19 Upgrade-compatible Commands Reference

About This Chapter

This chapter describes upgrade-compatible commands of each feature of all fixed switches.Upgrade-compatible commands are supported in earlier versions, but are deleted in the new version or have the command format changed. They exist to prevent configuration loss or impact on other configurations after the upgrade.

Due to version evolution, there may be changes on upgrade-compatible commands supported by some products. This chapter does not describe the differences.

Upgrade-compatible commands are classified into two types based on user operations:

- You can write these commands to the configuration file but cannot run them in the CLI after the device restarts.
- You can run these commands by entering commands in their complete format.

NOTE

You are not advised to use upgrade-compatible commands to perform operations on the device. If required, perform operations under the guidance of technical support personnel.

19.1 Basic Configuration Compatible Commands

19.1.1 set authentication password simple (upgrade-compatible command)

Function

The **set authentication password simple** command sets the simple format for a local authentiction password.

Format

set authentication password simple *password*

Parameters

Parameter	Description	Value
password	Specifies a password.	The value is a string of 1 to 16 characters. The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character. Special character except the question mark (?) and space.

Views

User view

Default Level

3: Management level

Task Name and Operations

Task Name	Operations
telnet-server	write

Usage Guidelines

It is replaced by the **set authentication password** command.

This command is saved in simple text after it is configured, which brings security risks. Saving the command configuration in ciphertext is recommended.

19.1.2 certificate load (upgrade-compatible command)

Function

The **certificate load** command loads a digital certificate in the Secure Sockets Layer (SSL) policy view.

The **undo certificate load** command unloads a digital certificate for the SSL policy.

By default, no digital certificate is loaded for the SSL policy.

Format

# Load a PEM digital certificate for the SSL policy.

certificate load pem-cert *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*

# Load a PFX digital certificate for the SSL policy.

certificate load pfx-cert *cert-filename* **key-pair** { **dsa** | **rsa** } { **mac** *mac-code* | **key-file** *key-filename* } **auth-code** *auth-code*

Load a PEM certificate chain for the SSL policy.

certificate load pem-chain *cert-filename* **key-pair** { **dsa** | **rsa** } **key-file** *key-filename* **auth-code** *auth-code*

Parameters

Parameter	Description	Value
pem-cert	Loads a PEM digital certificate for the SSL policy. A PEM digital certificate has a file name extension .pem. A PEM digital certificate transfers text data between systems.	-
cert-filename	Specifies the name of a certificate file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
key-pair	Specifies the key pair type.	-
dsa	Sets the key pair type to DSA.	-
rsa	Sets the key pair type to RSA.	-
key-file *key-filename*	Specifies the key pair file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code *auth-code*	Specifies the authentication code of the key pair file. The authentication code verifies user identity to ensure that only authorized clients access the server.	When the authentication code is in plain text, the value is a string of 1 to 31 case-sensitive characters without any space.
pfx-cert	Loads a PFX digital certificate for the SSL policy. A PFX digital certificate has a file name extension .pfx. A digital certificate can be converted from the PFX format to another format.	-

Parameter	Description	Value
mac *mac-code*	Specifies a message authentication code. The message authentication code ensures the packet data reliability and security.	When the authentication code is in plain text, the value is a string of 1 to 31 case-sensitive characters without any space.
pem-chain	Specifies a PEM certificate chain.	-

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SSL security mechanism includes:

- Data transmission security: Uses the symmetric key algorithm to encrypt data.
- Message integrity: uses the multiplexed analog component (MAC) algorithm to ensure message integrity.
- Identity authentication mechanism: authenticates users based on the digital signatures and certificates.

The Certificate Authority (CA) issues PEM, ASN1, and PFX digital certificates that provide user identity information. Based on digital certificates, users establish trust relationships with partners who require high security.

A digital certificate data includes the applicant information such as the applicant's name, applicant's public key, digital signature of the CA that issues the certificate, and the certificate validity period. A certificate chain can be released when a certificate is sent so that the receiver can have all certificates in the certificate chain.

Prerequisites

Before running the **certificate load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

- You can load a certificate or certificate chain for only one SSL policy. Before loading a certificate or certificate chain, you must unload the existing certificate or certificate chain.
- When you configure an SSL policy to load a certificate or certificate chain, ensure that the maximum length of the key pair in the certificate or certificate chain is 2048 bits. If the length of the key pair exceeds 2048 bits, the certificate file or certificate chain file cannot be uploaded to the device.

Example

# Load a PEM digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] certificate load pem-cert servercert.pem key-pair dsa key-file
serverkey.pem auth-code 123456
```

# Load a PFX digital certificate for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pfx-cert servercert.pfx key-pair dsa key-file
serverkey.pfx auth-code %$%$"DlqKik*GE*~`u4H+LFJ(K-=%$%$
```

# Load a PEM certificate chain for the SSL policy.

```
<HUAWEI> system-view
[HUAWEI] ssl policy http_server
[HUAWEI-ssl-policy-http_server] certificate load pem-chain chain-servercert.pem key-pair dsa key-file
chain-servercertkey.pem auth-code 123456
```

19.1.3 set device usb-deployment password (upgrade-compatible command)

Function

The **set device usb-deployment password** command sets an authentication password for USB-based deployment.

Format

set device usb-deployment password *password*

Parameters

Parameter	Description	Value
password	Specifies the authentication password for USB-based deployment.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

A user with a level lower than the management level cannot query the password configured using this command. If this user query the configuration file, the password is displayed as asterisks (******).

19.1.4 set save-configuration backup-to-server server (upgrade-compatible command)

Function

The **set save-configuration backup-to-server server** command specifies the server where the system periodically saves the configuration file.

The **undo set save-configuration backup-to-server server** command cancels the server where the system periodically saves the configuration file.

By default, the system does not periodically save configurations to the server.

Format

set save-configuration backup-to-server server *server-ip* [**transport-type** { **ftp** | **sftp** }] **path** *path* **user** *user-name* **password** *password*

set save-configuration backup-to-server server *server-ip* **user** *user-name* **password** *password* [**path** *path*]

undo set save-configuration backup-to-server server [*server-ip*]

Parameters

Parameter	Description	Value
server *server-ip*	Specifies the IP address of the server where the system periodically saves the configuration file.	-
transport-type	Specifies the mode in which the configuration file is transmitted to the server.	The value can be **ftp** or **sftp**.
user *user-name*	Specifies the name of the user who saves the configuration file on the server.	The value is a string of 1 to 64 case-sensitive characters without spaces.
password *password*	Specifies the password of the user who saves the configuration file on the server.	The value is a string of 1 to 16 or 32 case-sensitive characters without spaces.
path *path*	Specifies the relative save path on the server.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to periodically save the configuration file to the server.

Precautions

If the mode in which the configuration file is transmitted to the server is not specified, FTP is used.

If the specified path on the server does not exist, configuration files cannot be sent to the server. The system then sends an alarm message indicating the transmission failure to the NMS, and the transmission failure is recorded as a log message on the device.

The user name and password must be the same as those used in FTP or SFTP login mode.

Example

# Specify the server to which the system periodically sends the configuration file, and set the transmission mode to FTP.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration backup-to-server server 10.1.1.1 transport-type ftp path d:/ftp user
huawei password huawei@1234
```

19.1.5 set save-configuration (upgrade-compatible command)

Function

Using the **set save-configuration** command, you can enable automatic saving of configurations.

Using the **undo set save-configuration** command, you can disable automatic saving of configurations.

By default, automatic saving of configurations is not enabled.

Format

set save-configuration nochange-time *nochange-time*

undo set save-configuration nochange-time [*nochange-time*]

Parameters

Parameter	Description	Value
nochange-time *nochange-time*	Specifies a period and configures the system to automatically save configurations if no configurations are changed over the specified period.	The value is an integer ranging from 30 to 43200, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

If **nochange-time** *nochange-time* is specified in the command, the system automatically saves configurations if no configuration changes in the period specified by *nochange-time*.

If the interval from the time of the last configuration to the current time is shorter than the set interval, the system cancels the current automatic saving operation.

Example

# Configure the system to automatically save configurations at 60-minute intervals if no configuration changes in the period.

```
<HUAWEI> system-view
[HUAWEI] set save-configuration nochange-time 60
```

19.1.6 snmp-agent trap enable configuration (upgrade-compatible command)

Function

The **snmp-agent trap enable configuration** command enables the trap function of the Configuration module.

By default, the trap function of the Configuration module is disabled.

Format

snmp-agent trap enable configuration

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name configuration** command.

19.1.7 snmp-agent trap enable ssh (upgrade-compatible command)

Function

The **snmp-agent trap enable ssh** command enables the trap function of the SSH module.

By default, the alarm function of the SSH module is disabled.

Format

snmp-agent trap enable ssh

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.1.8 snmp-agent trap enable system (upgrade-compatible command)

Function

The **snmp-agent trap enable system** command enables the trap function of the system module.

By default, the trap function of the system module is enabled.

Format

snmp-agent trap enable system

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name system** command.

19.1.9 snmp-agent trap enable flash (upgrade-compatible command)

Function

The **snmp-agent trap enable flash** command enables the trap function of the flash module.

By default, the trap function of the flash module is disabled.

Format

snmp-agent trap enable flash

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name vfs** { **hwflhopernotification** | **hwflhsyncfailnotification** | **hwflhsyncsuccessnotification** } command.

19.1.10 super password (upgrade-compatible command)

Function

The **super password** command sets the password used to change a user from a lower level to a higher level.

The **undo super password** command cancels the current configuration.

By default, the system does not set the password used to change a user from a lower level to a higher level.

Format

super password [**level** *user-level*] **simple** *simple-password*

Parameters

Parameter	Description	Value
level *user-level*	Specifies a user level.	The value is an integer that ranges from 1 to 15. By default, the system sets passwords for users of level 3.
simple *simple-password*	Specifies the simple password for changing a user level.	The value is a string of 1 to 16 case-sensitive characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device makes it possible to switch a user from a lower level to a higher level. To prevent illegal intrusion of unauthorized users, when a user switches to a higher user level, the system authenticates the user identity by requiring the user to input the password for the higher user level.

- If the **cipher** *cipher-password* parameter is not specified, the system starts the interactive password setting mode. Enter a plain text password of 6 to 16 characters. The requirements for the password are the same as the requirements for the plain text password configured when the **cipher** keyword is specified. The password you enter will not be displayed on the device. You can press **CTRL_C** to cancel the password setting.
- The password is in plain or cipher text and displayed on the device when the **cipher** *cipher-password* parameter is specified. When you run the **super** command to switch the user level, the password must be entered in plain text.
- Whether the password is entered in **cipher** or interactive mode, the password is saved in cipher text to the configuration file. Therefore, the password cannot be obtained from the system after it is set. Keep the password secure.
- This command is saved in simple text after it is configured, which brings security risks. Saving the command configuration in ciphertext is recommended.

Example

# Set the password used when low-level users switch to level 10 to huawei2012.

```
<HUAWEI> system-view
[HUAWEI] super password level 10 simple huawei2012
```

19.1.11 trusted-ca load (upgrade-compatible command)

Function

The **trusted-ca load** command loads the trusted CA file for the SSL policy for the FTP client.

The **undo trusted-ca load** command unloads the trusted CA file of the SSL policy.

By default, no trusted CA file is loaded for the SSL policy.

Format

# Load the trusted CA file for the SSL policy in PFX format.

trusted-ca load pfx-ca *ca-filename* **auth-code** { *auth-code* | **cipher** *auth-code* }

Parameters

Parameter	Description	Value
pfx-ca	Load the trusted CA file for the SSL policy in PFX format.	-
ca-filename	Specifies the name of the trusted CA file. The file is in the subdirectory of the system directory **security**. If the **security** directory does not exist in the system, create this directory.	The value is a string of 1 to 64 characters. The file name is the same as that of the uploaded file.
auth-code *auth-code*	Specifies the verification code for the trusted CA file in PFX format. The authentication code verifies user identity to ensure that only authorized users can log in to the server.	When the authentication code is in plain text, the value is a string of 1 to 31 case-sensitive characters without any space.

Views

SSL policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

CAs that are widely trusted in the world are called root CAs. Root CAs can authorize other lower-level CAs. The identity information about a CA is provided in the file of a trusted CA. To ensure the communication security and verify the server validity, you must run the **trusted-ca load** command to load the trusted CA file.

Prerequisites

Before running the **trusted-ca load** command, you have run the **ssl policy** command to create the SSL policy in the system view.

Precautions

A maximum of four trusted CA files can be loaded for an SSL policy.

Example

# Load the trusted CA file for the SSL policy in PFX format.

```
<HUAWEI> system-view
```

```
[HUAWEI] ssl policy ftp_server
[HUAWEI-ssl-policy-ftp_server] trusted-ca load pfx-ca servercert.pfx auth-code cipher 123456
```

19.2 Device Management Compatible Commands

19.2.1 cpu-usage threshold (upgrade-compatible command)

Function

The **cpu-usage threshold** command sets the upper and lower CPU usage alarm thresholds.

Format

cpu-usage threshold [**unit** *unit-id*] { **high** | **low** } *threshold-value*

Parameters

Parameter	Description	Value
high	Specifies the upper CPU usage alarm threshold.	-
low	Specifies the lower CPU usage alarm threshold.	-

Parameter	Description	Value
unit *unit-id*	● Specifies the slot ID if stacking is not configured. ● Specifies the stack ID if stacking is configured.	The value range depends on the device configuration.
threshold-value	Specifies the alarm threshold of CPU usage.	● The value is an integer that ranges from 2 to 100 when specifies the upper CPU usage alarm threshold. ● The value is an integer that ranges from 1 to 99 when specifies the lower CPU usage alarm threshold.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the CPU usage is not within the allowed range, a log is recorded. You can conveniently know CPU usage through log information.

19.2.2 display autosave config (upgrade-compatible command)

Function

The **display autosave config** command displays the configuration about the autosave function, including the status of the autosave function, time for autosave check, threshold of the CPU usage, and interval during which configurations are not changed.

Format

display autosave config

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the autosave function is configured, you can run the **display autosave config** command to check whether the configured parameters are correct. You can also run this command to check whether the parameters about the autosave function are properly configured when autosave cannot function normally. If not, run the **set save-configuration** command to adjust the parameters to restore the normal state of the autosave function.

Example

# Display the configuration about the autosave function.

```
<HUAWEI> display autosave config
Auto save function status: enable
Auto save checking interval: 60 minutes
The threshold of the CPU usage: 50%
The interval of the configuration not changing: 30 minutes
```

Table 19-1 Description of the display autosave config command output

Item	Description
Auto save function status	Indicates the status of the autosave function: ● Enable ● Disable
Auto save checking interval	Indicates the time for autosave check.
The threshold of the CPU usage	Indicates the threshold of the CPU usage during the autosave operation.
The interval of the configuration not changing	Indicates the interval during which system configurations are not changed.

19.2.3 display fault-management (upgrade-compatible command)

Function

The **display fault-management** command displays the contents of an alarm message, active alarm message, or event.

Format

display fault-management { **alarm** | **active-alarm** | **event** } [**sequence-number** *sequence-number*]

Parameters

Parameter	Description	Value
alarm	Displays information about alarms.	-
active-alarm	Displays information about active alarms.	-
event	Displays information about events.	-
sequence-number *sequence-number*	Specifies the number of an alarm message, active alarm message, or event.	The value is an integer ranging from 0 to 2147483647. When the value is 0, information about all alarm messages, active messages, or events is displayed.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command helps you obtain the contents of all alarm messages or one alarm message on a device.

Example

# Display the contents of active alarm messages in the system.

```
<HUAWEI> display fault-management active-alarm
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  1/Independent/2008-10-13 01:49:45+08:00/-/0x41932001/hwLldpEnabled/Warning/Sta
rt/OID: 1.3.6.1.4.1.2011.5.25.134.2.1 Global LLDP is enabled.
  2/Independent/2008-10-13 01:50:06+08:00/-/0x41932000/lldpRemTablesChange/Warni
ng/Start/OID: 1.0.8802.1.1.2.0.0.1 Neighbor information is changed. (LldpStatsRe
mTablesInserts=1, LldpStatsRemTablesDeletes=0, LldpStatsRemTablesDrops=0, LldpSt
atsRemTablesAgeouts=0)
  5/Independent/2008-10-13 02:22:52+08:00/-/0x40c12014/hwPortPhysicalEthHalfDupl
exAlarm/Minor/Start/OID 1.3.6.1.4.1.2011.5.25.129.2.5.11 The port works in half
duplex mode. (EntityPhysicalIndex=10, BaseTrapSeverity=3, BaseTrapProbableCause=
1024, BaseTrapEventType=8, EntPhysicalName=GigabitEthernet0/0/5, RelativeResourc
e=interface GigabitEthernet0/0/5)
```

19.2.4 display fault-management alarm information (upgrade-compatible command)

Function

The **display fault-management alarm information** command displays registration information about an alarm message.

Format

display fault-management alarm information [*alarm-name*]

Parameters

Parameter	Description	Value
alarm-name	Specifies the name of an alarm message.	The value is a case-sensitive string of 1 to 256 characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

# Check registration information about the alarm message named linkUp.

```
<HUAWEI> display fault-management alarm information linkUp
***********************************
  AlarmName: linkUp
  AlarmType: Resume Alarm
  AlarmLevel: Cleared
  Suppress Period: NA
  CauseAlarmName: linkDown
  Match VB Name: ifIndex
***********************************
```

Table 19-2 Description of the display fault-management alarm information command output

Item	Description
AlarmName	Name of an alarm message
AlarmType	Type of an alarm

Item	Description
AlarmLevel	Level of an alarm
Suppress Period	Suppress period of an alarm
CauseAlarmName	Name of the corresponding root alarm
Match VB Name	Contents of the matching rule set for the alarm messages

19.2.5 dual-active detect mode direct (upgrade-compatible command)

Function

The **dual-active detect mode direct** command enables DAD in direct mode on a specified interface.

By default, DAD is disabled on an interface in a stack.

Format

dual-active detect mode direct

Parameters

None

Views

GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DAD in direct mode applies to a stack containing two DAD-supporting member switches.

Prerequisites

The stack containing two member switches is running properly, and DAD in relay mode is not configured for the stack.

Precautions

Disabling DAD in direct mode on an interface restores the forwarding function on the interface. If a loop exists on the network, a broadcast store occurs.

It is replaced by the **mad detect mode direct** command.

Example

# Configure DAD in direct mode on GigabitEthernet1/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dual-active detect mode direct
Warning: This command will block the port, and no other configuration running on this port is
recommended. Continue?[Y/N]:y
```

19.2.6 dual-active detect mode relay (upgrade-compatible command)

Function

The **dual-active detect mode relay** command enables DAD in relay mode on a specified interface.

By default, DAD is disabled on an interface in a stack.

Format

dual-active detect mode relay

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure DAD in relay mode only when a stack containing two member switches is configured with an inter-chassis Eth-Trunk and a proxy device supports the relay function.

Prerequisites

The stack containing two member switches is running properly, and DAD in direct mode is not configured for the stack.

Precautions

It is replaced by the **mad detect mode relay** command.

Example

# Configure DAD in relay mode on Eth-Trunk 10.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] dual-active detect mode relay
```

19.2.7 dual-active exclude (upgrade-compatible command)

Function

The **dual-active exclude** command excludes specified interfaces of a stack from shutdown.

By default, only physical member ports are excluded from shutdown.

Format

dual-active exclude interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-10>

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-type interface-number2*] }	Specifies the type and number of an interface: ● *interface-type* specifies the type of the interface. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the second interface.	The value of *interface-number2* must be larger than that of *interface-number1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **mad exclude** command.

19.2.8 dual-active relay (upgrade-compatible command)

Function

The **dual-active relay** command enables the relay function on a specified interface of a proxy device.

By default, the relay function is disabled on an interface.

Format

dual-active relay

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

In DAD in relay mode, you need to use the **dual-active relay** command to configure the relay function on a specified Eth-Trunk interface of a proxy device. Member interfaces of the Eth-Trunk interface forward DAD packets to each other so that member switches can exchange DAD packets.

It is replaced by the **mad relay** command.

Example

# Enable the relay function on Eth-Trunk 10 of a proxy device.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 10
[HUAWEI-Eth-Trunk10] dual-active relay
```

19.2.9 dual-active restore (upgrade-compatible command)

Function

The **dual-active restore** command restores the blocked interfaces of the standby switch that enters the Recovery state after its stack splits.

Format

dual-active restore

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a stack splits, if the active switch fails, you can restore the blocked interfaces of the standby switch that enters the Recovery state to make the standby switch to take over the active role.

Precautions

When the active switch is working properly, do not use this command. Otherwise, DAD detects a dual-active scenario again and blocks all service interfaces, causing interface status flapping.

It is replaced by the **mad restore** command.

Example

# Restore all the blocked interfaces of the standby switch that enters the Recovery state after its stack splits.

```
<HUAWEI> system-view
[HUAWEI] dual-active restore
```

19.2.10 fault-management alarm (upgrade-compatible command)

Function

The **fault-management alarm** command configures the type or level of an alarm message or event.

The **undo fault-management alarm** command cancels the type or level of an alarm message or event.

Format

fault-management alarm *alarm-name* **level** *alarm-level*

undo fault-management alarm *alarm-name* [**level**]

Parameters

Parameter	Description	Value
alarm *alarm-name*	Specifies the name of an alarm message or event.	The value is a case-sensitive string of 1 to 64 characters without spaces.

Parameter	Description	Value
level *alarm-level*	Specifies the level of an alarm message or event. Mappings between alarm levels and severity levels: 1. Critical: Indicates that a service affecting condition has occurred and an immediate corrective action is required. Such a severity can be reported. For example, when a managed object becomes totally out of service, its capability must be restored. 2. Major: Indicates that a service affecting condition has developed and an urgent corrective action is required. Such a severity can be reported. For example, when there is a severe degradation in the capability of a managed object, its full capability must be restored. 3. Minor: Indicates the existence of a non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious (for example, service affecting) fault. Such a severity can be reported. For example, when the detected alarm condition is not currently degrading the capacity of the managed object. 4. Warning: Indicates the detection of a potential or impending service affecting fault, before any significant effects have been felt. Action should be taken to further diagnose (if necessary) and correct the problem in order to prevent it from becoming a more serious service affecting fault. 5. Indeterminate: Indicates that the severity level cannot be determined. 6. Cleared: Indicates the clearing of one or more previously reported alarms. This alarm clears all alarms for this managed object that have the same Alarm type, Probable cause and Specific problems (if given). Multiple associated notifications may be cleared by using the Correlated notifications parameter.	The value is a character string. In the X.733 standard, according to the severity level and emergency level, alarm messages are classified into six levels. The more serious event an alarm message indicates, the smaller *alarm-level* is. **Critical** indicates the alarm severity 1; whereas **Cleared** indicates the alarm severity 6.

Views

System view

Default Level

3: Management level

Usage Guidelines

Alarm messages can be classified into root alarm messages and resume-alarm messages. All the alarms are saved on the device.

Events can be classified into critical events and events. Critical events are saved on a device and can be obtained by the NMS. Events are not saved on a device.

The **fault-management alarm** command can be used to promote or degrade the level of an alarm message according to the severity level and emergency level of the alarm message.

Example

# Set the alarm severity of the alarm message named hwCfgManEventlog to major respectively.

```
<HUAWEI> system-view
[HUAWEI] fault-management alarm hwCfgManEventlog level major
```

19.2.11 poe af-inrush enable (upgrade-compatible command)

Function

The **poe af-inrush enable** command changes the power supply standards of interfaces from 802.3at to 802.3af.

The **undo poe af-inrush enable** command restores the power supply standards of interfaces to 802.3at.

By default, interfaces comply with 802.3at.

Format

poe af-inrush enable [**slot** *slot-id*]

undo poe af-inrush enable [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the stack ID.	The value is 0 if stacking is not configured. The value ranges from 0 to 8 if stacking is configured.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, it is replaced by the **poe af-inrush enable** command in the interface view.

19.2.12 reset fault-management (upgrade-compatible command)

Function

The **reset fault-management** command clears all alarm messages.

Format

reset fault-management { **active-alarm** | **event** } [**sequence-number** *sequence-number*]

Parameters

Parameter	Description	Value
active-alarm	Clears information about active alarms.	-
event	Clears event information.	-
sequence-number *sequence-number*	Specifies the number of an alarm message.	The value is an integer ranging from 0 to 2147483647. If the value is 0, it indicates that all alarm messages are cleared.

Views

System view

Default Level

3: Management level

Usage Guidelines

If *sequence-number* is not specified, the system clears all the alarm messages on the device.

NOTICE

After this command is run, all alarm messages on a device are cleared and cannot be restored.

Example

# Clear all active alarm messages.

```
<HUAWEI> system-view
[HUAWEI] reset fault-management active-alarm
```

19.2.13 ntp-service authentication-keyid (upgrade-compatible command)

Function

The **ntp-service authentication-keyid** command sets NTP authentication key.

The **undo ntp-service authentication-keyid** command removes NTP authentication key.

By default, no authentication key is set.

Format

ntp-service authentication-keyid *key-id* **authentication-mode** { **md5** | **hmac-sha256** } **plain** *password-plain*

undo ntp-service authentication-keyid *key-id*

Parameters

Parameter	Description	Value
key-id	Indicates the key number.	Key ID is an integer and ranges from 1 to 4294967295.
authentication-mode md5	Indicates MD5 authentication mode.	-
authentication-mode hmac-sha256	Indicates HMAC-SHA256 authentication mode.	-
plain *password-plain*	Indicates that the configured password is displayed in plain text, and specifies the password. NOTICE If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks.	The password is a string of 1 to 255 case-sensitive characters without spaces.

Views

System view

Default Level

2: Management level

Usage Guidelines

Usage Scenario

On a network that requires high security, the NTP authentication must be enabled. You can configure password authentication between client and server, which guarantee the client only to synchronize with server successfully authenticated, and improve network security. If the NTP authentication function is enabled, a reliable key should be configured at the same time. Keys configured on the client and the server must be identical.

NOTE

In NTP symmetric peer mode, the symmetric active peer functions as a client and the symmetric passive peer functions as a server.

Follow-up Procedure

You can configure multiple keys for each device. After the NTP authentication key is configured, you need to set the key to reliable using the **ntp-service reliable authentication-keyid** command. If you do not set the key to reliable, the NTP key does not take effect.

Precautions

To ensure security, you are advised to use the HMAC-SHA256 algorithm, which is more secure, for NTP authentication.

You can configure a maximum of 1024 keys for each device.

If the NTP authentication key is a reliable key, it automatically becomes unreliable when you delete the key. You do not need to run the **undo ntp-service reliable authentication-keyid** command.

Example

# Set authentication text to **abc** in HMAC-SHA256 authentication with plain option.

```
<HUAWEI> system-view
[HUAWEI] ntp-service authentication-keyid 10 authentication-mode hmac-sha256 plain abc
```

19.3 Interface Management Compatible Commands

19.3.1 Ethernet Interface Compatible Commands

19.3.1.1 error-shutdown auto-recovery cause efm-threshold-event (upgrade-compatible command)

Function

The **error-shutdown auto-recovery cause efm-threshold-event** command enables an interface in error-shutdown state to go Up.

NOTE

An interface enters the error-shutdown state after being shut down due to an error.

Format

error-shutdown auto-recovery cause efm-threshold-event

Parameters

Parameter	Description	Value
cause	Indicates the cause for an interface in error-down state.	-
efm-threshold-event	Indicates that a threshold crossing event occurs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. You can associate an EFM crossing event with an interface. Then the system sets the administrative status of the interface to Down. In this manner, all services on the interface are interrupted.

By default, an interface can only be resumed by a network administrator after being shut down. To configure the interface to restore to the Up state automatically, run the **error-down auto-recovery** command to set an auto recovery.

Example

# Set the auto recovery after an EFM threshold crossing event is associated with an interface.

```
<HUAWEI> system-view
[HUAWEI] error-shutdown auto-recovery cause efm-threshold-event
```

19.3.1.2 error-shutdown auto-recovery interval (upgrade-compatible command)

Function

The **error-shutdown auto-recovery interval** command sets the auto recovery delay.

NOTE

An interface enters the error-shutdown state after being shut down due to an error.

Format

error-shutdown auto-recovery interval *interval-value*

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the auto recovery delay.	The value is an integer that ranges from 30 to 86400, in seconds. ● A smaller value indicates a higher frequency at which an interface alternates between Up and Down states. ● A larger value indicates longer traffic interruption.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an interface can only be resumed by a network administrator after being shut down. To configure the interface to restore to the Up state automatically, run the **error-shutdown auto-recovery interval** command to set an auto recovery delay. After the delay, the interface goes Up automatically.

Example

# Set the auto recovery delay to 50s.

```
<HUAWEI> system-view
[HUAWEI] error-shutdown auto-recovery interval 50
```

19.3.1.3 port-down holdoff-timer (upgrade-compatible command)

Function

Using the **port-down holdoff-timer** command, you can set the delay in reporting a port status change event.

Format

port-down holdoff-timer *interval*

Parameters

Parameter	Description	Value
interval	Specifies the delay timer.	The value is an integer. The value can be 0 or in the range of 50 to 50000, in milliseconds.

Views

GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the cable connected to an interface is faulty, the interface status may change frequently. When this occurs, the system frequently updates the matching entries. If link backup is configured on the interface, active/standby switchovers occur frequently. To prevent frequent status change, you can use the **port-down holdoff-timer** command to set the delay in reporting a port status change event.

If an interface is connected to a wavelength division multiplexing device, the interface becomes Down when a protective switchover occurs on the wavelength division multiplexing device, and services are interrupted. To prevent service interruption, you can set the delay in reporting a port Down event.

Configuration Impact

If you run the **port-down holdoff-timer** command multiple times in the same interface view, only the latest configuration takes effect.

It is replaced by the **carrier** { **up-hold-time** | **down-hold-time** } *interval* command.

Example

# Set the delay in reporting a port status change event to 1000 milliseconds on GigabitEthernet0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet0/0/1
[HUAWEI-GigabitEthernet0/0/1] port-down holdoff-timer 1000
```

19.3.1.4 snmp-agent trap enable port (upgrade-compatible command)

Function

The **snmp-agent trap enable port** command enables the system to generate an alarm when the inbound or outbound bandwidth usage on all Ethernet sub-interfaces exceeds the threshold.

Format

snmp-agent trap enable port { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Enables the system to generate an alarm when the inbound bandwidth usage on all Ethernet sub-interfaces exceeds the threshold.	-
output-rate	Enable the system to generate an alarm when the outbound bandwidth usage on all Ethernet sub-interfaces exceeds the threshold.	-

Views

System review

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

If the threshold for the inbound or outbound bandwidth usage has been configured on an Ethernet sub-interface, you can enable the system to generate an alarm when the threshold is exceeded. This allows you to determine whether the device is functioning normally.

After the configuration is complete, the system generates an alarm when the bandwidth usage exceeds or falls below the threshold.

Example

None

19.4 Ethernet Switching Compatible Commands

19.4.1 MAC Compatible Commands

19.4.1.1 mac-address blackhole (upgrade-compatible command)

Function

Using the **mac-address blackhole** command, you can add a blackhole MAC address entry.

Format

mac-address blackhole *mac-address* [*interface-type interface-number*] **vlan** *vlan-id1* [**ce-vlan** *vlan-id2*]

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address in a MAC address entry.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
interface-type interface-number	Specifies the outbound interface in a MAC address entry. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
vlan *vlan-id1*	Specifies the VLAN ID in the outer VLAN tag.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **mac-address blackhole** command.

19.4.1.2 mac-address static (upgrade-compatible command)

Function

Using the **mac-address static** command, you can add a static MAC address entry .

Format

mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id1*

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address in a MAC address entry.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
interface-type interface-number	Specifies the outbound interface in a MAC address entry. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
vlan *vlan-id1*	Specifies the VLAN ID in the VLAN tag.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **mac-address static vlan**, **mac-address static vlanif**, and **mac-address static vsi** command.

19.4.1.3 port-security maximum (upgrade-compatible command)

Function

The **port-security maximum** command sets the maximum number of MAC addresses that can be learned on an interface.

Format

port-security maximum *max-number*

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of MAC addresses that can be learned by an interface.	The value is an integer that ranges from 1 to 4096.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **port-security max-mac-num** command.

19.4.2 Link Aggregation Compatible Commands

19.4.2.1 mode lacp-static (upgrade-compatible command)

Function

The **mode** command configures the LACP mode of an Eth-Trunk.

Format

mode lacp-static

Parameters

none

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mode lacp** command.

19.4.2.2 lacp e-trunk system-id (Eth-Trunk interface view) (upgrade-compatible command)

Function

The **lacp e-trunk system-id** command configures the Link Aggregation Control Protocol (LACP) system ID of an E-Trunk.

The **undo lacp e-trunk system-id** command deletes the LACP system ID of an E-Trunk.

By default, the LACP system ID is the Ethernet MAC address of the device.

Format

lacp e-trunk system-id *mac-address*

undo lacp e-trunk system-id

Parameters

Parameter	Description	Value
system-id *mac-address*	Specifies the LACP system ID of the E-Trunk.	The value is in the format of H-H-H. An H contains 1 to 4 hexadecimal digits, such as 00e0 and fc01. If an H contains less than four digits, 0s are padded ahead. For example, if an H is specified as e0, it is displayed as 00e0. The LACP system ID cannot be all 0s or all Fs. **NOTE** The LACP system ID cannot be all 0s. If the value is all Fs, it indicates that the LACP system ID is restored to the default.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **lacp system-id** *mac-address* command.

19.4.2.3 snmp-agent trap enable eth-trunk (upgrade-compatible command)

Function

Using the **ssnmp-agent trap enable eth-trunk** command, you can enable the Simple Network Management Protocol (SNMP) trap function on an Eth-Trunk.

Using the **undo snmp-agent trap enable eth-trunk** command, you can disable the SNMP trap function on an Eth-Trunk.

By default, the SNMP trap function is disabled on an Eth-Trunk.

Format

snmp-agent trap enable eth-trunk

undo snmp-agent trap enable eth-trunk

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If the SNMP trap function is enabled on an Eth-Trunk, the system sends a trap to the network management system (NMS) server in case of when the following exceptions occurs:

- The negotiation of the LAG fails.
- The bandwidth of the LAG is lost. For example, if the lower threshold of the number of active interfaces is set by using the **least active-linknumber** command and if the number of active interfaces is smaller than this value, the Eth-Trunk becomes Down and the system sends the trap.
- Part of the bandwidth of the LAG is lost. When one of active interfaces fails, the system sends the trap because the number of active interfaces is reduced.

Example

# Enable the SNMP trap function on an Eth-Trunk so that the trap can be sent to the NMS server promptly when the status of the LAG changes.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable eth-trunk
```

19.4.3 VLAN Compatible Commands

19.4.3.1 port mux-vlan enable (upgrade-compatible command)

Function

The **port mux-vlan enable** command enables the MUX VLAN function on an interface.

The **undo port mux-vlan enable** command disables the MUX VLAN function on an interface.

By default, the MUX VLAN function is disabled on an interface.

Format

port mux-vlan enable

undo port mux-vlan enable

Parameters

None

Views

GE interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **port mux-vlan enable vlan** command.

19.4.4 Voice VLAN Compatible Commands

19.4.4.1 voice-vlan enable (upgrade-compatible command)

Function

The **voice-vlan enable** command enables the voice VLAN function on an interface.

By default, the voice VLAN function is disabled on an interface.

Format

voice-vlan enable

Parameters

None

Views

GE interface view, Ethernet interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **voice-vlan** *vlan-id* **enable** command.

19.4.5 GVRP Compatible Commands

19.4.5.1 garp leaveall timer (upgrade-compatible command)

Function

The **garp leaveall timer** command sets the GARP LeaveAll timer.

Format

garp leaveall timer *timer-value*

Parameters

Parameter	Description	Value
timer-value	Specifies the value of the GARP LeaveAll timer.	The value is an integer that ranges from 65 to 32765 and that can be exactly divided by 5, in centiseconds. The value of the LeaveAll timer must be greater than the values of Leave timers on all the interfaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GARP participant is enabled, the LeaveAll timer is started. When the LeaveAll timer expires, the GARP participant sends LeaveAll messages to request other GARP participants to re-register all its attributes. Then the LeaveAll timer restarts.

Devices on a network may have different settings for the LeaveAll timer. In this case, all the devices use the smallest LeaveAll timer value on the network. When the LeaveAll timer of a device expires, the device sends LeaveAll messages to other devices. After other devices receive the LeaveAll messages, they reset their LeaveAll timers. Therefore, only the LeaveAll timer with the smallest value takes effect even if devices have different settings for the LeaveAll timer.

Prerequisites

Before setting GARP timers on an interface, you must enable GVRP globally.

Precautions

The Leave timer length on an interface is restricted by the global LeaveAll timer length. When configuring the global LeaveAll timer, ensure that all the interfaces that have a GARP Leave timer configured are working properly.

Example

# Set the LeaveAll timer to 510 centiseconds.

```
<HUAWEI> system-view
[HUAWEI] garp leaveall timer 510
```

19.4.6 STP Compatible Commands

19.4.6.1 snmp-agent trap enable mstp (upgrade-compatible command)

Function

The **snmp-agent trap enable mstp** command enables the trap function for the MSTP module.

Format

snmp-agent trap enable mstp

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name mstp** command in the system view.

19.4.6.2 snmp-agent trap enable feature-name mstp (upgrade-compatible command)

Function

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

By default, the trap function is disabled for the MSTP module.

Format

snmp-agent trap enable feature-name mstp trap-name { **nnewroot** | **ntopologychange** }

undo snmp-agent trap enable feature-name mstp trap-name { **nnewroot** | **ntopologychange** }

Parameters

Parameter	Description	Value
trap-name	Enables the traps of spanning tree protocol events of specified types.	-
nnewroot	Enables the device to send trap when the current device is elected as the root bridge.	-
ntopologychange	Enables the device to send trap when the topology changes.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name mstp trap-name** { **newroot** | **topologychange** } command in the system view.

19.4.6.3 stp tc-protection (upgrade-compatible command)

Function

The **stp tc-protection** command enables the trap function for the Topology Change (TC) BPDU protection.

The **undo stp tc-protection** command disables the trap function for the TC BPDU protection.

By default, the trap function for the TC BPDU protection is disabled.

Format

stp tc-protection

undo stp tc-protection

Parameters

None

Views

System view or MST process region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The TC attack defense function is enabled by default, you can run the **stp tc-protection interval** command to set the time that a device needs to process the maximum number of TC BPDUs which is configured using the **stp tc-protection threshold** command. If there are packets exceeding the maximum number, the switch processes the packets after the time specified in the **stp tc-protection interval** command expires. For example, if the time is set to 10 seconds and the maximum number is set to 5, when a switch receives TC BPDUs, the switch processes only the first 5 TC BPDUs within 10 seconds and processes the other TC BPDUs after the time expires. In this way, the device does not frequently update its MAC address entries and ARP entries, reducing CPU usage.

To learn about detailed processing information on TC BPDUs, run the **stp tc-protection** command to enable the trap function for the TC BPDU protection. After the function is enabled, MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.15 hwMstpiTcGuarded and MSTP_1.3.6.1.4.1.2011.5.25.42.4.2.16 hwMstpProTcGuarded are generated.

Precautions

The trap function for the TC BPDU protection takes effect only when the **snmp-agent trap enable feature-name mstp** and **stp tc-protection** are both run.

19.4.7 L2PT Compatible Commands

19.4.7.1 bpdu-tunnel (upgrade-compatible command)

Function

The **bpdu-tunnel** command configures an interface to forward or discard BPDUs.

By default, an interface discards the received BPDUs.

Format

bpdu-tunnel { **enable** | **disable** }

Parameters

Parameter	Description	Value
enable | **disable**	Indicates the action that an interface performs on BPDUs. ● **enable**: The interface discards BPDUs. ● **disable**: The interface forwards BPDUs.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel stp** { **enable** | **disable** } command.

19.4.7.2 bpdu-tunnel enable (upgrade-compatible command)

Function

The **bpdu-tunnel enable** command enables Layer 2 protocol transparent transmission on an interface.

Format

bpdu-tunnel { **all** | *protocol-type* &<1-15> } **enable**

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol. You can specify multiple protocols in the command.	-

Views

Ethernet interface view, XGE interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel** { **all** | { *protocol-type* } &<1-15> | **user-defined-protocol** *protocol-name* } **enable** command.

19.4.7.3 bpdu-tunnel group-mac (upgrade-compatible command)

Function

The **bpdu-tunnel group-mac** command enables the switch to replace the multicast destination MAC address of Layer 2 protocol packets with a specified multicast MAC address.

Format

bpdu-tunnel *protocol-type* **group-mac** *group-mac*

Parameters

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol.	The value is a string of 1 to 31.
group-mac *group-mac*	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel** *protocol-type* **group-mac** *group-mac* command.

19.4.7.4 bpdu-tunnel stp group-mac (upgrade-compatible command)

Function

Using the **bpdu-tunnel stp group-mac** command, you can replace the global well-known MAC address of the STP BPDU packets with a multicast MAC address.

Format

bpdu-tunnel stp group-mac *group-mac*

Parameters

Parameter	Description	Value
group-mac *group-mac*	Specifies the multicast MAC address that replaces the well-known global MAC address of the BPDU packets.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value ranges from 0100-0000-0000 to 01ff-ffff-ffff.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel stp group-mac** *group-mac* command.

19.4.7.5 bpdu-tunnel stp vlan (upgrade-compatible command)

Function

Using the **bpdu-tunnel stp vlan** command, you can configure the interface to accept the BPDU packets whose tag values range from *low-vid* to *high-vid*.

Using the **undo bpdu-tunnel stp vlan** command, you can cancel the configuration.

By default, an interface does not accept the tagged BPDU packets.

Format

bpdu-tunnel stp vlan { *low-vid* [**to** *high-vid*] } &<1-10>

undo bpdu-tunnel stp vlan { *low-vid* [**to** *high-vid*] } &<1-10>

Parameters

Parameter	Description	Value
low-vid	Specifies the start VLAN ID of the BPDU packets that can be accepted by the interface.	The value is a decimal integer ranging from 1 to 4094. It must be smaller than *high-vid*.
high-vid	Specifies the end VLAN ID of the BPDU packets that can be accepted by the interface.	The value is a decimal integer ranging from 1 to 4094. It must be greater than *low-vid*.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel** **stp** { **vlan** *low-id* [**to** *high-id*] } &<1-10> command.

19.4.7.6 bpdu-tunnel vlan (upgrade-compatible command)

Function

The **bpdu-tunnel vlan** command enables VLAN-based Layer 2 protocol transparent transmission on an interface.

Format

bpdu-tunnel { **all** | *protocol-type* &<1-15> } **vlan** { *low-id* [**to** *high-id*] } &<1-10>

Parameters

Parameter	Description	Value
all	Enables or disables transparent transmission of packets of all standard Layer 2 protocols and user-defined Layer 2 protocols.	-
protocol-type	Enables or disables transparent transmission of packets of a specified Layer 2 protocol. You can specify multiple protocols in the command.	-
low-id	Specifies the start VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be smaller than the end VLAN ID.
high-id	Specifies the end VLAN ID.	The value is an integer that ranges from 1 to 4094. The value must be greater than the start VLAN ID.

Views

Ethernet interface view, XGE interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel vlan** command.

19.4.7.7 l2protocol-tunnel user-defined-protocol (upgrade-compatible command)

Function

The **l2protocol-tunnel user-defined-protocol** command defines the characteristics of a Layer 2 protocol whose packets are transparently transmitted, including the protocol name, Ethernet encapsulation type, destination MAC address of packets, multicast MAC address replacing the destination multicast MAC address of packets, and priority of packets.

By default, there is no user-defined characteristics of a Layer 2 protocol whose packets are transparently transmitted.

Format

l2protocol-tunnel user-defined-protocol *protocol-name* **protocol-mac** *protocol-mac* **encape-type** { **ethernetii protocol-type** *protocol-type* | **llc dsap** *dsap-value* **ssap** *ssap-value* | **snap protocol-type** *protocol-type* } **group-mac** { *group-mac* | **default-group-mac** } [**priority** *priority-id*]

Parameters

Parameter	Description	Value
protocol-name	Specifies the name of a user-defined Layer 2 protocol whose packets are transparently transmitted.	The name is a string of 1 to 31 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
protocol-mac *protocol-mac*	Specifies the destination multicast MAC address of the Layer 2 protocol packets that are transparently transmitted. This MAC address must be an ordinary MAC address that has not been used on the S1720, S2700, S5700, and S6720.	The address is in the format of H-H-H, H indicating a 4-bit hexadecimal number.

Parameter	Description	Value
encape-type	Defines the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **ethernetii**: indicates Ethernet_II, the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **llc**:: indicates Logical Link Control (LLC), the encapsulation format for Layer 2 protocol packets that are transparently transmitted. ● **snap**: indicates Sub-Network Access Protocol (SNAP), the encapsulation format for Layer 2 protocol packets that are transparently transmitted. When transparently-transmitted Layer 2 protocol packets carry the same protocol MAC address and protocol type, you can use the parameter **encap-type** to define different encapsulation formats to differentiate these packets.	-
protocol-type *protocol-type*	Specifies the value of Ethernet encapsulation type.	The value is a hexadecimal number ranging from 0600 to FFFF.
dsap *dsap-value*	Specifies the destination service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.
ssap *ssap-value*	Specifies the source service access point.	The value ranges from 0x00 to 0xff, in hexadecimal format.
group-mac *group-mac*	Specifies the multicast MAC address that replaces the destination multicast MAC address of the Layer 2 protocol packets that are transparently transmitted. The address must be an ordinary MAC address, which cannot be the MAC address of bridge protocol data units (BPDUs), the MAC address of Smart Link protocol packets, or a special MAC address.	The address is in the format of H-H-H, H indicating a 4-bit hexadecimal number.

Parameter	Description	Value
default-group-mac	Specifies the default MAC address of a multicast group, which is 0100-0ccd-cdd0. This parameter can simplify the configuration and reduce the configuration error. For example: Most Layer 2 protocols can be classified by types. Default MAC addresses of Layer 2 protocols in the same type are the same. In this case, you can attach the parameter **default-group-mac** to the **l2protocol-tunnel user-defined-protocol** command to reduce the configuration workload and the probability of configuration error.	-
priority *priority-id*	Specifies the priority of the Layer 2 protocol packets that are transparently transmitted.	The value is an integer that ranges from 1 to 7. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the upgrade, it is replaced by the **l2protocol-tunnel user-defined-protocol** command.

19.5 IP Service Compatible Commands

19.5.1 ARP Compatible Commands

19.5.1.1 arp learning ip-network-cross enable (upgrade-compatible command)

Function

The **arp learning ip-network-cross enable** command enables inter-network segment ARP learning on interfaces.

Format

arp learning ip-network-cross enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In V200R010C00 and later versions, inter-network segment ARP learning is disabled on interfaces by default. If the system software of a switch is upgraded from V200R005C00 or a later version to V200R010C00SPC600 or a later version, inter-network segment ARP learning is enabled on interfaces. If you run the **display this include-default** command in the system view after the configuration is restored, the command output includes **arp learning ip-network-cross enable**.

Precautions

This command can be used only in the configuration restoration stage. After the configuration is restored, you cannot configure this command manually.

19.5.2 DHCP Upgrade-compatible Commands

19.5.2.1 expired (upgrade-compatible command)

Function

The **expired** command sets the lease for IP addresses in a global IP address pool.

By default, the lease of IP addresses is one day.

Format

expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer ranging from 0 to 999, in days. The default value is 1.
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer ranging from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer ranging from 0 to 59, in minutes. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **expired-hide** command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment. Different hosts require different IP address leases. For example, if some hosts such as a DNS server need to use certain IP addresses for a long time, configure **expired** as **unlimited** to set the IP address lease of the specified global address pool to unlimited. If some hosts such as a portable computer just need to user temporary IP addresses, set the IP address lease of the specified global address pool to the required time so that the expired IP addresses can be released and assigned to other clients.

When a DHCP client starts or half of its IP address lease has passed, the DHCP client sends a DHCP Request packet to the DHCP server to renew the lease. If the IP address can still be assigned to the client, the DHCP server informs a renewed IP address lease to the client. If the IP address can no longer be assigned to this client, the DHCP server informs the client that the IP address lease cannot be renewed and it needs to apply for another IP address.

Prerequisites

Run the **ip pool** command to create a global IP address pool and the **dhcp enable** command to globally enable the DHCP server function.

Precautions

Different IP address leases can be specified for different global IP address pools on a DHCP server. In a global IP address pool, all addresses have the same lease.

Example

# Specify the IP address lease of the global address pool global1 to 1 day 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] expired  day 1 hour 2 minute 30
```

19.5.2.2 dhcp server expired (upgrade-compatible command)

Function

The **dhcp server expired** command sets the lease for IP addresses in an interface IP address pool.

By default, the lease of IP addresses is one day.

Format

dhcp server expired { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

Parameters

Parameter	Description	Value
day	Specifies the number of days in the IP address lease.	The value is an integer ranging from 0 to 999, in days. The default value is 1.
hour	Specifies the number of hours in the IP address lease.	The value is an integer ranging from 0 to 23, in hours. The default value is 0.
minute	Specifies the number of minutes in the IP address lease.	The value is an integer ranging from 0 to 59, in minutes. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server expired** command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment. Different hosts require different IP address leases. For example, if some hosts such as a DNS server need to use certain IP addresses for a long time, run the **dhcp server expired unlimited** command to set the IP address lease of the specified VLANIF interface address pool to unlimited. If some hosts such as a portable computer just need to user temporary IP addresses, run the **dhcp server expired** command to set the IP address lease of the specified VLANIF interface address pool to the required time so that the expired IP addresses can be released and assigned to other clients.

When a DHCP client starts or half of its IP address lease has passed, the DHCP client sends a DHCP Request packet to the DHCP server to renew the lease. If the IP address can still be assigned to the client, the DHCP server informs the client of a renewed IP address lease. If the IP address can no longer be assigned to this client, the DHCP server informs the client that the IP address lease cannot be renewed.

Prerequisites

Run the **dhcp enable** command to globally enable the DHCP function. Run the **dhcp select interface** command in the VLANIF interface view to enable the interface IP address pool.

Precautions

Different IP address leases can be specified for different interface IP address pools on a DHCP server. In an interface IP address pool, all IP addresses have the same lease.

Example

# Set the IP address lease of the IP address pool on VLANIF 100 to 2 days 2 hours and 30 minutes.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ip address 10.1.1.1 24
[HUAWEI-Vlanif100] dhcp select interface
[HUAWEI-Vlanif100] dhcp server expired day 2 hour 2 minute 30
```

19.5.2.3 dhcp server forbidden-ip (upgrade-compatible command)

Function

The **dhcp server forbidden-ip** command specifies the range of IP addresses that cannot be assigned to clients by the DHCP server.

By default, the system does not configure the range of IP addresses that cannot be assigned to clients by the DHCP server.

Format

dhcp server forbidden-ip *start-ip-address* [*end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address that cannot be automatically assigned.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address that cannot be automatically assigned. If *end-ip-address* is not specified, only *start-ip-address* cannot be assigned to clients.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server forbidden-ip** command applies to DHCP servers. In an IP address pool, some IP addresses need to be reserved for other services, and some IP addresses are statically assigned to certain hosts (such as the DNS server) and cannot be automatically assigned to clients. You can run the **dhcp server forbidden-ip** command to specify the range of the IP addresses that cannot be automatically assigned to clients from the IP address pool.

Precautions

- The excluded IP address must be in the IP address pool range.
- The excluded IP address or IP address segment cannot be automatically assigned to clients from a local address pool.
- If you run the **dhcp server forbidden-ip** command multiple times, you can specify multiple IP addresses or IP address segments that cannot be automatically assigned to clients from the specified address pool.

Example

# Configure that IP addresses in the address pool 10.10.10.10 to 10.10.10.20 cannot be automatically assigned to clients.

```
<HUAWEI> system-view
[HUAWEI] dhcp server forbidden-ip 10.10.10.10 10.10.10.20
```

19.5.2.4 dhcp server ip-pool (upgrade-compatible command)

Function

The **dhcp server ip-pool** command creates a global IP address pool.

The **undo dhcp server ip-pool** command deletes a global IP address pool.

By default, no IP address pool is created.

Format

dhcp server ip-pool *pool-name*

undo dhcp server ip-pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of a global IP address pool.	The value is a string of 1 to 64 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp server ip-pool** command applies to DHCP servers. When configuring a DHCP server, run the **dhcp server ip-pool** command to create an IP address pool and set parameters for the IP address pool, including a gateway address, the IP address lease, and a VPN instance. Then the configured DHCP server can assign IP addresses in the IP address pool to clients. If IP addresses in a global IP address pool are in use, this global address pool cannot be deleted.

Example

# Create a global IP address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] dhcp server ip-pool pool1
```

19.5.2.5 dhcp server ping (upgrade-compatible command)

Function

Using the **dhcp server ping** command, you can configure the maximum number of ping packets and the longest response-wait time for each ping packet.

By default, the DHCP server sends 2 ping packets and the maximum response time is 500 ms.

Format

dhcp server ping packets *packets-number*

dhcp server ping packets *packets-number* **timeout** *milliseconds*

dhcp server ping timeout *milliseconds* **packets** *packets-number*

Parameters

Parameter	Description	Value
packets *packets-number*	Specifies the maximum number of ping packets to be sent.	The value is an integer that ranges from 0 to 10.
timeout *milliseconds*	Specifies the maximum response time of a ping packet.	The value is an integer that ranges from 0 to 10000, in milliseconds. The value 0 indicates that no ping operation is performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The DHCP server detects the address usage by sending ping packets. This avoids address collision caused by the repeated allocation of IP addresses.

Example

# Set the maximum number of ping packets to be sent to 5.

```
<HUAWEI> system-view
[HUAWEI] dhcp server ping packets 5
```

19.5.2.6 dns-suffix (upgrade-compatible command)

Function

The **dns-suffix** command configures the domain name suffix to be assigned by the DHCP server to a DHCP client.

By default, no domain name suffix is configured for a DHCP client.

Format

dns-suffix *domain-name*

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name suffix to be assigned to a DHCP client.	The value is a string of 1 to 50 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dns-suffix** command applies to DHCP servers. Each client has a domain name. To enable DHCP clients to communicate by using their domain names and prevent IP address conflicts, the DHCP server needs to specify domain name suffixes for these clients when allocating IP addresses to them. On the DHCP server, the **dns-suffix** command specifies a domain name suffix for each global address pool. When allocating IP addresses to clients, the DHCP server also sends the domain name suffixes to the clients. During domain name resolution, users only need to enter a part of the domain name, and then the system uses a complete domain name suffix for resolution.

Precautions

If no domain name suffix is configured for a global IP address pool, the DHCP server cannot send a domain name suffix to clients. In this situation, the clients cannot communicate.

Example

# Configure **mydomain.com.cn** as the domain name suffix of the IP address pool **pool1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool pool1
[HUAWEI-ip-pool-pool1] dns-suffix mydomain.com.cn
```

19.5.2.7 ip relay address (upgrade-compatible command)

Function

Using the **ip relay address** command, you can configure DHCP server addresses on a VLANIF interface enabled with DHCP relay.

Using the **undo ip relay address** command, you can delete the configured DHCP server addresses.

By default, no DHCP server address is configured on a VLANIF interface enabled with DHCP relay.

Format

ip relay address *ip-address*

undo ip relay address { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.
all	Deletes all the DHCP server addresses configured on an interface.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip relay address** command is applicable to DHCP relay agents. When a DHCP client needs to send a DHCP request packet to a DHCP server on a different network segment by using a DHCP relay agent, run the **ip relay address** command on the DHCP relay agent to configure a DHCP server address.

Prerequisites

DHCP relay has been enabled on the VLANIF interface by using the **dhcp select relay** command.

Precautions

If you run the **ip relay address** command multiple times, multiple DHCP server addresses are configured.

Example

# Configure DHCP server addresses 10.2.2.2 on VLANIF100 enabled with DHCP relay.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] dhcp select relay
[HUAWEI-Vlanif100] ip relay address 10.2.2.2
```

19.5.2.8 lease (upgrade-compatible command)

Function

The **lease** command sets the lease for IP addresses in a global IP address pool.

By default, the lease of IP addresses is one day.

Format

lease *day* [*hour* [*minute*]]

Parameters

Parameter	Description	Value
day	Specifies the number of days in the IP address lease.	The value is an integer ranging from 0 to 999, in days. The default value is 1.
hour	Specifies the number of hours in the IP address lease.	The value is an integer ranging from 0 to 23, in hours. The default value is 0.
minute	Specifies the number of minutes in the IP address lease.	The value is an integer ranging from 0 to 59, in minutes. The default value is 0.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

After the upgrade, it is replaced by the **lease** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } command.

Example

# Specify the IP address lease of the global address pool **global1** to 1 day.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] lease 1
```

19.5.2.9 static-bind mac-address (upgrade-compatible command)

Function

The **static-bind mac-address** command binds a MAC address to a global IP address pool.

Format

static-bind mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind mac-address** command applies to DHCP servers. If some special clients such as the DNS server need to be statically assigned fixed IP addresses, run the **static-bind mac-address** command to bind fixed IP addresses to MAC addresses of these clients. When receiving a request for applying for an IP address from a special client, a DHCP server assigns the fixed IP address bound to the client's MAC address to this client.

Prerequisites

Run the **ip pool** command to create a global IP address pool and the **dhcp enable** command to globally enable the DHCP server function.

Example

# Bind a MAC address 2020-e2f3-2a3b to the global IP address pool **global1**.

```
<HUAWEI> system-view
[HUAWEI] ip pool global1
[HUAWEI-ip-pool-global1] static-bind mac-address 2020-e2f3-2a3b
```

19.5.2.10 dhcpv6 relay destination (upgrade-compatible command)

Function

The **dhcpv6 relay destination** command enables the DHCPv6 relay function on interfaces and configures the IPv6 address of the DHCPv6 server or next-hop relay agent.

By default, the DHCPv6 relay function is disabled on an interface.

Format

dhcpv6 relay destination *ipv6-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the destination address of relay messages, which can be the IPv6 address of the DHCPv6 server or next hop relay agent.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of the outbound interface of relay messages.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a client applies to a DHCPv6 server on a different network segment for an IPv6 address, you need to deploy a relay agent between the client and the DHCPv6 server. In this manner, the relay agent transmits DHCPv6 messages exchanged between the client and the DHCPv6 server.

19.6 IP Multicast Compatible Commands

19.6.1 MLD Snooping Compatible Commands

19.6.1.1 mld-snooping group-policy (interface view) (upgrade-compatible command)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy on an interface.

Format

mld-snooping group-policy *acl6-number* **vlan** *vlan-id mld-version* [**default-permit**]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 to 3999.
vlan *vlan-id*	Applies the IPv6 multicast group policy to a specified VLAN on an interface.	The value is an integer that ranges from 1 to 4094.

Parameter	Description	Value
mld-version	Specifies an MLD version. The multicast group policy is applied only to the MLD messages of this version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. ● 1: MLDv1 ● 2: MLDv2
default-permit	Configures the multicast group policy to permit all groups by default. That is, if the referenced ACL has no rules, the multicast group policy allows hosts in the VLAN to join all groups.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

# Prevent MLDv2 hosts in VLAN 10 on GE0/0/1 from joining IPv6 multicast group ff1c::3/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2000
[HUAWEI-acl6-basic-2000] rule deny source ff1c::3/32
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] mld-snooping enable
[HUAWEI-vlan10] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[HUAWEI-GigabitEthernet0/0/1] mld-snooping group-policy 2000 vlan 10 2 default-permit
```

19.6.1.2 mld-snooping group-policy (VLAN view) (upgrade-compatible command)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy in a VLAN.

Format

mld-snooping group-policy *acl6-number mld-version* [**default-permit**]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 to 3999.
mld-version	Applies the multicast group policy only to the MLD messages of the specified version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 3. ● 1: MLDv1 ● 2: MLDv2
default-permit	Configures the multicast group policy to permit all groups by default. That is, if the referenced ACL has no rules, the multicast group policy allows hosts in the VLAN to join all groups.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

# Prevent MLDv2 hosts in VLAN 4 from joining IPv6 multicast group ff1e::1/32.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 2001
[HUAWEI-acl6-basic-2001] rule deny source ff1e::1/32
[HUAWEI-acl6-basic-2001] quit
[HUAWEI] mld-snooping enable
[HUAWEI] vlan 4
[HUAWEI-vlan4] mld-snooping enable
[HUAWEI-vlan4] mld-snooping group-policy 2001 2 default-permit
```

19.7 MPLS compatible command

19.7.1 explicit-path (upgrade-compatible command)

Function

Using the **explicit-path** command, you can configure an explicit path of a tunnel.

By default, no explicit path of a tunnel is configured.

Format

explicit-path *path-name* { **enable** | **disable** }

Parameters

Parameter	Description	Value
path-name	Indicates the name of an explicit path.	The value is a string of 1 to 31 characters.
enable	Enables the explicit path of a tunnel.	-
disable	Disables the explicit path of a tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can configure an explicit path only after MPLS TE is enabled.

The addresses of the hops along the explicit path cannot overlap or loops cannot occur. If a loop occurs, CSPF detects the loop and fails to calculate the path.

When the explicit path is in use, you cannot perform the following operations:

- Run the **explicit-path** *path-name* **disable** command to disable the explicit path.
- Run the **undo explicit-path** command to delete the explicit path.

Example

# Create an explicit path named **path1**.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls te
[HUAWEI-mpls] quit
[HUAWEI] explicit-path path1 enable
[HUAWEI-explicit-path-path1]
```

19.7.2 mpls rsvp-te authentication handshake (upgrade-compatible command)

Function

The **mpls rsvp-te authentication handshake** command configures the RSVP-TE handshake mechanism and sets a local password.

The **undo mpls rsvp-te authentication handshake** command deletes the RSVP-TE handshake mechanism configuration.

By default, no RSVP-TE handshake mechanism is configured.

Format

mpls rsvp-te authentication handshake *local-secret*

undo mpls rsvp-te authentication handshake

Parameters

Parameter	Description	Value
local-secret	Specifies the local password.	The value is a string of 8 to 40 characters without spaces. It has no default value.

Views

VLANIF interface view, GE interface view, XGE interface view, 40GE interface view, Eth-trunk interface view, RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism and sets the local password.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication handshake** command can be used to configure the RSVP-TE handshake mechanism and sets the local password to prevent anti-replay and improve network security.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* } command in the interface view or the MPLS RSVP-TE neighbor view.

Precautions

local-secret is valid only on the local device and can be different from *local-secret* configured on neighbors.

Example

# Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] mpls
[HUAWEI-Vlanif100] mpls te
[HUAWEI-Vlanif100] mpls rsvp-te
[HUAWEI-Vlanif100] mpls rsvp-te authentication cipher beijing123
[HUAWEI-Vlanif100] mpls rsvp-te authentication handshake 12345678
```

# Configure the RSVP-TE handshake mechanism.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] undo portswitch
[HUAWEI-GigabitEthernet0/0/1] mpls
[HUAWEI-GigabitEthernet0/0/1] mpls te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication cipher beijing123
[HUAWEI-GigabitEthernet0/0/1] mpls rsvp-te authentication handshake 12345678
```

19.7.3 mpls rsvp-te send-message (upgrade-compatible command)

Function

The **mpls rsvp-te send-message** command configures the formats of objects in a sent message.

The **undo mpls rsvp-te send-message** command restores the default configuration.

By default, the formats of objects in the sent message are not configured.

Format

mpls rsvp-te send-message suggest-label exclude

undo mpls rsvp-te send-message suggest-label exclude

Parameters

Parameter	Description	Value
suggest-label exclude	Indicates that an RSVP message does not carry the suggest-label object.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls rsvp-te send-message** command controls the formats of objects in the messages sent by nodes. If required, you can use this command to adjust the transmission of messages so that downstream nodes can use the carried object format in processing.

Precautions

The modification takes effect only for new LSPs.

Configurations of the four formats of objects in a sent message can take effect simultaneously.

Example

# Exclude the suggest-label object from a message.

```
<HUAWEI> system-view
[HUAWEI] mpls
[HUAWEI-mpls] mpls rsvp-te send-message suggest-label exclude
```

19.7.4 mpls te max-reservable-bandwidth (upgrade-compatible command)

Function

The **mpls te max-reservable-bandwidth** command sets the maximum reservable bandwidth of a link.

The maximum reservable bandwidth of a link is not configured by default.

Format

mpls te max-reservable-bandwidth *bw-value* [**bc1** *bc1-bw-value*]

Parameters

Parameter	Description	Value
bw-value	Specifies the maximum reservable link bandwidth.	The value is an integer ranging from 0 to 40000000, in kbit/s. The default value is 0.
bc1 *bc1-bw-value*	Specifies the maximum reservable bandwidth for a BC1 link.	The value is an integer ranging from 0 to 40000000, in kbit/s. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **mpls te bandwidth max-reservable-bandwidth** command.

19.7.5 mpls te bypass-tunnel bandwidth (upgrade-compatible command)

Function

Using the **mpls te bypass-tunnel bandwidth** command, you can configure the bypass LSP bandwidth.

By default, no bypass LSP bandwidth is configured.

Format

mpls te bypass-tunnel bandwidth { *bandwidth* | { **bc0** | **bc1** } { *bandwidth* | **un-limited** } }

Parameters

Parameter	Description	Value
bandwidth	Specifies the bandwidth that the bypass tunnel can protect.	The value is an integer that ranges from 1 to 32000000, in kbit/s.
bc0	Indicates the BC0 bandwidth (global bandwidth) that the bypass tunnel can protect.	-
bc1	Indicates the BC1 bandwidth (subaddress pool bandwidth) that the bypass tunnel can protect.	-
un-limited	Indicates that there is no limit on the total bandwidth that can be protected.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The total bandwidth of LSPs protected by the bypass tunnel is not more than the bandwidth of the primary tunnel. When multiple bypass tunnels exist, the system selects a single bypass tunnel through the best-fit algorithm.

The total bandwidth of all the LSPs protected by the bypass tunnel is not greater than the bandwidth of the primary tunnel. When multiple bypass tunnels exist, the system determines the bypass tunnel through the best-fit algorithm.

Example

# Configure Tunnel1 to protect the LSPs that use the BC0 bandwidth and set no limit on the bandwidth to be protected.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol mpls te
[HUAWEI-Tunnel1] destination 2.2.2.2
[HUAWEI-Tunnel1] mpls te tunnel-id 100
[HUAWEI-Tunnel1] mpls te bypass-tunnel bandwidth bc0 un-limited
[HUAWEI-Tunnel1] mpls te commit
```

19.7.6 mpls te protect-switch manual (upgrade-compatible command)

Function

The **mpls te protect-switch manual** command sends a manual switchover request to a specified tunnel.

By default, no manual switching request for a specified tunnel is configured.

Format

mpls te protect-switch manual [**work-lsp** | **protect-lsp**]

Parameters

Parameter	Description	Value
work-lsp	Switches traffic manually to the primary tunnel.	-
protect-lsp	Switches traffic manually to a protection tunnel.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **mpls te protect-switch manual** command.

19.7.7 snmp-agent trap enable (MPLS) (upgrade-compatible command)

Function

The **snmp-agent trap enable** command enables SNMP traps with a related parameter.

The **undo snmp-agent trap enable** command disables SNMP traps with a related parameter.

Format

snmp-agent trap enable { **static-lsp** | **ldp** | **lsp** [**mplsxcup** | **mplsxcdown**] | **tunnel-ps** | **te** { **tunnel-reop** | **te-frr** [**private**] | **hot-standby** | **ordinary** | **bandwidth-change** } | [**te**] **tunnel** }

undo snmp-agent trap enable { **static-lsp** | **ldp** | **lsp** [**mplsxcup** | **mplsxcdown**] | **tunnel-ps** | **te** { **tunnel-reop** | **te-frr** [**private**] | **hot-standby** | **ordinary** | **bandwidth-change** } | [**te**] **tunnel** }

Parameters

Parameter	Description	Value
static-lsp	Enables the trap of static LSPs.	-
ldp	Enables LDP traps.	-
lsp mplsxcup	Enables the mplsXCUp trap.	-
lsp mplsxcdown	Enables the mplsXCDown trap.	-
tunnel-ps	Enables the TE protection switching trap.	-
te tunnel-reop	Enables trap of the TE route re-optimization.	-
te te-frr	Enables the public trap of TE FRR.	-
te-frr private	Enables the private trap of TE FRR.	-
te hot-standby	Enables the trap of the hot-standby CR-LSP.	-
te ordinary	Enables the trap of the ordinary CR-LSP.	-
bandwidth-change	Enables the system to send related private traps when the tunnel bandwidth changes.	-
tunnel	Enables the trap of the tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the trap function is disabled in the process of the MPLS LSP establishment.

To check the status of an LSP, run the **snmp-agent trap enable lsp** { **mplsxcup** | **mplsxcdown** } command when mplsXCUp or mplsXCDown is enabled.

After the **undo snmp-agent trap enable** command is run, information about mplsXCUp or mplsXCDown is not displayed, and the status of the trap is unchanged. When you run the **snmp-agent trap enable** command again, information about the restored trap is displayed.

Example

# Enable the private trap of TE FRR.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable te te-frr private
```

# Enable the mplsXCUp trap.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable lsp mplsxcup
 Warning: Enabling the alarm function will lead to the generation of excessive a
larms. Continue? [Y/N]
```

19.7.8 snmp-agent trap enable feature-name ldp (upgrade-compatible command)

Function

The **snmp-agent trap enable feature-name ldp** command enables the trap for the MPLS LDP module.

The **undo snmp-agent trap enable feature-name ldp** command disables the trap for the MPLS LDP module.

By default, the trap is disabled for the MPLS LDP module.

Format

snmp-agent trap enable feature-name ldp trap-name { **session-down** | **session-up** }

undo snmp-agent trap enable feature-name ldp trap-name { **session-down** | **session-up** }

Parameters

Parameter	Description	Value
trap-name	Enables the trap of MPLS LDP events of a specified type.	-
session-down	Enables the trap of the event that an LDP session goes Down in the MIB.	-
session-up	Enables the trap of the event that an LDP session goes Up in the MIB.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **snmp-agent trap enable feature-name ldp** command to enable the LDP session trap. Currently, all traps of the MPLS LDP module are non-excessive trap. The frequent LDP session status changes do not trigger a large number of traps.

Example

# Enable the trap of the event that an LDP session is reestablished.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name ldp trap-name session-up
```

19.7.9 static-cr-lsp ingress bandwidth (upgrade-compatible command)

Function

Using the **static-cr-lsp ingress bandwidth** command, you can configure a static CR-LSP and specify its bandwidth on the ingress LSR.

By default, no static CR-LSP on the ingress LSR is configured.

Format

static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* } **destination** *destination-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* **bandwidth** { **bc0** | **bc1** } *bandwidth*

Parameters

Parameter	Description	Value
tunnel-interface tunnel *interface-number*	Specifies the tunnel interface of a static CR-LSP. *interface-number* indicates the tunnel interface number.	-
tunnel-name	Specifies the name of a CR-LSP.	The name is a string of 1 to 19 case-sensitive characters, spaces and abbreviation not supported. If you use the **interface Tunnel 2** command to create a tunnel interface for a static CR-LSP, the tunnel name in the **static-cr-lsp ingress** command must be formatted as "Tunnel2", otherwise, the tunnel cannot be created. There is no such a limit for the transit node and egress node.
destination *destination-address*	Specifies the destination IP address of a static CR-LSP.	-
nexthop *next-hop-address*	Specifies the next-hop IP address of a static CR-LSP.	-
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outgoing interface. This parameter is only applicable to a P2P link.	-
out-label *out-label*	Specifies the value of an outgoing label.	*out-label* is an integer ranging from 16 to 1048575.
bc0	Specifies BC0 bandwidth of a static CR-LSP.	-
bc1	Specifies BC1 bandwidth of a static CR-LSP.	-
bandwidth	Specifies the bandwidth required by a CR-LSP.	The value ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions.

Example

# Configure the static CR-LSP named Tunnel1, with the destination IP address being 10.1.3.1, the next-hop address being 10.1.1.2, the outgoing label being 237, and the required bandwidth being 20 kbit/s from BC0 on the ingress.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp ingress tunnel-interface Tunnel 1 destination 10.1.3.1 nexthop 10.1.1.2 out-
label 237 bandwidth bc0 20
```

19.7.10 static-cr-lsp transit bandwidth (upgrade-compatible command)

Function

Using the **static-cr-lsp transit bandwidth** command, you can configure a static CR-LSP and specify its bandwidth on a transit LSR.

By default, no static CR-LSP on a transit LSR is configured.

Format

static-cr-lsp transit *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* **bandwidth** { **bc0** | **bc1** } *bandwidth* [**description** *description*]

Parameters

Parameter	Description	Value
lsp-name	Specifies the CR-LSP name.	The name is a string of 1 to 19 case-sensitive characters, spaces not supported.
incoming-interface *interface-type interface-number*	Specifies the name of an incoming interface.	-
in-label *in-label*	Specifies the value of an incoming label.	An integer ranging from 16 to 1023
nexthop *next-hop-address*	Specifies the next-hop address.	-
outgoing-interface *interface-type interface-number*	Specifies the name of an outgoing interface.	-

Parameter	Description	Value
out-label *out-label*	Specifies the value of an outgoing label.	An integer ranging from 16 to 1048575.
bc0	Obtains the bandwidth from BC0.	-
bc1	Obtains the bandwidth from BC1.	-
bandwidth	Specifies the bandwidth required by a CR-LSP.	The value ranges from 0 to 4000000000, in kbit/s. The default value is 0.
description *description*	Specifies the description information.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions.

Example

# Configure the static CR-LSP named tunnel34, with the incoming interface being VLANIF10, the incoming label being 123, the outgoing interface being VLANIF20, the outgoing label as 253, the required BC0 bandwidth being 20 kbit/s on the transit node.

```
<HUAWEI> system-view
[HUAWEI] static-cr-lsp transit tunnel34 incoming-interface vlanif 10 in-label 123 outgoing-interface
vlanif 20 out-label 253 bandwidth bc0 20
```

19.7.11 undo mpls te auto-frr (upgrade-compatible command)

Function

The **undo mpls te auto-frr** command disables MPLS TE Auto FRR in the interface view.

Format

undo mpls te auto-frr

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mpls te auto-frr block** command.

19.8 VPN compatible command

19.8.1 display ipv6 prefix-limit statistics (upgrade-compatible command)

Function

The **display ipv6 prefix-limit statistics** command displays the statistics of the prefix limits of IPv6 VPN instances.

Format

display ipv6 prefix-limit { **all-vpn6-instance** | **vpn6-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn6-instance	Indicates all IPv6 VPN instances.	-
vpn6-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipv6 prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified IPv6 VPN instance.

Example

# Display the statistics of the prefix limits of all IPv6 VPN instances.

```
<HUAWEI> display ipv6 prefix-limit all-vpn6-instance statistics
------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
        DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0             0            0
STATIC        0              0           0             0            0
OSPFv3       11              3           1             0            5
IS-IS       106              0           1             0            5
RIPng        98              0           1             1            5
BGP           2              0           1             1            5
------------------------------------------------------------------------------
IPv6 VPN instance name: VPN123

        DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0             0            0
STATIC        0              0           0             0            0
OSPFv3       11              3           1             0            5
IS-IS       106              0           1             0            5
RIPng        98              0           1             1            5
BGP           2              0           1             1            5
```

Table 19-3 Description of the display ipv6 prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

# Display the statistics of the prefix limit of the IPv6 VPN instance named **vrf1**.

```
<HUAWEI> display ipv6 prefix-limit vpn6-instance vrf1 statistics
-------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
          DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT          0                0            0               0              0
STATIC          0                0            0               0              0
OSPFv3         11                3            1               0              5
IS-IS         106                0            1               0              5
RIPng          98                0            1               1              5
BGP             2                0            1               1              5
```

19.8.2 display ipv6 vpn-instance (upgrade-compatible command)

Function

The **display ipv6 vpn6-instance** command displays information about an IPv6 VPN instance.

Format

display ipv6 vpn6-instance [**brief** | **verbose**] [*vpn6-instance-name*]

Parameters

Parameter	Description	Value
brief	Displays summary information about an IPv6 VPN instance.	-
verbose	Displays detailed information about the IPv6 VPN instances and their associated interfaces.	-

Parameter	Description	Value
vpn6-instance-name	Specifies the name of an IPv6 VPN instance.	The name is a string of 1 to 31 case-sensitive characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a VPN instance is configured, you can check the configuration of the instance by using the **display ipv6 vpn6-instance** command. You can also use this command to view the VPN instances configured on the local device.

When no parameters are specified, the command displays brief information about all the configured VPN instances.

Example

# View brief information about all the configured IPv6 VPN instances.

```
<HUAWEI> display ipv6 vpn6-instance
 Total VPN-Instances configured      : 3
 Total IPv4 VPN-Instances configured : 2
 Total IPv6 VPN-Instances configured : 1

  VPN-Instance Name               RD                    Address-family
  vpn1
  vpna                          100:1                 IPv4
  vpna                          100:3                 IPv6
  vpnb                          100:2                 IPv4
```

Table 19-4 Description of the display ip vpn-instance command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name	Name of the VPN instance.

Item	Description
RD	RD of the VPN instance IPv4 address family or IPv6 address family.
Creation Time	Time when an IPv4 or IPv6 address family is enabled for the VPN instance.
Address-family	Address family enabled for the VPN instance. The address family can be: ● Null, if no address family is enabled. ● ipv4, if only the IPv4 address family is enabled. ● ipv6, if only the IPv6 address family is enabled.

```
<HUAWEI> display ipv6 vpn6-instance brief
 Total VPN-Instances configured      : 3
 Total IPv4 VPN-Instances configured : 2
 Total IPv6 VPN-Instances configured : 1

  VPN-Instance Name              RD                  Address-family
  vpn1
  vpna                        100:1               IPv4
  vpna                        100:3               IPv6
  vpnb                        100:2               IPv4
```

# View detailed information about all IPv6 VPN instances.

```
<HUAWEI> display ipv6 vpn-instance verbose
 Total VPN-Instances configured      : 1
 Total IPv4 VPN-Instances configured : 1
 Total IPv6 VPN-Instances configured : 1

 VPN-Instance Name and ID : vpna, 6
  Description : vpna-1
  Service ID : 12
  Interfaces : Vlanif10
 Address family ipv4
  Create date : 2012/12/3 15:36:20 UTC+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Route Distinguisher : 100:1
  Export VPN Targets :  1:1
  Import VPN Targets :  1:1
  Label Policy : label per instance
  Per-Instance Label : 1024
  IP FRR Route Policy : 20
  VPN FRR Route Policy : 12
  Import Route Policy : 10
  Export Route Policy : 20
  Tunnel Policy : bindTE
  Maximum Routes Limit : 2000
  Threshold Routes Limit : 80%
  Maximum Prefixes Limit : 1024
  Threshold Prefixes Limit : 50%
  Install Mode : route-unchanged
  Log Interval : 10
 Address family ipv6
  Create date : 2012/12/3 15:36:20 UTC+08:00
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
```

```
Log Interval : 5
```

Table 19-5 Description of the display ip vpn-instance verbose command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name and ID	Name and ID of the VPN instance. The ID is assigned by the system, which facilitates indexing.
Description	Description of the VPN instance. This field is displayed in the command output only when the **description (VPN instance view)** command is used.
Service ID	Service ID of the VPN instance. This item is displayed only after the **service-id (VPN instance view)** command is run in the VPN instance view.
Interfaces	Interfaces bound to the VPN instance. This field is displayed only after the **ip binding vpn-instance** command is configured on these interfaces.
Address family ipv4	Information about the IPv4 address family enabled for the VPN instance.
Address family ipv6	Information about the IPv6 address family enabled for the VPN instance.
Create date	Time when the VPN instance is created.
Up time	Period during which the VPN instance maintains in the Up state.
Route Distinguisher	RD of the VPN instance IPv4 address family or IPv6 address family
Export VPN Targets	Route Target list in the outbound direction. To set the VPN target, run the **vpn-target** command.

Item	Description
Import VPN Targets	Route Target list in the inbound direction. To set the VPN target, run the **vpn-target** command.
Label Policy	Label policy: ● label per instance: indicates that the same label is allocated to routes of a VPN instance. This field is displayed in the command output only when the **apply-label per-instance** command is run in the VPN instance view. ● label per route: indicates that each route of a VPN instance is assigned a label. Label allocation for routes of a VPN instance is implemented in this mode.
Per-Instance Label	Label value used when all VPN routes of the VPN instance address family share one label. This field is displayed only after the **apply-label per-instance** command is run in the VPN instance address family view.
IP FRR Route Policy	IP FRR route policy used for the address family. This item is displayed only after the **ip frr** command is run in the VPN instance IPv4 address family view.
VPN FRR Route Policy	VPN FRR route policy used for the address family. This item is displayed only after the **vpn frr** command is run in the VPN instance IPv4 address family view.
Import Route Policy	Import Route-Policy applied to the VPN instance. This field is displayed only after the **import route-policy** command is run in the VPN instance address family view.
Export Route Policy	Export Route-Policy applied to the VPN instance. This field is displayed only after the **export route-policy** command is run in the VPN instance address family view.

Item	Description
Tunnel Policy	Tunnel policy applied to the VPN instance. This field is displayed only after the **tnl-policy** command is run in the VPN instance address family view.
Maximum Routes Limit	Maximum number of routes supported by the current address family. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Threshold Routes Limit	Percentage of the maximum number of routes specified for the current address family. When the maximum number of routes reaches the percentage threshold, an alarm is generated.This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Maximum Prefixes Limit	Maximum number of prefixes supported by the current address family of the VPN instanceThis field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Threshold Prefixes Limit	Percentage of the maximum number of prefixes specified for the current address family of the VPN instance. When the maximum number of prefixes reaches the percentage threshold, an alarm is generated.This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Install Mode	Method of processing routes. The **prefix limit** command can be used to specify the route processing method when the threshold is lowered due to the number of route prefixes exceeding the upper threshold. ● If **route-unchanged** is configured, routes in the routing information base (RIB) table remain unchanged. ● If **route-unchanged** is not configured, all routes in the RIB table are deleted and the routes are re-installed in the RIB table.

Item	Description
Log Interval	Interval for displaying log messages when the number of VPN instance routes exceeds the maximum value. The default interval is 5 seconds. The value can be set by the command **limit-log-interval**.

19.8.3 ipv6 binding vpn6-instance (upgrade-compatible command)

Function

The **ipv6 binding vpn6-instance** command binds the current interface to an IPv6 VPN instance.

The **undo ipv6 binding vpn6-instance** command unbinds the current interface from an IPv6 VPN instance.

By default, an interface is a public network interface and is not bound to any IPv6 VPN instance.

Format

ipv6 binding vpn6-instance *vpn6-instance-name*

undo ipv6 binding vpn6-instance *vpn6-instance-name*

Parameters

Parameter	Description	Value
vpn6-instance-name	Specifies the name of an IPv6 VPN instance.	The name is a string of 1 to 31 case-sensitive characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After an IPv6 VPN instance is created, the device interfaces belonging to the IPv6 VPN instance need to be bound to the instance; otherwise, the interfaces are public network interfaces.

After an interface is bound to an IPv6 VPN instance or an interface is unbound from an IPv6 VPN instance, the Layer 3 features such as the IPv6 address and IPv6 routing protocol configured on this interface are deleted.

19.8.4 ipv6 vpn6-instance (upgrade-compatible command)

Function

The **ipv6 vpn6-instance** command creates an IPv6 VPN instance and displays the IPv6 VPN instance view.

The **undo ipv6 vpn6-instance** command deletes a specified IPv6 VPN instance.

By default, no IPv6 VPN instance exists.

Format

ipv6 vpn6-instance *vpn6-instance-name*

undo ipv6 vpn6-instance *vpn6-instance-name*

Parameters

Parameter	Description	Value
vpn6-instance-name	Specifies the name of an IPv6 VPN instance.	The name is a string of 1 to 31 case-sensitive characters without any spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After this command is run, an IPv6 VPN instance is created and the IPv6 VPN instance view is displayed..

19.8.5 link-alive (upgrade-compatible command)

Function

The **link-alive** command enables the link-alive function on a GRE tunnel.

The **undo link-alive** command disables the link-alive function on a GRE tunnel.

By default, the link-alive function is disabled on a GRE tunnel.

Format

link-alive [**period** *period*] [**retry-times** *retry-times*]

undo link-alive

Parameters

Parameter	Description	Value
period	Specifies the interval for sending link-alive packets.	The value is an integer that ranges from 1 to 32767, in seconds. The default value is 5.
retry-times *retry-times*	Specifies the tunnel-unreachable counter value.	The value is an integer that ranges from 1 to 255. The default value is 3.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The link-alive function takes effect on a GRE tunnel immediately after you run the **link-alive** command on the tunnel interface. After you run the **undo link-alive** command, the link-alive function immediately becomes invalid. The source end of a GRE tunnel periodically sends link-alive packets. The tunnel-unreachable counter increases by 1 every time a link-alive packet is sent. If the source end does not receive any response packet when the tunnel-unreachable counter value reaches *retry-times*, the source end considers the remote end unreachable.

Example

# Enable the link-alive function on a GRE tunnel and retain the default parameter values.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] tunnel-protocol gre
[HUAWEI-Tunnel1] link-alive
```

# Disable the link-alive function on a GRE tunnel.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] undo link-alive
```

# Enable the link-alive function on a GRE tunnel. Set the interval for sending link-alive packets to 12 seconds and retain the default tunnel-unreachable counter value.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] link-alive period 12
```

# Enable the link-alive function on a GRE tunnel. Set the interval for sending link-alive packets to 12 seconds and the tunnel-unreachable counter to 4.

```
<HUAWEI> system-view
[HUAWEI] interface tunnel 1
[HUAWEI-Tunnel1] link-alive period 12 retry-times 4
```

19.8.6 snmp-agent trap enable feature-name l3vpn (upgrade-compatible command)

Function

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for the L3VPN module.

The **undo snmp-agent trap enable feature-name l3vpn** command disables the trap function for the L3VPN module.

By default, the trap function for the L3VPN module is disabled.

Format

snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_mid_exceed

undo snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_mid_exceed

Parameters

Parameter	Description	Value
trap-name	Enables the traps of L3VPN events of specified types.	-
l3vpn_mib_trap_mid_exceed	Enables the trap of the event indicating that the number of private route prefixes exceeds the middle threshold.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for L3VPN modules.

Example

# Enable the trap of the event indicating that the number of private route prefixes exceeds the middle threshold in the system view.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_mid_exceed
```

19.8.7 snmp-agent trap enable l3vpn (upgrade-compatible command)

Function

The **snmp-agent trap enable l3vpn** command enables the device to send the L3VPN trap message.

The **undo snmp-agent trap enable l3vpn** command prohibits the device from sending the L3VPN trap message.

By default, the L3VPN trap message cannot be sent.

Format

snmp-agent trap enable l3vpn

undo snmp-agent trap enable l3vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

# Permit the device to send the L3VPN trap message.

```
<HUAWEI> system-view
[HUAWEI] snmp-agent trap enable l3vpn
```

19.8.8 sa authentication-hex (upgrade-compatible command)

Function

The **sa authentication-hex** command sets an authentication in hexadecimal format or cipher text for Security Associations (SAs).

Format

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } **plain** *hex-plain-key*

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa authentication-hex** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa authentication-hex** command.	-
plain	Indicates the plain text used for authentication.	-

Parameter	Description	Value
hex-plain-key	Specifies the plain text key.	The value is in hexadecimal notation. ● If authentication algorithm Message Digest 5 (MD5) is used, the length of the key is 16 bytes. ● If authentication algorithm Secure Hash Algorithm-1 (SHA-1) is used, the length of the key is 20 bytes. ● If authentication algorithm SHA2-256 is used, the length of the key is 32 bytes. **NOTE** The MD5 and SHA-1 authentication algorithms have security risks; therefore, you are advised to use SHA-256 preferentially.

Views

SA view

Default Level

3: Management level

Usage Guidelines

This command is upgrade compatible and can be executed during configuration recovery. Users cannot manually configure this command.

After the upgrade, this command is no longer supported, and it is replaced by the **sa authentication-hex** command.

19.8.9 sa encryption-hex (upgrade-compatible command)

Function

The **sa encryption-hex** command configures an encryption key for manual Security Association (SA) in hexadecimal format.

Format

sa encryption-hex { **inbound** | **outbound** } { **ah** | **esp** } **plain** *hex-plain-key*

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa encryption-hex** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa encryption-hex** command.	-
plain	Indicates the plaintext used for authentication.	-
hex-plain-key	Specifies the plaintext key.	The value is in hexadecimal notation. ● If encryption algorithm Data Encryption Standard (DES) is used, the length of the key is 8 bytes. ● If encryption algorithm Triple Data Encryption Standard (3DES) is used, the length of the key is 24 bytes. ● If encryption algorithm Advanced Encryption Standard 128 (AES-128) is used, the length of the key is 16 bytes. ● If encryption algorithm AES-192 is used, the length of the key is 24 bytes. ● If encryption algorithm AES-256 is used, the length of the key is 32 bytes. **NOTE** The DES and 3DES encryption algorithms have security risks; therefore, you are advised to use AES-128, AES-192 or AES-256 preferentially.

Views

SA view

Default Level

3: Management level

Usage Guidelines

This command is upgrade compatible and can be executed during configuration recovery. Users cannot manually configure this command.

After the upgrade, this command is no longer supported, and it is replaced by the **sa encryption-hex** command.

19.8.10 sa string-key (upgrade-compatible command)

Function

The **sa string-key** command configures an authentication key in the string format.

Format

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } **plain** *string-plain-key*

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa string-key** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa string-key** command.	-
plain	Indicates the plaintext used for authentication.	-
string-plain-key	Specifies the plaintext key.	The value is a string of 1 to 127 case-sensitive characters.

Views

SA view

Default Level

3: Management level

Usage Guidelines

This command is upgrade compatible and can be executed during configuration recovery. Users cannot manually configure this command.

After the upgrade, this command is no longer supported, and it is replaced by the **sa string-key** command.

19.9 WLAN Compatible Commands

19.9.1 ap-location (upgrade-compatible command)

Function

ap-location command sets the latitude and longitude of an AP.

By default, no latitude or longitude is configured for an AP.

Format

ap-location longitude { **e** | **w** } *longitude-value* **latitude** { **s** | **n** } *latitude-value*

ap-location latitude { **s** | **n** } *latitude-value* **longitude** { **e** | **w** } *longitude-value*

Parameters

Parameter	Description	Value
longitude e *longitude-value*	Specifies the east longitude value of an AP.	The value supports two formats: degrees, minutes, and seconds (DMS) and decimal degrees (DD). ● The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. ● The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the east longitude value of an AP can be set to **longitude e** 120-45-23 in DMS format and **longitude e** 120.756333333 in DD format.
longitude w *longitude-value*	Specifies the west longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XXX-XX-XX. XXX ranges from 0 to 180, and XX ranges from 0 to 59. ● The DD format is XXX.XXXXXXXXX. XXX ranges from 0 to 180, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the west longitude value of an AP can be set to **longitude w** 120-45-23 in DMS format and **longitude w** 120.756333333 in DD format.
latitude s *latitude-value*	Specifies the south longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the south longitude value of an AP can be set to **latitude s** 78-45-23 in DMS format and **latitude s** 78.756333333 in DD format.

Parameter	Description	Value
latitude n *latitude-value*	Specifies the north longitude value of an AP.	The value supports two formats: DMS and DD. ● The DMS format is XX-XX-XX. The first XX ranges from 0 to 90, and the other XXs range from 0 to 59. ● The DD format is XX.XXXXXXXXX. XX ranges from 0 to 90, and XXXXXXXXX is a decimal supporting a maximum of 9 digits. For example, the north longitude value of an AP can be set to **latitude n** 78-45-23 in DMS format and **latitude n** 78.756333333 in DD format.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the longitude and latitude of an AP for easily locating it.

19.9.2 traffic-filter (AP wired port profile view) (upgrade-compatible command)

Function

The **traffic-filter** command configures ACL-based IPv4 packet filtering on an AP's wired interface.

The **undo traffic-filter** command cancels ACL-based IPv4 packet filtering configuration on an AP's wired interface.

By default, ACL-based IPv4 packet filtering is not configured on an AP's wired interface.

Format

traffic-filter { **inbound** | **outbound** } **acl** { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based IPv4 packet filtering in the inbound direction.	-
outbound	Configures ACL-based IPv4 packet filtering in the outbound direction.	-
acl	Filters IPv4 packets based on a specified ACL.	-
acl-number	Specifies an ACL number.	The ACL must exist. The value is an integer that ranges from 3000 to 3031.
name *acl-name*	Filters IPv4 packets based on a named ACL. *acl-name* indicates the ACL name.	The ACL name must exist. The value range is the same as that of the *acl-number* parameter.

Views

AP wired port profile view

Default Level

3: Management level

Usage Guidelines

Usage scenario

The rules for an AP's wired interface to filter IPv4 packets based on ACLs are as follows:

- If the action in the ACL rule is **deny**, the device discards IPv4 packets matching the rule.
- If the action in the ACL rule is **permit**, the device allows IPv4 packets matching the rule to pass through.
- If no rule is matched, IPv4 packets are allowed to pass through.

Prerequisites

An ACL rule has been created by running the **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }] or **acl name** *acl-name acl-number* [**match-order** { **auto** | **config** }] command.

Precautions

The **traffic-filter** command can reference an ACL with no rule configured. You can configure a rule for the ACL after running this command.

You can configure IPv4 packet filtering based on only one ACL in one direction. If a referenced ACL needs to be replaced, configure a new ACL to overwrite the original one.

19.9.3 traffic-filter (traffic profile view) (upgrade-compatible command)

Function

The **traffic-filter** command configures ACL-based IPv4 packet filtering in a traffic profile.

The **undo traffic-filter** command cancels configuration of ACL-based IPv4 packet filtering in a traffic profile.

By default, ACL-based IPv4 packet filtering is not configured in a traffic profile.

Format

traffic-filter { **inbound** | **outbound** } **acl** { *acl-number1* | *acl-number2* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Configures ACL-based IPv4 packet filtering in the inbound direction.	-
outbound	Configures ACL-based IPv4 packet filtering in the outbound direction.	-
acl	Filters IPv4 packets based on a specified ACL.	-
acl-number	Specifies an ACL number.	The ACL must exist. The value is an integer that ranges from 3000 to 3031 and from 6000 to 6031. ● 3000 to 3031: advanced ACLs ● 6000 to 6031: user ACLs

Parameter	Description	Value
name *acl-name*	Filters IPv4 packets based on a named ACL. *acl-name* indicates the ACL name.	The ACL name must exist. The value range is the same as that of the *acl-number* parameter.

Views

Traffic profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **traffic-filter** command is executed in the traffic profile view, the device filters packets matching a specified ACL rule:

- If the action in the ACL rule is **deny**, the device discards IPv4 packets matching the rule.
- If the action in the ACL rule is **permit**, the device allows IPv4 packets matching the rule to pass through.
- If no rule is matched, IPv4 packets are allowed to pass through.

Prerequisites

An ACL rule has been created by running the **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }] or **acl name** *acl-name acl-number* [**match-order** { **auto** | **config** }] command.

Precautions

The **traffic-filter** command can reference an ACL with no rule configured. You can configure a rule for the ACL after running this command.

You can configure IPv4 packet filtering based on only one ACL in one direction. If a referenced ACL needs to be replaced, configure a new ACL to overwrite the original one.

19.10 Reliability Compatible Commands

19.10.1 BFD Compatible Commands

19.10.1.1 bfd bind peer-ipv6 (upgrade-compatible command)

Function

The **bfd bind peer-ipv6** command creates a BFD6 session to test an IPv6 link.

By default, no BFD6 session is created to test an IPv6 link.

Format

bfd *bfd-name* **bind peer-ipv6** *peer-ipv6* [**vpn6-instance** *vpn6-instance-name*] [**interface** *interface-type interface-number*] [**source-ipv6** *ipv6-address*]

Parameters

Parameter	Description	Value
bfd-name	Specifies a BFD6 session name.	The value is a string of 1 to 15 characters, spaces not supported.
peer-ipv6 *peer-ipv6*	Specifies the peer IPv6 address that is to be bound to a BFD6 session.	-
vpn6-instance *vpn6-instance-name*	Specifies the name of the VPN instance that is bound to a BFD6 session. If no VPN instance is specified, the peer IP address is regarded as a public IP address.	The value is a string of 1 to 31 characters.
interface *interface-type interface-number*	Specifies the local Layer 3 interface that is bound to a BFD6 session.	-

Parameter	Description	Value
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD packets. Generally, you do not need to configure this parameter. If no source IPv6 address is specified, the device specifies one based on the following situations: ● During BFD for IPv6 negotiation, the device searches for the IPv6 address of an outbound interface that connects to the peer in the local routing table as the source IPv6 address before sending BFD packets. ● During BFD for IPv6 detection, the device sets the source IPv6 address to a fixed value. **NOTE** BFD works with unicast reverse path forwarding (URPF). When URPF checks the source IPv6 address in received packets, you must manually set the source IPv6 address for the BFD packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **bfd** *bfd-name* **bind peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ipv6** *ipv6-address*] command.

Example

# Create a BFD6 session named **test** to test the single-hop link.

```
<HUAWEI> system-view
[HUAWEI] bfd
[HUAWEI-bfd] quit
[HUAWEI] bfd test bind peer-ipv6 2001::1 vpn6-instance vpn1 interface gigabitethernet 0/0/1
[HUAWEI-bfd-session-test] discriminator local 1
[HUAWEI-bfd-session-test] discriminator remote 2
[HUAWEI-bfd-session-test] commit
```

19.10.1.2 display bfd statistics session (upgrade-compatible command)

Function

The **display bfd statistics session** command displays BFD statistics.

Format

display bfd statistics session peer-ipv6 *peer-ipv6* [{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*]

Parameters

Parameter	Description	Value
peer-ipv6 *peer-ipv6*	Displays statistics about a BFD6 session bound to a specified peer IPv6 address.	-
{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*	Displays statistics about a BFD6 session bound to a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **display bfd statistics session** **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] command.

19.10.1.3 display bfd session (upgrade-compatible command)

Function

The **display bfd session** command displays information about BFD sessions.

Format

display bfd session peer-ipv6 *peer-ipv6* [{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*] [**verbose**]

Parameters

Parameter	Description	Value
peer-ipv6 *peer-ipv6*	Displays the configuration of a BFD6 session bound to a specified peer IPv6 address.	-
{ **vpn-instance** | **vpn6-instance** } *vpn-instance-name*	Displays information about a BFD6 session bound to a specified VPN instance.	The value must be an existing VPN instance name.
verbose	Displays detailed information about the BFD6 configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **display bfd session** **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**verbose**] command.

19.10.1.4 display bfd configuration (upgrade-compatible command)

Function

The **display bfd configuration** command displays configurations of BFD sessions.

Format

display bfd configuration peer-ipv6 *peer-ipv6* [{ **vpn-instance** | **vpn6-instance** } *vpn6-instance-name*] [**verbose**]

Parameters

Parameter	Description	Value
peer-ipv6 *peer-ipv6*	Displays the configuration of a BFD6 session bound to a specified peer IPv6 address.	-

Parameter	Description	Value
{ **vpn-instance** | **vpn6-instance** } *vpn6-instance-name*	Displays the configuration of a BFD6 session bound to a specified VPN instance	The value must be an existing VPN instance name.
verbose	Displays detailed information about BFD6 configurations.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **display bfd configuration** **peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**verbose**] command.

19.10.1.5 snmp-agent trap enable bfd (upgrade-compatible command)

Function

The **snmp-agent trap enable bfd** command enables the trap function for the BFD module.

By default, the trap function is disabled for the BFD module.

Format

snmp-agent trap enable bfd

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **snmp-agent trap enable feature-name bfd** command in the system view.

19.10.2 DLDP Compatible Commands

19.10.2.1 snmp-agent trap enable dldp (upgrade-compatible command)

Function

The **snmp-agent trap enable dldp** command enables the trap function for the DLDP module.

By default, the trap function is disabled for the DLDP module.

Format

snmp-agent trap enable dldp

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name dldp** command.

19.10.2.2 dldp authentication-mode md5-compatible(upgrade-compatible command)

Function

The **dldp authentication-mode md5-compatible** command configures MD5-compatible authentication.

By default, DLDP packets are not authenticated.

Format

dldp authentication-mode md5-compatible *md5-password*

Parameters

Parameter	Description	Value
md5-compatible *md5-password*	Uses MD5-compatible to authenticate DLDP packets exchanged between the interfaces on the local and neighbor devices.*md5-password* specifies the MD5-compatible authentication password. **NOTE** To ensure security, the password is saved in cipher text in the configuration file.	The value is a string of 1 to 16 case-sensitive characters in plain text without any question mark (?) and space. **NOTE** During the upgrade, the device is compatible with the cipher-text passwords with different lengths before the upgrade.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

When the device that uses MD5 authentication is upgraded from V200R001 or V200R002 to V200R008 or later, to ensure compatibility, upgrade the DLDP authentication mode to MD5-compatible.

Running the **dldp authentication-mode md5-compatible** command is equivalent to running the **dldp authentication-mode** command in the system view.

19.10.3 Ethernet OAM Compatible Commands

19.10.3.1 ma format (upgrade-compatible command)

Function

The **ma** command creates an MA in an MD and displays the MA view. If the MA already exists, this command displays the MA view.

Format

ma *ma-name* **format** { **icc-based** | **string** }

Parameters

Parameter	Description	Value
ma-name	Specifies the name of an MA. Names of MAs in an MD are unique.	The value is a string of characters without spaces, hyphen (-), or question mark (?). The total length of the names of the MA and MD must be within 44 case-sensitive characters.

Parameter	Description	Value
icc-based	Specifies an ICC-based MA name carried in CCMs to be sent. ITU carrier codes (ICCs) are assigned to network operators or service providers and maintained by ITU-T Telecommunication Standardization Bureau (TSB) in compliance with ITU-T M.1400 Recommendation.	-
string	Specifies a string-based MA name carried in CCMs to be sent.	-

Views

MD view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **ma** *ma-name* [**format** { **icc-based** *iccbased-ma-format-name* | **string** *ma-format-name* }] command.

19.10.3.2 cfm md format (upgrade-compatible command)

Function

Using the **cfm md** command, you can create an MD and enter the MD view. If the MD exists, you can use this command to enter the MD view.

Format

cfm md *md-name* **format** { **dnsname-and-mdname** | **mac-address** | **md-name** } [**level** *level*]

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 characters, which are case sensitive. The characters, such as ?, -, and space are excluded. The name of an MD is used to identify the MD. Different MDs on a device cannot have the same name. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
dnsname-and-mdname	Indicates the MD name in the format that a DNS name is followed by an MD name.	-
mac-address	Indicates the MD name in the format that a MAC address is followed by an MD name.	-
md-name	Indicates that the MA ID field of the sent packet contains the MD name.	-
level *level*	Specifies the level of the MD.	The value is an integer ranging from 0 to 7. The greater the value, the higher the priority. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **cfm md** *md-name* [**format** { **no-md-name** | **dns** *dns-md-format-name* | **mac-address** *mac-md-format-name* | **string** *string-md-format-name* }] [**level** *level*] command.

19.10.3.3 delay-measure one-way continual receive (upgrade-compatible command)

Function

The **delay-measure one-way continual receive** command configures a remote device to receive DMMs to implement proactive one-way frame delay measurement.

By default, the remote device enabled with proactive one-way frame delay measurement in the maintenance association (MA) is not configured to receive DMMs.

Format

delay-measure one-way continual receive

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **delay-measure one-way continual receive mep** *mep-id* command.

19.10.3.4 delay-measure one-way receive (upgrade-compatible command)

Function

Using the **delay-measure one-way receive** command, you can configure the DM frame receiving function on the remote end of the local device enabled with one-way frame delay measurement.

By default, the DM frame receiving function is not configured for the remote end in an MA.

Format

delay-measure one-way receive

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **delay-measure one-way receive** **mep** *mep-id* [**peer-ip** *peer-ip* [**vc-id** *vc-id*]].

19.10.3.5 delay-measure two-way receive (upgrade-compatible command)

Function

Using the **delay-measure two-way receive** command, you can enable DM frame reception on the remote MEP to implement the two-way frame delay measurement.

By default, DM frame reception is not configured on the remote MEP in an MA.

Format

delay-measure two-way receive

Parameters

None

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **delay-measure two-way receive mep** *mep-id* [**8021p** { *8021p-value* } &<1-3>] [**peer-ip** *peer-ip* [**vc-id** *vc-id*]] command.

19.10.3.6 efm threshold-event trigger error-shutdown (upgrade-compatible command)

Function

Using the **efm threshold-event trigger error-shutdown** command, you can enable the error-triggered shutdown function on an interface. After this function is enabled, the interface is shut down when the number of EFM errored frames or errored codes reaches the threshold.

By default, the error-triggered shutdown function is disabled on an interface.

Format

efm threshold-event trigger error-shutdown

Parameters

None

Views

GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **efm threshold-event trigger error-down** command.

19.10.3.7 efm trigger if-net (upgrade-compatible command)

Function

The **efm trigger if-net** command associates EFM with an interface.

Format

efm trigger if-net

Parameters

None

Views

GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **efm trigger if-down** command.

19.10.3.8 oam-bind ingress interface egress cfm md ma (upgrade-compatible command)

Function

The **oam-bind ingress interface egress cfm md ma** command configures an interface to report faults to Ethernet CFM.

Format

oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?).
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphen (-), and question mark (?). The total length of the names of the MA and MD must be within 44 characters.

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, it is replaced by the **oam-bind ingress interface** *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down** command.

19.10.3.9 oam-bind ingress interface egress efm interface (upgrade-compatible command)

Function

The **oam-bind ingress interface egress efm interface** command enables an interface to report faults to EFM OAM.

Format

oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM OAM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, it is replaced by the **oam-bind ingress interface** *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down** command.

19.10.3.10 snmp-agent trap enable efm (upgrade-compatible command)

Function

The **snmp-agent trap enable efm** command enables the trap function for the EFM module.

By default, the trap function is disabled for the EFM module.

Format

snmp-agent trap enable efm

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name efm** command.

19.10.3.11 snmp-agent trap enable eoam-1ag (upgrade-compatible command)

Function

The **snmp-agent trap enable eoam-1ag** command enables the trap function for the Eoam-1ag module.

By default, the trap function is disabled for the Eoam-1ag module.

Format

snmp-agent trap enable eoam-1ag

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After an upgrade, this command is no longer supported, and it is replaced by the **snmp-agent trap enable feature-name eoam-1ag** command.

19.10.3.12 snmp-agent trap enable test-packet (upgrade-compatible command)

Function

The **snmp-agent trap enable test-packet** command enables an Ethernet OAM module to send traps to the NMS.

By default, an Ethernet OAM module is enabled to send traps to the NMS.

Format

snmp-agent trap enable test-packet

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **snmp-agent trap enable feature-name efm** command.

19.11 User Access and Authentication Compatible Commands

19.11.1 AAA Compatible Commands

19.11.1.1 adminuser-priority (upgrade-compatible command)

Function

The **adminuser-priority** command configures a user as an administrator to log in to the device and sets the administrator level during login.

Format

adminuser-priority *level*

Parameters

Parameter	Description	Value
level	Specifies the level of an administrator.	The value is an integer ranging from 0 to 15. After logging in to the device, a user can run only the commands of the same level or lower levels.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **13.1.16 admin-user privilege level** *level* command.

19.11.1.2 hwtacacs-server shared-key (upgrade-compatible command)

Function

The **hwtacacs-server shared-key** command configures the shared key of an HWTACACS server.

The **undo hwtacacs-server shared-key** command deletes the shared key of an HWTACACS server.

By default, no shared key of an HWTACACS server is configured.

Format

hwtacacs-server shared-key simple *key-string*

undo hwtacacs-server shared-key

Parameters

Parameter	Description	Value
simple	Indicates the shared key in simple text.	-

Parameter	Description	Value
key-string	Specifies the shared key of an HWTACACS server.	The value is a string of 1 to 255 characters in plain text and a string of 20 to 392 characters in cipher text.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **13.3.11 hwtacacs-server shared-key** [**cipher**] *key-string* command.

19.11.1.3 local-user (upgrade-compatible command)

Function

The **local-user** command creates a local user and sets parameters of the local user.

By default, the local user **admin** exists in the system. The priority of the user is **15**, and service type is **http**.

By default, a local user exists in the system. The priority of the user is **15**, and service type is **http**. The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

local-user *user-name* **password** { *key-string* [**old-password** *password*] | **simple** *simple-string* } [**access-limit** *max-number* | **idle-timeout** *minutes* [*seconds*] | **state** { **block** | **active** }] *

Parameters

Parameter	Description	Value
user-name	Specifies the user name. If the user name contains a delimiter "@", the character before "@" is the user name and the character after "@" is the domain name. If the value does not contain "@", the entire character string represents the user name and the domain name is the default one.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
password *key-string*	Specifies the password of a local user. It is recommended that you set the user password when creating a user.	The value is a string of 1 to 256 case-sensitive characters without spaces.
old-password *password*	Specifies the old password of a local user. **NOTE** This parameter cannot be automatically displayed through the question mark help function and must be entered completely. It should be configured by the network administrator on the NMS and delivered to the device. It is not recommended that you directly specify this parameter on the device.	The value is the password used by the local user for the current login.
password simple *simple-string*	Specifies the password of a local user. It is recommended that you set the user password when creating a user.	The value is a string of 1 to 256 case-sensitive characters without spaces.

Parameter	Description	Value
access-limit *max-number*	Specifies the number of connections that can be created with a specified user name. If this parameter is not specified, the number of connections that can be established by a specified user is not limited.	The value is is an integer that varies according to the types and number of devices.
idle-timeout *minutes* [*seconds*]	Specifies the timeout period for disconnection of the user. ● *minutes* is the period when the user interface is disconnected in minutes. ● *seconds* is the period when the user interface is disconnected in seconds. If this parameter is not specified, the device uses the user level configured by the **idle-timeout** command in the user view. If *minutes* [*seconds*] is set to **0 0**, the idle disconnection function is disabled.	● *minutes*: the value is an integer ranging from 0 to 35791 minutes. ● *seconds*: the value is an integer ranging from 0 to 59 seconds.

Parameter	Description	Value
state { **active** | **block** }	Specifies the status of a local user. ● **active** indicates that a local user is in active state. ● **block** indicates that a local user is in blocking state. If a user has established a connection with the device, when the user is set in blocking state, the connection still takes effect but the device rejects subsequent authentication requests from the user. If this parameter is not specified, the status of a local user is active.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **13.1.54 local-user** *user-name* { **password** { **cipher** | **irreversible-cipher** } *password* | **access-limit** *max-number* | **ftp-directory** *directory* | **idle-timeout** *minutes* [*seconds*] | **privilege level** *level* | **state** { **block** | **active** } } * command.

19.11.1.4 local-user level (upgrade-compatible command)

Function

The **local-user level** command sets the level of a local user.

Format

local-user *user-name* **level** *level*

Parameters

Parameter	Description	Value
user-name	Specifies the user name.	The value is a string of 1 to 64 case-insensitive characters without spaces.
level	Specifies the user level.	The value is an integer that ranges from 0 to 15. A greater value indicates a higher level of a user. After logging in to the device, a user can run only the commands of the same level or lower levels.

Views

AAA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **local-user** *user-name* **privilege level** *level* command.

19.11.1.5 radius-server accounting (upgrade-compatible command)

Function

The **radius-server accounting** command configures the RADIUS accounting server.

The **undo radius-server accounting** command deletes the configuration.

By default, no RADIUS accounting server is configured.

Format

radius-server accounting *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * **secondary**

radius-server accounting *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * **secondary**

undo radius-server accounting secondary

undo radius-server accounting *ip-address port* **source** { **loopback** | **ip-address** *ip-address* } **secondary**

undo radius-server accounting *ipv6-address port* **source** { **loopback** | **ip-address** *ipv6-address* } **secondary**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of a RADIUS accounting server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS accounting server is bound to.	The vpn-instance must already exist.
source loopback *interface-number*	Specifies the number of a loopback interface.	The loopback interface must already exist.
source ip-address *ipv4-address*	Specifies the source IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
source ip-address *ipv6-address*	Specifies the source IPv6 address of a RADIUS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
weight *weight-value*	Specifies the weight of a RADIUS accounting server.	The value is an integer that ranges from 0 to 100.

Parameter	Description	Value
secondary	Specifies the configured accounting server as the secondary accounting server. If you do not configure this parameter, it indicates that you configure the primary accounting server.	-

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **13.2.23 radius-server accounting** *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * or **13.2.23 radius-server accounting** *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * command.

19.11.1.6 radius-server authentication (upgrade-compatible command)

Function

The **radius-server authentication** command configures a RADIUS authentication server.

The **undo radius-server authentication** command deletes the configured RADIUS authentication server.

By default, no RADIUS authentication server is specified.

Format

radius-server authentication *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * **secondary**

radius-server authentication *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * **secondary**

undo radius-server authentication secondary

undo radius-server authentication *ipv4-address port* **source** { **loopback** | **ip-address** *ipv4-address* } **secondary**

undo radius-server authentication *ipv6-address port* **source** { **loopback** | **ip-address** *ipv6-address* } **secondary**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of a RADIUS authentication server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authentication server is bound to.	The value is a string of 1 to 31 case-sensitive characters without spaces.
source loopback *interface-number*	Specifies the IP address of the loopback interface taken as the source IP address. *interface-number* specifies the number of a loopback interface.	The value is an integer that ranges from 0 to 1023.
source ip-address *ipv4-address*	Specifies the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv4 address of the outbound interface is used as the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.

Parameter	Description	Value
source ip-address *ipv6-address*	Specifies the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv6 address of the outbound interface is used as the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
weight *weight-value*	Specifies the weight of a RADIUS authentication server.	The value is an integer that ranges from 0 to 100.
secondary	Specifies the configured authentication server as the secondary accounting server. If you do not configure this parameter, it indicates that you configure the primary authentication server.	-

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **13.2.28 radius-server authentication** *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* } | **weight** *weight-value*] * or **13.2.28 radius-server authentication** *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* } | **weight** *weight-value*] * command.

19.11.1.7 radius-server authorization (upgrade-compatible command)

Function

The **radius-server authorization** command configures the RADIUS authorization server.

The **undo radius-server authorization** command deletes the configured RADIUS authorization server.

By default, no RADIUS authorization server is configured.

Format

radius-server authorization *ip-address* [**vpn-instance** *vpn-instance-name*] { **server-group** *group-name* | **shared-key** { *key-string* | **simple** *simple-string* } } * [**ack-reserved-interval** *interval*]

undo radius-server authorization *ip-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a RADIUS authorization server.	The value is a valid unicast address in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authorization server is bound to.	The value is a string of 1 to 31 case-sensitive characters without spaces.
server-group *group-name*	Specifies the name of a RADIUS group corresponding to a RADIUS server template.	The value is a string of 1 to 32 case-sensitive characters without spaces.
shared-key *key-string*	Specifies the shared key in cipher text.	The value is a string of 32 characters in cipher text, for example, %$%$m^NF$L^SO%2@^y$T`^1'|lcZ%$%$, or a string of 1 to 16 characters in plain text, for example, 1234567.
shared-key simple *simple-string*	Specifies the shared key in plain text.	The value is a string of 1 to 16 case-sensitive characters, without spaces. By default, the key is converted to cipher text.

Parameter	Description	Value
ack-reserved-interval *interval*	Specifies the duration for retaining a RADIUS authorization response packet.	The value is an integer that ranges from 0 to 300, in seconds. By default, the value is 0s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **13.2.29 radius-server authorization** command.

19.11.1.8 radius-server shared-key (upgrade-compatible command)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

The default username and password are available in *S Series Switches Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

radius-server shared-key { *key-string* | **simple** *simple-string* }

Parameters

Parameter	Description	Value
key-string	Specifies a cipher text password.	The value is a case-sensitive character string of 1 to 256 without spaces, quotation mask ("), and question mask (?).

Parameter	Description	Value
simple *simple-string*	Specifies a simple text password.	The value is a string of 1 to 16 case-sensitive characters, without spaces.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server shared-key** **cipher** *key-string* command.

19.11.1.9 radius-server testuser (upgrade-compatible command)

Function

Using the **radius-server testuser** command, you can create a user account for automatic detection in the RADIUS server template.

Using the **undo radius-server testuser** command, you can delete a user account for automatic detection.

By default, a user account for automatic detection in the RADIUS server template is not created.

Format

radius-server testuser username *username* **password** *password*

undo radius-server testuser

Parameters

Parameter	Description	Value
username *username*	Specifies a user name used for automatic detection.	The value is a string of 1 to 64 characters without spaces. It is case insensitive.

Parameter	Description	Value
password *password*	Specifies the user password for automatic detection.	The value is a character string of 1 to 16 characters without spaces, single quotation marks and question marks. It is case sensitive. If it is in cipher text, the password is a string of 32 characters.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server testuser** **username** *username* **password cipher** *password* command.

19.11.1.10 radius-server test-user (upgrade-compatible command)

Function

Using the **radius-server test-user** command, you can create a user account for automatic detection in the RADIUS server template.

Using the **undo radius-server test-user** command, you can delete a user account for automatic detection.

By default, a user account for automatic detection in the RADIUS server template is not created.

Format

radius-server test-user *username password*

undo radius-server test-user

Parameters

Parameter	Description	Value
username	Specifies a user name used for automatic detection.	The value is a string of 1 to 64 characters without spaces. It is case insensitive.
password	Specifies the user password for automatic detection.	The value is a character string of 1 to 16 characters without spaces, single quotation marks and question marks. It is case sensitive. If it is in cipher text, the password is a string of 32 characters.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server testuser** **username** *username* **password cipher** *password* command.

19.11.1.11 radius-server test-user detect interval (upgrade-compatible command)

Function

The **radius-server test-user detect interval** command sets the interval for automatic user status detection.

Format

radius-server test-user detect interval *interval-time*

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for automatic user status detection.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **13.2.34 radius-server detect-server interval** **interval** *interval* command.

19.11.1.12 radius-server user-name domain-included force (upgrade-compatible command)

Function

The **radius-server user-name domain-included force** command configures the device encapsulate the domain name in the user name in RADIUS packets to be sent to a RADIUS server.

Format

radius-server user-name domain-included force

Parameters

None

Views

RADIUS server template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Its function is the same as that of the **radius-server user-name domain-included** command.

19.11.2 NAC Compatible Commands

19.11.2.1 authentication arp handshake (upgrade-compatible command)

Function

The **authentication arp handshake** command enables the handshake with pre-connection users and authorized users.

The **undo authentication arp handshake** command disables the handshake with pre-connection users and authorized users.

By default, the handshake with pre-connection users and authorized users is enabled.

Format

authentication arp handshake

undo authentication arp handshake

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **undo authentication handshake** command in the authentication profile view.

19.11.2.2 authentication handshake (upgrade-compatible command)

Function

The **authentication handshake** command enables the handshake with pre-connection users and authorized users.

The **undo authentication handshake** command disables the handshake with pre-connection users and authorized users.

By default, the handshake with pre-connection users and authorized users is enabled.

Format

authentication handshake

undo authentication handshake

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication handshake** command in the authentication profile view.

19.11.2.3 authentication event action authorize (upgrade-compatible command)

Function

The **authentication event action authorize** command configures the device to assign network access policies to users before the users are authenticated.

The **undo authentication event action authorize** command deletes the configured network access policies.

By default, no network access right is granted to users before the users are authenticated.

Format

authentication event pre-authen action authorize service-scheme *service-scheme*

undo authentication event pre-authen action authorize

authentication event { **authen-fail** | **authen-server-down** } **action authorize service-scheme** *service-scheme* [**response-fail**]

undo authentication event { **authen-fail** | **authen-server-down** } **action authorize**

Parameters

Parameter	Description	Value
pre-authen	Configures the device to assign network access policies to users when the users establish pre-connections with the device.	-
authen-fail	Configures the device to assign network access policies to users when the authentication server sends authentication failure packets to the device.	-

Parameter	Description	Value
authen-server-down	Configures the device to assign network access policies to users when the authentication server is Down and thereby the users fail to be authenticated.	-
response-fail	Configures the device to send authentication failure packets to users after assigning network access policies to the users. If this parameter is not specified, the device by default sends authentication success packets to users and therefore the users cannot know the fact that they fail to be authenticated. To solve this problem, specify this parameter so that the device will send authentication failure packets for the users to know their authentication results.	-
service-scheme *service-scheme*	Specifies the name of the service scheme based on which network access policies are assigned to users.	The value is a string of 1 to 32 case-sensitive characters without spaces and the following: \ / : < > | @ ' % * " ?

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event pre-authen action authorize service-scheme** *scheme-name* and **authentication event** { **authen-fail** | **authen-server-down** } **action authorize service-scheme** *service-scheme* [**response-fail**] commands in the authentication profile view.

19.11.2.4 authentication event authen-server-up action re-authen (upgrade-compatible command)

Function

The **authentication event authen-server-up action re-authen** command enables the device to re-authenticate users when the authentication server changes from Down to Up.

The **undo authentication event authen-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users when the authentication server changes from Down to Up.

Format

authentication event authen-server-up action re-authen

undo authentication event authen-server-up action re-authen

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event authen-server-up action re-authen** command in the authentication profile view.

19.11.2.5 authentication event client-no-response action authorize (upgrade-compatible command)

Function

The **authentication event client-no-response action authorize** command configures the device to assign network access policies to users before the users are authenticated.

The **undo authentication event client-no-response action authorize** command deletes the configured network access policies.

By default, no network access right is granted to users before the users are authenticated.

Format

authentication event client-no-response action authorize service-scheme *service-scheme*

undo authentication event client-no-response action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme*	Specifies the name of the service scheme based on which network access policies are assigned to users.	The value is a string of 1 to 32 case-sensitive characters without spaces and the following: \ / : < > | @ ' % * " ?

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event client-no-response action authorize service-scheme** *service-scheme* command in the 802.1X access profile view.

19.11.2.6 authentication event portal-server-down action authorize (upgrade-compatible command)

Function

The **authentication event portal-server-down action authorize** command configures network access policies for users when the Portal server is Down.

The **undo authentication event portal-server-down action authorize** command deletes the configured network access policies.

By default, no network access policy is configured for users when the Portal server is Down.

Format

authentication event portal-server-down action authorize service-scheme *service-scheme*

undo authentication event portal-server-down action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme*	Specifies the name of the service scheme based on which network access policies are assigned to users.	The value is a string of 1 to 32 case-sensitive characters without spaces and the following: \ / : < > | @ ' % * " ?

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event portal-server-down action authorize service-scheme** *service-scheme* command in the portal access profile view.

19.11.2.7 authentication event portal-server-up action re-authen (upgrade-compatible command)

Function

The **authentication event portal-server-up action re-authen** command enables the device to re-authenticate users when the Portal server changes from Down to Up.

The **undo authentication event portal-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users when the Portal server changes from Down to Up.

Format

authentication event portal-server-up action re-authen

undo authentication event portal-server-up action re-authen

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication event portal-server-up action re-authen** command in the portal access profile view.

19.11.2.8 authentication timer arp handshake-period (upgrade-compatible command)

Function

The **authentication timer arp handshake-period** command sets the handshake interval of the device with pre-connection users and authorized users.

The **undo authentication timer arp** command restores the default setting.

The default handshake interval of the device with pre-connection users and authorized users is 300 seconds.

Format

authentication timer arp handshake-period *handshake-period*

undo authentication timer arp

Parameters

Parameter	Description	Value
handshake-period	Specifies the handshake interval.	The value is an integer that ranges from 5 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer handshake-period** *handshake-period* command in the authentication profile view.

19.11.2.9 authentication timer handshake-period (upgrade-compatible command)

Function

The **authentication timer handshake-period** command sets the handshake interval of the device with pre-connection users and authorized users.

The **undo authentication timer handshake-period** command restores the default setting.

The default handshake interval of the device with pre-connection users and authorized users is 300 seconds.

Format

authentication timer handshake-period *handshake-period*

undo authentication timer handshake-period

Parameters

Parameter	Description	Value
handshake-period	Specifies the handshake interval.	The value is an integer that ranges from 5 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer handshake-period** *handshake-period* command in the authentication profile view.

19.11.2.10 authentication timer authen-fail-user-aging (upgrade-compatible command)

Function

The **authentication timer authen-fail-user-aging** command configures the aging time for entries of the users who fail to be authenticated.

The **undo authentication timer authen-fail-user-aging** command restores the default aging time for entries of the users who fail to be authenticated.

By default, the aging time for entries of the users who fail to be authenticated is 23 hours.

Format

authentication timer authen-fail-user-aging *aging-time*

undo authentication timer authen-fail-user-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer authen-fail-aging** *aging-time* command in the authentication profile view.

19.11.2.11 authentication timer pre-authen-user-aging (upgrade-compatible command)

Function

The **authentication timer pre-authen-user-aging** command configures the aging time for pre-connection user entries.

The **undo authentication timer pre-authen-user-aging** command restores the default aging time for pre-connection user entries.

By default, the aging time for pre-connection user entries is 23 hours.

Format

authentication timer pre-authen-user-aging *aging-time*

undo authentication timer pre-authen-user-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer pre-authen-aging** *aging-time* command in the authentication profile view.

19.11.2.12 authentication timer re-authen (upgrade-compatible command)

Function

The **authentication timer re-authen** command configures the interval for re-authenticating pre-connection users or users who fail to be authenticated.

The **undo authentication timer re-authen** command restores the default setting.

By default, pre-connection users and users who fail to be authenticated are re-authenticated at an interval of 60 seconds.

Format

authentication timer re-authen { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* }

undo authentication timer re-authen { **pre-authen** | **authen-fail** }

Parameters

Parameter	Description	Value
pre-authen *re-authen-time*	Specifies the interval for re-authenticating pre-connection users.	The value is an integer that ranges from 0 or 30 to 7200, in seconds. The value **0** indicates that the re-authentication function is disabled for pre-connection users.
authen-fail *re-authen-time*	Specifies the interval for re-authenticating users who fail to be authenticated.	The value is an integer that ranges from 30 to 7200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication timer re-authen** { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* } command in the authentication profile view.

19.11.2.13 authentication device-type voice authorize (upgrade-compatible command)

Function

The **authentication device-type voice authorize** command enables voice terminals to go online without authentication.

The **undo authentication device-type voice authorize** command disables voice terminals from going online without authentication.

By default, voice terminals are disabled from going online without authentication.

Format

authentication device-type voice authorize [**service-scheme** *scheme-name*]

undo authentication device-type voice authorize [**service-scheme**]

Parameters

Parameter	Description	Value
service-scheme	Assigns network access rights to voice terminals based on a specified service scheme.	-
scheme-name	Specifies the name of the service scheme based on which network access rights are assigned to voice terminals.	The value must be an existing service scheme name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication device-type voice authorize service-scheme** *scheme-name* command in the authentication profile view.

19.11.2.14 authentication free-rule (upgrade-compatible command)

Function

The **authentication free-rule** command configures the NAC authentication-free rule for users.

The **undo authentication free-rule** command restores the default configuration.

By default, no NAC authentication-free rule is configured.

Format

authentication free-rule *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } } *

undo authentication free-rule { *rule-id* | **all** }

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of the NAC authentication-free rule.	The value is an integer of which the range depends on product models
destination	Specifies the destination network resources that the authentication-free users can access.	-
source	Specifies the source information of the authentication-free users.	-
any	Specifies any condition. When **any** is used together with different keywords, the effect of the command is different.	-

Parameter	Description	Value
ip *ip-address*	Specifies the IP address in the rule. This parameter can specify the source or destination address depending on the keyword.	The value is in dotted decimal notation.
mask *mask-length*	Specifies the mask length of an IP address. This parameter can specify the source or destination address mask depending on the keyword.	The value is an integer that ranges from 1 to 32.
mask *ip-mask*	Specifies the IP address mask. This parameter can specify the source or destination address mask depending on the keyword.	The value is in dotted decimal notation.
tcp destination-port *port*	Specifies the TCP destination port number.	The value is an integer that ranges from 1 to 65535.
udp destination-port *port*	Specifies the UDP destination port number.	The value is an integer that ranges from 1 to 65535.
interface *interface-type interface-number*	Specifies the type and number of the source interface in the rule. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Specifies the VLAN ID of the source packet in the rule.	The value is an integer that ranges from 1 to 4094.
all	Specifies all rules.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **free-rule** *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } [**tcp destination-port** *port* | **udp destination-port** *port*] | **any** } } | **source** { **any** | { **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } | **vlan** *vlan-id* } * } } * command in the authentication-free rule profile view.

19.11.2.15 authentication max-user (upgrade-compatible command)

Function

The **authentication max-user** command configures the maximum number of authenticated users allowed in a VAP profile.

The **undo authentication max-user** command restores the default setting.

By default, a maximum of 128 authenticated users are allowed in a VAP profile.

Format

authentication max-user *max-user-number*

undo authentication max-user

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of users.	The value is an integer that ranges from 1 to 128.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication wlan-max-user** *max-user-number.*

19.11.2.16 authentication mode (upgrade-compatible command)

Function

The **authentication mode** command configures the user access mode.

The **undo authentication mode** command restores the default user access mode.

By default, the user access mode is **multi-authen**.

Format

authentication mode { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [**max-user** *max-user-number*] }

undo authentication mode [**multi-authen max-user**]

Parameters

Parameter	Description	Value
single-terminal	Specifies the interface to allow only one user to go online.	-
single-voice-with-data	Specifies the interface to allow only one data user and one voice user to go online. This mode applies to the scenario in which a data user connects to a network through a voice terminal.	-
multi-share	Specifies the interface to allow multiple users to go online. In this mode, the device only authenticates the first user. If the first user can be authenticated, the subsequent users share the same network access rights with the first user. If the first user goes offline, other users are also offline.	-
multi-authen	Specifies the interface to allow multiple users to go online. In this mode, the device authenticates each access user. If users can be authenticated, the users have their individual network access rights. If a user goes offline, other users are not affected.	-

Parameter	Description	Value
max-user *max-user-number*	Specifies the maximum number of access users on the interface in **multi-authen** mode.	The value is an integer that depends on device types.

Views

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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication mode** { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [**max-user** *max-user-number*] } command in the authentication profile view.

19.11.2.17 authentication (upgrade-compatible command)

Function

The **authentication** command enables NAC authentication.

The **undo authentication** command disables NAC authentication.

By default, NAC authentication is disabled.

Format

Layer 2 interface view:

authentication { { **dot1x** | **mac-authen** } * [**portal**] | **portal** }

undo authentication { **dot1x** | **mac-authen** | **portal** } *

VLANIF interface view:

authentication { **mac-authen** [**portal**] | **portal** }

undo authentication { **mac-authen** | **portal** } *

Layer 3 interface view:

authentication portal

undo authentication portal

Parameters

Parameter	Description	Value
dot1x	Enables 802.1X authentication.	-
mac-authen	Enables MAC address authentication.	-
portal	Enables Portal authentication.	-

Views

VLANIF interface 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x-access-profile** *access-profile-name*, **mac-access-profile** *access-profile-name*, and **portal-access-profile** *access-profile-name* commands in the authentication profile view.

19.11.2.18 authentication single-access (upgrade-compatible command)

Function

The **authentication single-access** command enables the device to allow users to access in only one authentication mode.

The **undo authentication single-access** command restores the default setting.

By default, the device allows users to access in different authentication modes.

Format

authentication single-access

undo authentication single-access

Parameters

None

Views

System view, VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication single-access** command in the authentication profile view.

19.11.2.19 authentication trigger-condition dhcp dhcp-option (upgrade-compatible command)

Function

The **authentication trigger-condition dhcp dhcp-option** command enables the device to send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

The **undo authentication trigger-condition dhcp dhcp-option** command restores the default configuration.

By default, the device does not send DHCP option information to the authentication server when triggering MAC address authentication through DHCP packets.

Format

authentication trigger-condition dhcp dhcp-option *option-code*

undo authentication trigger-condition dhcp dhcp-option *option-code*

Parameters

Parameter	Description	Value
option-code	Specifies the option that the device sends to the authentication server.	The value is fixed as 82.

Views

System 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication trigger-condition dhcp dhcp-option** *option-code* command in the mac access profile view.

19.11.2.20 authentication trigger-condition (802.1X authentication) (upgrade-compatible command)

Function

The **authentication trigger-condition** command configures the packet types that can trigger 802.1X authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP packets can trigger 802.1X authentication.

Format

authentication trigger-condition { **dhcp** | **arp** } *

undo authentication trigger-condition [**dhcp** | **arp**] *

Parameters

Parameter	Description	Value
dhcp	Triggers 802.1X authentication through DHCP packets.	-
arp	Triggers 802.1X authentication through ARP packets.	-

Views

System view, VLANIF interface 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication trigger-condition** { **dhcp** | **arp** } * command in the 802.1X access profile view.

19.11.2.21 authentication trigger-condition (MAC address authentication) (upgrade-compatible command)

Function

The **authentication trigger-condition** command configures the packet types that can trigger MAC address authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP/DHCPv6/ND packets can trigger MAC address authentication.

Format

authentication trigger-condition { **dhcp** | **arp** | **dhcpv6** | **nd** } *

undo authentication trigger-condition [**dhcp** | **arp** | **dhcpv6** | **nd**] *

Parameters

Parameter	Description	Value
dhcp	Triggers MAC address authentication through DHCP packets.	-
arp	Triggers MAC address authentication through ARP packets.	-
dhcpv6	Triggers MAC address authentication through DHCPv6 packets.	-
nd	Triggers MAC address authentication through ND packets.	-

Views

System view, VLANIF interface 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **authentication trigger-condition** { **dhcp** | **arp** | **dhcpv6** | **nd** } * command in the mac access profile view.

19.11.2.22 domain (upgrade-compatible command)

Function

The **domain** command configures the default domain or force domain for users.

The **undo domain** command deletes the configured default domain or force domain.

By default, no default domain or force domain is configured for users.

Format

Layer 2 interface view:

domain name *domain-name* [**dot1x** | **mac-authen** | **portal**] [**force**]

undo domain name *domain-name* [**dot1x** | **mac-authen** | **portal**] [**force**]

VLANIF interface view:

domain name *domain-name* [**mac-authen** | **portal**] [**force**]

undo domain name *domain-name* [**mac-authen** | **portal**] [**force**]

Layer 3 interface view:

domain name *domain-name* [**portal**] [**force**]

undo domain name *domain-name* [**portal**] [**force**]

System view (for all access authentication users):

domain *domain-name* **force** [**mac-address** *mac-address* **mask** *mask*]

undo domain *domain-name* **force** [**mac-address** *mac-address*]

System view (only for MAC address authentication users):

domain *domain-name* **mac-authen force**

undo domain *domain-name* **mac-authen force**

domain name *domain-name* **mac-authen force** [**mac-address** *mac-address* **mask** *mask*]

undo domain name *domain-name* **mac-authen force** [**mac-address** *mac-address*]

Parameters

Parameter	Description	Value
name *domain-name*	Specifies the name of the default domain or force domain. If no user authentication mode is specified, the default domain or force domain takes effect for all access authentication users.	The value must be an existing domain name on the device.
dot1x	Specifies 802.1X authentication as the user authentication mode.	-
mac-authen	Specifies MAC address authentication as the user authentication mode.	-
portal	Specifies Portal authentication as the user authentication mode.	-

Views

System view, VLANIF interface 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **access-domain** *domain-name* [**dot1x** | **mac-authen** | **portal**]* [**force**] command in the authentication profile view.

19.11.2.23 dot1x authentication-method (upgrade-compatible command)

Function

The **dot1x authentication-method** command sets the authentication mode for 802.1X users.

The **undo dot1x authentication-method** command restores the default authentication mode for 802.1X users.

By default, the global 802.1X user authentication mode is CHAP authentication and the 802.1X user authentication mode on interfaces is the same as the mode globally configured.

Format

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

Parameters

Parameter	Description	Value
chap	Indicates the CHAP-based EAP termination authentication mode.	-
pap	Indicates the PAP-based EAP termination authentication mode.	-
eap	Indicates that the EAP relay mode.	-

Views

System 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x authentication-method** { **chap** | **pap** | **eap** } command in the 802.1X access profile view.

19.11.2.24 dot1x eap-notify-packet (upgrade-compatible command)

Function

The **dot1x eap-notify-packet** command enables the device to send an EAP packet code number to users.

The **undo dot1x eap-notify-packet** command disables the device from sending an EAP packet code number to users.

By default, the device is disabled from sending an EAP packet code number to users.

Format

dot1x eap-notify-packet eap-code *code-number* **data-type** *type-number*

undo dot1x eap-notify-packet [**eap-code** *code-number* **data-type** *type-number*]

Parameters

Parameter	Description	Value
eap-code *code-number*	Specifies an EAP packet code number sent to users.	The value is an integer that ranges from 5 to 255. The default value is 255.
data-type *type-number*	Specifies the data type in EAP packets sent to users.	The value is an integer that ranges from 1 to 255. The default value is 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x eap-notify-packet eap-code** *code-number* **data-type** *type-number* command in the 802.1X access profile view.

19.11.2.25 dot1x handshake (upgrade-compatible command)

Function

The **dot1x handshake** command enables the device to send handshake packets to online 802.1X users.

The **undo dot1x handshake** command disables the device from sending handshake packets to online 802.1X users.

By default, the device handshake function is disabled for online 802.1X users.

Format

dot1x handshake

undo dot1x handshake

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x handshake** command in the dot1x access profile view.

19.11.2.26 dot1x reauthenticate (upgrade-compatible command)

Function

The **dot1x reauthenticate** command enables periodic 802.1X re-authentication on an interface.

The **undo dot1x reauthenticate** command disables periodic 802.1X re-authentication on an interface.

By default, periodic 802.1X re-authentication is disabled on an interface.

Format

dot1x reauthenticate

undo dot1x reauthenticate

Parameters

None

Views

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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x reauthenticate** command in the 802.1X access profile view.

19.11.2.27 dot1x retry (upgrade-compatible command)

Function

The **dot1x retry** command sets the maximum number of times an authentication request is sent to an 802.1X user.

The **undo dot1x retry** command restores the default setting.

By default, the device sends an authentication request to an 802.1X user twice.

Format

dot1x retry *max-retry-value*

undo dot1x retry

Parameters

Parameter	Description	Value
max-retry-value	Specifies the maximum number of times an authentication request is sent to an 802.1X user. The default value is recommended.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x retry** *max-retry-value* command in the 802.1X access profile view.

19.11.2.28 dot1x timer reauthenticate-period (upgrade-compatible command)

Function

The **dot1x timer reauthenticate-period** command sets the re-authentication interval for 802.1X authentication users.

The **undo dot1x timer reauthenticate-period** command restores the default re-authentication interval.

By default, the re-authentication interval is 3600 seconds.

Format

dot1x timer reauthenticate-period *reauthenticate-period-value*

undo dot1x timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for 802.1X address authentication users.	The value is an integer that ranges from 60 to 7200, in seconds.

Views

System 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x timer reauthenticate-period** *reauthenticate-period-value* command in the802.1X access profile view.

19.11.2.29 dot1x timer (upgrade-compatible command)

Function

The **dot1x timer** command sets values of timers used in 802.1X authentication.

The **undo dot1x timer** command restores the default settings of timers used in 802.1X authentication.

By default, the values of timers used in 802.1X authentication are not set.

Format

dot1x timer { **client-timeout** *client-timeout-value* | **handshake-period** *handshake-period-value* | **eth-trunk-access handshake-period** *handshake-period-value* }

undo dot1x timer { **client-timeout** | **handshake-period** | **eth-trunk-access handshake-period** }

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the timeout interval of the authentication response from the client. For details, see **19.11.2.27 dot1x retry (upgrade-compatible command)**.	The value is an integer that ranges from 1 to 120, in seconds. By default, the timeout interval of the authentication response from the client is 5 seconds.
handshake-period *handshake-period-value*	Specifies the handshake interval between the device and 802.1X authentication client connected to a non-Eth-Trunk interface. For details, see **19.11.2.25 dot1x handshake (upgrade-compatible command)**.	The value is an integer that ranges from 5 to 7200, in seconds. By default, the interval for sending handshake packets is 15 seconds.

Parameter	Description	Value
eth-trunk-access handshake-period *handshake-period-value*	Specifies the handshake interval between the device and 802.1X authentication client connected to an Eth-Trunk. For details, see **19.11.2.25 dot1x handshake (upgrade-compatible command)**.	The value is an integer that ranges from 30 to 7200, in seconds. By default, the interval for sending handshake packets is 120 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x timer** { **client-timeout** *client-timeout-value* | **handshake-period** *handshake-period-value* | **eth-trunk-access handshake-period** *handshake-period-value* } command in the 802.1X access profile view.

19.11.2.30 dot1x trigger dhcp-binding (upgrade-compatible command)

Function

The **dot1x trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-connection phase.

The **undo dot1x trigger dhcp-binding** command restores the default setting.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

Format

dot1x trigger dhcp-binding

undo dot1x trigger dhcp-binding

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x trigger dhcp-binding** command in the dot1x access profile view.

19.11.2.31 dot1x unicast-trigger (upgrade-compatible command)

Function

The **dot1x unicast-trigger** command enables 802.1X authentication triggered by unicast packets.

The **undo dot1x unicast-trigger** command disables 802.1X authentication triggered by unicast packets.

By default, 802.1X authentication triggered by unicast packets is disabled.

Format

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

None

Views

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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **dot1x unicast-trigger** command in the 802.1X access profile view.

19.11.2.32 mac-authen offline dhcp-release (upgrade-compatible command)

Function

The **mac-authen offline dhcp-release** command enables the device to clear user entries when receiving DHCP Release packets from MAC address authentication users.

The **undo mac-authen offline dhcp-release** command restores the default configuration.

By default, the device does not clear user entries when receiving DHCP Release packets from MAC address authentication users.

Format

In the system view:

mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

undo mac-authen offline dhcp-release interface { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>

In the interface view:

mac-authen offline dhcp-release

undo mac-authen offline dhcp-release

Parameters

Parameter	Description	Value
interface *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. *interface-number2* and *interface-number1* together specify an interface range.	-

Views

System 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen offline dhcp-release** command in the mac access profile view.

19.11.2.33 mac-authen permit mac-address (upgrade-compatible command)

Function

The **mac-authen permit mac-address** command specifies the MAC address range allowed for MAC address authentication.

The **undo mac-authen permit mac-address** command deletes the MAC address range allowed for MAC address authentication.

By default, no MAC address range is specified for MAC address authentication.

Format

mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

undo mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for MAC address authentication.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the MAC address mask.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask-length*	Specifies the MAC address mask length.	The value is an integer that ranges from 1 to 48.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen permit mac-address** *mac-address* **mask** { *mask* | *mask-length* } command in the mac access profile view.

19.11.2.34 mac-authen reauthenticate dhcp-renew (upgrade-compatible command)

Function

The **mac-authen reauthenticate dhcp-renew** command enables the device to re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

The **undo mac-authen reauthenticate dhcp-renew** command restores the default setting.

By default, the device does not re-authenticate the users when receiving DHCP lease renewal packets from MAC address authentication users.

Format

mac-authen reauthenticate dhcp-renew

undo mac-authen reauthenticate dhcp-renew

Parameters

None

Views

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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen reauthenticate dhcp-renew** command in the mac access profile view.

19.11.2.35 mac-authen reauthenticate (upgrade-compatible command)

Function

The **mac-authen reauthenticate** command enables periodic MAC address re-authentication on a specified interface.

The **undo mac-authen reauthenticate** command disables periodic MAC address re-authentication on a specified interface.

By default, periodic MAC address re-authentication is enabled on a specified interface.

Format

mac-authen reauthenticate

undo mac-authen reauthenticate

Parameters

None

Views

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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen reauthenticate** command in the mac access profile view.

19.11.2.36 mac-authen timer reauthenticate-period (upgrade-compatible command)

Function

The **mac-authen timer reauthenticate-period** command sets the re-authentication interval for MAC address authentication users.

The **undo mac-authen timer reauthenticate-period** command restores the default re-authentication interval.

By default, the re-authentication interval is 1800 seconds.

Format

mac-authen timer reauthenticate-period *reauthenticate-period-value*

undo mac-authen timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the re-authentication interval for MAC address authentication users.	The value is an integer that ranges from 60 to 7200, in seconds.

Views

System 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen timer reauthenticate-period** *reauthenticate-period-value* command in the mac access profile view.

19.11.2.37 mac-authen username (upgrade-compatible command)

Function

The **mac-authen username** command configures the user name format for MAC address authentication.

The **undo mac-authen username** restores the default user name format.

By default, the MAC address without hyphens (-) is used as the user name and password for MAC address authentication.

Format

mac-authen username { **fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** | **without-hyphen** } [**password cipher** *password*]] | **dhcp-option** *option-code* { **circuit-id** | **remote-id** } **password cipher** *password* }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** | **without-hyphen** } [**password cipher** *password*]] | **dhcp-option** *option-code* [**password cipher** *password*]]

Parameters

Parameter	Description	Value
fixed *username*	Specifies the fixed user name for MAC address authentication.	The value is a string of 1 to 64 case-sensitive that do not contain spaces and question marks (?).

Parameter	Description	Value
password cipher *password*	Specifies the password displayed in cipher text for MAC address authentication. ● The user with a fixed name can log in without a password if no password is set, which is not recommended. ● When a MAC address is used as the user name, the MAC address can be used as the password if no password is set. When local authentication is specified in the AAA authentication scheme, you must set a password. ● If the DHCP option is used as the user name, you must set a password. **NOTE** If fixed user names are configured in the VLANIF interface view, Eth-Trunk interface view or Port group view, the password must be set. If a MAC address is configured as the user name in the Port group view, the password cannot be set.	The value is a case-sensitive string without question marks (?) or spaces. The password contains 1 to 128 characters in plain text or 48 to 188 characters in cipher text. **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.
macaddress	Specifies that the user name in MAC address authentication is the MAC address.	-
format	Specifies the format of the MAC address.	-
with-hyphen	Specifies that the MAC address with hyphens is used as the user name, for example, 0005-e01c-02e3.	-

Parameter	Description	Value
without-hyphen	Specifies that the MAC address without hyphens is used as the user name, for example, 0005e01c02e3.	-
dhcp-option *option-code*	Specifies the name of the MAC address authentication user to a specified DHCP option. ● **circuit-id**: Specifies the circuit ID in the DHCP Option82 as the user name in MAC address authentication. ● **remote-id**: Specifies the remote ID in the DHCP Option82 as the user name in MAC address authentication. **NOTE** In VLANIF interface view, the parameter does not support.	The value is an integer. In the current version, the value is fixed as 82.

Views

System view, VLANIF interface 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **mac-authen username** command in the mac access profile view.

19.11.2.38 portal auth-network (upgrade-compatible command)

Function

The **portal auth-network** command configures a source subnet for Portal authentication.

The **undo portal auth-network** command restores the default source subnet for Portal authentication.

By default, the source subnet for Portal authentication is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

Format

portal auth-network *network-address* { *mask-length* | *mask-address* }

undo portal auth-network { *network-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
network-address	Specifies the IP address of the source subnet for Portal authentication.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 1 to 32.
mask-address	Specifies the mask of the source subnet for Portal authentication.	The value is in dotted decimal notation.
all	Deletes all Portal authentication subnets.	-

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **portal auth-network** *network-address* { *mask-length* | *mask-address* } command in the portal access profile view.

19.11.2.39 portal local-server anonymous (upgrade-compatible command)

Function

The **portal local-server anonymous** command enables anonymous login for users in built-in Portal authentication.

The **undo portal local-server anonymous** command disables anonymous login for users in built-in Portal authentication.

By default, anonymous login for users in built-in Portal authentication is disabled.

Format

portal local-server anonymous

undo portal local-server anonymous

Parameters

None

Views

VLANIF interface 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **portal local-server anonymous** command in the portal access profile view.

19.11.2.40 portal timer offline-detect (upgrade-compatible command)

Function

The **portal timer offline-detect** command sets the Portal user offline detection interval.

The **undo portal timer offline-detect** command restores the default Portal user offline detection interval.

By default, the Portal user offline detection interval is 300 seconds.

Format

portal timer offline-detect *time-length*

undo portal timer offline-detect

Parameters

Parameter	Description	Value
time-length	Specifies the Portal user offline detection interval.	The value is 0 or an integer that ranges from 30 to 7200, in seconds. The default value is 300. The value 0 indicates that offline detection is not performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **portal timer offline-detect** *time-length* command in the portal access profile view.

19.11.2.41 url (URL template view) (upgrade-compatible command)

Function

The **url** command configures the redirection URL or pushed URL.

The **undo url** command cancels the redirection URL or pushed URL.

By default, no redirection URL or pushed URL is configured.

Format

url [**ssid** *ssid*] [**push-only** | **redirect-only**] *url-string*

Parameters

Parameter	Description	Value
url-string	Specifies the redirection URL of the Portal server or pushed URL.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?).

Parameter	Description	Value
ssid *ssid*	Specifies the SSID that users associate with.	The SSID must already exist.
push-only	Specifies the URL as a pushed URL.	-
redirect-only	Specifies the URL as a redirection URL.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

# Set the redirection URL to http://10.1.1.1.

```
<HUAWEI> system-view
[HUAWEI] url-template name huawei
[HUAWEI-url-template-huawei] url http://10.1.1.1
```

19.11.2.42 ucl-group (upgrade-compatible command)

Function

The **ucl-group** command creates a UCL group.

By default, no UCL group is created.

Format

ucl-group name *group-name* [**extend**]

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a UCL group.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Parameter	Description	Value
extend	Extends the maximum number of UCL groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

# Create a UCL group named **abc**.

```
<HUAWEI> system-view
[HUAWEI] ucl-group name abc
```

19.11.2.43 voice-vlan (service scheme view) (upgrade-compatible command)

Function

The **voice-vlan** command configures a voice VLAN in a service scheme.

The **undo voice-vlan** command deletes the voice VLAN configured in the service scheme.

By default, no voice VLAN is configured in the service scheme.

Format

voice-vlan *vlan-id*

undo voice-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the voice VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

Example

# Configure voice VLAN 100 in the service scheme **huawei**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] service-scheme huawei
[HUAWEI-aaa-service-huawei] voice-vlan 100
```

19.11.2.44 web-auth-server (interface view) (upgrade-compatible command)

Function

The **web-auth-server** command binds a Portal server template to an interface.

The **undo web-auth-server** command unbinds a Portal server template from an interface.

By default, no Portal server template is bound to an interface.

Format

- Layer 2 interface view

  web-auth-server *server-name* [*bak-server-name*] **direct**

  undo web-auth-server [*server-name* [*bak-server-name*] **direct**]
- VLANIF interface view

  web-auth-server *server-name* [*bak-server-name*] { **direct** | **layer3** }

  undo web-auth-server [*server-name* [*bak-server-name*] { **direct** | **layer3** }]
- Routed main interface view

  web-auth-server *server-name* [*bak-server-name*] **layer3**

  undo web-auth-server [*server-name* [*bak-server-name*] **layer3**]

Parameters

Parameter	Description	Value
server-name	Specifies the name of the Portal server template.	The value must be an existing Portal server template name.
bak-server-name	Specifies the name of the secondary Portal server template. **NOTE** The name of the secondary Portal server template cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server template name.
direct	Specifies Layer 2 authentication as the Portal authentication mode. When there is no Layer 3 forwarding device between the device and users, configure the Layer 2 authentication mode.	-
layer3	Specifies Layer 3 authentication as the Portal authentication mode. When there is a Layer 3 forwarding device between the device and users, configure the Layer 3 authentication mode.	-

Views

VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, 40GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **web-auth-server** *server-name* [*bak-server-name*] { **direct** | **layer3** } command in the portal access profile view.

19.12 Security Compatible Commands

19.12.1 ACL Compatible Commands

19.12.1.1 acl ipv6 (upgrade-compatible command)

Function

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

The **undo acl ipv6** command deletes an ACL.

Format

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

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

Parameters

Parameter	Description	Value
number *acl6-number*	Indicates the ID of an ACL6.	The value of *acl6-number* is an integer that ranges from 2000 to 3999. In these options, • ACL6s numbered from 2000 to 2999 are basic ACL6s. • ACL6s numbered from 3000 to 3999 are advanced ACL6s.

Parameter	Description	Value
name *acl6-name*	Specifies a named ACL6.	The value of *acl6-name* is a string of 1 to 64 case-sensitive characters without spaces. The name starts with a letter (case-sensitive) and can contain letters, digits, and symbols such as the number sign (#), percentage symbol (%), and hyphen (-).
all	Deletes all ACL6s.	-
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 ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. 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 which packets need to be filtered.

Example

# Create an ACL6 named test and numbered 3100.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3100 name test
[HUAWEI-acl6-adv-test]
```

19.12.1.2 acl (upgrade-compatible command)

Function

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

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

Format

acl [**number**] *acl-number* [**name** *acl-name*]

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

Parameters

Parameter	Description	Value
number *acl-number*	Indicates the ID of an ACL.	The value of *acl-number* is an integer that ranges from 2000 to 5999. ● ACLs numbered from 2000 to 2999 are basic ACLs. ● ACLs numbered from 3000 to 3999 are advanced ACLs. ● ACLs numbered from 4000 to 4999 are Layer 2 ACLs. ● ACLs numbered from 5000 to 5999 are customized ACLs.
name *acl-name*	Specifies a named ACL.	The value of *acl-name* is a string of 1 to 32 case-sensitive characters without spaces. The name starts with a letter (case-sensitive) and can contain letters, digits, and symbols such as the number sign (#), percentage symbol (%), and hyphen (-).
all	Deletes all ACLs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An ACL consists of a list of rules. Each rule contains a permit or deny clause. Before creating an ACL rule, you must create an ACL.

Example

# Create an ACL named test and numbered 3100.

```
<HUAWEI> system-view
[HUAWEI] acl number 3100 name test
[HUAWEI-acl-adv-test]
```

19.12.1.3 rule (advanced ACL6 view) (upgrade-compatible command)

Function

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

Format

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

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

Parameters

Parameter	Description	Value
rule-id	Indicates the ID of an ACL6 rule.	The value ranges from 0 to 2047. ● If the ID of a rule is specified and the rule exists, the new rule is added to the rule with this ID, that is, the old rule is modified. ● If the rule associated with a rule ID does not exist, a rule can be created with this rule ID and its position in the ACL is determined by the rule ID. ● If no rule ID is specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order.
deny	Discards packets that do not match ACL rules.	-
permit	Allows packets to pass.	-
ipv6-ah	Indicates the protocol type.	-

Parameter	Description	Value
ipv6-esp	Indicates the protocol type.	-
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 value of a Differentiated Services CodePoint (DSCP).	The value ranges from 0 to 63.
fragment	Indicates that the rule is valid for only non-initial fragments.	-
logging	Indicates whether to record logs for packets that meet ACL rules.	Log contents include the ACL rule ID, pass or discard of packets, type of the protocol over IP, source or destination address, source or destination port number, and number of packets.
precedence *precedence*	Filters packets by priority.	The value is a name or a digit that 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.
time-range *time-name*	Specifies the time range only in which ACL6 rules are effective. *time-name* indicates the name of the time range.	The value is a string of 1 to 32 characters.
tos *tos*	Filters packets by Type of Service (ToS).	The value is a name or a digit that ranges from 0 to 15.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The vpn-instance must already exist.

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.

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 may 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. Exercise caution when you run the **undo rule** command.

Example

# Create an advanced ACL6 with ID 3000 and configure a rule that allows only IPv6 ESP packets with the source IPv6 address 2030:5060::9050 and mask 64 to pass.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 number 3000
[HUAWEI-acl6-adv-3000] rule 0 permit ipv6-esp source 2030:5060::9050/64
```

19.12.2 Local Attack Defense Compatible Commands

19.12.2.1 blacklist (upgrade-compatible command)

Function

The **blacklist** command configures an ACL-based blacklist.

By default, no blacklist is configured.

Format

blacklist *blacklist-id* **acl** *acl-number* **soft-drop**

Parameters

Parameter	Description	Value
acl *acl-number*	Indicates the ACL ID. The ACL referenced by a blacklist 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.
soft-drop	Indicates that the blacklist is implemented through software.	-
blacklist-id	Specifies the number of an ACL6 referenced by a blacklist.	The value is an integer that ranges from 2000 to 3999. ● 2000 to 2999: basic ACL6s ● 3000 to 3999: advanced ACL6s

Views

System view, Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

A maximum of 8 blacklists can be configured in an attack defense policy on the device. You can set the attributes of a blacklist by defining ACL rules.

The packets sent from users in the blacklist are discarded after reaching the device.

Example

# Reference ACL 2001 in the blacklist.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] blacklist acl 2001 soft-drop
```

19.12.2.2 car cpu-port (upgrade-compatible command)

Function

The **car cpu-port** command configures the CIR of all the packets to be sent to the CPU.

By default, the CIR value of all the packets to be sent to the CPU is 1024 kbit/s on the device.

Format

car cpu-port cir *cir-rate*

Parameters

Parameter	Description	Value
cir *cir-rate*	Sets the CIR of all the packets to be sent to the CPU.	The value is an integer that ranges from 64 to 2048, in kbit/s.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

The **car cpu-port** command limits the total rate of all protocol packets sent to the CPU. The **car packet-type** command limits the rate of packets of a specified protocol. However, the total CIR of packets of specified protocols cannot exceed the CIR of all the packets sent to the CPU.

When the CIR is exceeded, excess packets including unicast, multicast, and broadcast packets are not sent to the CPU. In addition, the unicast packets are discarded directly.

Example

# Set the CIR of all the packets to be sent to the CPU to 512 kbit/s on the device.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] car cpu-port cir 512
```

19.12.2.3 deny (upgrade-compatible command)

Function

The **deny** command sets the discard action taken for packets sent to the CPU.

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

By default, the device limits the rate of protocol packets and user-defined flows based on the CAR configuration.

Format

deny packet-type bpdu

deny packet-type ftp-dynamic

deny packet-type hotlimit

deny packet-type smlk-rrpp

deny packet-type nac-dhcp

undo deny packet-type bpdu

undo deny packet-type ftp-dynamic

undo deny packet-type hotlimit

undo deny packet-type smlk-rrpp

undo deny packet-type nac-dhcp

Parameters

Parameter	Description	Value
packet-type bpdu	Discards bpdu packets .	-
packet-type ftp-dynamic	Discards ftp-dynamic packets.	-
packet-type hotlimit	Discards hop-limit packets.	-
packet-type smlk-rrpp	Discards smlk-rrpp packets.	-
packet-type nac-dhcp	Discards nac-dhcp packets.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

If you run the **deny** and **car** commands for the same type of packets sent to the CPU, the command that runs later takes effect. The **undo deny** command restores the default action taken for packets sent to the CPU. After you run this command, the system limits the rate of packets sent to the CPU based on the configured CIR and CBS values.

Example

# Set the discard action taken for bpdu packets sent to the CPU attack in defense policy test.

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

19.12.3 Attack Defense Compatible Commands

19.12.3.1 application-apperceive default drop (upgrade-compatible command)

Function

The **application-apperceive default drop** command enables the device to discard the received packets when no matching application layer association policy exists.

The **undo application-apperceive default drop** command enables the device to deliver the received packets to the upper layer when no matching application layer association policy exists.

By default, the device is enabled to deliver the received packets to the upper layer when no matching application layer association policy exists.

Format

application-apperceive default drop

undo application-apperceive default drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **application-apperceive default drop** command is run, if a protocol is not enabled in the system view nor in the interface view, the device discards all the packets of this protocol type.

Example

# Enable the device to discard the received packets when no matching application layer association policy exists.

```
<HUAWEI> system-view
[HUAWEI] application-apperceive default drop
```

19.12.4 Traffic Suppression Compatible Commands

19.12.4.1 broadcast-suppression (upgrade-compatible command)

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 traffic rate of broadcast packets that can pass through an interface.

Format

broadcast-suppression { *broadcast-pct* | **packets** *packets-per-second* }

undo broadcast-suppression

Parameters

Parameter	Description	Value
broadcast-pct	Specifies the maximum percentage of broadcast traffic on an interface.	The value ranges from 0 to 100. The default value is 100. By default, broadcast traffic is not suppressed on interfaces.
packets *packets-per-second*	Specifies the maximum number of broadcast packets allowed to pass through an interface per second.	The value of *packets-per-second* is an integer.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the traffic rate of broadcast packets exceeds the maximum value, the system discards excess broadcast packets to control the traffic rate and ensure normal operation of network services.

Example

# Set the maximum percentage of broadcast traffic to 20% of interface bandwidth on Eth-Trunk1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] broadcast-suppression 20
```

19.12.4.2 multicast-suppression (upgrade-compatible command)

Function

The **multicast-suppression** command sets the maximum traffic rate of multicast packets that can pass through an interface.

The **undo multicast-suppression** command restores the default traffic rate of multicast packets that can pass through an interface.

Format

multicast-suppression { *multicast-pct* | **packets** *packets-per-second* }

undo multicast-suppression

Parameters

Parameter	Description	Value
multicast-pct	Specifies the maximum percentage of multicast traffic on an Ethernet interface.	The value ranges from 0 to 100. The default value is 100. By default, multicast traffic is not suppressed on interfaces.
packets *packets-per-second*	Specifies the maximum number of multicast packets allowed to pass through an interface per second.	The value of *packets-per-second* is an integer.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the traffic rate of multicast packets exceeds the maximum value, the system discards excess multicast packets to control the traffic rate and ensure normal operation of network services.

Example

# Set the maximum percentage of multicast traffic to 20% of interface bandwidth on Eth-Trunk1.

```
<HUAWEI> system-view
[HUAWEI] interface eth-trunk 1
[HUAWEI-Eth-Trunk1] multicast-suppression 20
```

19.12.4.3 unicast-suppression (upgrade-compatible command)

Function

The **unicast-suppression** command sets the maximum traffic rate of unknown unicast packets that can pass through an interface.

The **undo unicast-suppression** command restores the default traffic rate of unknown unicast packets that can pass through an interface.

Format

unicast-suppression { *unicast-pct* | **packets** *packets-per-second* }

undo unicast-suppression

Parameters

Parameter	Description	Value
unicast-pct	Specifies maximum percentage of unknown unicast traffic on an Ethernet interface.	The value ranges from 0 to 100. The default value is 100. By default, unknown unicast traffic is not suppressed on interfaces.
packets *packets-per-second*	Specifies the maximum number of unknown unicast packets allowed to pass through an interface per second.	The value of *packets-per-second* is an integer.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When the traffic rate of unknown unicast packets exceeds the maximum value, the system discards excess unknown unicast packets to control the traffic rate and ensure normal operation of network services.

Example

# Set the maximum percentage of unknown unicast traffic to 20% of interface bandwidth on Eth-Trunk1.

```
<HUAWEI> system-view
```

```
[HUAWEI] interface eth-trunk1
[HUAWEI-Eth-Trunk1] unicast-suppression 20
```

19.12.4.4 storm-control action (upgrade-compatible command)

Function

The **storm-control action** sets the storm control action to **shutdown**.

The **undo storm-control action** command cancels the configuration.

By default, no storm control action is configured.

Format

storm-control action shutdown

undo storm-control action

Parameters

Parameter	Description	Value
shutdown	Shuts down an interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **storm-control action error-down** command.

Example

# Configure the storm control action is **shutdown** on GE0/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] storm-control action shutdown
```

19.12.5 ARP Security Compatible Commands

19.12.5.1 arp anti-attack rate-limit (upgrade-compatible command)

Function

The **arp anti-attack rate-limit** command sets the maximum rate and rate limit duration of ARP packets globally, in a VLAN, or on an interface, 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 limit 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 in 1 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-number* [*interval-value*]

Interface view

arp anti-attack rate-limit *packet-number* [*interval-value* | **block timer** *timer*]*

undo arp anti-attack rate-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum rate of sending ARP packets, that is, the number of ARP packets allowed to pass through in the rate limit duration.	The value is an integer that ranges from 1 to 16384. The default value is 100.
interval-value	Specifies the rate limit 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, GE interface view, XGE 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 limit duration of ARP packets globally, in a VLAN, or on an interface. In the rate limit 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 limit duration are 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.

If the maximum rate and rate limit duration are set globally or on an interface at the same time, the configurations on an interface and globally take effect in descending order of priority.

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, only when the number of ARP packets sent to the CPU exceeds the limit, the device discards subsequent ARP packets on the interface.

Example

# Configure GE0/0/1 to allow 200 ARP packet 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 200 10 block timer 60
```

19.12.5.2 arp filter source (upgrade-compatible command)

Function

The **arp filter source** command enables ARP gateway protection for the specified IP address.

The **undo arp filter source** command disables ARP gateway protection for the specified IP address.

By default, ARP gateway protection is disabled.

Format

arp filter source *ip-address*

undo arp filter 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

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, it is replaced by the **arp trust source** command.

19.12.6 DHCP Snooping Compatible Commands

19.12.6.1 dhcp option82 format (upgrade-compatible command)

Function

The **dhcp option82 format** command configures the format of the Option 82 field in DHCP messages.

Format

dhcp option82 [**circuit-id** | **remote-id**] **format userdefined** *text*

Parameters

Parameter	Description	Value
circuit-id	Specifies the format of the circuit-id (CID).	-
remote-id	Specifies the format of the remote-id (RID).	-
userdefined *text*	Indicates the user-defined format of the Option 82 field.	*text* is the user-defined character string of the Option 82 field.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp option82 format** command to configure the format of the Option 82 field in DHCP messages.

Example

# Configure the user-defined string for the CID in the Option 82 field and use the hexadecimal format to encapsulate the CID type (0, indicating the hexadecimal format), length (excluding the length of the CID type and the length keyword itself), outer VLAN ID, slot ID (5 bits), subslot ID (3 bits), and port number (8 bits).

```
<HUAWEI> system-view
[HUAWEI] dhcp option82 circuit-id format userdefined 0 %length %svlan %5slot %3subslot %8port
```

19.12.6.2 dhcp snooping alarm { user-bind | mac-address | untrust-reply } enable (upgrade-compatible command)

Function

The **dhcp snooping alarm enable** command enables the alarm function for DHCP snooping.

The **undo dhcp snooping alarm enable** command disables the alarm function for DHCP snooping.

By default, the alarm function for discarded DHCP messages is disabled.

Format

dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** *threshold* }

undo dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** }

Parameters

Parameter	Description	Value
user-bind	Generates an alarm when the number of DHCP messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-

Parameter	Description	Value
mac-address	Generates an alarm when the number of DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address in the Ethernet frame header reaches the threshold.	-
untrust-reply	Generates an alarm when the number of DHCP Reply messages discarded by untrusted interfaces reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCP 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, Eth-Trunk interface view, Port-group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

It is replaced by the **dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **enable** [**threshold** *threshold*] command.

Example

# On GE0/0/1, enable DHCP snooping, and enable the alarm function for DHCP snooping.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping enable
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping alarm user-bind enable
```

19.12.6.3 dhcp snooping bind-table autosave (upgrade-compatible command)

Function

The **dhcp snooping bind-table autosave** command configures a device to automatically back up DHCP snooping binding entries in a specified file.

Format

dhcp snooping bind-table autosave *file-name* [**write-delay** *delay-time*]

Parameters

Parameter	Description	Value
file-name	Specifies the path for storing the file that backs up DHCP snooping binding entries and the file name. You must specify both the path and name of the file supported by the system.	The value is a string of 1 to 51 characters.
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 system backs up the DHCP snooping binding table every two days.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping bind-table** command to back up DHCP snooping binding entries in a specified file.

Example

# Configure a device to automatically back up DHCP snooping binding entries in the file **backup.tbl** in the flash memory.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping bind-table autosave flash:/backup.tbl
```

19.12.6.4 dhcp snooping check enable (upgrade-compatible command)

Function

The **dhcp snooping check enable** enables the device to check DHCP messages.

The **undo dhcp snooping check enable** disables the device from checking DHCP messages.

By default, the device does not check DHCP messages.

Format

In the system view:

dhcp snooping check { **user-bind** | **mac-address** } **enable vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

undo dhcp snooping check { **user-bind** | **mac-address** } **enable vlan** { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

In the VLAN view, Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, Port-group view:

dhcp snooping check { **user-bind** | **mac-address** } **enable**

undo dhcp snooping check { **user-bind** | **mac-address** } **enable**

Parameters

Parameter	Description	Value
user-bind	Check DHCP messages against the DHCP snooping binding table.	-
mac-address	Compare the MAC address in DHCP ACK or DHCP Request messages with the CHADDR value.	-
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Enables the device to check the HCP 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*.	The value is an integer that ranges from 1 to 4094.

Views

VLAN view, System view, Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, Port-group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the command is used, you can check DHCP messages against the DHCP snooping binding table or Compare the MAC address in DHCP ACK or DHCP Request messages with the CHADDR value.

Example

# Enable the function of checking DHCP messages against the binding table in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping check user-bind enable
```

19.12.6.5 dhcp snooping check dhcp-rate alarm enable (upgrade-compatible command)

Function

The **dhcp snooping check dhcp-rate alarm enable** command enables the device to generate 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 check dhcp-rate alarm { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
threshold *threshold*	Specifies the alarm threshold for checking the rate of sending DHCP messages to the processing unit. An alarm is generated after the rate for sending DHCP messages is checked and the number of discarded DHCP messages reaches the alarm threshold.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the alarm function is enabled, the device sends a trap message when the number of discarded DHCP messages reaches the alarm threshold.

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 snooping check dhcp-rate alarm enable
```

19.12.6.6 dhcp snooping check dhcp-rate enable alarm dhcp-rate enable (upgrade-compatible command)

Function

Using the **dhcp snooping check dhcp-rate enable alarm dhcp-rate enable** command, you can:

- Enable the function of checking the rate of sending DHCP messages to the DHCP protocol stack.
- Set the rate limit of sending DHCP messages to the DHCP protocol stack.
- Enable the DHCP message discard alarm.
- Set the alarm threshold for discarded DHCP messages.

By default, the function of checking the rate of sending DHCP messages to the DHCP stack is disabled; the rate limit of sending DHCP messages to the DHCP stack is 100 pps; the DHCP message discard alarm is disabled; the alarm threshold for discarded DHCP messages is 100.

Format

dhcp snooping check dhcp-rate { **enable** | [**enable**] [**rate**] *rate* } **alarm dhcp-rate** { **enable** | [**enable**] **threshold** *threshold-value* }

Parameters

Parameter	Description	Value
[**rate**] *rate*	Specifies the rate limit of sending DHCP messages to the DHCP protocol stack.	The value ranges from 1 to 100, in pps. The default value is 100.
alarm dhcp-rate enable	Enables the DHCP message discard alarm.	-

Parameter	Description	Value
threshold *threshold-value*	Specifies the alarm threshold for discarded DHCP messages. After the function is enabled, an alarm is generated when the number of discarded DHCP messages reaches the alarm threshold on an interface.	The value ranges from 1 to 1000. The default value is 100.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, Port-group view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the command is used, the DHCP message discard alarm is enabled. If the number of discarded messages reaches the alarm threshold, an alarm is generated.

Example

# On GE 0/0/1, enable the function of checking the rate of sending DHCP messages, set the rate limit of sending DHCP messages to the DHCP protocol stack to 50 pps, enable the DHCP message discard alarm, and set the alarm threshold for discarded DHCP messages to 50.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable
threshold 50
```

19.12.6.7 dhcp snooping check dhcp-rate enable alarm enable (upgrade-compatible command)

Function

Using the **dhcp snooping check dhcp-rate enable alarm enable** command, you can:

- Enable the function of checking the rate of sending DHCP messages to the processing unit.

- Set the rate limit of sending DHCP messages to the processing unit.
- Enable the device to generate an alarm when the number of discarded DHCP messages reaches the threshold.
- Set the alarm threshold for the number of discarded DHCP messages.

By default, the device does not check the rate of sending DHCP messages to the processing unit; the maximum rate of sending DHCP messages to the processing unit is 100 pps; the device does not generate an alarm when the number of discarded DHCP messages reaches the threshold; the alarm threshold for the number of discarded DHCP messages is 100.

Format

dhcp snooping check dhcp-rate enable [[**rate**] *rate*] **alarm** [**dhcp-rate**] { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
[**rate**] *rate*	Specifies the rate limit of sending DHCP messages to the processing unit.	The value is an integer that ranges from 1 to 100, in pps. The default value is 100.
dhcp-rate	Generates an alarm when the number of discarded DHCP messages reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When 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

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

After the command is used, the DHCP message discard alarm is enabled. If the number of discarded messages reaches the alarm threshold, an alarm is generated.

Example

# Enable the function of checking the rate of sending DHCP messages to the processing unit, set the rate limit of sending DHCP messages to the processing unit to 50 pps, enable the DHCP message discard alarm, and set the alarm threshold for discarded DHCP messages to 50.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping check dhcp-rate enable 50 alarm dhcp-rate enable threshold 50
```

19.12.6.8 dhcp snooping check { dhcp-request | dhcp-chaddr | dhcp-giaddr | user-bind | mac-address} enable alarm (upgrade-compatible command)

Function

The **dhcp snooping check { dhcp-request | dhcp-chaddr | dhcp-giaddr | user-bind | mac-address } enable alarm enable** command enables the DHCP packet check and alarm function.

By default, the DHCP packet check and alarm function is disabled.

Format

dhcp snooping check { **dhcp-request** | **dhcp-chaddr** | **dhcp-giaddr** | **user-bind** | **mac-address** } **enable alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** | **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
dhcp-request or **user-bind**	Generates an alarm when the number of DHCP messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-
dhcp-chaddr or **mac-address**	Generates an alarm when the number of DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address in the Ethernet frame header reaches the threshold.	-
dhcp-reply or **untrust-reply**	Generates an alarm when the number of DHCP Reply messages discarded by untrusted interfaces reaches the threshold.	-

Parameter	Description	Value
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCP messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This function equals to the combination of the **dhcp snooping check dhcp-giaddr enable**, **dhcp snooping check dhcp-chaddr enable**, **dhcp snooping check dhcp-request enable** and **dhcp snooping alarm threshold** commands.

Example

# Enable the **user-bind** check function on GE0/0/1. Set the alarm threshold to 1000 for the discarded packet in the **user-bind** check.

```
<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-request enable alarm dhcp-request enable
threshold 100
```

19.12.6.9 dhcp snooping check enable alarm enable (upgrade-compatible command)

Function

The **dhcp snooping check enable alarm enable** command enables the DHCP packet check and alarm function.

By default, the DHCP packet check and alarm function is disabled.

Format

dhcp snooping check { **dhcp-request** | **dhcp-chaddr** | **dhcp-giaddr** } **enable alarm** { **user-bind** | **mac-address** | **untrust-reply** } { **enable** | [**enable**] **threshold** *threshold* }

Parameters

Parameter	Description	Value
dhcp-request	Matches DHCP packets with entries in the binding table.	-
dhcp-chaddr	Checks whether the MAC address and CHADDR field in DHCP packets are consistent.	-
dhcp-giaddr	Checks whether the GIADDR field in DHCP packets is not zero.	-
user-bind	Generates an alarm when the number of DHCP packets discarded because they do not match DHCP snooping binding entries reaches the threshold.	-
mac-address	Generates an alarm when the number of DHCP packets discarded because the CHADDR field in the DHCP packet does not match the source MAC address in the Ethernet frame header reaches the threshold.	-
untrust-reply	Generates an alarm when the number of DHCP Reply packets discarded by untrusted interfaces reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCP packets reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade. This function equals to the combination of the **14.8.14 dhcp snooping check dhcp-giaddr enable**, **14.8.17 dhcp snooping check dhcp-chaddr enable**, **14.8.18 dhcp snooping check dhcp-request enable**, and **dhcp snooping alarm** { **dhcp-request** | **dhcp-chaddr** | **dhcp-reply** } **threshold** *threshold* commands.

19.12.6.10 dhcp snooping global max-user-number (upgrade-compatible command)

Function

The **dhcp snooping global max-user-number** command sets the maximum number of global DHCP users.

By default, the maximum number of global DHCP users is 1024.

Format

dhcp snooping global max-user-number *max-user-number*

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of global DHCP users.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp snooping global max-user-number** command takes effect only when DHCP snooping is enabled globally and is valid for only DHCP users. When the number of global DHCP users reaches the threshold set by this command, no more users can access.

You can use the **dhcp snooping global max-user-number** command to set the maximum number of global users.

Example

# Set the maximum number of global DHCP users to 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping global max-user-number 100
```

19.12.6.11 dhcp snooping information circuit-id (upgrade-compatible command)

Function

The **dhcp snooping information circuit-id** command configures the Option 82 circuit-id format.

Format

System view:

dhcp snooping information circuit-id string *string*

Interface view:

dhcp snooping information [**vlan** *vlan-id*] **circuit-id string** *string*

Parameters

Parameter	Description	Value
string *string*	Specifies the circuit-id format.	The value is a string of 1 to 63 characters.
vlan *vlan-id*	Specifies a 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, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping information circuit-id** command to configure the Option 82 circuit-id format.

Example

# Configure the Option 82 circuit-id format.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping information circuit-id string teststring
```

19.12.6.12 dhcp snooping information format (upgrade-compatible command)

Function

The **dhcp snooping information format** command configures the Option 82 field format.

Format

dhcp snooping information format { **hex** | **ascii** }

Parameters

Parameter	Description	Value
hex	Sets the Option 82 format to hexadecimal.	-
ascii	Sets the Option 82 format to ASCII.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping information format** command to configure the Option 82 field format.

Example

# Set the Option 82 format to ASCII.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping information format ascii
```

19.12.6.13 dhcp snooping information remote-id (upgrade-compatible command)

Function

The **dhcp snooping information remote-id** command configures the Option 82 remote-id format.

Format

System view:

dhcp snooping information remote-id { **sysname** | **string** *string* }

Interface view:

dhcp snooping information [**vlan** *vlan-id*] **remote-id string** *string*

Parameters

Parameter	Description	Value
sysname	System name.	-
string *string*	Specifies the remote-id format.	The value is a string of 1 to 63 characters.
vlan *vlan-id*	Specifies a 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, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping information remote-id** command to configure the Option 82 remote-id format.

Example

# Configure the Option 82 remote-id format.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping information remote-id string teststring
```

19.12.6.14 dhcp snooping max-user-number global (upgrade-compatible command)

Function

The **dhcp snooping max-user-number global** command sets the maximum number of global DHCP users.

By default, the maximum number of global DHCP users is 1024.

Format

dhcp snooping max-user-number *max-user-number* **global**

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of global DHCP users.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

The command takes effect only when DHCP snooping is enabled globally and is valid for only DHCP users. When the number of global DHCP users reaches the threshold set by this command, no more users can access. You can use the command to set the maximum number of global users.

Example

# Set the maximum number of global DHCP users to 100.

```
<HUAWEI> system-view
[HUAWEI] dhcp snooping enable
[HUAWEI] dhcp snooping max-user-number 100 global
```

19.12.6.15 dhcp snooping sticky-mac (upgrade-compatible command)

Function

The **dhcp snooping sticky-mac** command enables the device to generate static MAC address entries based on dynamic DHCP snooping binding entries.

The **undo dhcp snooping sticky-mac** command disables the device from generating static MAC address entries based on dynamic DHCP snooping binding entries.

By default, the device is disabled to generate static MAC address entries based on dynamic DHCP snooping binding entries.

Format

dhcp snooping sticky-mac

undo dhcp snooping sticky-mac

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Dynamic MAC address entries are learned and generated by the device, and static MAC address entries are configured by command lines. A MAC address entry consists of the MAC address, VLAN ID, and port number of a DHCP client. The device implements Layer 2 forwarding based on MAC address entries.

After the **dhcp snooping sticky-mac** command is executed on an interface, the device generates static MAC address entries (snooping type) of DHCP users on the interface based on the corresponding dynamic binding entries, clears all the dynamic MAC address entries on the interface, disables the interface to learn dynamic MAC address entries, and enables the device to match the source MAC address based on MAC address entries. Then only the message with the source MAC address matching the static MAC address entry can pass through the interface; otherwise, messages are discarded. Therefore, the administrator needs to manually configure static MAC address entries (the static type) for non-DHCP users on the interface so that messages sent from non-DHCP users can pass through; otherwise, DHCP messages are discarded. This prevents attacks from non-DHCP users.

NOTE

- If a DHCP snooping binding entry is updated, the corresponding static MAC address entry is automatically updated.
- If you run the **dhcp snooping sticky-mac** command on the interface, DHCPv6 users cannot go online. Run the **nd snooping enable** command in the system view and interface view to enable ND snooping and the **savi enable** command in the system view to enable SAVI.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

The **dhcp snooping sticky-mac** command cannot be used with the following commands on an interface.

Command	Description
dot1x enable	Enables 802.1X authentication on an interface.
mac-authen	Enables MAC address authentication on an interface.
mac-address learning disable	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

# Enable the device to generate static MAC address entries based on DHCP snooping binding entries 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 sticky-mac
```

19.12.6.16 dhcp snooping trusted interface no-user-binding (upgrade-compatible command)

Function

The **dhcp snooping trusted interface no-user-binding** command configures a trusted interface.

The **undo dhcp snooping trusted interface no-user-binding** command deletes a trusted interface.

By default, no trusted interface is configured.

Format

dhcp snooping trusted interface *interface-type interface-number* **no-user-binding**

undo dhcp snooping trusted interface *interface-type interface-number* **no-user-binding**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

You can use the **dhcp snooping trusted interface no-user-binding** command to configure a trusted interface in the VLAN view.

Before using this command:

- Enable DHCP snooping globally.
- Add the interface to a VLAN.

This command can only be used during a configuration restoration.

Example

# Configure a trusted interface GE0/0/1 in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] dhcp snooping trusted interface gigabitethernet 0/0/1 no-user-binding
```

19.12.6.17 dhcp snooping trusted no-user-binding (upgrade-compatible command)

Function

The **dhcp snooping trusted no-user-binding** command configures an interface as the trusted interface.

The **undo dhcp snooping trusted no-user-binding** command restores the default state of an interface.

By default, no trusted interface is configured.

Format

dhcp snooping trusted no-user-binding

undo dhcp snooping trusted no-user-binding

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

When DHCP snooping is enabled on an interface, the interface is an untrusted interface by default. After you use the **dhcp snooping trusted no-user-binding** command in the interface view, the interface becomes a trusted interface.

This command can only be used during a configuration restoration.

Example

# Configure a trusted interface 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 trusted no-user-binding
```

19.12.7 Keychain Upgrade-compatible Commands

19.12.7.1 receive-time (upgrade-compatible command)

Function

The **receive-time** command makes a key act 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 utc *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } }

Parameters

Parameter	Description	Value
utc	Specifies that the given time is in Coordinated Universal Time (UTC) format.	-
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	Specifies that the key will be acting as an active receive key forever from the configured start-time.	-
to	Acts as a separator.	-
end-time	Specifies the end receive time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end-time should be greater than the start-time.
end-date	Specifies the end date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.

Views

key-id view

Default Level

2: Configuration Level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **receive-time** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } } command.

19.12.7.2 send-time (upgrade-compatible command)

Function

The **send-time** command makes a key act as a send key for the specified interval of time.

The **undo send-time** command deletes the send-time configuration.

By default, no send-time is configured.

Format

send-time utc *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } }

Parameters

Parameter	Description	Value
utc	Specifies that the given time is in Coordinated Universal Time (UTC) format.	-
start-time	Specifies the start send time.	In HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specify 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 send time in minutes.	The value ranges from 1 to 26280000.
infinite	Specifies that the key will be acting as a send key forever from the configured start-time.	-
to	Acts as a separator.	-
end-time	Specifies the end send time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end-time should be greater than the start-time.
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 send timing for the given key.	-

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

It is replaced by the **send-time** *start-time start-date* { **duration** { *duration-value* | **infinite** } | { **to** *end-time end-date* } } command.

19.12.8 PKI Compatible Commands

19.12.8.1 fingerprint (upgrade-compatible command)

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 sha2 *fingerprint*

undo fingerprint

Parameters

Parameter	Description	Value
sha2	Sets the digital fingerprint algorithm to SHA1.	-

Parameter	Description	Value
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.

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.12.8.2 password (upgrade-compatible command)

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 simple *password*

undo password

Parameters

Parameter	Description	Value
simple *password*	Specifies the challenge password used for certificate application through SCEP. The password is displayed in plain text.	-

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.12.8.3 usage (upgrade-compatible command)

Function

The **usage** command configures the purpose description for a certificate public key.

By default, a certificate public key does not have a purpose description.

Format

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.	-

Parameter	Description	Value
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

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **key-usage** { **ike** | **ssl-client** | **ssl-server** } * command.

19.13 QoS Compatible Commands

19.13.1 count (upgrade-compatible command)

Function

Using the **count** command, you can enable the function of counting packets that match traffic classification rules.

By default, the counting function is disabled.

Format

count

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

When there are many traffic classification rules on the switch, you can run the **count** command to count the specific traffic. The counting start time is the time when the policy is applied.

Currently, the switch counts packets rather than bytes.

Example

# Configure the traffic policy **p1** so that the switch counts packets that flow through GigabitEthernet 0/0/1. After a period of time, the switch displays the traffic statistics.

```
<HUAWEI> system-view
[HUAWEI] traffic classifier c1
[HUAWEI-classifier-c1] if-match any
[HUAWEI-classifier-c1] quit
[HUAWEI] traffic behavior b1
[HUAWEI-behavior-b1] count
[HUAWEI-behavior-b1] quit
[HUAWEI] traffic policy p1
[HUAWEI-trafficpolicy-p1] classifier c1 behavior b1
[HUAWEI-trafficpolicy-p1] quit
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] traffic-policy p1 inbound
[HUAWEI-GigabitEthernet0/0/1] display traffic policy interface gigabitethernet 0/0/1
 Interface: GigabitEthernet0/0/1

 Direction: Inbound

 Policy: p1
  Classifier: c1
    Rule(s) : if-match any
    Behavior: b1
     Count
       Matched : 10 (Packets)
```

19.14 Network Management Compatible Commands

19.14.1 SNMP Compatible Commands

19.14.1.1 snmp-agent group (upgrade-compatible command)

Function

The **snmp-agent group** command creates an SNMP group by mapping SNMP users to SNMP views.

The **undo snmp-agent group** command deletes a specified SNMP user group.

By default, no SNMP group is configured.

Format

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view*] * [**acl** *acl-number*]

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

Parameters

Parameter	Description	Value
v3	Indicates that the SNMP group uses the security mode in SNMPv3.	-
group-name	Specifies the name of an SNMP group.	It is a string of 1 to 32 case-sensitive characters without spaces.
authentication | **privacy**	Indicates the security level of the SNMP group. ● **authentication**: authenticates SNMP messages without encryption. ● **privacy**: authenticates and encrypts SNMP messages.	To ensure security, it is recommended that you set the security level of the SNMP group to **privacy**.
read-view *read-view*	Specifies a read-only view.	It is a string of 1 to 32 case-sensitive characters without spaces. *read-view* specified by the **snmp-agent mib-view** command.
write-view *write-view*	Specifies a read-write view.	It is a string of 1 to 32 case-sensitive characters without spaces. *write-view* is specified by the **snmp-agent mib-view** command.

Parameter	Description	Value
notify-view *notify-view*	Specifies a notify view.	It is a string of 1 to 32 case-sensitive characters without spaces. *notify-view* is specified by the **snmp-agent mib-view** command.
acl *acl-number*	Specifies a basic ACL. **NOTE** The ACL configured by the **acl** *acl-number* parameter takes effect on both IPv4 and IPv6 networks.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.1.2 snmp-agent trap enable (upgrade-compatible command)

Function

The **snmp-agent trap enable** command enables a specified trap for a specified feature.

The **undo snmp-agent trap enable** command disables a specified trap for a specified feature.

The default configuration of the **snmp-agent trap enable** command can be checked using the **display snmp-agent trap all** command.

Format

snmp-agent trap enable *feature-name*

undo snmp-agent trap enable *feature-name*

Parameters

Parameter	Description	Value
feature-name	Specifies the name of the feature that generates traps.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.1.3 snmp-agent trap enable standard (upgrade-compatible command)

Function

Using the **snmp-agent trap enable standard** command, you can enable the trap function of standard SNMP.

Using the **undo snmp-agent trap enable standard** command, you can disable the trap function of standard SNMP.

By default, no trap messages are sent to a device.

Format

snmp-agent trap enable standard [**authentication** | **coldstart** | **warmstart** | **linkup** | **linkdown**] *

undo snmp-agent trap enable standard [**authentication** | **coldstart** | **warmstart** | **linkup** | **linkdown**] *

Parameters

Parameter	Description	Value
Authentication	Indicates that a trap message is sent when packets failed to be authenticated through SNMP.	-
Coldstart	Indicates that a trap message is sent when the system is cold started.	-
Warmstart	Indicates that a trap message is sent when the system is hot started.	-
Linkup	Indicates that a trap message is sent when the interface goes Up.	-
Linkdown	Indicates that a trap message is sent when the interface goes Down.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.1.4 snmp-agent usm-user (upgrade-compatible command)

Function

The **snmp-agent usm-user** command adds a user to an SNMP user group.

The **undo snmp-agent usm-user** command deletes a user from an SNMP user group.

By default, the SNMP user group has no users added.

NOTE

It is recommended that you deliver the **snmp-agent usm-user v3** *user-name group-name* **authentication-mode** { **md5** | **sha** } *password* [**privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } *encrypt-password*] [**acl** *acl-number*] to the switch from the NMS. Do not directly configure the command on the switch.

Format

snmp-agent usm-user v3 *user-name group-name* **simple** [**authentication-mode** { **md5** | **sha** } *password* [**privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } *encrypt-password*]] [**acl** *acl-number*]

snmp-agent usm-user v3 *user-name group-name* [**cipher**] [**authentication-mode** { **md5** | **sha** } *password* [**privacy-mode** { **des56** | **aes128** | **aes192** | **aes256** | **3des** } *encrypt-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* [**engineid** *engineid* | **local**]

Parameters

Parameter	Description	Value
v3	Indicates that the security mode in SNMPv3 is adopted.	-
user-name	Specifies the name of a user.	It is a string of 1 to 32 case-sensitive characters without spaces.
group-name	Specifies the name of the group to which a user belongs.	It is a string of 1 to 32 case-sensitive characters without spaces.

Parameter	Description	Value
simple	Indicates the simple authentication.	-
cipher	Specifies that the password is in ciphertext, which is the default password type. If this parameter is specified, you can enter only a password in ciphertext. This type of password can be viewed using the configuration file.	-
authentication-mode	Sets the authentication mode. **NOTE** Authentication is a process in which the SNMP agent (or the NMS) confirms that the message is received from an authorized NMS (or SNMP agent) and the message is not changed during transmission. RFC 2104 defines Keyed-Hashing for Message Authentication Code (HMAC), an effective tool that uses the security hash function and key to generate the message authentication code. This tool is widely used in the Internet. HMAC used in SNMP includes HWAC-MD5-96 and HWAC-SHA-96. The hash function of HWAC-MD5-96 is MD5 that uses 128-bit authKey to generate the key. The hash function of HWAC-SHA-96 is SHA-1 that uses 160-bit authKey to generate the key.	-
md5 | **sha**	Indicates the authentication protocol. ● **md5**: Specifies HMAC-MD5-96 as the authentication protocol. ● **sha**: Specifies HMAC-SHA-96 as the authentication protocol.	-

Parameter	Description	Value
password	Specifies the password for user authentication.	For plain-text password, the value is a string of 6 to 64 characters by default, and the minimum length is 6 characters. If the **set password min-length** command is run to set the minimum length of passwords to a value greater than 6, the minimum length is the value configured using the **set password min-length** command. For cipher-text password, the value is a string of 32 to 104 characters. **NOTE** The password cannot be the same as the user name or reverse of the user name. The password must contain at least two types of characters, including letters, digits, and special characters. The special characters cannot be question mark (?) or space.
privacy-mode	Specifies the authentication with encryption. The system adopts the cipher block chaining (CBC) code of the data encryption standard (DES) and uses 128-bit privKey to generate the key. The NMS uses the key to calculate the CBC code and then adds the CBC code to the message while the SNMP agent fetches the authentication code through the same key and then obtains the actual information. Like the identification authentication, the encryption requires the NMS and the SNMP agent to share the same key to encrypt and decrypt the message.	-

Parameter	Description	Value
des56 | **aes128** | **aes192** | **aes256** | **3des**	Indicates the encryption protocol.	-
encrypt-password	Indicates the encryption password.	For plain-text password, the value is a string of 6 to 64 characters by default, and the minimum length is 6 characters. If the **set password min-length** command is run to set the minimum length of passwords to a value greater than 6, the minimum length is the value configured using the **set password min-length** command. For cipher-text password, the value is a string of 32 to 104 characters. **NOTE** The password cannot be the same as the user name or reverse of the user name. The password must contain at least two types of characters, including letters, digits, and special characters. The special characters cannot be question mark (?) or space.
acl *acl-number*	Specifies the ACL number of the access view.	The value is an integer that ranges from 2000 to 2999.
engineid *engineid*	Specifies the ID of the engine associated with a user.	The value is a string of 10 to 64 case-insensitive characters without spaces.
local	Indicates the local entity user.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

19.14.2 NQA Compatible Commands

19.14.2.1 send-trap overthreshold (upgrade-compatible command)

Function

Using the **send-trap overthreshold** command, you can configure conditions for sending trap messages.

Using the **undo send-trap overthreshold** command, you can delete the previous configuration.

By default, the device is disabled from sending traps.

Format

send-trap overthreshold

undo send-trap overthreshold

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

This command is available to aid upgrade compatibility. It can only be run during the configuration restoration phase of the upgrade.

After the upgrade, this command is no longer supported, and it is replaced by the **send-trap rtd** command.

19.14.3 Mirror Compatible Commands

19.14.3.1 port-mirroring (upgrade-compatible command)

Function

The **port-mirroring** command configures a mirroring behavior on an interface.

Format

port-mirroring to observe-port *index*

Parameters

Parameter	Description	Value
index	Specifies the index of a global observing interface.	The value is integer.

Views

Traffic behavior view

Default Level

3: Management level

Usage Guidelines

This command is available to aid upgrade compatibility. It can be run when it is entered in full.

Example

# Mirror traffic to observing interface with index 1.

```
<HUAWEI> system-view
[HUAWEI] traffic behavior b1
[HUAWEI-traffic-behavior-b1] port-mirroring to observe-port 1
```