tolerance configuration.

By default, no receive tolerance is configured.

Format

receive-tolerance { *value* | **infinite** }

undo receive-tolerance

Parameters

Parameter	Description	Value
value	Specifies the receive tolerance value for a keychain.	The integer value ranges from 1 to 14400 in minutes.
infinite	Indicates that the receive tolerance is infinite. That is, the receive key is always valid.	-

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key string dynamically. Each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm is used.

Due to the networking environment or clock asynchronization on the packet sender and receiver, packets may be delayed. The receiver may receive a packet sent from the sender after its key for packet receiving becomes invalid. As a result, the receiver discards the packet and packet transmission is interrupted. To address this problem, set a tolerance time to ensure that the validity period of the receive key on the receiver expires after all packets sent from the sender reach the receiver.

Implementation Procedure

After a tolerance time is set, the tolerance time is added to the start time and end time when the key ID for packet receiving becomes valid.

Precautions

A tolerance time is required for each keychain. The configured tolerance time takes effect for all keys in the keychain.

Example

# Configure the receive tolerance time as 570 minutes.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
[HUAWEI-keychain-huawei] receive-tolerance 570
```

14.14.10 send-time

Function

The **send-time** command configures a key as a send key at a specified interval.

The **undo send-time** command deletes the send time configuration.

By default, no send-time is configured.

Format

send-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

send-time daily *start-time* **to** *end-time*

send-time day { *start-day-name* **to** *end-day-name* | *day-name* &<1-7> }

send-time date { *start-date-value* **to** *end-date-value* | *date-value* &<1-31> }

send-time month { *start-month-name* **to** *end-month-name* | *month-name* &<1-12> }

undo send-time

Parameters

Parameter	Description	Value
start-time	Specifies the start send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specify the start date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the send time, in minutes.	The value ranges from 1 to 26280000.
infinite	Indicates that the key will act as a send key forever from the configured start time.	-
to	Indicates a separator.	-

Parameter	Description	Value
end-time	Specifies the end send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start time.
end-date	Specifies the end date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily send time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end send day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end date of the month to be configured as the send date for the given key.	the The value ranges from 2 to 31. The end date must be greater than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-

Parameter	Description	Value
start-month-name	Specifies the month of the year to be configured as the start send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
end-month-name	Specifies the end send month. The end month must be greater than the start month.	It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. The end month must be later than the start month.
month-name &<1-12>	Specifies the month of the year to be configured as the send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different send and receive keys to be valid within different time periods.

When the system is within the send time range of the key, the device will use the algorithm and key of the configured key to encrypt the packet.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which send keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys can not be active at the same time. Only one key takes effect during a period in a keychain.

Example

# Configure the time for packet sending with the timing mode as absolute.

```
<HUAWEI> system-view
[HUAWEI] keychain one mode absolute
[HUAWEI-keychain-one] key-id 5
[HUAWEI-keychain-one-keyid-5] send-time 14:52 2014-11-1 to 14:52 2040-10-1
```

# Configure the time for packet sending with the timing mode as daily periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain two mode periodic daily
[HUAWEI-keychain-two] key-id 5
[HUAWEI-keychain-two-keyid-5] send-time daily 14:52 to 18:10
```

# Configure the time for packet sending with the timing mode as weekly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain three mode periodic weekly
[HUAWEI-keychain-three] key-id 5
[HUAWEI-keychain-three-keyid-5] send-time day mon
```

# Configure the time for packet sending with the timing mode as monthly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain four mode periodic monthly
[HUAWEI-keychain-four] key-id 5
[HUAWEI-keychain-four-keyid-5] send-time date 12
```

# Configure the time for packet sending with the timing mode as yearly periodic.

```
<HUAWEI> system-view
[HUAWEI] keychain five mode periodic yearly
[HUAWEI-keychain-five] key-id 5
[HUAWEI-keychain-five-keyid-5] send-time month apr
```

# Configure the time for packet sending with the timing mode as yearly periodic, and a few months are available.

```
<HUAWEI> system-view
[HUAWEI] keychain six mode periodic yearly
[HUAWEI-keychain-six] key-id 5
[HUAWEI-keychain-six-keyid-5] send-time month oct to dec
```

Related Topics

14.14.8 receive-time

14.14.11 tcp-algorithm-id

Function

The **tcp-algorithm-id** command specifies a TCP algorithm ID to represent an algorithm supported by the keychain.

The **undo tcp-algorithm-id** command restores the default settings.

By default, mapping between the TCP algorithm and algorithm ID supported by IANA is used.

Format

tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** } *algorithm-id*

undo tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** }

Parameters

Parameter	Description	Value
hmac-md5	Specifies that message authentication algorithm used is HMAC-MD5. **NOTE** HMAC-MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
hmac-sha-256	Specifies that message authentication algorithm used is HMAC-SHA-256.	-
hmac-sha1-12	Specifies that message authentication algorithm used is HMAC-SHA1-12.	-
hmac-sha1-20	Specifies that message authentication algorithm used is HMAC-SHA1-20.	-
md5	Specifies that message authentication algorithm used is MD5. **NOTE** MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
sha-1	Specifies that message authentication algorithm used is SHA-1. **NOTE** To ensure high security, do not use the SHA-1 algorithm.	-
sha-256	Specifies that message authentication algorithm used is SHA-256.	-
algorithm-id	Specifies the TCP algorithm ID to represent the algorithm.	The value ranges from 1 to 63. Default algorithm id for algorithm types are: **md5** is 3, **hmac-sha-256** is 7, **sha-1** is 4, **hmac-md5** is 5, **hmac-sha1-12** is 2, **hmac-sha1-20** is 6 and **sha-256** is 8.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

The TCP connection is authenticated using the authentication algorithm specified by the algorithm ID. The algorithm ID is not defined by IANA. Different vendors use different algorithm IDs to identify authentication algorithms. When two devices of different vendors are connected, ensure that algorithm IDs configured on the two devices are the same.

The characteristics of each authentication algorithm are as follows:

- MD5(Message Digest 5): The 128-bit MD5 message digest is calculated based on the entered message of any length.
- SHA-1(Secure Hash Algorithm): The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5(Keyed-Hashing for Message Authentication-md5): The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.
- SHA-256: The 256-bit SHA-2 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-SHA-256: The 256-bit HMAC-SHA-256 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 256 bits are used as the authentication code.

The calculation speed of the MD5 algorithm is faster than that of the SHA algorithm; the SHA algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA, HMAC is more secure, but slower in calculation speed. MD5 or SHA-1 algorithm has a low security level, so they are not recommended.

Prerequisites

Before configuring algorithm IDs for the communicating parties, run the **tcp-kind** command to configure TCP types for the communicating parties.

Precautions

Each algorithm has a unique algorithm ID. And the algorithm IDs configured for the two communication devices must be identical.

Example

# Configure the TCP algorithm ID of **hmac-sha-256** as 1.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
[HUAWEI-keychain-huawei] tcp-algorithm-id hmac-sha-256 1
```

Related Topics

14.14.12 tcp-kind

14.14.12 tcp-kind

Function

The **tcp-kind** command specifies the option type in the TCP enhanced authentication option.

The **undo tcp-kind** command restores the default TCP kind value.

By default, the default kind value is 254.

Format

tcp-kind *kind-value*

undo tcp-kind

Parameters

Parameter	Description	Value
kind-value	Specifies the TCP kind value to be used for that keychain.	The value ranges from 28 to 255.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

TCP connection request packets carry enhanced authentication options and are authenticated by a specified authentication algorithm. Different vendors use different kind values to specify the enhanced authentication option. Kind values configured for the communicating parties must be the same.

Follow-up Procedure

After configuring the same TCP kind value for the communicating parties, run the **tcp-algorithm-id** command to specify TCP algorithm IDs for the communicating parties.

Precautions

Communicating parties using the keychain authentication must establish a TCP connection when configuring the kind value. Otherwise, the TCP authentication does not take effect.

If TCP connection request packets carry enhanced authentication options, the kind value must be specified in the packets.

Example

# Configure the TCP kind value as 252 for the keychain **huawei**.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei mode absolute
[HUAWEI-keychain-huawei] tcp-kind 252
```

Related Topics

14.14.5 keychain

14.14.11 tcp-algorithm-id

14.14.13 time mode

Function

The **time mode** command configures the time mode for Keychain.

The **undo time mode** command restores the default time mode for Keychain.

By default, the time mode of Keychain is Local Mean Time (LMT).

Format

time mode { **utc** | **lmt** }

undo time mode

Parameters

Parameter	Description	Value
utc	Specifies that the configured time is in Universal Time Coordinated (UTC) format.	-
lmt	Specifies that the configured time is in LMT format.	-

Views

Keychain view

Default Level

2: Configuration level

Usage Guidelines

Each keychain consists of multiple key IDs that are valid within different time periods and each key ID is configured with an authentication algorithm. When a key ID becomes valid, the corresponding authentication algorithm is used, ensuring the dynamic change of authentication algorithms. Configure different key IDs for packet sending and receiving to be valid within different time periods.

To configure the time mode for Keychain, run the **time mode** command. You can configure UTC or LMT for Keychain based on the network planning. Ensure that the time mode remains the same on the entire network.

Example

# Configure the time mode for Keychain as UTC.

```
<HUAWEI> system-view
[HUAWEI] keychain huawei1 mode absolute
[HUAWEI-keychain-huawei1] time mode utc
```

Related Topics

14.14.5 keychain

14.15 MPAC Configuration Commands

14.15.1 Command Support

Only the S5720EI, S5720HI, S6720EI, and S6720S-EI support MPAC.

14.15.2 description (MPAC policy)

Function

The **description** command configures the description for an MPAC policy.

The **undo description** command deletes the description of an MPAC policy.

By default, an MPAC policy does not have a description.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an MPAC policy.	The value is a string of 1 to 255 case-sensitive characters with spaces supported.

Views

MPAC policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure description for a created MPAC policy, use the **description** command. The descriptions facilitate MPAC policy management on the device.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Example

# Configure a description for an MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 huawei
[HUAWEI-service-sec-huawei] description SwitchA-GE0/0/1 to SwitchB-GE0/0/1
```

Related Topics

14.15.10 service-security policy

14.15.3 display service-security binding

Function

The **display service-security binding** command displays the MPAC policies bound to an interface or bound globally.

Format

display service-security binding { **ipv4** | **ipv6** } [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
ipv4	Indicates the IPv4 MPAC policy.	-
ipv6	Indicates the IPv6 MPAC policy.	-
interface *interface-type interface-number*	Indicates the interface to which MPAC policies are bound.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check information about bound MPAC policies, run this command.

The **display service-security binding** { **ipv4** | **ipv6** } command displays all MPAC policies bound to interfaces and bound globally.

The **display service-security binding** { **ipv4** | **ipv6** } **interface** *interface-type interface-number* command displays the MPAC policies bound to a specified interface.

Example

# Display all IPv4 MPAC policies bound on the device.

```
<HUAWEI> display service-security binding ipv4
Configured  : Global
Policy Name : huawei

Interface  : GigabitEthernet0/0/1
Policy Name: A1

Interface  : Eth-Trunk1
Policy Name: A2
```

# Display the IPv4 MPAC policies bound to GE0/0/1.

```
<HUAWEI> display service-security binding ipv4 interface GigabitEthernet 0/0/1
Interface  : GigabitEthernet0/0/1
Policy Name: A1
```

Table 14-74 Description of the display service-security binding command output

Item	Description
Configured	The MPAC policy bound globally. This field has a fixed value of **Global**. If no MPAC policy is bound globally, this field is not displayed.
Interface	Interface to which MPAC policies are bound.
Policy Name	Name of an MPAC policy.

Related Topics

14.15.7 rule (MPAC policy)

14.15.10 service-security policy

14.15.8 service-security binding

14.15.9 service-security global-binding

14.15.4 display service-security policy

Function

The **display service-security policy** command displays MPAC policy configurations.

Format

display service-security policy { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Displays the specified IPv4 MPAC policy.	-
ipv6	Displays the specified IPv6 MPAC policy.	-
security-policy-name	Specifies the name of an MPAC policy to be displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An MPAC policy protects device security by controlling the packets destined for the CPUs.

To check the MPAC rules, step, and description configured on a device, run the **display service-security policy** command.

Example

# Display all IPv4 MPAC policy configurations on a device.

```
<HUAWEI> display service-security policy ipv4
Policy Name : A1
Step        : 5

Policy Name : huawei
Description : RouterA-GE1/0/1 to ROUTERB-GE1/0/1
Step        : 5
 rule 5 permit protocol udp source-port 3503
```

# Display the configuration of the IPv4 MPAC policy **huawei**.

```
<HUAWEI> display service-security policy ipv4 huawei
Policy Name : huawei
Step        : 5
 rule 5 permit protocol tcp source-ip 127.1.1.1 0 source-port 1000
 rule 10 permit protocol ip source-ip 10.10.1.0 0.0.0.255
```

Table 14-75 Description of the display service-security policy command output

Item	Description
Policy Name	Name of an MPAC policy.

Item	Description
Description	Description of an MPAC policy.
Step	Step between two MPAC rule IDs.
rule	MPAC rules.

Related Topics

14.15.7 rule (MPAC policy)

14.15.10 service-security policy

14.15.8 service-security binding

14.15.9 service-security global-binding

14.15.5 display service-security statistics

Function

The **display service-security statistics** command displaysstatistics about matched rules in MPAC policies.

Format

display service-security statistics { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Displays statistics about matched rules in IPv4 MPAC policy.	-
ipv6	Displays statistics about matched rules in IPv6 MPAC policy.	-
security-policy-name	Indicates the name of an MPAC policy.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An MPAC policy protects device security by controlling the packets destined for the CPUs.

The **display service-security statistics** command displays MPAC policy information and how many times MPAC rules are matched.

Example

# Display statistics about matched rules in all IPv4 MPAC policies.

```
<HUAWEI> display service-security statistics ipv4
Policy Name : A1
Step        : 5

Policy Name : beijing
Description : mpac policy for ipv4
Step        : 2
 rule 2 permit protocol any (0 times matched)
 rule 4 deny protocol any (0 times matched)
 rule 6 permit protocol bgp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (1 times matched)
 rule 12 permit protocol ftp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 14 permit protocol ip source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 16 permit protocol ldp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 20 permit protocol ntp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 22 permit protocol ospf source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 24 permit protocol rip source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 26 permit protocol rsvp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 28 permit protocol snmp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 30 permit protocol ssh source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 32 permit protocol tcp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 34 permit protocol telnet source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)
 rule 36 permit protocol tftp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0times matched)
 rule 38 permit protocol udp source-ip 10.1.1.1 0 destination-ip 10.1.1.2 0 (0 times matched)

Policy Name : huawei
Step        : 5
 rule 5 permit protocol tcp source-ip 127.1.1.1 0 source-port 1000 (10 times matched)
 rule 10 permit protocol ip source-ip 10.10.1.0 0.0.0.255 (1 times matched)
```

# Display statistics about matched rules in the IPv4 MPAC policy named **huawei**.

```
<HUAWEI> display service-security statistics ipv4 huawei
Policy Name : huawei
Step        : 5
 rule 5 permit protocol tcp source-ip 127.1.1.1 0 source-port 1000 (10 times matched)
 rule 10 permit protocol ip source-ip 10.10.1.0 0.0.0.255 (1 times matched)
```

Table 14-76 Description of the display service-security statistics command output

Item	Description
Policy Name	Name of an MPAC policy.
Description	Description of an MPAC policy.
Step	Step between two MPAC rule IDs.
rule	MPAC rules.
(0 times matched)	Number of times the MPAC rules are matched.

Related Topics

14.15.7 rule (MPAC policy)

14.15.10 service-security policy

14.15.8 service-security binding

14.15.9 service-security global-binding

14.15.6 reset service-security counters

Function

The **reset service-security counters** command deletes MPAC policy statistics.

Format

reset service-security counters { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Deletes IPv4 MPAC policy statistics.	-
ipv6	Deletes IPv6 MPAC policy statistics.	-
security-policy-name	Specifies the name of an MPAC policy to be deleted.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If excess MPAC policy statistics are generated on a device and you want to view new MPAC information, run the **reset service-security counters** to delete the existing statistics first.

With the *security-policy-name* parameter specified, you can delete statistics about the specified IPv4 or IPv6 MPAC policy. Without the *security-policy-name* parameter specified, you can delete statistics about all IPv4 or IPv6 MPAC policies.

Precautions

All existing MPAC policy statistics will be deleted after this command is executed.

Example

# Delete statistics about the IPv4 MPAC policy **huawei**.

```
<HUAWEI> reset service-security counters ipv4 huawei
```

14.15.7 rule (MPAC policy)

Function

The **rule** command adds a rule to the MPAC policy view.

The **undo rule** command deletes a rule or some configurations from the MPAC policy view.

By default, an MPAC policy does not have a rule.

Format

rule [*rule-id*] { **permit** | **deny** } **protocol** { *protocol-number* | **ftp** | **ssh** | **snmp** | **telnet** | **tftp** | **bgp** | **ldp** | **rsvp** | **ospf** | **rip** | **ntp** | **lsp-ping** | **dhcp-c** | **dhcp-r** | **ip** } [[**source-ip** { *source-ipv4-address* { *source-ipv4-mask* | 0 } | **any** }] | [**destination-ip** { *destination-ipv4-address* { *destination-ipv4-mask* | 0 } | **any** }]] *

rule [*rule-id*] { **permit** | **deny** } **protocol** { **tcp** | *tcp-protocol-number* | **udp** | *udp-protocol-number* } [[**source-port** *source-port-number*] | [**destination-port** *destination-port-number*] | [**source-ip** { *source-ipv4-address* { *source-ipv4-mask* | 0 } | **any** }] | [**destination-ip** { *destination-ipv4-address* { *destination-ipv4-mask* | 0 } | **any** }]] *

rule [*rule-id*] { **deny** | **permit** } **protocol** { **any** | **isis** }

rule [*rule-id*] { **permit** | **deny** } **protocol** { *protocol-number* | **ftp** | **ssh** | **snmp** | **telnet** | **tftp** | **bgp** | **ldp** | **rsvp** | **ospf** | **rip** | **ntp** | **lsp-ping** | **dhcp-c** | **dhcp-r** | **ip** } [[**source-ip** { *source-ipv6-address source-ipv6-prefix-length* | *source-ipv6-address/prefix-length* | **any** }] | [**destination-ip** { *destination-ipv6-address destination-ipv6-prefix-length* | *destination-ipv6-address/prefix-length* | **any** }]] *

rule [*rule-id*] { **permit** | **deny** } **protocol** { **tcp** | *tcp-protocol-number* | **udp** | *udp-protocol-number* } [[**source-port** *source-port-number*] | [**destination-port** *destination-port-number*] | [**source-ip** { *source-ipv6-address source-ipv6-prefix-length* | *source-ipv6-address/prefix-length* | **any** }] | [**destination-ip** { *destination-ipv6-address destination-ipv6-prefix-length* | *destination-ipv6-address/prefix-length* | **any** }]] *

undo rule *rule-id* [**source-ip** | **destination-ip** | **source-port** | **destination-port**] *

Parameters

Parameter	Description	Value
rule-id	Indicates the MPAC rule ID.	The value is an integer that ranges from 0 to 4294967294.
deny	Prevents protocol packets matching the rules from being sent to the CPU.	-
permit	Allows the protocol packets matching the rules to be sent to the CPU.	-
protocol	Specifies the protocol name or number.	-
tcp	Indicates the Transmission Control Protocol (TCP).	-
tcp-protocol-number	Indicates the TCP protocol number.	It has a fixed value of 6.
udp	Indicates the User Datagram Protocol (UDP).	-
udp-protocol-number	Indicates the UDP protocol number.	It has a fixed value of 17.
source-port *source-port-number*	Specifies the source port number of protocol packets.	The value is an integer that ranges from 1 to 65535.
destination-port *destination-port-number*	Specifies the destination port number of protocol packets.	The value is an integer that ranges from 1 to 65535.
protocol-number	Specifies a protocol number.	The value is an integer that ranges from 1 to 255.
ftp	Indicates the File Transfer Protocol (FTP).	-
ssh	Indicates the Secure Shell (SSH) protocol.	-
snmp	Indicates the Simple Network Management Protocol (SNMP).	-

Parameter	Description	Value
telnet	Indicates the Telnet protocol.	-
tftp	Indicates the Trivial File Transfer Protocol (TFTP).	-
bgp	Indicates the Border Gateway Protocol (BGP).	-
ldp	Indicates the Label Distribution Protocol (LDP).	-
rsvp	Indicates the Resource Reservation Protocol (RSVP).	-
ospf	Indicates the Open Shortest Path First (OSPF) protocol.	-
rip	Indicates the Routing Information Protocol (RIP).	-
ntp	Indicates the Network Time Protocol (NTP).	-
lsp-ping	Indicates the Label Switched Path (LSP)-PING protocol.	-
dhcp-c	Indicates the Dynamic Host Configuration Protocol-C (DHCP-C) protocol.	-
dhcp-r	Indicates the DHCP-R protocol.	-
ip	Indicates the Internet Protocol (IP).	-
source-ip	Indicates the source address of protocol packets.	-
source-ipv4-address	Specifies a source IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
source-ipv4-mask | 0	Specifies the mask of the source IPv4 address. The protocol packets from the specified subnet are allowed to be sent to the CPU or discarded. 0 Specifies the source host name. The protocol packets from the specified host are allowed to be sent to the CPU or discarded.	The value is in dotted decimal notation.
destination-ip	Indicates the destination address of protocol packets.	-
destination-ipv4-address	Specifies a destination IPv4 address.	The value is in dotted decimal notation.
destination-ipv4-mask | 0	Specifies the mask of the destination IPv4 address. The protocol packets destined for the specified subnet are allowed to be sent to the CPU or discarded. 0 Specifies the destination host name. The protocol packets destined for the specified host are allowed to be sent to the CPU or discarded.	The value is in dotted decimal notation.
any	Indicates any IP address.	-
isis	Indicates the Intermediate System to Intermediate System (IS-IS) protocol.	-
source-ipv6-address	Specifies a source IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source-ipv6-prefix-length	Specifies the prefix length of a source IPv6 address.	The value is an integer that ranges from 1 to 128.

Parameter	Description	Value
source-ipv6-address/ prefix-length	Specifies the source IPv6 address and prefix length.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X/M. M is an integer that ranges from 1 to 128.
destination-ipv6-address	Specifies a destination IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
destination-ipv6-prefix-length	Specifies the prefix length of a destination IPv6 address.	The value is an integer that ranges from 1 to 128.
destination-ipv6-address/ prefix-length	Specifies the destination IPv6 address and prefix length.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X/M. M is an integer that ranges from 1 to 128.

Views

MPAC policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To match specific users or packets, run the **rule** command with the protocol name or five packet attributes specified.

The MPAC matching rules for TCP/UDP are described in **Table 14-77**.

Table 14-77 Description of the MPAC matching rules for TCP/UDP

Protocol	TCP/UDP	Description
FTP	TCP	The source/destination port number is 21.
SSH	TCP	The source/destination port number is 22.

Protocol	TCP/UDP	Description
Telnet	TCP	The source/destination port number is 23.
BGP	TCP	The source/destination port number is 179.
LDP	TCP/UDP	TCP: The source/destination port number is 646. UDP: The destination port number is 646.
DHCP-R	UDP	IPv4: The destination port number is 67. IPv6: The destination port number is 547.
DHCP-C	UDP	IPv4: The destination port number is 68. IPv6: The destination port number is 546.
NTP	UDP	The destination port number is 123.
SNMP	UDP	The destination port number is 161.
RIP	UDP	IPv4: The destination port number is 520. IPv6: The destination port number is 521.
LSP-PING	UDP	The source/destination port number is 3503.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Precautions

- The MPAC rules configured in the service6-sec policy view do not support ISIS.
- Exercise caution when using the **rule** [*rule-id*] **deny protocol any** command. If this command is executed in the system view, no protocol packets can be sent to the CPU, causing the device to be out of management.
- If a whitelist is configured for an MPAC IPv6 policy, run the **rule permit protocol** *58* command to allow ICMPv6 packets to pass.

Example

# Add a rule to an MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 huawei
```

```
[HUAWEI-service-sec-huawei] rule 5 permit protocol udp source-port 3503 destination-ip 127.0.0.1
255.255.255.255
```

14.15.8 service-security binding

Function

The **service-security binding** command binds an MPAC policy to an interface.

The **undo service-security binding** command unbinds an MPAC policy from an interface.

By default, no MPAC policy is applied to an interface.

Format

service-security binding { **ipv4** | **ipv6** } *security-policy-name*

undo service-security binding { **ipv4** | **ipv6** }

NOTE

The **ipv6** parameter is not supported in the subinterface view.

Parameters

Parameter	Description	Value
ipv4	Binds an IPv4 MPAC policy to an interface.	-
ipv6	Binds an IPv6 MPAC policy to an interface.	-
security-policy-name	Specifies the name of an MPAC policy.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

Ethernet interface view, Ethernet subinterface view, GE interface view, GE subinterface view, XGE interface view, XGE subinterface view, 40GE interface view, 40GE subinterface view, Eth-Trunk interface view, Eth-Trunk subinterface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some attackers may pose as authorized users to send protocol packets to network devices or control these devices. Such attacks affect network running. You can configure MPAC on network devices to allow the specified protocol packets to be sent to the CPUs or discard these packets, improving device security and reliability.

After an MPAC policy is created, run the **service-security binding** command to bind it to interfaces.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Example

# Create an IPv4 MPAC policy and apply it to an interface.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 huawei
[HUAWEI-service-sec-huawei] rule 5 permit protocol tcp source-port 1000 source-ip 127.1.1.1 0
[HUAWEI-service-sec-huawei] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] service-security binding ipv4 huawei
```

# Create an IPv6 MPAC policy and apply it to an interface.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv6 huawei1
[HUAWEI-service6-sec-huawei1] rule 10 deny protocol tcp
[HUAWEI-service6-sec-huawei1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] service-security binding ipv6 huawei1
```

Related Topics

14.15.10 service-security policy

14.15.9 service-security global-binding

Function

The **service-security global-binding** command binds an MPAC policy to a device globally.

The **undo service-security global-binding** command unbinds an MPAC policy from a device.

By default, no MPAC policy is globally applied.

Format

service-security global-binding { **ipv4** | **ipv6** } *security-policy-name*

undo service-security global-binding { **ipv4** | **ipv6** }

Parameters

Parameter	Description	Value
ipv4	Binds an IPv4 MPAC policy to a device globally.	-
ipv6	Binds an IPv6 MPAC policy to a device globally.	-
security-policy-name	Specifies the name of an MPAC policy to be bound.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some attackers may pose as authorized users to send protocol packets to network devices or control these devices. Such attacks affect network running. You can configure MPAC on network devices to allow the specified protocol packets to be sent to the CPUs or discard these packets, improving device security and reliability.

After an MPAC policy is created, run the **service-security global-binding** command to bind it to a device globally.

Prerequisites

An MPAC policy has been created using the **service-security policy** command.

Example

# Create an IPv4 MPAC policy and apply it to a device globally.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 huawei
[HUAWEI-service-sec-huawei] rule 5 permit protocol tcp source-port 1000 source-ip 127.1.1.1 0
[HUAWEI-service-sec-huawei] quit
[HUAWEI] service-security global-binding ipv4 huawei
```

# Create an IPv6 MPAC policy and apply it to a device globally.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv6 huawei1
[HUAWEI-service6-sec-huawei1] rule 10 deny protocol tcp
[HUAWEI-service6-sec-huawei1] quit
[HUAWEI] service-security global-binding ipv6 huawei1
```

Related Topics

14.15.10 service-security policy

14.15.10 service-security policy

Function

The **service-security policy** command creates an MPAC policy and displays its view.

The **undo service-security policy** command deletes an MPAC policy.

By default, no MPAC policy exists on a device.

Format

service-security policy { **ipv4** | **ipv6** } *security-policy-name*

undo service-security policy { **ipv4** | **ipv6** } [*security-policy-name*]

Parameters

Parameter	Description	Value
ipv4	Creates an IPv4 MPAC policy and displays its view.	-
ipv6	Creates an IPv6 MPAC policy and displays its view.	-
security-policy-name	Specifies the name of an MPAC policy.	The value is a string of 1 to 31 case-sensitive characters without spaces. It must start with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Some attackers may pose as authorized users to send protocol packets to network devices or control these devices. Such attacks affect network running. You can configure MPAC on network devices to allow the specified protocol packets to be sent to the CPUs or discard these packets, improving device security and reliability.

Example

# Create an IPv4 MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 huawei
[HUAWEI-service-sec-huawei]
```

# Create an IPv6 MPAC policy.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv6 huawei1
[HUAWEI-service6-sec-huawei1]
```

14.15.11 step (MPAC policy)

Function

The **step** command sets the step between two MPAC rule IDs.

The **undo step** command restores the default step between MPAC rule IDs.

By default, the step between two MPAC rule IDs is 5.

Format

step *step-value*

undo step

Parameters

Parameter	Description	Value
step-value	Specifies the step between two MPAC rule IDs.	The value is an integer that ranges from 1 to 20.

Views

MPAC policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A step is an increment between neighboring MPAC rule IDs automatically allocated by the system. For example, if the step is 5, the system allocates MPAC rules with IDs 5, 10, 15, 20...

To allow insertion of new rules, set a step for MPAC rule IDs by using the **step** command.

Prerequisites

MPAC policies have been created using the **service-security policy** command.

Configuration Impact

After you set a step, all the rule IDs in the MPAC policy are re-arranged using the new step.

Precautions

Setting the step only changes rule IDs, but will not change the rule priorities.

Example

# Set the step for MPAC rule IDs to 10.

```
<HUAWEI> system-view
[HUAWEI] service-security policy ipv4 huawei
[HUAWEI-service-sec-huawei] step 10
```

14.16 Traffic Isolation Between the Service and Management planes Configuration Commands

14.16.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.16.2 management-plane isolate enable

Function

The **management-plane isolate enable** command enables management plane separation.

The **undo management-plane isolate enable** command disables the function.

By default, management plane separation is enabled.

Format

management-plane isolate enable

undo management-plane isolate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **management-plane isolate enable** command enables separation of the management plane to prevent unauthorized users from attacking the management network through the service network. After the command is run, the switch prevents unauthorized users from accessing the management interface through a service interface. That is, if the destination address of a packet received by a service interface is the management interface address, the user cannot access the switch. The access from the management interface to service interface is not restricted.

Precautions

Disabling this function may cause the management network port to be attacked. Therefore, you are advised not to disable this function.

The **management-port isolate enable** and **management-plane isolate enable** command functions are different. The **management-port isolate enable** command isolates traffic between the management and service interfaces by marking the network segment routes with the outbound interfaces being the management interface as the blackhole route, whereas the **management-plane isolate enable** command isolates service interfaces from the management interface by marking the host and broadcast routes with the outbound interfaces being the management interface as the blackhole route.

When a version earlier than V200R005C02 (except V200R005C00SPC500) is upgraded to V200R005C02, a version later than V200R005C02, or V200R005C00SPC500, the **undo management-plane isolate enable** configuration is automatically generated.

Example

# Enables management plane separation.

```
<HUAWEI> system-view
[HUAWEI] management-plane isolate enable
```

14.16.3 management-port isolate enable

Function

The **management-port isolate enable** command isolates management interfaces from service interfaces.

The **undo management-port isolate enable** command disables the function.

By default, management interface separation is enabled.

Format

management-port isolate enable

undo management-port isolate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **management-port isolate enable** command enables separation of the management interface to prevent unauthorized users from attacking the packet forwarding service. After the command is run, the switch forbids packet exchange between the management and service interfaces. That is, the packets received by the management interface will not be sent out through a service interface, and the packets received by a service interface will not be sent out through the management interface.

Precautions

Disabling this function may cause the management network port to be attacked. Therefore, you are advised not to disable this function.

For the S5720HI, when disabling this function, also run the **arp-miss message-cache disable** command to disable the function of packetizing ARP Miss messages. Otherwise, disabling management interface separation cannot take effect. After management interface separation is disabled, the device needs to send ICMP unreachable and redirection packets, which however cannot be sent when the function of packetizing ARP Miss messages is enabled.

The interval between management-port isolate enable and undo management-port isolate enable command must be longer than 30 seconds.

When a version earlier than V200R005C02 (except V200R005C00SPC500) is upgraded to V200R005C02, a version later than V200R005C02, or V200R005C00SPC500, the **undo management-port isolate enable** configuration is automatically generated.

Example

# Isolate management interfaces from service interfaces.

```
<HUAWEI> system-view
[HUAWEI] management-port isolate enable
```

14.17 Security Risk Commands

14.17.1 Command Support

Commands provided in this section and all the parameters in the commands are supported by all switch models by default, unless otherwise specified. For details, see specific commands.

14.17.2 display security risk

Function

The **display security risk** command displays security risks in the system and suggested solutions for the risks.

Format

display security risk [**feature** *feature-name*] [**level** { **high** | **medium** | **low** }]

Parameters

Parameter	Description	Value
feature *feature-name*	Displays security risks of a specified feature.	Enumerated type. The value depends on the registered module.
level high	Displays security risks of High level.	-
level medium	Displays security risks of Medium level.	-
level low	Displays security risks of Low level.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Protocols have different security performances, and some protocols may have security risks. Run the **display security risk** command to identify security risks in the system. Then clear the security risks according to the repair action in the command output. For example, if SNMPv1 is configured, the **display security risk** command output will prompt for the use of SNMPv3.

You can filter the security risks by specifying the security level, feature, or both.

Precautions

The security risks that are displayed vary with user levels. The system administrators can view all security risks in the system. Other users can only view the security risks matching their levels.

Example

# Display security risks in the system.

```
<HUAWEI> display security risk
Risk level       : high
Feature name     : SNMP
Risk information : SNMPv1/SNMPv2c is enabled.
Repair action    : Use SNMPv3.

Risk level       : high
Feature name     : TELNET
Risk information : None authentication is configured for Telnet
users.
Repair action    : Use AAA authentication.

Risk level       : medium
Feature name     : CONSOLE
Risk information : No authentication is configured, password authentication is configured but no password
is specified, or none auth
entication is configured on the console interface.
Repair action    : Use AAA authentication.

Risk level       : medium
Feature name     : SSH
Risk information : SSHv1 is supported.
Repair action    : Close SSHv1.

Risk level       : medium
Feature name     : TELNET
Risk information : The Telnet server function is used.
Repair action    : Use Stelnet.
```

# Display security risks of the TELNET feature.

```
<HUAWEI> display security risk feature telnet
Risk level       : high
Feature name     : TELNET
Risk information : None authentication is configured for Telnet
users.
Repair action    : Use AAA authentication.

Risk level       : medium
Feature name     : TELNET
Risk information : The Telnet server function is used.
Repair action    : Use Stelnet.
```

# Display security risks of Medium level.

```
<HUAWEI> display security risk level medium
Risk level       : medium
Feature name     : CONSOLE
```

```
Risk information : No authentication is configured, password authentication is configured but no password
is specified, or none auth
entication is configured on the console interface.
Repair action    : Use AAA authentication.

Risk level       : medium
Feature name     : SSH
Risk information : SSHv1 is supported.
Repair action    : Close SSHv1.

Risk level       : medium
Feature name     : TELNET
Risk information : The Telnet server function is used.
Repair action    : Use Stelnet.
```

NOTE

The command output provided here is used for reference only. The actual output information depends on the situation.

Table 14-78 Description of the **display security risk** command output

Item	Description
Risk level	Security risk level. It can be any value of the following: ● high; ● medium; ● low.
Feature name	Feature name.
Risk information	Information about the security risks.
Repair action	Suggested solutions for the security risks.

14.18 PKI Configuration Commands

14.18.1 Command Support

Only S5720EI, S5720HI, S6720EI, and S6720S-EI support PKI.

14.18.2 auto-enroll

Function

The **auto-enroll** command enables automatic certificate enrollment and update.

The **undo auto-enroll** command disables automatic certificate enrollment and update.

By default, the automatic certificate enrollment and update are disabled.

Format

auto-enroll [*percent*] [**regenerate** [*key-bit*]] [**updated-effective**]

undo auto-enroll [**updated-effective**]

Parameters

Parameter	Description	Value
percent	Specifies the percentage of the certificate's validity period after which a new certificate is requested automatically.	The value is an integer that ranges from 10 to 100. The default value is 100. When the old certificate expires, the system requests a new certificate.
regenerate	Indicates the RSA key pair will be generated during certificate updates.	-
key-bit	Specifies the number of bits in the RSA key pair generated during certificate updates.	The value is an integer that ranges from 2048 to 4096. The default value is 2048.

Parameter	Description	Value
updated-effective	Indicates that the certificate takes effect immediately after being updated. By default, an updated certificate takes effect only after the old one expires.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Automatic certificate enrollment: When the certificates are unavailable, will expire, or have expired, an entity automatically requests a new certificate or renews the certificate using the Simple Certification Enrollment Protocol (SCEP).

By default, the automatic certificate enrollment and update function is disabled. When a certificate has expired, you must request a certificate for an entity manually. You can still request a certificate for an entity manually when the automatic certificate enrollment and update function is enabled.

Precautions

- If you do not specify **regenerate**, the system uses the original RSA key pairs during automatic updates.
- If you specify **regenerate**, the system generates new RSA key pairs during certificate updates for certificate requests and overwrites the original certificates and RSA key pairs with the new ones.
- After this command is run, the device checks whether the certificate has expired every 60 minutes. If the certificate has expired, the device updates the certificate.

Example

# Enable automatic certificate enrollment and update for the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] auto-enroll 50 regenerate
```

14.18.3 ca id

Function

The **ca id** command specifies a certificate authority (CA) trusted by a PKI realm.

The **undo ca id** command deletes the CA trusted by a PKI realm.

By default, no trusted CA is configured in a PKI realm.

Format

ca id *ca-name*

undo ca id

Parameters

Parameter	Description	Value
ca-name	Specifies the name of a CA trusted by a PKI realm.	The value is a string of 1 to 64 case-insensitive characters.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After the **ca id** command is executed to specify the CA trusted by the device, the CA then requests, obtains, revokes, or queries the device's certificate.

Example

# Specify the CA **root_ca** trusted by the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] ca id root_ca
```

Related Topics

14.18.26 display pki realm

14.18.70 pki realm (system view)

14.18.4 cdp-url

Function

The **cdp-url** command configures the CRL distribution point (CDP) URL.

The **undo cdp-url** command deletes the configured CDP URL.

By default, no CDP URL is configured.

Format

cdp-url [**esc**] *url-addr*

cdp-url from-ca

undo cdp-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-addr	Specifies the CDP URL.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.
from-ca	Specifies that the CDP URL address is obtained from the CA certificate.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity needs to use HTTP to update CRL, it must set up a connection with the HTTP server based on CDP URL, and obtain the CRL from the HTTP server. By default, a PKI entity locates and downloads CRL based on the method (HTTP) in the CDP information of the local certificate. If you do not want to download CRL based on the CDP URL in the local certificate, run this command to configure the PKI entity to obtain CDP URL from the CA certificate or manually configure the CDP URL.

When CRL is automatically updated by SCEP, you can also manually configure a CDP URL address.

Configuration Impact

Manually configuring a CDP URL address overwrites the CDP carried in the certificate. If the certificate does not contain CDP information and no CDP URL address is manually configured, the device requests the CRL from the CA server using SCEP.

Keyword **esc** only supports the URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

# Set the CDP URL to http://10.1.1.1/certenroll/ca_root.crl.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl scep
[HUAWEI-pki-realm-d1] cdp-url http://10.1.1.1/certenroll/ca_root.crl
```

# Set the CDP URL to http://www.***.com/certenroll/ca_root.crl.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl scep
[HUAWEI-pki-realm-d1] cdp-url http://www.***.com/certenroll/ca_root.crl
```

14.18.5 certificate-check

Function

The **certificate-check** command sets the method of checking whether a certificate in the PKI realm is revoked.

The **undo certificate-check** command cancels the method of checking whether a certificate in the PKI realm is revoked.

By default, the system checks using CRLs whether a certificate in the PKI realm is revoked.

Format

certificate-check { { **crl** | **ocsp** } * [**none**] | **none** }

undo certificate-check

NOTE

Only devices in cloud management mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
crl	Sets the check method to Certificate Revocation List (CRL).	-
ocsp	Sets the check method to Online Certificate Status Protocol (OCSP).	-

Parameter	Description	Value
none	Indicates that the system does not check whether a certificate is revoked.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the PKI entity validates the peer certificate, for example, whether the peer certificate has expired and whether it is added to CRL.

The system supports the following methods to check whether a certificate in the PKI realm is revoked:

- CRL
  - If the CA server can function as a CDP, the certificate issued by CA contains the CDP information about obtaining the certificate CRL. The PKI entity then uses the specified method (HTTP) to find the CRL from the specified location and download the CRL. If the CDP URL is configured in the PKI realm, the PKI entity obtains the CRL from the specified URL.
  - If the CA does not support CDPs and no CDP URL is configured on the PKI entity, the PKI entity uses the SCEP protocol to obtain the CRL.
- OCSP

  The PKI entity can use OCSP to check certificate status online, and you do not need to frequently download CRLs.

  When two PKI entities use certificates to perform IPSec negotiation, they check the peer certificate status through OCSP in real time.
- None

  This mode is used when no CRL or OCSP server is available to the PKI entity or the PKI entity does not need to check the peer certificate status. In this mode, the PKI entity does not check whether a certificate has been revoked.

Select the following configurations:

- If the **certificate-check crl** command is configured for a certificate, the CRL mode is used.
- If the **certificate-check ocsp** command is configured for a certificate, the OCSP mode is used.
- If the **certificate-check crl none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the certificate is regarded as valid.

- If the **certificate-check crl ocsp** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check ocsp crl** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check crl ocsp none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp crl none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check none** command is configured for a certificate, the certificate is regarded as valid.

Precautions

After the **certificate-check crl** command is configured, if the device does not have the CRL file, the device fails the certificate verification, and the certificate becomes invalid.

It is not recommended that the none parameter be specified in the**certificate-check** command, because such a configuration poses security risks.

Example

# Set the certificate check method to **crl none** in PKI realm **test**. If the CRL mode is unavailable, the certificate is regarded as valid.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] certificate-check crl none
```

14.18.6 common-name

Function

The **common-name** command configures a common name for an entity.

The **undo common-name** command cancels the configuration.

By default, a PKI entity does not have a common name.

Format

common-name *common-name*

undo common-name

Parameters

Parameter	Description	Value
common-name	Specifies the common name of an entity.	The value is a string of 1 to 64 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

After a PKI entity is created, a common name must be configured to uniquely identify the PKI entity.

After the common name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the common name of the PKI entity.

Example

# Set the common name to **test** for an entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] common-name test
```

Related Topics

14.18.21 display pki entity

14.18.7 country (PKI entity view)

Function

The **country** command configures a country code for an entity.

The **undo country** command deletes the country code of a PKI entity.

By default, no country code is configured for a PKI entity.

Format

country *country-code*

undo country

Parameters

Parameter	Description	Value
country-code	Specifies the country code of a PKI entity.	A country code must be two-character long. If the entered country code contains lower case letters, the system automatically changes the lower case letters into upper case letters when you create a certificate request file. You can query country codes in ISO3166. For example, CN is the legitimate country code of China, and US is the legitimate country code of the USA.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure the country code for the PKI entity, which is used as an alias of the entity.

After the country code is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this country code. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the country code of the PKI entity.

Example

# Configure the country code to CN for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] country CN
```

Related Topics

14.18.21 display pki entity

14.18.8 crl auto-update enable

Function

The **crl auto-update enable** command enables the automatic CRL update function.

The **undo crl auto-update enable** command disables the automatic CRL update function.

By default, automatic CRL update is enabled.

Format

crl auto-update enable

undo crl auto-update enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To configure the automatic CRL update function, enable the function first.

Example

# Enable the automatic certificate update function.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl auto-update enable
```

14.18.9 crl cache

Function

The **crl cache** command configures the device to use the cached CRL.

The **undo crl cache** command configures the device to retrieve the latest CRL each time.

By default, the PKI realm is allowed to use cached CRLs.

Format

crl cache

undo crl cache

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The system overwrites the CRL in memory with the cached URL for certificate verification. If the PKI realm is not allowed to use cached CRL, the system must download the latest CRL every time to overwrite the CRL in memory.

Example

# Allow the device to use the cached CRL in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] crl cache
```

14.18.10 crl http

Function

The **crl http** command enables automatic CRL update using HTTP.

By default, the CRL is updated automatically using HTTP.

Format

crl http

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using HTTP, and ensure that there is sufficient space in the device storage for the CRL file.

Example

# Configure the automatic CRL update using HTTP.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl http
```

14.18.11 crl scep

Function

The **crl scep** command configures a device to use SCEP to automatically update a CRL.

By default, a device uses HTTP to automatically update a CRL.

Format

crl scep

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using SCEP, and ensure that there is sufficient space in the device storage for the CRL file.

Example

# Use SCEP to automatically update a CRL.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl scep
```

14.18.12 crl update-period

Function

The **crl update-period** command sets the interval for automatic CRL update.

The **undo crl update-period** command restores the default interval for automatic CRL update.

By default, the automatic CRL update interval is 8 hours.

Format

crl update-period *interval*

undo crl update-period

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a CRL is automatically updated.	The value is an integer that ranges from 1 to 720, in hours.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The CRL update interval is the interval at which a PKI entity using a certificate downloads a CRL from the CRL storage server. The CA/RA does not issue the CRL to an entity. Instead, the entity initiates CRL query to obtain a CRL.

Example

# Set the interval at which a CRL is automatically updated to 21 hours.

```
<HUAWEI> system-view
[HUAWEI] pki realm d1
[HUAWEI-pki-realm-d1] crl update-period 21
```

14.18.13 display pki ca-capability

Function

The **display pki ca-capability** displays the CA capabilities of a PKI realm.

Format

display pki ca-capability realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Indicates the name of a PKI realm.	The PKI realm name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display pki ca-capability** command displays the CA capabilities of a PKI realm.

Example

# Display the CA capabilities of the PKI realm **asdf**.

```
<HUAWEI> display pki ca-capability realm asdf
 PKI CA Capabilities :
  GetNextCACert      :  ----
  POSTPKIOperation   :  ----
  Renewal            :  ----
  SHA-512            :  ----
  SHA-256            :  ----
  SHA-1              :  ----
  DES3               :  ----
```

Table 14-79 Description of the **display pki ca-capability** command output

Item	Description
PKI CA Capabilities	PKI CA capabilities.
GetNextCACert	Get next CA certificate.
POSTPKIOperation	Post PKI operation messages.
Renewal	Certificate renewal.
SHA-512	SHA-512 algorithm.
SHA-256	SHA-256 algorithm.
SHA-1	SHA-1 algorithm.

Item	Description
DES3	DES3 algorithm.

14.18.14 display pki cert-req

Function

The **display pki cert-req** command displays the content of a certificate request file.

Format

display pki cert-req filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate request file.	The certificate request file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays content of a certificate request file, including the subject, public key algorithm, key modulus, attributes, and signature algorithm.

Example

# Display the content of a certificate request file named **test.req**.

```
<HUAWEI> display pki cert-req filename test.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:01:cf:95:bb:fb:35:f0:3e:cd:1d:10:9e:11:
                    08:2e:77:48:ba:1b:e6:00:1b:43:30:56:f9:9a:6b:
                    ed:8b:fe:3e:03:57:38:02:48:88:e3:9b:39:d0:1c:
                    2b:8f:6a:9b:91:17:9b:ce:cb:fc:87:40:78:39:08:
                    1c:53:c3:71:cc:db:64:6f:ec:5a:cd:33:a5:68:5e:
```

```
            e6:52:61:ad:a1:58:55:f0:a0:0f:db:ab:05:eb:a4:
            fe:e1:68:61:8c:af:2c:3a:34:95:d2:41:ee:09:e7:
            b0:fc:59:d9:f4:12:00:de:ab:14:b6:a3:fe:29:75:
            f7:dd:7b:aa:03:81:fc:ae:41:8c:e4:ad:e3:d9:65:
            d4:be:a0:c1:e0:43:8a:91:ad:20:7b:6f:12:25:6e:
            0d:67:7d:4c:fe:8d:1b:6d:f3:96:07:31:ed:73:d3:
            71:6b:51:18:64:bd:41:d6:18:2d:2d:86:b7:fa:26:
            eb:cc:cb:a3:0f:0b:61:22:fd:dd:5f:b4:4d:9b:7d:
            bc:fa:af:e6:95:d7:27:f1:60:31:56:83:58:2c:40:
            1a:5e:6a:94:63:aa:70:2f:9b:00:e0:a3:9e:fb:73:
            62:5e:1c:3c:5f:48:42:7c:26:8f:5f:cf:39:b9:5d:
            25:90:8e:6c:e0:04:ec:e2:1b:1f:a8:0d:d2:ef:20:
            41:79
          Exponent: 65537 (0x10001)
      Attributes:
        challengePassword        :******
      Requested Extensions:
        X509v3 Subject Alternative Name:
          IP Address:10.1.1.1, DNS:example.com, email:test@example.com
    Signature Algorithm: sha256WithRSAEncryption
      71:e7:c0:5f:36:c9:16:eb:fc:0c:8e:d1:4f:3d:ee:25:6b:47:
      65:86:4b:89:ec:22:01:42:a5:0e:5c:aa:01:0a:57:a9:25:ba:
      1b:59:6d:77:5f:74:80:3b:af:f9:37:75:97:9a:ca:80:73:8b:
      36:14:2c:4b:9a:2f:53:5c:5b:4a:93:31:88:94:0f:4d:58:84:
      36:41:e8:a8:6c:cd:f0:bb:9f:51:50:b2:a4:40:f4:ec:37:c5:
      42:08:69:b5:c5:fd:af:3d:8a:aa:47:53:d3:ce:bc:76:ec:47:
      ca:36:90:0b:49:2b:2f:04:c4:1f:f1:12:b6:99:d0:f8:33:d8:
      08:d0:32:ac:ee:34:0f:07:ef:72:9f:6b:71:80:3e:8d:37:cc:
      ca:b5:c1:56:3d:65:c7:e6:99:1b:2b:53:01:69:f5:8a:18:05:
      d1:b1:48:3e:50:e0:4c:7f:db:dc:b7:cd:a2:37:f9:96:cd:0d:
      ee:61:c2:80:61:6b:99:c0:76:0d:ab:2c:46:ce:b7:aa:6a:12:
      72:b7:6f:64:cc:78:b7:16:bd:c5:32:45:79:42:cf:4c:28:91:
      ce:cd:7d:da:eb:2b:3a:cf:90:1f:61:5e:02:25:fe:3c:82:66:
      d4:e8:c7:f8:5e:84:2c:f6:b2:f0:ba:ee:7a:c1:9b:d4:68:02:
      a4:e3:27:89
```

Table 14-80 Description of the **display pki cert-req** command output

Item	Description
Certificate Request	Information about a certificate request file.
Data	Data of a certificate request file.
Version	Version of a certificate request file.

Item	Description
Subject	Subject of a certificate request file. The subject includes the following attributes: ● C: country code of a PKI entity. It is configured using the **14.18.7 country (PKI entity view)** command. ● ST: name of the state or province to which a PKI entity belongs. It is configured using the **14.18.82 state (PKI entity view)** command. ● L: geographic area where a PKI entity is located. It is configured using the **14.18.37 locality** command. ● O: organization to which a PKI entity belongs. It is configured using the **14.18.43 organization** command. ● OU: department to which a PKI entity belongs. It is configured using the **14.18.42 organization-unit** command. ● CN: common name of a PKI entity. It is configured using the **14.18.6 common-name** command.
Subject Public Key Info	Information about the subject public key of a certificate request file.
Public Key Algorithm	Public key algorithm.
Public-Key	RSA public key. It is configured using the **14.18.79 rsa local-key-pair** command.
Modulus	Key modulus.
Exponent	Key exponent.
Attributes	Attributes of a certificate request file.
challengePassword	The challenge password used in certificate application. It is configured using the **14.18.50 pki enroll-certificate** command.
Requested Extensions	Certificate request extension.
X509v3 Subject Alternative Name	Alternative name of the X.509v3 subject.

Item	Description
IP Address	IP address of a PKI entity. It is configured using the **14.18.35 ip-address** command.
DNS	DNS name of a PKI entity. It is configured using the **14.18.34 fqdn** command.
email	Email address of a PKI entity. It is configured using the **14.18.28 email** command.
Signature Algorithm	Signature algorithm. It is configured using the **14.18.30 enrollment-request signature message-digest-method** command.

14.18.15 display pki certificate

Function

The **display pki certificate** command displays the content about the CA or local certificate loaded to the device and OCSP server certificate.

Format

display pki certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

NOTE

Only devices in cloud management mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Displays content about the CA certificate.	-
local	Displays content about the local certificate.	-
ocsp	Displays content about the Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about the CA certificate, local certificate, and OCSP server's certificate, including signature algorithm, issuer, validity period, subject, and subject public key.

Example

# Display information about the CA certificate.

```
<HUAWEI> display pki certificate ca realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Jun  4 14:58:17 2015 GMT
            Not After : Jun  4 15:07:10 2020 GMT
        Subject: CN=ca_root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:5f:2a:93:cb:66:18:59:8c:26:80:db:cd:73:
                    d5:68:92:1b:04:9d:cf:33:a2:73:64:3e:5f:fe:1a:
                    53:78:0e:3d:e1:99:14:aa:86:9b:c3:b8:33:ab:bb:
                    76:e9:82:f6:8f:05:cf:f6:83:8e:76:ca:ff:7d:f1:
                    bc:22:74:5e:8f:4c:22:05:78:d5:d6:48:8d:82:a7:
                    5d:e1:4c:a4:a9:98:ec:26:a1:21:07:42:e4:32:43:
                    ff:b6:a4:bd:5e:4d:df:8d:02:49:5d:aa:cc:62:6c:
                    34:ab:14:b0:f1:58:4a:40:20:ce:be:a5:7b:77:ce:
                    a4:1d:52:14:11:fe:2a:d0:ac:ac:16:95:78:34:34:
                    21:36:f2:c7:66:2a:14:31:28:dc:7f:7e:10:12:e5:
                    6b:29:9a:e8:fb:73:b1:62:aa:7e:bd:05:e5:c6:78:
                    6d:3c:08:4c:9c:3f:3b:e0:e9:f2:fd:cb:9a:d1:b7:
                    de:1e:84:f4:4a:7d:e2:ac:08:15:09:cb:ee:82:4b:
                    6b:bd:c6:68:da:7e:c8:29:78:13:26:e0:3c:6c:72:
                    39:c5:f8:ad:99:e4:c3:dd:16:b5:2d:7f:17:e4:fd:
                    e4:51:7a:e6:86:f0:e7:82:2f:55:d1:6f:08:cb:de:
                    84:da:ce:ef:b3:b1:d6:b3:c0:56:50:d5:76:4d:c7:
                    fb:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C5
            X509v3 CRL Distribution Points:
                Full Name:
                  URI:http://vasp-e6000-127.china.huawei.com/CertEnroll/ca_root.
crl
                  URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl

            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
         52:21:46:b8:67:c8:c3:4a:e7:f8:cd:e1:02:d4:24:a7:ce:50:
         be:33:af:8a:49:47:67:43:f9:7f:79:88:9c:99:f5:87:c9:ff:
         08:0f:f3:3b:de:f9:19:48:e5:43:0e:73:c7:0f:ef:96:ef:5a:
         5f:44:76:02:43:83:95:c4:4e:06:5e:11:27:69:65:97:90:4f:
         04:4a:1e:12:37:30:95:24:75:c6:a4:73:ee:9d:c2:de:ea:e9:
         05:c0:a4:fb:39:ec:5c:13:29:69:78:33:ed:d0:18:37:6e:99:
         bc:45:0e:a3:95:e9:2c:d8:50:fd:ca:c2:b3:5a:d8:45:82:6e:
         ec:cc:12:a2:35:f2:43:a5:ca:48:61:93:b9:6e:fe:7c:ac:41:
         bf:88:70:57:fc:bb:66:29:ae:73:9c:95:b9:bb:1d:16:f7:b4:
         6a:da:03:df:56:cf:c7:c7:8c:a9:19:23:61:5b:66:22:6f:7e:
         1d:26:92:69:53:c8:c6:0e:b3:00:ff:54:77:5e:8a:b5:07:54:
         fd:18:39:0a:03:ac:1d:9f:1f:a1:eb:b9:f8:0d:21:25:36:d5:
         06:de:33:fa:7b:c8:e9:60:f3:76:83:bf:63:c6:dc:c1:2c:e4:
         58:b9:cb:48:15:d2:a8:fa:42:72:15:43:ef:55:63:39:58:77:
         e8:ae:0f:34

Pki realm name: abc
Certificate file name: abc_ca.cer
Certificate peer name: -
```

Table 14-81 Description of the **display pki certificate** command output

Item	Description
The x509 object type is certificate.	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

Item	Description
Subject	Subject of a certificate. The subject includes the following attributes: ● C: country code of a PKI entity. ● ST: name of the state or province to which a PKI entity belongs. ● L: geographic area where a PKI entity is located. ● O: organization to which a PKI entity belongs. ● OU: department to which a PKI entity belongs. ● CN: common name of a PKI entity.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Key Usage	X509v3 key usage.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trusted.
X509v3 Subject Key Identifier	Identifier of a subject key.
X509v3 CRL Distribution Points	CRL distribution points.
Full Name	Full name of CDP.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

14.18.16 display pki certificate built-in-ca

Function

The **display pki certificate built-in-ca** command displays the content of the SSL decryption certificate uploaded on the device.

Format

display pki certificate built-in-ca

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about the SSL decryption certificate, including signature algorithm, issuer, validity period, subject, subject public key, PKI realm name, and certificate file name.

Example

# Display information about the **built-in-ca** certificate.

```
<HUAWEI> display pki certificate built-in-ca
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f2:1c:74:f0:df:e0:2f:c6
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Validity
            Not Before: Oct 23 23:44:55 2015 GMT
            Not After : Oct 13 23:44:55 2055 GMT
        Subject: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:63:50:17:73:de:cc:9e:2b:41:fe:0e:58:28:
                    47:b7:ce:6b:77:5c:29:b1:3e:cf:d3:e0:53:63:1e:
                    21:cc:f6:11:34:7c:eb:8a:d7:08:b5:96:c4:0b:4a:
                    4d:33:6c:77:23:21:51:bb:10:d6:7d:d3:82:a0:6a:
                    f5:f6:8d:17:e0:f2:73:99:7b:c7:89:c8:fc:61:42:
                    0b:a5:d7:1a:11:47:ed:e1:5f:60:a6:c5:93:f0:07:
                    3f:73:fe:80:16:98:02:23:df:ab:04:85:13:25:32:
                    61:69:e8:f3:ab:a0:d8:e9:41:f8:c2:5f:14:9e:b7:
                    3b:49:1d:48:b4:b2:8d:bf:b9:00:ee:25:5d:7a:11:
                    a6:d3:23:61:99:ad:0f:54:be:00:a1:58:dd:d2:91:
                    ad:5c:6f:9d:d0:8c:e0:6f:a3:4e:df:ba:fd:b1:e3:
                    6f:1b:b3:1f:e6:42:91:1c:1a:4f:a3:a7:0e:3c:2c:
                    4c:f9:18:1f:9d:22:f8:09:da:ff:a7:7c:b8:77:20:
                    19:8a:90:d0:00:21:e4:1f:41:cc:f0:0c:ba:8f:23:
                    c3:9f:f9:ae:d8:49:95:be:75:49:7d:d7:d0:ce:3c:
                    28:27:e9:11:02:4d:c0:1a:d0:f7:38:7f:94:f8:9c:
                    9d:78:71:43:50:d3:05:01:07:18:f4:2f:c5:ec:96:
                    5d:d5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.1.1.1, DNS:example.com, email:test@example.com
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                3F:D2:BC:62:6B:F5:10:29:C4:59:9D:B9:71:A7:EB:B1:C4:16:91:9F
            Netscape Cert Type:
                SSL CA
            Netscape Comment:
                example comment extension
    Signature Algorithm: sha1WithRSAEncryption
         89:d5:47:31:23:c3:f9:df:fd:96:c5:38:fb:1e:b5:52:00:bd:
         21:fd:f0:18:af:8e:e8:01:b7:e6:b3:a1:0e:51:4b:61:4d:d5:
         52:1e:60:60:6a:67:9f:82:90:e3:1d:97:36:8f:c4:30:20:f4:
         14:58:4c:78:61:3c:4a:d4:0f:98:a9:05:e0:b5:cb:6a:78:eb:
         c6:40:9d:00:7b:31:8d:0e:21:72:db:31:34:83:5d:e5:42:98:
         85:09:6d:1e:c5:23:ce:e3:72:46:67:79:4b:1b:18:ba:cb:5e:
         ba:08:ee:0e:24:e5:58:07:0c:2e:b8:cf:e6:6b:09:67:76:80:
         e5:0e:66:a2:cb:3a:a1:bc:56:27:1c:1b:fd:5a:b5:ad:9f:a4:
         32:2b:32:3e:9a:9d:f5:04:ee:e5:e1:1c:76:8a:c2:45:f1:3e:
         8c:da:ab:f6:cf:82:d0:b3:4c:91:7a:c8:ad:b5:2c:28:54:e0:
         79:40:b6:b5:f1:6f:92:23:4d:94:8b:20:0d:92:86:43:98:17:
         d5:9b:b0:7f:99:f2:f1:df:0f:d3:f2:5c:9d:35:bc:64:25:13:
         39:62:ba:98:cb:cc:6a:08:fc:2c:86:2e:2e:91:80:8b:3e:27:
         14:f7:45:fe:9f:f8:1a:87:05:c9:21:c3:61:d1:69:82:e3:05:
         5c:44:c5:82

Pki realm name: -
Certificate file name: buzzcer
Certificate peer name: -
```

Table 14-82 Description of the **display pki certificate built-in-ca** command output

Item	Description
The x509 object type is certificate	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

Item	Description
Subject	Certificate subject. The subject includes the following attributes: - C: country code of a PKI entity. It is configured using the **14.18.7 country (PKI entity view)** command. - ST: name of the state or province to which a PKI entity belongs. It is configured using the **14.18.82 state (PKI entity view)** command. - L: geographic area where a PKI entity is located. It is configured using the **14.18.37 locality** command. - O: organization to which a PKI entity belongs. It is configured using the **14.18.43 organization** command. - OU: department to which a PKI entity belongs. It is configured using the **14.18.42 organization-unit** command. - CN: common name of a PKI entity. It is configured using the **14.18.35 ip-address** command.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm. It is configured using the **14.18.73 pki rsa local-key-pair create** command.
Public-Key	RSA public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Subject Alternative Name	Alternative name of the X.509v3 subject.
IP Address	IP address of the PKI entity. It is configured using the **14.18.35 ip-address** command.
DNS	DNS name of a PKI entity. It is configured using the **14.18.34 fqdn** command.

Item	Description
email	Email address of a PKI entity. It is configured using the **14.18.28 email** command.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trust.
X509v3 Key Usage	X.509v3 key use.
X509v3 Subject Key Identifier	Identifier of a X.509v3 subject key.
Netscape Cert Type	Netscape Certificate Type.
Netscape Comment	Netscape Comment.
Signature Algorithm	Signature algorithm.
Pki realm name	PKI realm name. It is configured using the **14.18.70 pki realm (system view)** command.
Certificate file name	Name of a certificate file. It is configured using the **14.18.56 pki generate built-in-ca certificate** command.
Certificate peer name	Name of a certificate peer. It is configured using the **14.18.62 pki import-certificate peer** command.

14.18.17 display pki certificate enroll-status

Function

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Format

display pki certificate enroll-status [**realm** *realm-name*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Example

# Display the certificate enrollment status.

```
<HUAWEI> display pki certificate enroll-status realm abc
 Certificate Request Transaction 1
    Status: Pending
    Key Usage: ENC&SIG
    Entity name: test
    Remain polling count: 1
    Next polling after : 35 seconds
<HUAWEI> display pki certificate enroll-status realm abc
 info: No certificate request transaction in realm abc.
```

Table 14-83 Description of the **display pki certificate enroll-status** command output

Item	Description
Certificate Request Transaction	Certificate enrollment request process.
Status	Certificate enrollment status. Pending: A certificate is being enrolled.
Key Usage	Functions of a certificate public key: ● ENC: The public key is used for encryption. ● SIG: The public key is used for signature.
Entity name	Entity name.
Remain polling count	Number of times a certificate enrollment request can be initiated again.
Next polling after	Next time a certificate enrollment request is initiated.
No certificate request transaction	There is no certificate enrollment request process.

14.18.18 display pki certificate filename

Function

The **display pki certificate** command displays the content about the CA or local certificate loaded to the device and OCSP server certificate.

Format

display pki certificate filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about the certificate including signature algorithm, issuer, validity period, subject, and subject public key.

Example

# Display information about the certificate ca.cer.

```
<HUAWEI> display pki certificate filename ca.cer
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f3:a3:3a:46:f6:09:8d:18
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
        Validity
            Not Before: May 16 11:48:04 2017 GMT
            Not After : May 14 11:48:04 2027 GMT
        Subject: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:cc:ef:2f:55:9c:d0:09:c5:1b:d2:52:63:92:
                    c8:f0:88:ed:1b:88:f1:e4:3c:90:07:85:01:8c:d5:
                    80:d9:91:ef:64:e9:79:0c:7d:0e:b9:6c:00:a2:72:
                    e2:1b:aa:9b:2d:11:6b:6f:2d:de:5d:58:22:cf:9e:
                    2f:7d:f1:ad:71:e9:25:0e:bc:26:f1:77:57:02:3d:
                    7f:09:8f:49:63:ae:11:75:57:65:a0:bd:9c:94:c6:
```

```
                    df:21:f7:c8:5a:4d:5e:f8:5e:84:b0:b0:fd:a6:c7:
                    e0:78:d1:1c:8a:55:d9:e9:66:1c:e5:4e:ce:88:dd:
                    fa:0f:60:d0:7e:86:a1:ec:b1:34:aa:f7:dd:72:c6:
                    0a:90:c7:4a:6b:a0:86:01:30:b6:6f:23:ff:ce:ae:
                    39:fb:de:18:ce:2f:b9:d7:17:09:8c:29:19:34:7a:
                    69:75:dc:ee:bf:2e:d4:93:fb:f6:a6:5b:f8:2a:6d:
                    fe:bd:f4:8b:30:49:5c:a8:94:76:12:9d:64:78:4a:
                    48:d3:2d:63:da:0a:79:b2:ee:8e:2d:5a:a0:71:99:
                    cf:b9:68:77:d3:d9:cf:12:64:80:bb:42:8c:28:1f:
                    d9:bf:7c:4b:8f:39:1e:dc:92:a4:ff:8e:b3:02:58:
                    c5:79:96:f2:a1:f9:17:cb:ea:49:57:b0:b0:3c:af:
                    db:19
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                83:08:A4:F4:BC:EC:1B:B6:7D:B0:27:F6:10:47:77:AA:2A:66:59:D5
            Netscape Cert Type:
                SSL CA
    Signature Algorithm: sha256WithRSAEncryption
         1e:6b:2a:76:7e:8e:b0:0e:72:4e:02:53:b0:77:0d:13:28:4e:
         c3:e5:f8:0b:76:fd:56:2c:e6:5b:d1:f8:48:19:17:95:1a:79:
         5e:d9:50:b9:68:bd:36:c4:ce:7b:ce:0c:98:55:b1:44:9f:20:
         66:66:33:3c:b5:40:ad:50:c8:64:1c:07:0e:08:42:72:88:35:
         d4:af:f0:8d:5d:64:90:5d:ec:f0:5c:07:76:10:ed:9b:22:18:
         ef:44:4e:c2:29:32:40:68:fe:04:dc:0e:f6:2b:25:c2:73:f5:
         9b:64:df:25:56:c6:bb:6e:a4:2f:07:b3:9d:c0:18:60:72:cb:
         51:62:94:ee:f7:21:0a:a0:92:58:a1:bf:c8:30:0e:0c:0a:91:
         cb:f4:8f:07:52:ba:df:25:88:8a:b3:3f:f0:68:fa:4c:b7:31:
         c8:97:e0:49:08:8a:74:fc:c2:90:d7:3c:0b:00:38:90:3b:19:
         ab:66:96:24:1f:86:b9:62:49:6d:9c:2d:02:99:38:bb:96:b6:
         dd:0f:3c:6e:24:7b:3d:1e:77:58:e7:46:2b:42:cc:14:6a:a4:
         16:45:ed:3c:b1:d6:30:94:c0:30:d0:46:fa:bc:da:9a:2b:f1:
         fa:f3:df:1b:84
```

Table 14-84 Description of the **display pki certificate filename** command output

Item	Description
The x509 object type is certificate.	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

Item	Description
Subject	Subject of a certificate. The subject includes the following attributes: ● C: country code of a PKI entity. ● ST: name of the state or province to which a PKI entity belongs. ● L: geographic area where a PKI entity is located. ● O: organization to which a PKI entity belongs. ● OU: department to which a PKI entity belongs. ● CN: common name of a PKI entity.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trusted.
X509v3 Subject Key Identifier	Identifier of a subject key.
X509v3 Key Usage	X509v3 key usage.
Netscape Cert Type	Netscape certificate type.

14.18.19 display pki credential-storage-path

Function

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

By default, the certificate file is stored in **flash:/**.

Format

display pki credential-storage-path

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

Example

# Display the default path where a PKI certificate is stored.

```
<HUAWEI> display pki credential-storage-path
 The pki credential-storage-path is flash:/ .
```

14.18.20 display pki crl

Function

The **display pki crl** command displays the content of the CRL in the device.

Format

display pki crl { **realm** *realm-name* | **filename** *filename* }

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm associated with the CRL.	The PKI realm name must already exist.
filename *filename*	Specifies the file name of the certificate to be imported.	The certificate file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about local CRL, including signature algorithm, issuer, update time, revoked certificate, CRL sequence number, and revocation time.

Example

# Display information about the CRL associated with the PKI realm **abc**.

```
<HUAWEI> display pki crl realm abc
 The x509 object type is CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /CN=ca_root
        Last Update: Dec 15 08:24:28 2015 GMT
        Next Update: Dec 22 20:44:28 2015 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 CRL Number:
                365
            1.3.6.1.4.1.311.21.4:
151222083428Z   .
Revoked Certificates:
    Serial Number: 28C63371000000003E04
        Revocation Date: Dec 15 08:34:27 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 28C2AB44000000003E01
        Revocation Date: Dec 15 08:30:35 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2364247C000000003D48
        Revocation Date: Dec 14 07:29:05 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 23627E0F000000003D47
        Revocation Date: Dec 14 07:27:29 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2360F397000000003D46
        Revocation Date: Dec 14 07:25:48 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Signature Algorithm: sha1WithRSAEncryption
         7a:71:54:d1:66:13:6f:9f:62:03:ac:9a:5f:42:10:15:87:46:
         e2:a1:49:0f:44:19:ce:ed:6f:c3:0e:9f:31:fe:62:d5:08:0b:
         a4:a7:7e:80:4d:9a:5b:a9:55:5c:1a:73:30:62:48:e1:28:0e:
         5b:bd:ae:04:7e:83:36:43:62:fc:f7:12:0d:f9:f6:ac:2b:be:
         9c:50:6c:67:19:43:12:31:67:c2:06:31:97:e1:34:75:1c:87:
         53:5f:e6:15:a1:33:ad:00:e7:14:68:59:05:67:28:78:a0:91:
         49:7b:ab:87:9f:9e:53:18:4b:54:53:1c:b7:1c:2d:3e:b3:57:
         63:95:1d:01:29:9e:6c:41:07:40:2d:28:d8:82:7b:d6:22:e6:
         0d:0c:4c:af:84:96:8e:f1:29:28:d4:9e:1c:37:3b:1b:2e:34:
         a7:15:e3:29:d1:c0:69:0a:7f:24:b1:ce:00:f1:b3:da:ef:8a:
         1b:14:36:f9:14:6c:b0:66:86:a8:92:95:fc:e3:78:aa:d6:d0:
         cb:4d:26:b4:bc:41:c4:47:19:d0:2a:0c:ac:c6:aa:95:c2:03:
```

```
        33:8a:39:45:3e:c3:ad:46:7d:8a:03:4d:08:e2:d0:9a:ae:39:
        fa:8d:61:d0:1c:6c:03:d4:48:2e:4d:37:60:a1:06:a4:ea:c8:
        0d:20:59:c2

Pki realm name: abc
CRL file name: abc.crl
```

Table 14-85 Description of the **display pki crl** command output

Item	Description
The x509 object type is CRL	x509 object type is CRL.
Certificate Revocation List (CRL)	Information about the CRL.
Signature Algorithm	Algorithm of signature.
Issuer	Information of issuer.
Last Update	Last time the CRL has been updated.
Next Update	Next time the CRL will be updated.
CRL extensions	CRL extended attribute.
X509v3 Authority Key Identifier	X509v3 authority key identifier.
X509v3 CRL Number	X509v3 CRL number.
Revoked Certificates	Certificate that is revoked.
Serial Number	Serial number of the CRL.
Revocation Date	Date when the certificate was revoked.
CRL entry extensions	CRL entry extensions.
X509v3 CRL Reason Code	Reason why CRL is revoked.
Signature Algorithm	Signature algorithm. It is configured using the **14.18.30 enrollment-request signature message-digest-method** command.
Pki realm name	PKI realm name. It is configured using the **14.18.70 pki realm (system view)** command.
CRL file name	CRL file name. It is configured using the **14.18.63 pki import-crl** command.

14.18.21 display pki entity

Function

The **display pki entity** command displays information about PKI entities.

Format

display pki entity [*entity-name*]

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity. If the *entity-name* parameter is not specified, information about all entities is displayed.	The value must be an existing PKI entity name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about PKI entities, including names, common names, countries, province, and location where the entities reside, and organizations to which entities belong.

Example

# Display information about all PKI entities.

```
<HUAWEI> display pki entity
PKI Entity Information:

 Entity Name      : a
 Common name      : chi
 Country          : -
 State            : A
 Locality         : -
 Organization     : A
 Organization unit: -
 FQDN             : www. e
 IP address       : -
 Email            : -
 Serial-number    : -
Total Number: 1
```

Table 14-86 Description of the **display pki entity** command output

Item	Description
PKI Entity Information	Information of the PKI entity.
Entity Name	Entity name. It is configured using the **14.18.51 pki entity** command.

Item	Description
Common name	Common name of the entity. It is configured using the **14.18.6 common-name** command.
Country	Country where a PKI entity resides. It is configured using the **14.18.7 country (PKI entity view)** command.
State	Province where a PKI entity resides. It is configured using the **14.18.82 state (PKI entity view)** command.
Locality	Location of a PKI entity. It is configured using the **14.18.37 locality** command.
Organization	Organization to which a PKI entity belongs. It is configured using the **14.18.43 organization** command.
Organization unit	Organization unit to which a PKI entity belongs. It is configured using the **14.18.42 organization-unit** command.
FQDN	FQDN name of a PKI entity. It is configured using the **14.18.34 fqdn** command.
IP address	IP address of a PKI entity. It is configured using the **14.18.35 ip-address** command.
Email	Email address. It is configured using the **14.18.28 email** command.
Serial-number	Serial number of the entity. It is configured using the **14.18.80 serial-number** command.

Related Topics

14.18.51 pki entity

14.18.7 country (PKI entity view)

14.18.82 state (PKI entity view)

14.18.37 locality

14.18.43 organization

14.18.42 organization-unit

14.18.6 common-name

14.18.35 ip-address

14.18.34 fqdn

14.18.28 email

14.18.80 serial-number

14.18.22 display pki ocsp cache statistics

Function

The **display pki ocsp cache statistics** command displays statistics about cached OCSP responses.

Format

display pki ocsp cache statistics

NOTE

Only devices in cloud management mode support this command.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command shows statistics about cached OCSP responses, including the maximum number of OCSP responses that can be cached, cache update interval, and number of cached responses.

Example

# Display statistics about cached OCSP responses.

```
<HUAWEI> display pki ocsp cache statistics

=====================================================
   OCSP Cache Function: Enable
   OCSP Cache Max Number: 2
   OCSP Cache Refresh Interval: 5 minutes
   OCSP Cache Current Number: 0
=====================================================
```

Table 14-87 Description of the **display pki ocsp cache statistics** command output

Item	Description
OCSP Cache Function	Whether OCSP caching is enabled. ● Enable ● Disable It is configured using the **14.18.67 pki ocsp response cache enable** command.
OCSP Cache Max Number	Maximum size of OCSP cache. It is configured using the **14.18.68 pki ocsp response cache number** command.
OCSP Cache Refresh Interval	OCSP cache update interval. It is configured using the **14.18.69 pki ocsp response cache refresh interval** command.
OCSP Cache Current Number	Number of cached OCSP responses.

Related Topics

14.18.67 pki ocsp response cache enable

14.18.68 pki ocsp response cache number

14.18.69 pki ocsp response cache refresh interval

14.18.23 display pki ocsp cache detail

Function

The **display pki ocsp cache detail** displays the detail information of the OCSP cache.

NOTE

Only devices in cloud management mode support this command.

Format

display pki ocsp cache detail

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view detail information of the OCSP cache.

Example

# Display the detail information of the OCSP cache.

```
<HUAWEI> display pki ocsp cache detail
==================================================
Cache Hash Status Info:
num_items              = 0
num_nodes              = 8
num_alloc_nodes        = 16
num_expands            = 0
num_expand_reallocs    = 0
num_contracts          = 0
num_contract_reallocs = 0
num_hash_calls         = 0
num_comp_calls         = 0
num_insert             = 0
num_replace            = 0
num_delete             = 0
num_no_delete          = 0
num_retrieve           = 0
num_retrieve_miss      = 0
num_hash_comps         = 0

Cache Hash Node Status Info:
node      0 ->   0
node      1 ->   0
node      2 ->   0
node      3 ->   0
node      4 ->   0
node      5 ->   0
node      6 ->   0
node      7 ->   0

Cache Hash Node Usage Status Info:
0 nodes used out of 8
0 items
====================================================
```

Table 14-88 Description of the **display pki ocsp cache detail** command output

Item	Description
Cache Hash Status Info	Hash status of the OCSP cache.
num_items	Number of available hash elements.
num_nodes	Number of requested hash nodes.

Item	Description
num_alloc_nodes	Maximum number of hash nodes that can be expanded.
num_expands	Number of hash node expansion application times.
num_expand_reallocs	Number of expanded hash nodes.
num_contracts	Number of hash node reduction times.
num_contract_reallocs	Number of reduced hash nodes.
num_hash_calls	Number of times the hash function is invoked.
num_comp_calls	Number of times the hash comparison function is invoked.
num_insert	Number of inserted hash nodes.
num_replace	Number of replaced hash nodes.
num_delete	Number of deleted hash nodes.
num_no_delete	Number of undeleted hash nodes.
num_retrieve	Number of times the hash nodes in the OCSP cache are matched.
num_retrieve_miss	Number of times the hash nodes in the OCSP cache are not matched.
num_hash_comps	Number of times the hash nodes in the OCSP cache are compared.
Cache Hash Node Status Info	Hash node status in the OCSP cache. For example, **node 0 -> 0** indicates that the number 0 node is unused; **node 0 -> 1** indicates that the number 0 node is in use.
Cache Hash Node Usage Status Info	Hash node use status in the OCSP cache.
n nodes used out of 8	There are 8 hash nodes, and n nodes are in use.
n items	The nth hash element.

14.18.24 display pki ocsp server down-information

Function

The **display pki ocsp server down-information** command displays the DOWN state information of the OCSP server recorded on the device.

NOTE

Only devices in cloud management mode support this command.

Format

display pki ocsp server down-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to DOWN. In this case, the device will not send OCSP requests to the URL for 10 minutes.

Example

# Display the DOWN state information of the OCSP server.

```
<HUAWEI> display pki ocsp server down-information

=====================================================

  Server URL: http://10.1.1.1/ocsp
  Timeout Times: 1
  Last timeout until now: 5 seconds
=====================================================
```

Table 14-89 Description of the **display pki ocsp server down-information** command output

Item	Description
Server URL	URL of an unreachable OCSP server. It is configured using the **14.18.40 ocsp url** command.
Timeout Times	Connection timeouts.

Item	Description
Last timeout until now	Time elapsed since the last connection timeout and now.

14.18.25 display pki peer-certificate

Function

The **display pki peer-certificate** command displays the imported certificates of the remote device.

Format

display pki peer-certificate { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate.	The value must be an existing peer certificate file name.
all	Displays brief information about all certificates of the remote device.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about imported certificates of the remote device, including signature algorithm, issuer, validity period, subject, public key, and PKI realm.

Example

# Display brief information about all certificates of the remote device.

```
<HUAWEI> display pki peer-certificate all
  Peer certificate name :abcd
  Serial Number:
    12 19 3c d3 00 00 00 00 04 9a
  Subject:
    CN=a

Total Number: 1
```

# Display detailed information about the certificate **abcd** of the remote device.

```
<HUAWEI> display pki peer-certificate name abcd
The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:19:3c:d3:00:00:00:00:04:9a
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=CA_ROOT
        Validity
            Not Before: Feb 19 13:00:22 2013 GMT
            Not After : Feb 19 13:10:22 2014 GMT
        Subject: CN=a
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (512 bit)
                Modulus:
                    00:b9:8b:47:65:a9:99:ed:58:b2:63:74:65:56:d1:
                    08:bb:1d:8f:4e:ed:72:a2:4a:ef:d8:45:3d:53:db:
                    c8:eb:df:53:9e:5f:c7:96:46:65:14:1a:ab:72:e9:
                    a2:71:c8:7a:f0:51:0c:cc:39:bb:14:75:7d:f1:bc:
                    88:2c:a7:2e:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E2:5B:8A:03:58:01:C8:E3:14:BC:18:5B:F9:BD:00:68:5B:D1:90:4E
            X509v3 Authority Key Identifier:
                keyid:CE:BA:CA:39:C7:AD:6A:CB:85:17:D0:8A:8E:28:02:0B:52:D4:D9:2
B

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://10.1.1.1:8080/CertEnroll/CA_ROOT.crl

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=CA_ROOT,CN=AIA,CN=Public%20Key%20Ser
vices,CN=Services,CN=Configuration,DC=esap,DC=com?cACertificate?base?objectClass
=certificationAuthority
                CA Issuers - URI:http://www.example.com/CertEnroll/www.example.c
om_CA_ROOT.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
         bb:8b:77:af:ae:df:2e:0c:bd:7a:29:6e:76:23:ad:7d:69:6d:
         0d:16:d9:18:82:ad:4f:52:b3:cd:1c:1a:fc:34:00:33:36:8d:
         47:2a:20:24:52:b7:02:75:cc:ab:3b:4c:f8:2a:a9:a9:4f:46:
         fb:c2:21:00:c1:b5:c2:67:0c:b1:99:2a:62:7b:71:4d:e7:c2:
         93:29:bb:ec:b1:e9:28:82:2f:77:61:ec:28:66:35:cb:5f:15:
         04:73:77:d8:26:91:7b:a2:56:74:51:33:0b:f1:04:28:24:b2:
         71:58:ad:5c:f8:96:17:0d:f7:b7:5f:4b:b9:ed:09:79:bc:54:
         21:c5:9b:90:f7:7b:21:aa:5a:aa:6f:51:e4:79:ce:b8:35:8b:
         19:90:51:94:e6:c2:61:f8:24:46:85:4c:a9:69:bd:8a:ef:c2:
         64:b8:19:ab:0b:6b:ec:34:41:8d:43:43:44:d1:1b:4c:4a:23:
         cd:40:52:7a:2e:8c:5d:b6:62:55:93:45:c8:3e:de:b1:51:82:
         d0:bb:7c:b8:09:7b:97:08:7b:93:17:40:a8:6f:2d:ed:f4:3e:
         36:10:2a:20:e3:47:e1:fb:ad:fe:97:73:a7:53:d0:f8:52:ca:
         b6:0e:e8:f1:df:6c:7a:37:39:bb:82:f9:03:c9:4a:71:65:df:
         6f:37:e6:b7
```

```
Pki realm name: -
Certificate file name: -
Certificate peer name: abcd
```

Table 14-90 Description of the **display pki peer-certificate** command output

Item	Description
Peer certificate name	Peer certificate name.
The x509 object type is certificate	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.
Subject	Subject of the certificate.
Subject Public Key Info	Public key of the certificate.
Public Key Algorithm	Algorithm of the Public key.
Public-Key	Information about the RSA public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X509v3 certificate extensions.
X509v3 Subject Key Identifier	Identifier of a subject key.
X509v3 CRL Distribution Points	CRL distribution points.
Full Name	Full name of CDP.
Authority Information Access	Authority information access.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

14.18.26 display pki realm

Function

The **display pki realm** command displays PKI realm information.

Format

display pki realm [*realm-name*]

Parameters

Parameter	Description	Value
realm-name	Displays the detailed information about a PKI realm. If the parameter is left blank, information about all PKI realms is displayed.	The PKI realm name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays details about a PKI realm, including PKI realm name, associated CA, CA certificate subject name, URL of the certificate enrolled through SCEP, PKI entity name, digital fingerprint algorithm of CA certificate, and digital fingerprint of CA certificate.

Example

# Display information about all PKI realms.

```
<HUAWEI> display pki realm abc
 Realm Name : abc
 CA ID: CA_ROOT
 CA Name: "/CN=ca_root"
 Enrollment URL: http://10.136.7.196:8080/certsrv/mscep/mscep.dll
 Certificate Request Interval(Minutes): 1
 Certificate Request Times: 5
 Enrollment Mode: RA
 Enrollment Method: SCEP
 Entity Name: abc
 CA Certificate Fingerprint Arithmetic: sha256
 CA Certificate Fingerprint: e71add0744360e91186b828412d279e06dcc15a4ab4bb3d1384
2820396b526a0
 OCSP Nonce: Enable
 OCSP URL: -
 Method for Getting CRL: HTTP
 CDP URL: -
 Certificate Revocation Check Method: -
 RSA Key Name: abc
 Auto-enroll: Enable
 Auto-enroll Percent: 100%
 Auto-enroll Regenerate: Enable
 Auto-enroll Regenerate Key-size: 2048
 Auto-enroll Updated-effective: Disable
 Password Cipher: Enable
 Password: %^%#:,3/YY@~[@(`1DBbZ&o$s`B\@S+3:UT0tF9EzSM:%^%#
 Crl Update-period(Hours): 8
 Crl Cache: Enable
 Key-usage: -
 Vpn-instance: -
 Source Interface: -
 Enrollment-request Signature Message-digest-method: SHA256

 Total Number: 1
```

Table 14-91 Description of the **display pki realm** command output

Item	Description
Realm Name	PKI realm name. It is configured using the **14.18.70 pki realm (system view)** command.
CA ID	ID of the CA associated with the PKI realm.
CA Name	Subject name of a CA certificate.
Enrollment URL	URL of the certificate enrolled on the SCEP server. It is configured using the **14.18.31 enrollment-url** command.
Certificate Request Interval(Minutes)	Interval between two certificate enrollment status queries.
Certificate Request Times	Maximum number of certificate enrollment status queries.
Enrollment Mode	Certificate enrollment mode (whether enrolled through RA). It is configured using the **14.18.31 enrollment-url** command.
Enrollment Method	Certificate enrollment method, including: ● SCEP: obtains certificate from CA using the SCEP protocol. ● Self-Signed: obtains certificate using self-signature.
Entity Name	PKI entity name. It is configured using the **14.18.32 entity** command.
CA Certificate Fingerprint Arithmetic	Fingerprint algorithm of the CA certificate. It is configured using the **14.18.33 fingerprint** command.

Item	Description
CA Certificate Fingerprint	Digital fingerprint of the CA certificate. It is configured using the **14.18.33 fingerprint** command.
OCSP Nonce	Whether a nonce extension is added to the OCSP request sent by a PKI entity. ● Enable: A nonce extension is added to the OCSP request sent by a PKI entity. ● Disable: A nonce extension is not added to the OCSP request sent by a PKI entity. It is configured using the **14.18.38 ocsp nonce enable** command.
OCSP URL	OCSP server's URL. It is configured using the **14.18.40 ocsp url** command.
Method for Getting CRL	Method of obtaining CRL. ● SCEP: updates the CRL automatically using SCEP. It is configured using the **14.18.11 crl scep** command. ● HTTP: updates the CRL automatically using HTTP. It is configured using the **14.18.10 crl http** command.
CDP URL	URL of the CDP. It is configured using the **14.18.4 cdp-url** command.
Crl Cache	Whether the PKI realm is allowed to use the CRL in cache. ● Enable: The PKI realm is allowed to use the CRL in cache. ● Disable: The PKI realm is not allowed to use the CRL in cache. To configure whether to allow the PKI realm to use the CRL in cache, run the **14.18.9 crl cache** command.
Certificate Revocation Check Method	Certificate status check method. It is configured using the **14.18.5 certificate-check** command.
RSA Key Name	RSA key. It is configured using the **14.18.79 rsa local-key-pair** command.
Auto-enroll	Whether automatic certificate enrollment is enabled. ● Enable: Automatic certificate enrollment is enabled. ● Disable: Automatic certificate enrollment is disabled. It is configured using the **14.18.2 auto-enroll** command.
Auto-enroll Percent	The percentage of the certificate's validity period. It is configured using the **14.18.2 auto-enroll** command.

Item	Description
Auto-enroll Regenerate	Whether the RSA key pair will be generated during certificate updates. - Enable: The RSA key pair will be generated during certificate updates. - Disable: The RSA key pair will not be generated during certificate updates. It is configured using the **14.18.2 auto-enroll** command.
Auto-enroll Regenerate Key-size	RSA key length. It is configured using the **14.18.2 auto-enroll** command.
Auto-enroll Updated-effective	Whether the certificate takes effect immediately after being updated. - Enable: The certificate takes effect immediately after being updated. - Disable: The certificate does not take effect immediately after being updated. It is configured using the **14.18.2 auto-enroll** command.
Password Cipher	Whether the challenge password can be used. - Enable: The challenge password can be used. - Disable: The challenge password cannot be used.
Password	Password used to apply for or revoke a certificate. It is configured using the **14.18.44 password (PKI realm view)** command.
Crl Update-period(Hours)	CRL update interval. It is configured using the **14.18.12 crl update-period** command.
Key-usage	Purpose information carried in a certificate request packet. It is configured using the **14.18.36 key-usage** command.
Vpn-instance	VPN to which the PKI realm is added. It is configured using the **14.18.83 vpn-instance** command.
Source Interface	Source interface used by the device to communicate with the PKI server. It is configured using the **14.18.81 source interface** command.
Enrollment-request Signature Message-digest-method	Digest method used for the enrollment request packet of signed certificate. It is configured using the **14.18.30 enrollment-request signature message-digest-method** command.

14.18.27 display pki rsa local-key-pair

Function

The **display pki rsa local-key-pair** command displays the public key in the RSA key pair.

Format

display pki rsa local-key-pair { **pem** | **pkcs12** } *filename* [**password** *password*]

display pki rsa local-key-pair [**name** *key-name*] **public** [**temporary**]

Parameters

Parameter	Description	Value
pem	Indicates that the file format is PEM.	-
pkcs12	Indicates that the file format is PKCS12.	-
filename	Specifies the name of the file that contains the RSA key pair.	The file name must already exist.
password *password*	Specifies the decryption password of RSA key pair. The value must be the same as the password set by **14.18.54 pki export rsa-key-pair**.	The value must be the name of an existing decryption password of the RSA key pair.
name *key-name*	Specifies the RSA key pair name.	The RSA key pair name must already exist.
temporary	Displays information about the RSA key pair saved in the temporary zone.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about the RSA key pair and public key, including key pair creation time, key pair name, whether the key can be exported, and public key information.

If *key-name* is not specified, all RSA key pairs and public keys are displayed. If *key-name* is specified, the specified RSA key pair and public key are displayed.

Example

# Display information about all RSA key pairs.

```
<HUAWEI> display pki rsa local-key-pair public
```

```
=========================================================
Time of Key pair created: 17:43:42  2016/4/18
Key Name: abc
Key Index: 0
Key Modules: 2048 bit
Key Exportable: Yes
Key Type: RSA signature key
=========================================================
Key code:
30820109
  02820100
    C23344E1 B2C2D653 EB134011 9266C6CC 7C18C45F
    440AF31F 98B29D4C D436757B F6785BB5 09EFA2A1
    09FDBB24 62F1914D 4F10678F 3BE8E3C0 E6F02FC9
    AFE2ADDE 98E07D2C A5732288 A5280D2B 6A785F59
    A8D19D37 9B80F7EF 1B15FB77 BD9C54D0 01AF270F
    90258F65 1A631282 50002C4F 23EF0482 1F62E356
    AC700041 B31AB3B4 5C7EB4C0 AFF2E5AF 3DDA4F4E
    F5B86502 08BA7AFE 37204C67 7149AE52 1462F25E
    16B777E8 E71BCFBE 0E9E02A7 C5FE6120 304BE6C3
    CEB2575A EA24EBB6 BA420994 C50F3662 D8F24F25
    0D833865 5A127754 2E954F7F 16292DAA AF9D2371
    E669ADFF 4EA9FFF8 CE8488D7 344EBCEB AAA74116
    B30EF506 C64A726E B1013CB4 E8FA6707
  0203
    010001
```

Table 14-92 Description of the **display pki rsa local-key-pair** command output

Item	Description
Time of Key pair created	Time when the RSA key pair is created.
Key Name	Name of a key pair. It is configured using the **14.18.73 pki rsa local-key-pair create** command.
Key Index	Index of the key.
Key Modules	Number of bits of the key.
Key Exportable	Whether the key can be exported.
Key Type	Type of the key.
Key code	Public key in the RSA key pair.

14.18.28 email

Function

The **email** command configures an email address for a PKI entity.

The **undo email** command cancels the configuration.

By default, no email address for an entity is configured.

Format

email *email-address*

undo email

Parameters

Parameter	Description	Value
email-address	Specifies the email address of an entity.	The value is a string of 1 to 128 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an email address for the PKI entity, which is used as an alias of the entity.

After the email address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this email address. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the email address of the PKI entity.

Example

# Set the email address to test@example.com for an entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] email test@example.com
```

Related Topics

14.18.21 display pki entity

14.18.29 enrollment self-signed

Function

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm.

The **undo enrollment self-signed** command restores the default certificate obtaining method.

By default, self-signed certificate obtaining in the PKI realm is not configured.

Format

enrollment self-signed

undo enrollment self-signed

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm. The device can use the self-signed certificate obtained from the PKI realm to support default HTTPS functions.

Prerequisites

The RSA key pair has been configured by using the **14.18.79 rsa local-key-pair** command.

Precautions

The device generates a self-signed certificate only when the PKI domain is applied to the service.

The device does not support lifecycle management for self-signed certificates. For example, self-signed certificates cannot be registered, updated, or revoked on the device. To ensure security of the device and certificates, it is recommended the user's certificate be used.

To configure self-signed certificate obtaining, delete the certificate in the PKI realm.

After the **enrollment self-signed** command is run, the device will not generate certificate expiration logs when its self-signed certificate expires.

Example

# Configure self-signed certificate obtaining in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] enrollment self-signed
```

Related Topics

14.18.70 pki realm (system view)

14.18.26 display pki realm

14.18.30 enrollment-request signature message-digest-method

Function

The **enrollment-request signature message-digest-method** command sets the message digest method of signature for the enrollment request.

The **undo enrollment-request signature message-digest-method** command restores the default message digest method.

By default, the message digest method of signature for the enrollment request is **sha-256**.

Format

enrollment-request signature message-digest-method { **md5** | **sha1** | **sha-256** | **sha-384** | **sha-512** }

undo enrollment-request signature message-digest-method

Parameters

Parameter	Description	Value
md5	Sets the digest method used for the enrollment request packet of signed certificate to MD5.	-
sha1	Sets the digest method used for the enrollment request packet of signed certificate to SHA1.	-
sha-256	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-256.	-
sha-384	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-384.	-
sha-512	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-512.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

In SCEP local certificate application mode, after a CA server receives a certificate enrollment request from a PKI entity, the CA server requests a signature for authentication, and generates a local certificate only after the authentication is successful.

Other algorithms are more secure than MD5 and SHA1 algorithms and so are recommended.

Example

# Set the message-digest method of signature for enrollment request to be **sha-384**.

```
<HUAWEI> system-view
[HUAWEI] pki realm e
[HUAWEI-pki-realm-e] enrollment-request signature message-digest-method sha-384
```

14.18.31 enrollment-url

Function

The **enrollment-url** command configures the URL of the CA server.

The **undo enrollment-url** command deletes the URL of the CA server.

By default, the URL of the CA server is not configured.

Format

enrollment-url [**esc**] *url* [**interval** *minutes*] [**times** *count*] [**ra**]

undo enrollment-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-

Parameter	Description	Value
url	Specifies the URL of the CA server. The URL is in the format of *http://server_location/ca_script_location*. *server_location* can use only the IP address format and domain name resolution. *ca_script_location* is the path where CA's application script is located. For example, **http://10.1.1.1:8080/certsrv/mscep/mscep.dll**.	The value is a string that starts with **http://** and consists of 1 to 128 case-sensitive characters without spaces.
interval *minutes*	Specifies the interval between two certificate enrollment status queries.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 1.
times *count*	Specifies the maximum number of certificate enrollment status queries.	The value is an integer that ranges from 1 to 100. The default value is 5.
ra	Configures an RA to authenticate a PKI entity's identity information during local certificate application. By default, a CA authenticates a PKI entity's identity information during local certificate application.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The URL refers to the address provided by a CA server for certificate application. For example, a CA server running Windows Server 2008 uses a URL address in the format http://host:port/certsrv/mscep/mscep.dll, in which *host* indicates the IP address of the CA server and *port* indicates the port number.

The keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

# Create a PKI realm **test** and configure the URL of the CA server.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] enrollment-url http://10.1.1.1:8080/certsrv/mscep/mscep.dll ra
```

14.18.32 entity

Function

The **entity** command specifies a PKI entity that applies for a certificate.

The **undo entity** command cancels a PKI entity.

By default, no PKI entity is specified.

Format

entity *entity-name*

undo entity

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value must be an existing PKI entity name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity requests the local certificate in the PKI realm, the device encapsulates the configuration of the specified PKI entity into the certificate request.

Prerequisites

1. The specified PKI entity has been configured by using the **14.18.51 pki entity** command.
2. The common name of the PKI entity has been configured using the **14.18.6 common-name** command.

Precautions

A PKI realm can be bound to only one PKI entity.

Example

# Bind the PKI entity **a** to the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki entity a
[HUAWEI-pki-entity-a] common-name test
[HUAWEI-pki-entity-a] quit
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] entity a
```

Related Topics

14.18.51 pki entity

14.18.6 common-name

14.18.26 display pki realm

14.18.33 fingerprint

Function

The **fingerprint** command configures the CA certificate fingerprint used in CA certificate authentication.

The **undo fingerprint** command deletes the CA certificate fingerprint used in CA certificate authentication.

By default, no CA certificate fingerprint is configured for CA certificate authentication.

Format

fingerprint { **md5** | **sha1** | **sha256** } *fingerprint*

undo fingerprint

Parameters

Parameter	Description	Value
md5	Sets the digital fingerprint algorithm to MD5.	-
sha1	Sets the digital fingerprint algorithm to SHA1.	-
sha256	Sets the digital fingerprint algorithm to SHA256.	-
fingerprint	Specifies the digital fingerprint value. This value needs to be obtained from the CA server offline. For example, from a CA server running Windows Server 2008, you can obtain the digital fingerprint at http://*host*:*port*/certsrv/mscep_admin/, in which *host* indicates the server's IP address and *port* indicates the port number.	The digital fingerprint value is a hexadecimal string of case-insensitive characters. ● An MD5 fingerprint consists of 32 characters (16 bytes). ● An SHA1 fingerprint consists of 40 characters (20 bytes). ● An SHA256 fingerprint consists of 64 characters (32 bytes).

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When obtaining a CA certificate, the device uses an algorithm to calculate the CA certificate fingerprint and compares the CA certificate fingerprint with the configured fingerprint. If the two values are the same, the device receives the CA certificate. When verifying a certificate, the device uses the public key of the CA certificate to authenticate the digital signature. If the digital signature can be decrypted, the certificate is verified.

Precautions

You can configure an algorithm to calculate the CA certificate fingerprint. If you run the **fingerprint** command multiple times in the same PKI realm view, only the latest configuration takes effect.

The MD5 and SHA1 algorithms have a low security level. SHA256 is recommended.

Example

# Configure the CA certificate fingerprint used in CA certificate authentication.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] fingerprint sha256
e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
```

14.18.34 fqdn

Function

The **fqdn** command configures a fully qualified domain name (FQDN) for an entity.

The **undo fqdn** command cancels the configuration.

By default, no FQDN is configured for a PKI entity.

Format

fqdn *fqdn-name*

undo fqdn

Parameters

Parameter	Description	Value
fqdn-name	Specifies the FQDN of an entity.	The value is a string of 1 to 255 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an FQDN for the PKI entity, which is used as an alias of the entity.

An FQDN is the unique identifier of a PKI entity. It consists of a host name and a domain name, and can be translated into an IP address. A sample of an FQDN is www.example.com.

After the FQDN is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this FQDN. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the FQDN of the PKI entity.

Example

# Set the FQDN to **example.com** for an entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] fqdn example.com
```

Related Topics

14.18.21 display pki entity

14.18.35 ip-address

Function

The **ip-address** configures an IP address for an entity.

The **undo ip-address** deletes the configuration.

By default, a PKI entity does not have an IP address.

Format

ip-address { *ipv4-address* | *interface-type interface-number* }

undo ip-address

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a PKI entity.	The value is in dotted decimal notation.

Parameter	Description	Value
interface-type interface-number	Specifies an interface IP address of a PKI entity. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To facilitate applicant identification, configure an IP address for the PKI entity, which is used as an alias of the PKI entity.

After an IP address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this IP address. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device IP address.

Example

# Set the IP address for a PKI entity to 10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] ip-address 10.1.1.1
```

Related Topics

14.18.21 display pki entity

14.18.36 key-usage

Function

The **key-usage** command configures the purpose description for a certificate public key.

The **undo key-usage** command deletes the purpose description of a certificate public key.

By default, a certificate public key does not have a purpose description.

Format

key-usage { **ike** | **ssl-client** | **ssl-server** } *

undo key-usage { **ike** | **ssl-client** | **ssl-server** } *

Parameters

Parameter	Description	Value
ike	Specifies the usage of a key as ike. That is, the key is used to set up an IPSec tunnel.	-
ssl-client	Specifies the usage of a key as ssl-client. That is, the key is used by the SSL client to set up an SSL session.	-
ssl-server	Specifies the usage of a key as ssl-server. That is, the key is used by the SSL server to set up an SSL session.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To improve certificate security, you can add the usage information of a key to the certificate request packet sent from the device to the CA server.

After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the usage information of the key.

For example, when setting up an SSL session, the SSL client adds a digital signature and encrypts the key by using the certificate. After you specify the usage of a key as ssl-client by using the **key-usage ssl-client** command, the certificate generated by the CA server carries the usage information, including a digital signature and encrypted key. If you use this key to encrypt data, the key will be invalid.

Example

# Specify the usage of a key as ssl-client.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] key-usage ssl-client
```

14.18.37 locality

Function

The **locality** command configures a locality name for a PKI entity.

The **undo locality** command cancels the configuration.

By default, a PKI entity does not have a locality name.

Format

locality *locality-name*

undo locality

Parameters

Parameter	Description	Value
locality-name	Specifies the locality name of an entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a locality name for the PKI entity, which is used as an alias of the entity.

After the locality name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this locality name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the locality name of the PKI entity.

Example

# Set the locality name to **Beijing** for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] locality Beijing
```

Related Topics

14.18.21 display pki entity

14.18.38 ocsp nonce enable

Function

The **ocsp nonce enable** command adds a nonce extension to the OCSP request sent by a PKI entity.

The **undo ocsp nonce enable** command cancels the configuration.

By default, the OCSP request sent by a PKI entity contains a nonce extension.

NOTE

Only devices in cloud management mode support this command.

Format

ocsp nonce enable

undo ocsp nonce enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To improve security and reliability of communication between PKI entity and OCSP server, this command adds a nonce extension (a random value) to the OSCP request sent by the PKI entity. If the nonce extension values on the PKI entity and OCSP server are different, communication fails.

Example

# Add a nonce extension to the OCSP request sent by a PKI entity

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] ocsp nonce enable
```

14.18.39 ocsp signature enable

Function

The **ocsp signature enable** command enables the function of signing OCSP request packets.

The **undo ocsp signature enable** command disables the function of signing OCSP request packets.

By default, the function of signing OCSP request packets is disabled.

NOTE

Only devices in cloud management mode support this command.

Format

ocsp signature enable

undo ocsp signature enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

When the certificate check mode is set to OCSP, the device sends OCSP request packets to the OCSP server. To improve access security, run this command to enable signing on OCSP request packets.

Example

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] ocsp signature enable
```

14.18.40 ocsp url

Function

The **ocsp url** command configures the Uniform Resource Locator (URL) address for the Online Certificate Status Protocol (OCSP) server.

The **undo ocsp url** command deletes the URL address of the OCSP server.

By default, an OCSP server does not have a URL address.

NOTE

Only devices in cloud management mode support this command.

Format

ocsp url [**esc**] *url-address*

undo ocsp url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-address	Indicates the OCSP server's URL address.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP does not contain the AIA option, run this command to configure the OCSP server's URL. If the certificate contains the AIA option, run the **ocsp-url from-ca** command to configure the PKI entity to obtain OSCP server's URL from the AIA option.

Keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?). Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\) to \x3f and enter **http://www.***.com\x3fpage1\\x3f.**

Example

# Set the OCSP server's URL address to http://10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] ocsp url http://10.1.1.1
```

14.18.41 ocsp-url from-ca

Function

The **ocsp-url from-ca** command configures the PKI entity to obtain the OCSP server's URL from the Authority Info Access (AIA) option in the CA certificate.

The **undo ocsp-url from-ca** command disables the PKI entity from obtaining the OCSP server's URL from the Authority Info Access (AIA) option in the CA certificate.

By default, a PKI entity does not obtain OCSP server's URL from the CA certificate's AIA option.

NOTE

Only devices in cloud management mode support this command.

Format

ocsp-url from-ca

undo ocsp-url from-ca

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP contains the AIA option, run this command to configure the PKI entity to obtain OSCP server's URL from the AIA option. If the certificate does not contain the AIA option, run the **ocsp url** command to configure the OCSP server's URL.

Example

# Configure the PKI entity to obtain OCSP server's URL from the CA certificate's AIA option.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] ocsp-url from-ca
```

14.18.42 organization-unit

Function

The **organization-unit** command configures the department name for a PKI entity.

The **undo organization-unit** command restores the default setting.

By default, no department name is configured for a PKI entity.

Format

organization-unit *organization-unit-name*

undo organization-unit

Parameters

Parameter	Description	Value
organization-unit-name	Specifies the department name for a PKI entity.	The department name is a string of 1 to 31 case-sensitive characters. Names of departments are separated by commas (,). The total length of all department names ranges from 1 to 191. The characters can be letters, integers, apostrophe ('), equal sign (=), brackets (), plus sign (+), comma (,), minus sign (-), dot (.), slash (/), colon (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a department name for the PKI entity, which is used as an alias of the entity.

After the department name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this department name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the department name of the PKI entity.

Example

# Configure the department name of a PKI entity to **Group1, Sale**.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] organization-unit Group1,Sale
```

Related Topics

14.18.21 display pki entity

14.18.43 organization

Function

The **organization** command configures a PKI entity's organization name.

The **undo organization** command deletes a PKI entity's organization name.

By default, a PKI entity does not have an organization name.

Format

organization *organization-name*

undo organization

Parameters

Parameter	Description	Value
organization-name	Specifies the organization name of the PKI entity.	It is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an organization name for the PKI entity, which is used as an alias of the entity.

After the organization name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this organization name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the organization name of the PKI entity.

Example

# Set the organization name of the PKI entity to **org1**.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] organization org1
```

Related Topics

14.18.21 display pki entity

14.18.44 password (PKI realm view)

Function

The **password** command sets the challenge password used for certificate application through SCEP, which is also used to revoke a certificate.

The **undo password** command deletes the challenge password used for certificate application through SCEP.

By default, no challenge password is configured.

Format

password cipher *password*

undo password

Parameters

Parameter	Description	Value
cipher *password*	Specifies the challenge password used for certificate application through SCEP. The password is displayed in ciphertext.	The value is a string of case-sensitive characters. It cannot contain question marks (?). The *password* is in plaintext that contains 1 to 64 characters or in ciphertext that contains 48 to 108 characters. **NOTE** To improve communication security, it is recommended that the certificate revocation password contains at least three types of lowercase letters, uppercase letters, numerals, and special characters, and contains at least six characters.

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

When a PKI entity uses SCEP to apply for a certificate from CA, CA needs to verify the challenge password of the entity. CA accepts the certificate application request only when the challenge password is correct. You need to run this command to set a challenge password for the PKI entity.

The challenge password is also used to revoke a certificate. It avoids misoperations in certificate revocation.

Example

# Set the challenge password used to apply for certificate through SCEP.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] password cipher 6AE73F21E6D3571D
```

14.18.45 pki built-in-ca match-rsa-key

Function

The **pki built-in-ca match-rsa-key** command configures a device to search for the RSA key pair associated with a specific SSL decryption certificate.

Format

pki built-in-ca match-rsa-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of an SSL decryption certificate.	It must be the name of an existing SSL decryption certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to view the RSA key pair associated with an SSL decryption certificate. Then the system searches all local RSA key pairs for the desired one, and displays the key pair name.

Prerequisites

An SSL decryption certificate has been generated using the **14.18.56 pki generate built-in-ca certificate** command or an SSL decryption certificate has been imported.

Example

# Configure a device to search for the RSA key pair that matches certificate file **rsakey_builtinca.cer**.

```
<HUAWEI> system-view
[HUAWEI] pki generate built-in-ca certificate rsa-key-pair rsakey entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : rsakey_builtinca.cer
 Info: Generate built in CA certificate successfully.
[HUAWEI] pki built-in-ca match-rsa-key certificate-filename rsakey_builtinca.cer
 Info: The file rsakey_builtinca.cer contains certificates 1.
 Info: Certificate 1 from file rsakey_builtinca.cer matches RSA key rsakey.
```

Related Topics

14.18.56 pki generate built-in-ca certificate

14.18.46 pki create-certificate

Function

The **pki create-certificate** command creates a self-signed certificate.

Format

pki create-certificate self-signed filename *file-name*

Parameters

Parameter	Description	Value
self-signed	Creates a self-signed certificate.	-
filename *file-name*	Specifies the name of a certificate file.	The value is a string of 1 to 64 case-insensitive characters without spaces or question marks.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a self-signed certificate or local certificate is generated by the device, the certificate file is saved in the storage device as a PEM file. You can export the certificate for other devices to use. This simplifies certificate issue process.

When you run the **pki create-certificate** command, the system asks you to enter certificate information, for example, PKI entity parameters, certificate file name, the validity time of certificate and RSA key length.

Precautions

The device does not provide lifecycle management for self-signed certificates. For example, self-signed certificates cannot be updated or revoked on the device. To ensure security of the device and certificates, a local certificate is recommended.

Example

# Create a self-signed certificate **huawei**.

```
<HUAWEI> system-view
[HUAWEI] pki create-certificate self-signed filename huawei
```

14.18.47 pki delete-certificate

Function

The **pki delete-certificate** command deletes a certificate from the memory.

Format

pki delete-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

NOTE

Only devices in cloud management mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Deletes a CA certificate.	-
local	Deletes a local certificate.	-
ocsp	Deletes an Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the name of the PKI realm to which a certificate belongs.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the certificate expires or you want to apply for a new certificate, run this command to delete the CA, OCSP, or local server certificate from the memory.

Prerequisites

Example

# Delete the local certificate from the memory.

```
<HUAWEI> system-view
[HUAWEI] pki delete-certificate local realm abc
```

Related Topics

14.18.70 pki realm (system view)

14.18.48 pki delete-certificate built-in-ca

Function

The **pki delete-certificate built-in-ca** command deletes an SSL decryption certificate from the memory.

Format

pki delete-certificate built-in-ca filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of the SSL decryption certificate file.	The SSL decryption certificate file name must already exist in the memory.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSL decryption certificate expires or you want to apply for a new certificate, run the **pki delete-certificate built-in-ca** command to delete the current SSL decryption certificate from the memory. This command will not delete the certificate files in the device storage.

Prerequisites

The SSL decryption certificate has been imported to the memory using the **14.18.61 pki import-certificate built-in-ca** command.

Example

# Delete an SSL decryption certificate from the memory.

```
<HUAWEI> system-view [HUAWEI] pki import-certificate built-in-ca filename test_builtinca.cer  Info: Succeeded in importing the built-in CA certificate.   [HUAWEI] pki delete-certificate built-in-ca filename test_builtinca.cer
```

Related Topics

14.18.61 pki import-certificate built-in-ca

14.18.49 pki delete-crl

Function

The **pki delete-crl** command deletes a CRL from the memory.

Format

pki delete-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm that the certificate belongs to.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a CRL expires, run this command to delete a CRL file from the memory. This command will not delete the CRL files in storage card.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Example

# Delete the CRL of PKI realm **abc** from the memory.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki delete-crl realm abc
```

Related Topics

14.18.70 pki realm (system view)

14.18.20 display pki crl

14.18.50 pki enroll-certificate

Function

The **pki enroll-certificate** command configures manual certificate enrollment.

Format

pki enroll-certificate realm *realm-name* [**pkcs10** [**filename** *filename*]] [**password** *password*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of a PKI realm.	The PKI realm name must already exist.
pkcs10	Uses the PKCS#10 format to display the local certificate request information. It can be used to request certificates in offline mode.	-
filename *filename*	Saves the certificate request information in a specified file. The certificate request information is saved in the file in PKCS#10 format and is sent to the CA in outband mode.	The value is a string of 1 to 64.

Parameter	Description	Value
password *password*	Indicates a challenge password, which is used to request certificates in online mode. When the CA server processes the certificate request using the challenge password, you must set a challenge password on the entity, and the challenge password must be the same as the password configured on the CA server.	The value is a string of case-sensitive characters without question marks (?) or spaces. It can be a plain-text string of 1 to 64 characters or a cipher-text string of 48 to 108 characters. **NOTE** To improve certificate security, it is recommended that a password consist of at least two of the following: lowercase letters, uppercase letters, numerals and special characters. In addition, the password must contain at least 6 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Manual certificate application is online or offline.

- Online mode (in-band mode)

  In online requests, entities request certificates from CAs using the SCEP protocol. Then the entities store the obtained certificates on the flash of devices.
- Offline mode (out-of-band mode)

  The device generates a certificate request file. The administrator sends the file to the CA server using methods such as disks and emails.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Precautions

- If **pkcs10** is specified, an entity applies to a CA for a certificate in offline mode. The entity saves the certificate request information in a file in PKCS#10 format and sends the file to the CA in outband mode.

- If **pkcs10** is not specified, an entity applies to a CA for a certificate in online mode.
- In online mode, a PKI entity obtains a CA certificate and imports it to memory, and then obtains a local certificate and imports it to memory.
- After the **enrollment self-signed** command is used in the PKI realm, it is not allowed to use the **pki enroll-certificate** command to configure manual certificate enrollment.

Example

# Enroll a certificate for the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki enroll-certificate realm abc
```

Related Topics

14.18.70 pki realm (system view)

14.18.51 pki entity

Function

The **pki entity** command creates a PKI entity and displays the PKI entity view, or displays the view of an existing PKI entity.

The **undo pki entity** command deletes a PKI entity.

By default, no PKI entity is configured.

Format

pki entity *entity-name*

undo pki entity *entity-name*

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A PKI entity refers to the applicant or user of a certificate. A PKI entity is required when you use PKI features. After a PKI entity is created, you can configure attributes for it, for example, common name, country code, email address, FQDN, IP address, geographic area, organization, department, state, and province. These attributes include identity information of the PKI entity. The identity information will be added to the subject of a PKI entity.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Example

# Configure a PKI entity **entity1** and enter the PKI entity view.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1]
```

14.18.52 pki export-certificate

Function

The **pki export-certificate** command exports a certificate to the device storage.

Format

pki export-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name* { **pem** | **pkcs12** }

NOTE

Only devices in cloud management mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Exports a CA certificate.	-
local	Exports a local certificate.	-
ocsp	Exports the Online Certificate Status Protocol (OCSP) certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate.	The PKI realm name must already exist.

Parameter	Description	Value
pem	Exports a certificate in PEM format.	-
pkcs12	Exports a certificate in P12 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To copy a certificate to another device, run the **pki export-certificate** command to export a certificate to the flash of the local device first, and then transfer the certificate to another device using a file transfer protocol.

Before using this command, run the **14.18.15 display pki certificate** command to view information about certificates on the device.

Prerequisites

A PKI realm has been created using the **14.18.70 pki realm (system view)** command.

Precautions

When the exported certificate file does not contain a private key, the device does not encrypt this file.

When you export the private key, the system asks you to enter the private key file name. If the private key file name and the certificate file name are the same, the private key and certificate are stored in the same file. If they are different, they are stored in different files.

When you export the private key, the system asks you to enter the private key file format and set the password. The password will be used when you run the **14.18.60 pki import-certificate** command to import this private key.

After the **enrollment self-signed** command is used in the PKI realm, you cannot use the **pki export-certificate** command to export certificates to files.

Example

# Export the local certificate in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki export-certificate local realm abc pem
 Please enter the name of certificate file <length 1-127>: aa
```

```
If you only export the certificate, do not export the private key.
You can directly enter empty of private key file.
Please enter the name of private key file <length 1-127>:
Info: Succeeded in exporting the certificate.
```

Related Topics

14.18.70 pki realm (system view)

14.18.60 pki import-certificate

14.18.15 display pki certificate

14.18.53 pki export built-in-ca rsa-key-pair

Function

The **pki export built-in-ca rsa-key-pair** command exports the RSA key pair to the flash.

Format

pki export built-in-ca rsa-key-pair *key-name* [**and-certificate** *certname*] { **pem** *file-name* [**3des** | **aes** | **des**] | **pkcs12** *file-name* } **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the RSA key pair name.	The value must be an existing RSA key pair name.
and-certificate *certname*	Indicates that the SSL decryption certificate is exported together with the associated RSA key pair.	The value must be an existing SSL decryption certificate name.
pem *file-name*	Indicates that the RSA key pair to be exported is in the PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.

Parameter	Description	Value
pkcs12 *file-name*	Indicates that the RSA key pair to be exported is in the PKCS12 format and specifies the file name to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
3des | **aes** | **des**	Sets the encryption algorithm to AES, DES or 3DES if a file is exported in the PEM format. By default, AES is used. **NOTE** For security, DES and 3DES algorithms are not recommended.	-
password *password*	Specifies the password for the RSA key pair file. This password is used when you import an RSA key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). To enhance security, a password must meet the minimum strength requirements, that is, the password needs to contain at least three types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to transfer or back up the RSA key pair. After the configuration is complete, you can generate a PEM or PKCS12 file containing the RSA key pair (or also the SSL decryption certificate) in the flash.

Prerequisites

The RSA key pair has been created for the SSL decryption certificate using the **14.18.72 pki rsa built-in-ca** command with the **exportable** parameter specified, or the RSA key pair of the SSL decryption certificate has been imported to the memory using the **14.18.64 pki import built-in-ca rsa-key-pair** command with the **exportable** parameter specified.

Precautions

An RSA key pair is sensitive information. Delete or destroy the exported RSA key pair from your device or storage device immediately after you do not use it.

Example

# Export RSA key pair **key2** to file **aaa.pem** and set the encryption method to AES.

```
<HUAWEI> system-view [HUAWEI] pki rsa built-in-ca key2 create exportable  Info: The name of the
new key-pair will be: key2  The size of the public key ranges from 512 to 4096.  Input the bits in the
modules:2048  Generating key-pairs... .......+++  ............................+++   [HUAWEI] pki export built-in-ca rsa-
key-pair key2 pem aaa.pem aes password Hello@123  Warning: Exporting the key pair impose security
risks, are you sure you want to  export it? [y/n]:y                                              Info: Succeeded
in exporting the RSA key pair in PEM format.
```

Related Topics

14.18.64 pki import built-in-ca rsa-key-pair

14.18.61 pki import-certificate built-in-ca

14.18.54 pki export rsa-key-pair

Function

The **pki export rsa-key-pair** command exports the RSA key pair to the flash and allows the export of the associated certificate.

Format

pki export rsa-key-pair *key-name* [**and-certificate** *certificate-name*] { **pem** *file-name* [**3des** | **aes** | **des**] | **pkcs12** *file-name* } **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value must be an existing RSA key pair name.
and-certificate *certificate-name*	Indicates that the certificate related to the RSA key pair are exported.	The value must be an existing certificate file name.
pem *file-name*	Indicates that the RSA key pair to be exported is in the PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pkcs12 *file-name*	Indicates that the RSA key pair to be exported is in the PKCS12 format and specifies the file name to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
3des | **aes** | **des**	Sets the encryption algorithm to DES, 3DES or AES if a file is exported in the PEM format. The default value is AES. **NOTE** DES and 3DES are less secure than AES and are not recommended.	-

Parameter	Description	Value
password *password*	Specifies the encryption password for the RSA key pair file. This password is used when you import an RSA key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). To enhance security, a password must contain at least two types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To transfer or back up an RSA key pair, run this command to generate the PEM or PKCS12 file carrying this RSA key pair (which may include the certificate) in the flash.

Before using this command, run the **14.18.27 display pki rsa local-key-pair** command to view information about the RSA key pairs on the device.

Prerequisites

The RSA key pair has been created and configured to be exportable using the **14.18.73 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **14.18.65 pki import rsa-key-pair** command.

Precautions

The RSA key pair is sensitive information. Delete and destroy the exported RSA key pair on the device or storage device immediately after you do not need it.

Example

# Export the RSA key pair **key1** to the file **aaa.pem** and set the encryption method to AES.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create key1 exportable
 Info: The name of the new key-pair will be: key1
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
......+++
....................+++
[HUAWEI] pki export rsa-key-pair key1 pem aaa.pem aes password Admin@1234
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting the RSA key pair in PEM format.
```

Related Topics

14.18.73 pki rsa local-key-pair create

14.18.65 pki import rsa-key-pair

14.18.27 display pki rsa local-key-pair

14.18.55 pki file-format

Function

The **pki file-format** command sets the format for the saved certificate request, certificate, and CRL.

By default, the device stores certificate request, certificate, and CRL in PEM format.

Format

pki file-format { **der** | **pem** }

Parameters

Parameter	Description	Value
der	Indicates that the format of a certificate request file is DER.	-
pem	Indicates that the format of a certificate request file is PEM.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To change the format for the saved certificate request, certificate, and CRL, for example, to use the certificate and CRL obtained through SCEP, run the **pki file-format** command.

However, the certificate and CRL obtained through HTTP are downloaded directly and are not saved in the format configured using this command. The created self-signed certificate or local certificate can only be saved in PEM format.

Example

# Set the format of saved certificate request, certificate, and CRL to DER.

```
<HUAWEI> system-view
[HUAWEI] pki file-format der
```

14.18.56 pki generate built-in-ca certificate

Function

The **pki generate built-in-ca certificate** command generates an SSL decryption certificate.

Format

pki generate built-in-ca certificate rsa-key-pair *rsa-key-pair-name* **entity** *entity-name*

Parameters

Parameter	Description	Value
rsa-key-pair *rsa-key-pair-name*	Specifies the name of the RSA key pair in an SSL decryption certificate.	The RSA key pair must exist in the memory.
entity *entity-name*	Specifies the PKI entity name.	The PKI entity must have been configured and have a common name. If the PKI entity does not have a common name, an SSL decryption certificate cannot be generated.

Views

System view:

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable a proxy for SSL connection, the device complies with the certificate information on the real server and issues another certificate to the client using the SSL decryption certificate.

The generated SSL decryption certificate files are saved to the **flash:/** directory.

Prerequisites

1. An RSA key pair of the SSL decryption certificate has been created using the **14.18.72 pki rsa built-in-ca** command or the RSA key pair has been imported to the memory of the device using the **14.18.64 pki import built-in-ca rsa-key-pair** command.
2. A PKI entity has been created using the **14.18.51 pki entity** command.
3. The common name of the PKI entity has been configured using the **14.18.6 common-name** command.

Example

# Generate an SSL decryption certificate.

```
<HUAWEI> system-view
[HUAWEI] pki rsa built-in-ca rsakey create
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
........++++++
........++++++
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] common-name huawei
[HUAWEI-pki-entity-entity1] quit
[HUAWEI] pki generate built-in-ca certificate rsa-key-pair rsakey entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : key1
Info: Generate built in CA certificate successfully.
```

Related Topics

14.18.72 pki rsa built-in-ca

14.18.64 pki import built-in-ca rsa-key-pair

14.18.51 pki entity

14.18.6 common-name

14.18.16 display pki certificate built-in-ca

14.18.57 pki get-certificate

Function

The **pki get-certificate** command downloads a certificate to the device storage.

Format

pki get-certificate ca realm *realm-name*

Parameters

Parameter	Description	Value
ca	Specifies a CA or RA certificate to be obtained.	-

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of a certificate to be obtained.	The value must be an existing PKI realm name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you request a local certificate for the PKI entity through SCEP, run this command to download a CA certificate to the device storage, and request a local certificate using the encrypted CA public key.

Prerequisites

A PKI realm has been created using the **14.18.70 pki realm (system view)** command.

Precautions

After obtaining a CA certificate, the device automatically imports the certificate to the device memory.

If the same certificate exists on the device, delete the existing one; otherwise, the certificate cannot be obtained.

Example

# Obtain the CA certificate in the PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki get-certificate ca realm abc
```

Related Topics

14.18.70 pki realm (system view)

14.18.58 pki get-crl

Function

The **pki get-crl** command updates CRL immediately.

Format

pki get-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of the CRL.	The value must be an existing PKI realm name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CRL status is checked periodically when it is updated automatically. If the CRL on the device is likely to expire, configure this command to update CRL immediately.

After this command is executed, the new CRL replaces the old CRL in the storage, and is automatically imported to the memory to replace the old one.

Prerequisites

A PKI realm has been created using the **14.18.70 pki realm (system view)** command.

Example

# Configure the CRL immediate update.

```
<HUAWEI> system-view
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] quit
[HUAWEI] pki get-crl realm test
```

Related Topics

14.18.70 pki realm (system view)

14.18.59 pki http

Function

The **pki http** command configures a device to use HTTP to download a CA certificate, local certificate, or CRL.

Format

pki http [**esc**] *url-address save-name*

Parameters

Parameter	Description	Value
esc	Specifies the entering of URLs in the ASCII code.	-
url-address	Specifies the URL of a CA certificate, local certificate, or CRL.	The value is a string of 1 to 128 case-sensitive characters.
save-name	Specifies the name of a CA certificate, local certificate, or CRL saved on the flash of the device.	The value is a string of 1 to 64 case-insensitive characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Before you configure a device to use HTTP to download a CA certificate, local certificate, or CRL, ensure that the flash of the device has enough space to accommodate the CA certificate, local certificate, or CRL.

Keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?). Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\) to \x3f and enter **http://www.***.com\x3fpage1\\x3f.**

Example

# Configure a device to use HTTP to download a local certificate.

```
<HUAWEI> system-view
[HUAWEI] pki http http://10.1.1.1/test.cer local.cer
```

# Configure a device to use HTTP to download a local certificate.

```
<HUAWEI> system-view
[HUAWEI] pki http esc http://www.***.com\x3fpage1\\x3f local.cer
```

14.18.60 pki import-certificate

Function

The **pki import-certificate** command imports a certificate to the device memory.

Format

pki import-certificate { **ca** | **local** } **realm** *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*] [**replace**] [**no-check-validate**] [**no-check-hash-alg**]

pki import-certificate { **ca** | **local** } **realm** *realm-name* **pkcs12 filename** *filename* [**no-check-validate**] [**no-check-hash-alg**] **password** *password*

pki import-certificate ocsp realm *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*]

pki import-certificate ocsp realm *realm-name* **pkcs12 filename** *filename* **password** *password*

NOTE

Only devices in cloud management mode support the **ocsp** parameter.

Parameters

Parameter	Description	Value
ca	Imports a CA certificate. For example, when the device works as an SSL proxy, import the SSL proxy CA certificate and use the private key in the certificate to sign the SSL client certificate again.	-
local	Imports a local certificate.	-
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The PKI realm name must already exist. NOTE The domain name cannot contain spaces. Otherwise, the certificate cannot be imported.
der	Imports a certificate in DER format.	-
pkcs12	Imports a certificate in PKCS12 format.	-
pem	Imports a certificate in PEM format.	-

Parameter	Description	Value
filename *filename*	Specifies the name of the imported certificate.	The file name must already exist.
replace	Deletes the original certificate and RSA key pair and imports the new certificate when there are repeated certificates in the domain. **NOTE** If the RSA key pair of the original certificate is not referenced by other domains, the certificate and key pair are deleted. If the RSA key pair of the original certificate is referenced by other domains, only the original certificate is deleted but the key pair is not deleted.	-
no-check-validate	Specifies whether the validity check is performed on the imported certificate.	-
no-check-hash-alg	Specifies whether a check is performed on the hash algorithm used for the signature of the imported certificate.	-
ocsp	Imports the Online Certificate Status Protocol (OCSP) server's certificate.	-
password *password*	Specifies the decryption password of the certificate, and the password is the same as the password set by the **14.18.52 pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a certificate is saved to the storage, run this command to import the certificate to the memory for it to take effect.

The device supports the following certificate import modes:

- terminal: Import or copy the certificate file of the peer to the local device. That is, you can open the PEM certificate file using a text tool and copy the certificate content to the local device.
- file: The **filename** parameter is specified to import the certificate file of the peer.

Multiple certificates can be imported on the device, including the CA certificate, local certificate, and private key.

NOTE

If you do not know the format of the certificate you want to import, configure each format in turn and check whether the certificate is successfully imported.

Prerequisites

The PKI realm has been created using the **14.18.70 pki realm (system view)** command, and the certificate file already exists on the storage device.

Precautions

If a certificate file contains a key pair file, the **pki import-certificate** command imports only the certificate file, but not the key pair file. To import the key pair file, run the **pki import rsa-key-pair** command after the **pki import-certificate** command, or run the **pki import rsa-key-pair** command to import the certificate and key pair files simultaneously.

It is not recommended that multiple local certificates be imported into the same PKI realm. Otherwise, certificate-related services may use the certificates that do not match the services, causing services to become unavailable.

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_localx.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported should be less than 50 characters, so the total certificate file name does not exceed 64 characters, and the certificate file cannot be imported to the storage component.

The device supports importing digital certificates generated through RSA encryption algorithms.

Example

# Import a local certificate to PKI realm **abc** in file transfer mode.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki import-certificate local realm abc pem filename local.cer
 Info: Succeeded in importing the certificate.
```

Related Topics

14.18.19 display pki credential-storage-path

14.18.70 pki realm (system view)

14.18.52 pki export-certificate

14.18.59 pki http

14.18.61 pki import-certificate built-in-ca

Function

The **pki import-certificate built-in-ca** command imports the SSL decryption certificate to the memory.

Format

pki import-certificate built-in-ca filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the file name of the SSL decryption certificate.	The value must be the name of an existing SSL decryption certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Import the SSL decryption certificate to the memory to use it; otherwise, the certificate will not take effect.

When importing the SSL decryption certificate, make sure that the matching RSA key pair in the SSL decryption certificate exists on the device. The mapping relationship is created when the SSL decryption certificate is created. Search for the RSA key pair that corresponds to the SSL decryption certificate using the **14.18.45 pki built-in-ca match-rsa-key** command.

Prerequisites

The SSL decryption certificate file already exists on the storage device, and is generated using the **14.18.56 pki generate built-in-ca certificate** command.

Example

Import the SSL decryption certificate **key1_builtinca.cer** to the memory.

```
<HUAWEI> system-view
[HUAWEI] pki generate built-in-ca certificate rsa-key-pair key1 entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : key1_builtinca.cer
 Info: Generate built in CA certificate successfully.
[HUAWEI] pki import-certificate built-in-ca filename key1_builtinca.cer
```

Related Topics

14.18.19 display pki credential-storage-path

14.18.56 pki generate built-in-ca certificate

14.18.45 pki built-in-ca match-rsa-key

14.18.62 pki import-certificate peer

Function

The **pki import-certificate peer** command imports a certificate of the remote device to the device memory.

Format

pki import-certificate peer *peer-name* { **der** | **pem** | **pkcs12** } **filename** [*filename*]

pki import-certificate peer *peer-name* **pkcs12 filename** *filename* **password** *password*

Parameters

Parameter	Description	Value
peer-name	Specifies the name of peer certificate. A certificate cannot be imported to multiple peers.	The value is a string of 1 to 32 case-insensitive characters without spaces. If the character string is quoted by double quotation marks, it can contain spaces.
der	Imports a certificate of the remote device in DER format.	-
pem	Imports a certificate of the remote device in PEM format.	-
pkcs12	Imports a certificate of the remote device in P12 format.	-
filename *filename*	Imports a certificate of the remote device in file mode.	The value is an existing name of certificate of the remote device.

Parameter	Description	Value
password *password*	Specifies the decryption password of the certificate, and the password is the same as the password set by the **14.18.52 pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Where digital envelop authentication is used, configure the public key of the remote device. The public key can be obtained from the public and private key management module or certificate of the remote device.

Prerequisites

The certificate file of the remote device must already exist on the storage device.

Precautions

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_localx.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported cannot exceed 50 characters. Otherwise, the total certificate file name will exceed 64 characters, and the certificate file cannot be imported to the storage component.

You can import a peer certificate generated using the RSA encryption algorithm to the device.

Example

# Import the certificate **aa.pem** of the remote device in the file mode.

```
<HUAWEI> system-view
[HUAWEI] pki import-certificate peer abcd pem file aa.pem
 Info: Succeeded in importing the peer certificate.
```

Related Topics

14.18.19 display pki credential-storage-path

14.18.25 display pki peer-certificate

14.18.63 pki import-crl

Function

The **pki import-crl** command imports the CRL to the memory.

Format

pki import-crl realm *realm-name* **filename** *file-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name.	The value must be an existing PKI realm name.
filename *file-name*	Specifies the name of an imported certificate or CRL file. The certificates only support the PEM and DER formats.	The value must be an existing certificate or CRL file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable the CRL that is obtained in out-of-band mode or is updated manually, run this command to import the CRL to the memory.

Prerequisites

A PKI realm has been created using the **14.18.70 pki realm (system view)** command and the CRL file has been downloaded using HTTP.

Example

Import the CRL in the PKI realm to the memory.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki http esc http://www.***.com\x3fpage1\\x3f abc.crl
[HUAWEI] pki import-crl realm abc filename abc.crl
```

Related Topics

14.18.19 display pki credential-storage-path

14.18.70 pki realm (system view)

14.18.59 pki http

14.18.20 display pki crl

14.18.64 pki import built-in-ca rsa-key-pair

Function

The **pki import built-in-ca rsa-key-pair** command imports an RSA key pair in the SSL decryption certificate to the device memory.

Format

pki import built-in-ca rsa-key-pair *key-name* { **pem** | **pkcs12** } *file-name* [**exportable**] **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
pem *file-name*	Specifies the format of the imported RSA key pair as PEM, and specifies the name of the RSA key pair file.	The value must be an existing certificate file name.
pkcs12 *file-name*	Specifies the format of the imported RSA key pair as PKCS12, and specifies the name of the RSA key pair file.	The value must be an existing certificate file name.
exportable	Specifies the imported RSA key pair as exportable.	-

Parameter	Description	Value
password *password*	Specifies the decryption password of the RSA key pair, and the password is the same as the password set by the **14.18.53 pki export built-in-ca rsa-key-pair** command.	The value must be the name of an existing decryption password of the RSA key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When using the DSA key pair generated by other entities, store the RSA key pair on the flash of the local device. To make the RSA key pair take effect, run this command to import it to the memory.

Prerequisites

The RSA key pair must already exist on the storage device.

Example

# Import RSA key pair **aaa.pem**. In the system, the RSA key pair name is **key-1** and password **Test!123**, and can be marked **exportable**.

```
<HUAWEI> system-view
[HUAWEI] pki import built-in-ca rsa-key-pair key-1 pem aaa.pem exportable password Test!123
 Info: Succeeded in importing the RSA key pair in PEM format.
```

Related Topics

14.18.19 display pki credential-storage-path

14.18.53 pki export built-in-ca rsa-key-pair

14.18.65 pki import rsa-key-pair

Function

The **pki import rsa-key-pair** command imports the RSA key pair to the device memory.

Format

pki import rsa-key-pair *key-name* { **pem** | **pkcs12** } *file-name* [**exportable**] [**password** *password*]

pki import rsa-key-pair *key-name* **der** *file-name* [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
pem *file-name*	Indicates that the RSA key pair to be imported is in the PEM format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
pkcs12 *file-name*	Indicates that the RSA key pair to be imported is in the PKCS12 format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
der *file-name*	Indicates that the RSA key pair to be imported is in the DER format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
exportable	Indicates that the imported RSA key pair can be exported.	-
password *password*	Specifies the decryption password of the RSA key pair. , and the password is the same as the password set by the **14.18.54 pki export rsa-key-pair** command	The value must be the name of an existing decryption password of the RSA key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to use the RSA key pair generated by other entities. After the configuration, the imported RSA key pair can be referenced by the PKI module for operations such as signing.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

If you do not know the format of the key pair you want to import, configure each format in turn and check whether the key pair is successfully imported.

Prerequisites

The RSA key pair must already exist on the storage device.

Example

# Import RSA key pair **aaa.pem**. In the system, the RSA key pair name is **key-1**, and the password is **Test!123456**. The RSA key pair name can be marked **exportable**.

```
<HUAWEI> system-view
[HUAWEI] pki import rsa-key-pair key-1 pem aaa.pem exportable password Test!123456
 Info: Succeeded in importing the RSA key pair in PEM format.
```

Related Topics

14.18.19 display pki credential-storage-path

14.18.54 pki export rsa-key-pair

14.18.66 pki match-rsa-key

Function

The **pki match-rsa-key** command configures a device to search for the RSA key pair associated with a specific certificate.

Format

pki match-rsa-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
certificate-filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to check the RSA key pair corresponding to a certificate. After configuration, the system searches for all the local RSA key pairs, compares them with the specified certificate and outputs the matched RSA key pair name once it is searched out.

Example

# Configure a device to search for the RSA key pair that matches certificate file **local.cer**.

```
<HUAWEI> system-view
[HUAWEI] pki match-rsa-key certificate-filename local.cer
 Info: The file local.cer contains certificates 1.
 Info: Certificate 1 from file local.cer matches RSA key rsa2.key.
```

14.18.67 pki ocsp response cache enable

Function

The **pki ocsp response cache enable** command enables a device to cache OCSP responses.

The **undo pki ocsp response cache enable** command disables a device from caching OCSP responses.

By default, the PKI OCSP response cache function is disabled.

NOTE

Only devices in cloud management mode support this command.

Format

pki ocsp response cache enable

undo pki ocsp response cache enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After you enable a PKI entity to cache OCSP responses, the PKI entity first searches its cache for the certificate revocation status. If the search fails, the PKI entity sends a request to the OCSP server. In addition, the device caches valid OCSP responses for subsequent query. The OCSP responses have a validity period. With OCSP response cache enabled, a PKI entity refreshes the cached OCSP responses every minute to clear expired OCSP responses.

Example

# Enable the PKI OCSP response cache function.

```
<HUAWEI> system-view
[HUAWEI] pki ocsp response cache enable
```

14.18.68 pki ocsp response cache number

Function

The **pki ocsp response cache number** command sets the maximum number of OCSP responses that can be cached on a PKI entity.

The **undo pki ocsp response cache number** command restores the maximum number of OCSP responses that can be cached on a PKI entity to the default value.

By default, the maximum number of OCSP responses that can be cached on a PKI entity is 2.

NOTE

Only devices in cloud management mode support this command.

Format

pki ocsp response cache number *number*

undo pki ocsp response cache number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of OCSP responses that can be cached on a PKI entity.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

A PKI entity caches valid OCSP responses for subsequent query. If the number of cached OCSP responses reaches the value specified by *number*, the PKI entity stops caching OCSP responses.

Example

# Set the maximum number of OCSP responses that can be cached on a PKI entity to 3.

```
<HUAWEI> system-view
[HUAWEI] pki ocsp response cache number 3
```

14.18.69 pki ocsp response cache refresh interval

Function

The **pki ocsp response cache refresh interval** command sets the interval at which the OCSP response cache is refreshed.

The **undo pki ocsp response cache refresh interval** command restores the interval at which a PKI entity refreshes the OCSP response cache to the default value.

By default, the interval at which a PKI entity refreshes the OCSP response cache is 5 minutes.

NOTE

Only devices in cloud management mode support this command.

Format

pki ocsp response cache refresh interval *interval*

undo pki ocsp response cache refresh interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the OCSP response cache is refreshed.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

A PKI entity refreshes the OCSP response cache periodically and deletes the OCSP responses that have expired based on the *interval* value.

Example

# Set the interval at which the OCSP response cache is refreshed to 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] pki ocsp response cache refresh interval 30
```

14.18.70 pki realm (system view)

Function

The **pki realm** command creates a PKI realm and displays the PKI realm view, or displays the view of an existing PKI realm.

The **undo pki realm** command deletes a PKI realm.

By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

Format

pki realm *realm-name*

undo pki realm *realm-name*

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PKI realm is a set of identity information required when a PKI entity enrolls a certificate.

Precautions

A PKI realm configured on a device is unavailable to certificate authorities (CAs) or other devices.

When a certificate is requested using a PKI realm, the system names the certificate file *PKI realm name***_local.cer**. Therefore, if you will use a created PKI realm to request certificates, ensure that the PKI realm name length is shorter than 50 characters, because a certificate file with a name longer than 64 characters cannot be saved on a storage device.

Example

# Create a PKI realm **abc**.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc]
```

Related Topics

14.18.26 display pki realm

14.18.71 pki release-certificate peer

Function

The **pki release-certificate peer** command releases a certificate of the remote device.

Format

pki release-certificate peer { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate to be released.	The value must be an existing peer certificate file name.
all	Releases all certificates of the remote device.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the specified certificate of the remote device is not required, run the **pki release-certificate peer** command to release the certificate of the remote device.

Before using this command, run the **14.18.25 display pki peer-certificate** command to view the certificate information of the remote device.

Prerequisites

The **14.18.62 pki import-certificate peer** command has been used to import the certificate of the remote device.

Example

# Release the certificate **huawei** of the remote device.

```
<HUAWEI> system-view
[HUAWEI] pki release-certificate peer name huawei
 Info: Succeeded in releasing the peer certificate.
```

Related Topics

14.18.62 pki import-certificate peer

14.18.25 display pki peer-certificate

14.18.72 pki rsa built-in-ca

Function

The **pki rsa built-in-ca** command creates, overwrites, or destroys the RSA key pair in an SSL decryption certificate.

Format

pki rsa built-in-ca *key-name* { **create** [**exportable**] | **destroy** }

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair in an SSL decryption certificate.	The value is a string of 1 to 64 case-sensitive characters without question marks and spaces. If the character string is quoted by double quotation marks, it can contain spaces and question marks.
create	Specifies the created RSA key pair of the SSL decryption certificate.	-
exportable	Specifies the created RSA key pair as exportable.	-
destroy	Specifies the destroyed RSA key pair of the SSL decryption certificate.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device uses the SSL decryption certificate to perform the proxy function for the SSL connection, the certificate must contain a public key. Run this command to create the RSA key pair of the SSL decryption certificate.

If the RSA key pair is referenced by the certificate and has been imported to the memory, you cannot overwrite or destroy the pair directly. To overwrite or destroy the RSA key pair, you can run the **14.18.48 pki delete-certificate built-in-ca** command to delete the SSL decryption certificate from the memory first.

When creating or overwriting the RSA key pair, you must enter the number of bits of the RSA key pair. The default value is 2048.

Precautions

The name of an RSA key pair cannot exceed 50 characters. Because when an RSA key pair is imported, if the certificate is imported at the same time, the PKI system adds **_builtinca.cer** after the name of the RSA key pair to generate a new certificate file name, and saves it to the storage component. If the name exceeds 50 characters, the total number of characters exceeds 64, and the certificate file cannot be saved to the storage component.

When creating the key pair, the system prompts the user to enter the number of bits of the RSA key pair. The longer the key pair, the harder it is to crack, and the more secure but slow the encryption algorithm. It is recommended that the number of bits of the RSA key pair exceed 2048; otherwise, it has security risks.

Example

# Create an RSA key pair **rsakey**.

```
<HUAWEI> system-view
[HUAWEI] pki rsa built-in-ca rsakey create
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from  to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
........++++++
........++++++
```

Related Topics

14.18.48 pki delete-certificate built-in-ca

14.18.73 pki rsa local-key-pair create

Function

The **pki rsa local-key-pair create** command creates the specified RSA key pair.

Format

pki rsa local-key-pair create *key-name* [**modulus** *modulus-size*] [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be created.	The value is a string of 1 to 64 case-sensitive characters without question marks (?) and spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
modulus *modulus-size*	Specifies the size of the RSK key pair.	The value is an integer that ranges from 2048 to 4096. The default value is 2048.

Parameter	Description	Value
exportable	Indicates that the new RSA key pair can be exported from the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a PKI entity requests a certificate from the CA, the certificate enrollment request that it sends contains information such as the public key. Run this command to create the RSA key pair for the certificate request.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Precautions

When creating the key pair, the system prompts the user to enter the number of bits of the RSA key pair. The longer the key pair, the harder it is to crack, and the more secure but slow the encryption algorithm. It is recommended that the number of bits of the RSA key pair exceed 2048; otherwise, it has security risks.

The name of an RSA key pair cannot exceed 50 characters. Because when an RSA key pair is imported, if the certificate is imported at the same time, the PKI system adds **_localx.cer** after the name of the RSA key pair to generate a new certificate file name, and saves it to the storage component. If the name exceeds 50 characters, the total number of characters exceeds 64, and the certificate file cannot be saved to the storage component.

The RSA key pair referenced by PKI realms cannot be overwritten. They can be overwritten only after the reference relationship is removed.

If the name of the new RSA key pair is the same as that of a pair on the device, the system prompts the user to decide whether to overwrite the existing pair.

Example

# Create 2048-bit RSA key pair **test**.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create test
```

```
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
......+++
.......+++
```

Related Topics

14.18.27 display pki rsa local-key-pair

14.18.74 pki rsa local-key-pair destroy

Function

The **pki rsa local-key-pair destroy** command deletes the specified RSA key pair.

Format

pki rsa local-key-pair destroy *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be deleted.	The value must be the name of an existing key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It is recommended that you run this command to destroy the specified RSA key pair if it is leaked, damaged, unused, or lost.

After this command is executed, the specified RSA key pair is deleted from the active device and the standby device.

Prerequisites

The RSA key pair has been created using the **14.18.73 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **14.18.65 pki import rsa-key-pair** command.

Precautions

The RSA key pair in the creation process cannot be deleted.

The RSA key pair referenced by a PKI realm cannot be deleted. They can be deleted only after the reference relationship is removed.

Example

# Delete the RSA key pair **test**.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
........................+++
[HUAWEI] pki rsa local-key-pair destroy test
 Warning: The name of the key pair to be deleted is test.
 Are you sure you want to delete the key pair? [y/n]:y
 Info: Delete RSA key pair success.
```

Related Topics

14.18.65 pki import rsa-key-pair

14.18.73 pki rsa local-key-pair create

14.18.75 pki set-certificate expire-prewarning

Function

The **pki set-certificate expire-prewarning** command sets the expiration warning date for the local certificate and the CA certificate in the memory.

The **undo pki set-certificate expire-prewarning** command restores the expiration warning date for the local certificate and the CA certificate in the memory to the default value.

By default, the expiration warning date for the local certificate and the CA certificate in the memory is seven days.

Format

pki set-certificate expire-prewarning *day*

undo pki set-certificate expire-prewarning

Parameters

Parameter	Description	Value
day	Specifies the expiration warning date.	The value is an integer that ranges from 7 to 180. By default, the value is 7.

Views

System view

Default Level

3: Management level

Usage Guidelines

After this command is executed, you will be prompted the expiration of a certificate in advance. If the system detects that a certificate in the memory is to expire in less than *day*, the device sends an expiration warning to the user.

Example

Set the expiration warning date for the local certificate and the CA certificate in the memory as 30 days.

```
<HUAWEI> system-view
[HUAWEI] pki set-certificate expire-prewarning 30
```

14.18.76 pki validate-certificate

Function

The **pki validate-certificate** command allows you to verify the validity of a CA certificate or a local certificate.

Format

pki validate-certificate { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Checks validity of the CA certificate.	-
local	Checks validity of the local certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an end entity verifies a peer certificate, it checks the status of the peer certificate. For example, the end entity checks whether the peer certificate has expired and whether the certificate is in a CRL.

To verify the validity of a CA certificate or a local certificate, run the **pki validate-certificate** command.

Prerequisites

A PKI realm has been configured using the **pki realm (system view)** command.

Precautions

The **pki validate-certificate ca** command allows you to verify only the root CA certificate, but not subordinate CA certificates. When multiple CA certificates are imported on a device, you can use only the **pki validate-certificate local** command to verify the validity of subordinate certificates.

Example

# Configure the device to check validity of the local certificate using CRL.

```
<HUAWEI> system-view
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] certificate-check crl
[HUAWEI-pki-realm-abc] quit
[HUAWEI] pki validate-certificate local realm abc
```

14.18.77 reset pki ocsp response cache

Function

The **reset pki ocsp response cache** command resets an OCSP response cache.

NOTE

Only devices in cloud management mode support this command.

Format

reset pki ocsp response cache

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The PKI entity caches valid OCSP responses for future searches. If the number of cached OCSP responses reaches the maximum value, no more OCSP responses can be cached. To ensure that the latest OCSP responses can be cached, you can run this command to clear the OCSP response cache first.

Example

# Reset an OCSP response cache.

```
<HUAWEI> reset pki ocsp response cache
```

14.18.78 reset pki ocsp server down-information

Function

The **reset pki ocsp server down-information** command clears the DOWN status information of the OCSP server recorded on the device.

NOTE

Only devices in cloud management mode support this command.

Format

reset pki ocsp server down-information [**url** [**esc**] *url-addr*]

Parameters

Parameter	Description	Value
url [**esc**] *url-addr*	Specifies the OCSP server's URL address. If no URL address is specified, clear the DOWN status information on all OCSP servers. If the **esc** parameter is specified, the URL address in ASCII format is supported.	The value is a string starting with http:// and consisting of 1 to 128 case-sensitive characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to DOWN. In this case, the device will not send OCSP requests to the URL for 10 minutes.

However, this mechanism may falsely set the state of a transiently disconnected server to DOWN. Using this command, the user can manually clear the falsely reported DOWN state of the OCSP server so that the device can send OCSP requests to the server.

The keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

# Clear the OCSP server DOWN information of the specified URL.

```
<HUAWEI> reset pki ocsp server down-information
```

14.18.79 rsa local-key-pair

Function

The **rsa local-key-pair** command configures the RSA key pair used to request a certificate using the SCEP or in an offline mode.

The **undo rsa local-key-pair** command deletes the RSA key pair used to request a certificate using the SCEP or in an offline mode.

By default, the system does not configure the RSA key pair used to request a certificate using the SCEP or in an offline mode.

Format

rsa local-key-pair *key-name*

undo rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair.	The value must be an existing RSA key pair name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PKI entity that requests a certificate from the CA using the SCEP or in offline PKCS#10 mode must contain a public key. Run this command to configure the RSA key pair.

Prerequisites

The RSA key pair for certificate application has been created using the **14.18.73 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **14.18.65 pki import rsa-key-pair** command.

Precautions

An RSA key pair can be specified to only one PKI.

Example

# Configure the RSA key pair that is referenced by the PKI realm **test**.

```
<HUAWEI> system-view
[HUAWEI] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
........................+++
................................................................................
........+++
[HUAWEI] pki realm test
[HUAWEI-pki-realm-test] rsa local-key-pair test
```

Related Topics

14.18.73 pki rsa local-key-pair create

14.18.65 pki import rsa-key-pair

14.18.80 serial-number

Function

The **serial-number** command adds the serial number of a device to the PKI entity.

The **undo serial-number** command restores the default setting.

By default, the serial number of a device is not added to the PKI entity.

Format

serial-number

undo serial-number

Parameters

None

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To further identify the applicant, add the serial number of the device to the PKI entity.

After the serial number of the device is added to a PKI entity, the certificate request packet sent by the device to the CA server carries this serial number. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device serial number.

Example

# Add the serial number of the device to a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] serial-number
```

Related Topics

14.18.21 display pki entity

14.18.81 source interface

Function

The **source interface** command configures the source interface used in TCP connection setup.

The **undo source interface** command restores the default source interface used in TCP connection setup.

By default, the device uses the outbound interface as the source interface for TCP connection setup.

Format

source interface *interface-type interface-number*

undo source interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies an interface's IP address as the source IP address used in TCP connection setup. ● *interface-type* indicates the type of the interface. ● *interface-number* indicates the number of the interface.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **source interface** command specifies the source interface for establishing a connection between the device and the Simple Certificate Enrollment Protocol (SCEP) or Online Certificate Status Protocol (OCSP) server. This interface IP address is the source IP address of the TCP connection.

In the multi-output scenario, if the interfaces for sending and receiving a TCP packet are different, the IP address in the received TCP packet is different from the IP address of the receiving interface. Then the TCP packet is dropped, and the TCP connection is torn down. In this situation, you can run this command to specify the loopback interface address.

Precautions

Ensure that the interface is at Layer 3 and has an IP address configured.

Example

# Configure the source interface used in TCP connection setup to VLANIF 100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.136.2.25 24
[HUAWEI-Vlanif100] quit
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] source interface vlanif 100
```

14.18.82 state (PKI entity view)

Function

The **state** command configures a state or province name for an entity.

The **undo state** command deletes the configuration.

By default, no state or province name is configured for a PKI entity.

Format

state *state-name*

undo state

Parameters

Parameter	Description	Value
state-name	Specifies the state or province name of an entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a state or province name for a PKI entity.

After the state or province name is configured for a PKI entity, the certificate request packet sent by the device to the CA server contains this province name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the state or provision name of the PKI entity.

Example

# Configure the province name to **Jiangsu** for a PKI entity.

```
<HUAWEI> system-view
[HUAWEI] pki entity entity1
[HUAWEI-pki-entity-entity1] state Jiangsu
```

Related Topics

14.18.21 display pki entity

14.18.83 vpn-instance

Function

The **vpn-instance** command adds a PKI to a specified VPN.

The **undo vpn-instance** command unbinds a PKI from a specified VPN.

By default, a PKI does not belong to any VPN.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain and verify certificates, the device needs to communicate with the CA or SCEP server. When the CA or SECP server is in a VPN, add the PKI to the specified VPN.

Prerequisites

1. A VPN instance has been created using the **10.4.36 ip vpn-instance** command.
2. The RD has been configured using the **10.4.47 route-distinguisher** command.

Example

# Add the PKI to the VPN named **vrf1**.

```
<HUAWEI> system-view
[HUAWEI] ip vpn-instance vrf1
[HUAWEI-vpn-instance-vrf1] route-distinguisher 22:1
```

```
[HUAWEI-vpn-instance-vrf1-af-ipv4] quit
[HUAWEI-vpn-instance-vrf1] quit
[HUAWEI] pki realm abc
[HUAWEI-pki-realm-abc] vpn-instance vrf1
```

Related Topics

10.4.36 ip vpn-instance

10.4.47 route-distinguisher